Contents

1 Preliminary **3**

2 Group Theory **5**

2.1 Introduction 5
2.2 Subgroup 7
2.3 A counting principle 8
2.4 Normal subgroups 10
2.5 Homomorphism 10
2.6 Automorphism 11
2.7 Cayley's theorem 12
2.8 Permutation group 12

Chapter 1

Preliminary

$R \subset A \times A$ is an equivalence relations if

Reflexive: $\forall a \in A, (a, a) \in R$.

Symmetric: $(a, b) \in R \implies (b, a) \in R$.

Transitive: $(a, b) \in R, (b, c) \in R \implies (a, c) \in R$.

A binary relations can be also denoted as aRb whenever $(a, b) \in R$.
If A is a set and if $\sim$ is an equivalence relation on A, then the equivalence class of $a \in A$ is the set $\{x \in A \,|\, x \sim a\}$ denoted by $\mathrm{cl}(a)$.

Theorem 1.1. *Equivalence classes partition the set into mutually disjoint subsets and conversely, mutually disjoint subsets give rise to equivalence classes.*

If S and T are non-empty sets, then a mapping from S to T is a subset $M \subset S \times T$ such that for every $s \in S$ there is a unique $t \in T$ that $(s, t) \in M$. $\sigma : S \to T$ maybe denoted as $t = s\sigma$ or $t = \sigma(s)$.

Chapter 2

Group Theory

2.1 Introduction

Definition: A set S equipped with an associative binary operation is a **semigroup**.

A semigroup can have multiple left or right identities. However, if it has both left identity, e, and right identity, f, then those two are equal since $e = ef = f$. Two sided identity are unique. We have the same story with inverses.

Definition: A non-empty set of elements G together with a binary operation $\circ$ are said to be a **group** if

Closure: $\forall a, b \in G, a \circ b \in G$.

Associative: $\forall a, b, c \in G, (a \circ b) \circ c = a \circ (b \circ c)$.

Identity: $\exists e \in G$ such that $\forall a \in G, a \circ e = e \circ a = a$.

Inverse: $\forall a \in G\ \exists b \in G$ such that $a \circ b = b \circ a = e$.

Definition: A group G is said to be **abelian** or **commutative** if for any two element a and b commute. i.e. $a \circ b = b \circ a$.

Definition: The number of elements in a group is called the **order** of the group and it is denoted by $o(G)$.

Definition: Let $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. If for some choice of a, $G = \langle a \rangle$, then G is said to be a **cyclic group**. More generally, for a set $W \subset G$, $\langle W \rangle = \bigcap W \subset H \subset GH$ where H is a subgroup of G.

Lemma 2.1. *Given $a, b \in G$ the equation $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$.*

Proof. Note that a^{-1} and b^{-1} are unique. Therefore, $x = a^{-1}b$ and $y = ba^{-1}$ are unique. $\square$

Exercises

1. Let S be a finite semi-group. Prove that there exists $e \in S$ such that $e^2 = e$.

Proof. Pick $a \in S$ and consider $a_i = a^{2^i}$ for $i \geq 1$. After some point, a_is repeat, by the pigeon hole principle. Let that point be a_j. Therefore, for some $m \geq 1$.

$$a_j = (a_j)^{2^m}$$

Let $e = a_j^{2^m - 1}$, then

$$e^2 = a_j^{2^{m+1}-2} = a_j^{2^m} a_j^{2^m - 2} = a_j a_j^{2^m - 2} = e$$

we are done. ∎

2. Show that if a group G is abelian, then for $a, b \in G$ and any integer n, $(ab)^n = a^n b^n$.

   Proof. Induct over positive n. It is trivially true for $n = 1$. Suppose it is true for $n = k$, then
   $$(ab)^{k+1} = (ab)^k ab = a^k b^k ab = a^k a b^k b = a^{k+1} b^{k+1}$$
   For negative n, note that
   $$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} \implies (ab)^n = ((ab)^{-1})^{-n} = (a^{-1}b^{-1})^{-n} = a^n b^n$$
   hence it is true for all integers n. ∎

3. If a group has an even order, then there exists $a \neq e$ such that $a^2 = e$.

   Proof. Let $A = \{g \,|\, g \neq g^{-1}\}$ and $B = \{g \,|\, g = g^{-1}\}$. Note that, $|A|$ is even since $g \in A \implies g^{-1} \in A$. Moreover, $o(G) = |A| + |B|$, therefore $|B|$ must be even and since $e \in B$, $|B| \geq 2$. ∎

4. For any $n > 2$ construct a non-abelian group of order $2n$.

   Proof. Consider ϕ, ψ where $\psi^n = \phi^2 = e$ and $\psi\phi = \phi\psi^{-1}$. Then
   $$G = \left\{I, \phi, \psi, \psi^2, \ldots, \psi^{n-1}, \phi\psi, \ldots, \phi\psi^{n-1}\right\}$$
   is a group of order $2n$. Because, by the product rules defined, any combination of ψ and ϕ can be reduced to $\phi^b \psi^k$ where $b = 0, 1$ and $k = 0, 1, \ldots, n-1$. It is cleary non-abelian as well. ∎

5. Find the order of $\mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathrm{SL}_2(\mathbb{Z}_p)$ for a prime p.

   Proof.
   $$o(\mathrm{GL}_2(\mathbb{Z}_p)) = (p+1)p(p-1)^2$$
   $$o(\mathrm{SL}_2(\mathbb{Z}_p)) = (p+1)p(p-1)$$
   which be can be calculate with some basic casing. ∎

2.2 Subgroup

Definition: A non-empty subset H of a group G is called a **subgroup** if under the product in G, H itself forms a group.

Lemma 2.2. *H is a subgroup of G if and only if*

1. $\forall a, b \in H, ab \in H$.
2. $\forall a \in H, a^{-1} \in H$.

Proof. If H is a subgroup, then the conditions hold. Suppose H is a subset of G that satisfies the conditions. Then,

1. $e \in H$ since $(a \in H \implies a^{-1} \in H) \implies e = aa^{-1} \in H$.
2. Associativity is inherited from G.

invertibility and closure are given from the conditions. Therefore, H is a subgroup. □

Lemma 2.3. *If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.*

Proof. Since H is non-empty there exists a $a \in H$. By closure, a^n for positive integer n, are also in H. We know that for some N, $a^N = e$ and therefore $a^{-1} = a^{N-1} \in H$. By , H is a subgroup. □

Definition: Let G be a group and H a subgroup of G. For $a, b \in G$ we say that a is congruent to $b \mod H$, written as $a \equiv b \mod H$ if $ab^{-1} \in H$.

Lemma 2.4. *The relation $a \equiv b \mod H$ is an equivalence relation.*

Proof. We show the equivalence axioms:

1. for any a, $a \equiv a \mod H$ becuase, $aa^{-1} = e \in H$.
2. for any a, b, $a \equiv b \mod H \implies b \equiv a \mod H$ since $ab^{-1} \in H$ because of invertibility implies that $(ab^{-1})^{-1} = ba^{-1} \in H$.
3. for any a, b, c, $a \equiv b \mod H, b \equiv c \mod H \implies a \equiv c \mod H$ since $ab^{-1}, bc^{-1} \in H$ because of closure implies that $ab^{-1}bc^{-1} = bc^{-1} \in H$. □

Definition: If H is a subgroup of G and $a \in G$, then $Ha = \{ha \mid h \in H\}$ is a **right coset** of H in G. Similary, $aH = \{ah \mid h \in H\}$ is a **left coset** of H in G.

Lemma 2.5. *For all $a \in G$,*

$$Ha = \{x \in G \mid a \equiv x \mod H\}$$

Proof. Suppose $x \in G$ and $x \equiv a \mod H$. That is, $xa^{-1} = h$ for some $h \in H$. Then, $x = ha$. Suppose $h \in H$ and $x = ha$. Then, $xa^{-1} = h$ and hence $x \equiv a \mod H$. □

This implies, two right/left coset of H are either identical or disjoint.

Lemma 2.6. *There is a one-to-one correspondence between any two right/left cosets of H.*

Proof. Let R_1, R_2 be two right cosets of H with $a_1 \in R_1$ and $a_2 \in R_2$. Note that, $R_1 = Ha_1$ and $R_2 = Ha_2$, therefore the map $g \mapsto ga_1^{-1}a_2$ is a bijective map from R_1 to R_2. □

Theorem 2.7 (Lagrange's theorem). *If G is a finite group and H is a subgroup of G, then $o(H) \mid o(G)$.*

Proof. By and , and from finiteness of G, the order of G is equal to the number of right cosets multiplied by the cardinality of a right coset which is equal to the order of H. Hence, $o(H) \mid o(G)$ ■

Definition: If H is a subgroup of G, the **index** of H in G is the number of distince right cosets of H, denoted by $[G : H]$ or $i_G(H)$.

Definition: Let G be a group and $a \in G$, then the **order** or **period** of a is the least positive integer m such that $a^m = e$. If no such integer exists we say that a is of infinite order. The order of a is denoted by $\mathrm{ord}_G(a)$.

Corollary 2.8. *If G is a finite group, then*

1. $o(G) = i_G(H)o(H)$.
2. $\mathrm{ord}_G(a) \mid o(G)$.
3. $a^{o(G)} = e$.
4. *If $o(G)$ is a prime, then G is cyclic.*

2.3 A counting principle

Let H and K be two subgroups of G, then

$$HK = \{hk \,|\, h \in H, k \in K\}$$

Lemma 2.9. *HK is a subgroup of G if and only if $HK = KH$.*

Proof. Suppose HK is a subgroup. If $hk \in HK$, then

$$k^{-1}h^{-1} \in HK \implies k^{-1} \in H, h^{-1} \in K \implies k \in H, h \in K \implies hk \in KH$$

hence $HK \subset KH$. If $kh \in KH$, then

$$hk \in HK \implies k^{-1} \in H, h^{-1} \in K \implies k \in H, h \in K \implies kh \in HK$$

thus $HK = KH$. Suppose $HK = KH$ with $h_1k_1, h_2k_2 \in HK$.

1. for closure we have

$$h_1k_1h_2k_2 = h_1k_1(k_2'h_2') = h_1(k_1k_2')h_2' = h_1(k^*h_2') = h_1h_2''k^{*'}$$

2. for inverse

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h_1'k_1'$$

Corollary 2.10. *If H and K are subgroups of an abelian group G, then HK is a subgroup of G.*

Lemma 2.11. *If H and K are finite subgroups G, then*

$$|HK| = \frac{o(H)o(K)}{o(H \cap K)}$$

Proof. If $h_1 \in H \cap K$ then $hk = (hh_1)(h_1^{-1}k)$. Therefore, hk appears at least $o(H \cap K)$ times. If $hk = h'k'$, then $h'^{-1}h = k'k^{-1} \in H \cap K$. Let $u = h'^{-1}h$ then $h' = hu^{-1}$ and $k' = uk$. Thus, all duplicates are accounted for. □

Corollary 2.12. *If H and K are subgroups of G and $o(H), o(K) > \sqrt{o(G)}$, then $H \cap K \neq \{e\}$.*

Proof. $HK \subset G$ therefore, $|HK| \leq o(G)$ and

$$o(G) \geq |HK| = \frac{o(H)o(K)}{o(H \cap K)} > \frac{o(G)}{o(H \cap K)}$$

which implies that $o(H \cap K) > 1$. ■

Exercises

1. Let G be a group such that the intersection of all of its subgroups that are different from $\{e\}$ is different from $\{e\}$. Prove that every element in G has finite order.

   Proof. For the sake of contradiction, suppose $a \in G$ has infinite order. Then, a^k are all different and

   $$\bigcup_{k=1}^{\infty} \langle a^k \rangle = \{e\}$$

   which is a contradiction. ■

2. Show that there is one-to-one correspondence between the right and left cosets of a subgroup.

3. Suppose H and K are finite index subgroups in G. Show that $H \cap K$ is a finite subgroup in G.

   Proof. Let $Ha_1, \ldots, Ha_n$ be the right cosets of H in G and $Kb_1, \ldots, Kb_m$ be the right costs of K in G. Then,

   $$G = G \cap G = \bigcap_i Ha_i \cap \bigcap_j Kb_j = \bigcap_{i,j} Ha_i \cap Kb_j$$

   Suppose $Ha_i \cap Kb_j$ is not empty. Let $g \in Ha_i \cap Kb_j$, then $Hg = Ha_i$ and $Kg = Kb_j$. Thus,

   $$Ha_i \cap Kb_j = Hg \cap Kg = (H \cap K)g$$

   Therefore, $Ha_i \cap Kb_j$ are either empty or a right coset of $H \cap K$. Since there finitely many $Ha_i \cap Kb_j$, there finitely many right cosets of $H \cap K$ in G. Moreover, $[G : H \cap K] \leq$

$[G:H][G:K]$ by this construction. Note that, $H \cap K$ is finite index in H, and let $(H\cap K)c_1, \ldots, (H\cap K)c_l$ be the right cosets of $H\cap K$ in H. We claim that $(H\cap K)c_r a_i$ are the right cosets of $H \cap K$ in G. By definition, for each $x \in G$, there exists i such that $x \in Ha_i$and hence $x = ha_i$ for some $h \in H$. Similary, there exists r such that $h \in (H \cap K)c_r$ and hence $h = fc_r$ for some $f \in H \cap K$. Therefore, $x = fc_r a_i$ and $x \in (H \cap K)c_r a_i$. Lastly, we must show that $(H \cap K)c_r a_i$ are disjoint. Consider $(H \cap K)c_{r_1} a_{i_1}$ and $(H \cap K)c_{r_2} a_{i_2}$. Since $(H \cap K)c_{r_1}, (H \cap K)c_{r_2} \subset H$, then

$$\begin{aligned}(H \cap K)c_{r_1} a_{i_1} = (H \cap K)c_{r_2} a_{i_2} &\implies a_{i_1} = a_{i_2}, (H \cap K)c_{r_1} = (H \cap K)c_{r_2} \\ &\implies a_{i_1} = a_{i_2}, c_{r_1} = c_{r_2}\end{aligned}$$

As a result, $[G : H \cap K] = [G : H][H : H \cap K]$. ■

4. Let H be a finite index subgroup in G. Show that there is only finitely many subgroups of form aHa^{-1} in G.

   Proof. Let $a_1H, \ldots, a_nH$ be left cosets of H. Then, $Ha_1^{-1}, \ldots, Ha_n^{-1}$ are right cosets of H. Suppose $aH = a_iH$, then $Ha^{-1} = Ha_i^{-1}$ and therefore, $aHa^{-1} = a_iHa_i^{-1}$. Since there are finitely many $a_iHa_i^{-1}$, then there are finitely many aHa^{-1}. ■

5.

2.4 Normal subgroups

Definition: A subgroup N of G is **normal** if $\forall g \in G, n \in N,\ gng^{-1} \in N$.

Lemma 2.13. *N is normal if and only if $gNg^{-1} = N$ for every $g \in G$.*

Lemma 2.14. *N is a normal subgroup if and only if every left coset of N is a right coset.*

Definition: G/N is called a **quotient group** is the set of all right cosets of N.

2.5 Homomorphism

Definition: A mapping ϕ from a group G to another group $\bar{G}$ is a **homomorphism** if for all $a, b \in G$

$$\phi(ab) = \phi(a)\phi(b)$$

Lemma 2.15. *Suppose G is a group, N a normal subgroup of G, $\phi : G \to G/N$ given by $\phi(x) = Nx$ for all $x \in G$. Then, ϕ is a homomorphism.*

Definition: If ϕ is a homomorphism of G into $\bar{G}$, the **kernel** of ϕ, K_ϕ is defined as $K_\phi = \{x \in G \,|\, \phi(x) = \bar{e}\}$.

Lemma 2.16. *$\phi : G \to \bar{G}$ is a homomorphism if*

1. *$\phi(e) = \bar{e}$.*
2. *$\phi(x^{-1}) = (\phi(x))^{-1}$.*

Lemma 2.17. *If ϕ is a homomorphism, then K_ϕ is a normal subgroup of G.*

Lemma 2.18. *If ϕ is a homomorphism, then the set all iverse images of $\bar{g} \in \bar{G}$ under ϕ is given by $K_\phi x$ for any particular inverse image of $\bar{g}$.*

Definition: A homomorphism $\phi : G \to \bar{G}$ is an **isomorphism** if ϕ is one-to-one.

Definition: Two groups G and $\bar{G}$ are **isomorphic** if there exists an isomorphism of G onto $\bar{G}$. Isomorphic groups are denoted by $G \approx \bar{G}$.

Corollary 2.19. *ϕ is isomorphism if and only if $K_\phi = \{e\}$.*

Theorem 2.20. *If $\phi : G \to \bar{G}$ is a homomorphism, then $G/K_\phi \approx \bar{G}$*

Thus, we can find all homomorphic images of G by going through normal subgroups of G.

Definition: A group is **simple** if it has no non-trivial homomorphic images.

Theorem 2.21. *Suoppose G is a finite abelian group, and $p \mid o(G)$ where p is a prime number. Then, there is an element $a \neq e$ such that $a^p = e$.*

Theorem 2.22. *Suppose G is a finite abelian group and $p^\alpha \mid\mid o(G)$, then G has a unique subgroup of order p^α.*

Lemma 2.23. *Suppose $\phi : G \to \bar{G}$ is a homomorphism and $\bar{H}$ is a subgroup of $\bar{G}$. Let $H = \{x \in G \,|\, \phi(x) \in \bar{H}\}$. Then, H is a subgroup of G and $H \supset K_\phi$. If $\bar{H}$ is normal in $\bar{G}$, then H is normal. Moreover, this association sets up a one-to-one mapping from the set of all subgroups $\bar{G}$ onto the set of all subgroups of G which contain K_ϕ.*

Theorem 2.24. *Let $\phi : G \to \bar{G}$ be a homomorphism, $\bar{N}$ a normal subgroup of $\bar{G}$, and $N = \{x \in G \,|\, \phi(x) \in N\}$. Then, $G/N \approx \bar{G}/\bar{N}$ if and only if $G/N \approx (G/K_\phi)/(N/K_\phi)$.*

2.6 Automorphism

Definition: An isomorphism of a group onto iteslf is called an **automorphism**.

Lemma 2.25. *If G is a group, then $\mathscr{A}(G)$, the set of all automorphisms of G is also a group. The $\mathscr{A}(G)$ is also denoted by* $\mathrm{Aut}(G)$.

Example 2.1. $T_g : G \to G$ with $xT_g = g^{-1}xg$. T_g is an automorphisms. T_g is called the **inner automorphism corresponding to** g. Let $\mathscr{T}(G) = \{T_g \in \mathrm{Aut}(G) \,|\, g \in G\}$ is the **inner automorphism group** and is also denoted by $\mathrm{Inn}(G)$. $\Psi : G \to \mathrm{Aut}(G)$ given by $g\Psi = T_g$ is a homomorphism. The kernel of Ψ is the **center** of G, $Z(G)$, the set of the elements that commute with all other elements. Note that, if $g_o \in K_\Psi$, then $T_{g_0} = I$, hence $g_0^{-1}xg_0 = x$ implying $g_0x = xg_0$ for all $x \in G$. If $g_0 \in Z(G)$, then $xg_0 = g_0x$ for all x, thus $T_{g_0} = I$ and $g_0 \in K_\Psi$.

Lemma 2.26. $\mathrm{Inn}(G) \sim G/Z$.

Lemma 2.27. *Let G be a group and ϕ be an automorphism of G. If $a \in G$ is of order $o(a) > 0$, then $o(\phi(a)) = o(a)$.*

2.7 Cayley's theorem

Theorem 2.28 (Cayley). *Every group is isomorphic to a subgroup of $A(S)$ for some set S.*

Theorem 2.29. *If G is a group, H a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism $\theta : G \to A(S)$ and the kernel of θ is the largest normal subgroup of G which is contained in H.*

Lemma 2.30. *If G is a finite group, and $H \neq G$ is a subgroup of G such that $o(G) \not| i(H)!$, then H must contain a non-trivial normal subgroup of G. In particular, G is not simple.*

2.8 Permutation group

Suppose S is a finite set having n elements $x_1, \ldots, x_n$. If $\phi \in A(S)$, then ϕ is a one-to-one correspondence and it can be represented as

$$\phi : \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}$$

where $x_{i_j} = \phi(x_j)$. More simply

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

By considering composition of $\theta, \psi \in A(S)$, we can define multiplication on their representation.

For $\theta \in A(S)$ and $a, b \in S$, $a \equiv b \iff a = b\theta^i$ for some $i \in \mathbb{Z}$. This defines an equivalence relation.

–add the axioms

We cakk the equivalence classes of $s \in S$, the **orbit** of s under θ. The orbit of s consists of all elements in form of $s\theta^i$, $i \in \mathbb{Z}$. If S is finite, then there is a smallest positive integer $l = l(s)$ such that $s\theta^l = s$. By **cycle** of θ we mean the ordered set $(s, s\theta, \ldots, s\theta^{l-1})$.

Lemma 2.31. *Every permutation is a product of its cycles.*

Lemma 2.32. *Every cycle can be written as a product of 2-cycle or* ***transpositions****.*

Definition: A permutation $\theta \in S_n$ is said to be an even permuation if it can be represented as a product of an even number of transpositions,

– add well-definition of even

Let $A_n \subset S_n$ be the set of even permutations. A_n is a subgroup of S_n and it is called the **alternating group**.

Lemma 2.33. *The alternating group is a normal subgroup of S_n of index 2, .*