GROUP THEORY

Manish Kumar, notes by Ramdas Singh

Third Semester

List of Symbols

Placeholder

Contents

Chapter 1

INTRODUCTION TO GROUP THEORY

1.1 Set Theory

July 22nd.

We begin with some basic assumptions to introduce set theory. The symbol $\in$ is used to denote membership in a set. A statement using this in set theory may be stated as $x \in y$, which can be either true or false. Once we have developed this language to discuss sets, we can introduce some axioms.

Axiom 1.1. There exists a set with no elements, the *empty set* $\emptyset$.

Formally, the above axiom is $\exists x(\forall y(y \notin x))$.

Axiom 1.2. Two sets are equal if they have the same elements.

From the above two axioms, we can infer a unique empty set. A notion of subsets may also be declared.

Definition 1.3. We say the set A is a *subset* of the set B, denoted $A \subseteq B$, if every element of A is also an element of B.

We also have a bunch of similarity axioms stated below.

Axiom 1.4 (Similarity axioms)**.** We have the following:

1. If x, y are sets, then $\{x, y\} \Rightarrow \{x, \{x, y\}\}$ (not an ordered pair).
2. If A is a set, then $\bigcup A = \{x \mid \exists y \in A,\ x \in y\}$ is a set.
3. There exists a *power set* for every set; given a set A, there exists a set $P(A)$ such that for all $B \subseteq A$, $B \in P(A)$. Formally, $\forall A \exists P(A)(\forall B \subseteq A, B \in P(A))$.
4. The *infinite axiom*: Formally, $\exists I(\emptyset \in I \wedge \forall y \in I(P(y) \in I))$.
5. If A and B are sets, then $A \times B = \{(x, y) \mid x \in A, y \in B\}$ is a set.

Before discussing the last axiom, we define a relation on sets.

Definition 1.5. A *relation* R on a set A is a subset $R \subseteq A \times A$. If $(x, y) \in R$, we write xRy.

Axiom 1.6 (The *axiom of choice*)**.** Let A be a collection of non-empty and disjoint sets. Then there exists a set C consisting of exactly one element from each set in A.

Definition 1.7. A relation R on a set A is said to be:

- *reflexive* if $xRx \forall x \in A$,
- *symmetric* if $xRy \Rightarrow yRx$,
- *transitive* if $xRy \wedge yRz \Rightarrow xRz$,
- *antisymmetric* if $xRy \wedge yRx \Rightarrow x = y$.

Definition 1.8. A *partial order* on a set A is a reflexive, transitive, and antisymmetric relation on A.

Some examples of partially ordered sets include $(R, \leq)$, $(P(\mathbb{R}), \subseteq)$.

Definition 1.9. A *total order* R on a set A is a partial order such that for all $x, y \in A$, either xRy or yRx.

Again, $(R, \leq)$ is a totally ordered set, but not $(P(\mathbb{R}), \subseteq)$.

Definition 1.10. A total order $\leq$ on a set A is said to be a *well-order* if given any non-empty subset $B \subseteq A$, there exists $x \in B$ such that for all $y \in B$, $x \leq y$.

The below theorem may be derived from the above definitions and axioms.

Theorem 1.11 (The *well-ordering principle*)**.** *Every set can be well-ordered.*

We may note that the well-ordering principle and the axiom of choice are equivalent.

Definition 1.12. A *chain* in partially ordered set A, with relation $\prec$, is a subset of A which is totally ordered with respect to $\prec$.

Definition 1.13. Let $C \subseteq A$ be a subset in a partially ordered set $(A, \prec)$. An element $x \in A$ is an *upper bound* of C if for all $y \in C$, $y \prec x$.

Definition 1.14. An element $x \in A$ is a *maximal element* of a partially ordered set $(A, \prec)$ if for all $y \in A$, $x \prec y \Rightarrow x = y$.

Lemma 1.15 (*Zorn's lemma*)**.** *Let A be a set and let $\prec$ be a partial order on A such that every chain in A has an upper bound. Then A has a maximal element.*

Theorem 1.16. *The following are equialent:*

1. *The axiom of choice,*
2. *The well-ordering principle,*
3. *Zorn's lemma.*

Proof. We begin with 2. implies 3.; let A be a non-empty set. Consider

$$\mathcal{C} = \{(B, \leq) \mid B \subseteq A \text{ and } \leq \text{ is a well-order on } B\}. \tag{1.1}$$

We note that $\mathcal{C}$ is non-empty since if we pick $B = \{x\}$ for some $x \in A$, then $x \leq x$ and $(B, \leq) \in \mathcal{C}$. Let $(B, \leq), (C, \leq') \in \mathcal{C}$. We say $(B, \leq) \preceq (C, \leq')$ if there exists $y \in C$ such that

$$B = \{x \in C \mid x \lneq' y\} \ (= I(c, y)) \text{ and } \leq = \leq'|_B, \text{ or } (B, \leq) = (C, \leq') \tag{1.2}$$

Note that $\preceq$ is a partial order on $\mathcal{C}$ and is clearly reflexive.

For transitivity, if we take $B \preceq C$ and $C \preceq D$, then $B = C$ or $B = I(C, y)$ for some $y \in C$, and $C = D$ or $C = I(D, z)$ for some $z \in D$. If equality holds in either case, then clearly $B \preceq D$. If $B = I(C, y)$ and $C = I(D, z)$. Clearly, $B = I(D, y)$.

Now let $T = (\{(B_i, \leq_i) \mid i \in I\})$ be a chain in $\mathcal{C}$. Let $B = \bigcup_{i \in I} B_i$, and $\leq = \bigcup_{i \in I} \leq_i$. Note that this makes sense since if $x \in B_i$ and $y \in B_j$ with $B_i \preceq B_j$, then $x, y \in B_j$. So, we assign $x \leq y$ if $x \leq_j y$. Now let $C \subseteq B$ be non-empty. Also let $x \in C$; then $x \in B_i$ for some $i \in I$. Let $w = \min(B_i \cap C)$. We claim that $w = \min C$. For $y \in C$, if $y \in B_i$ then $w \leq y$. If $y \notin B_i$ then $y \in B_j \in T$. Since T is a chain, either $B_i \preceq B_j$ or $B_j \preceq B_i$; the latter is not possible since $y \notin B_i$. Thus, $B_i = I(B_j, z)$, for some $z \in B_j$, and for any $x \in B_i$, $w \leq x \leq y$.

So $(B, \leq) \in \mathcal{C}$ and it is an upper bound of T; to realize it is an upper bound, we show that $B_i \preceq B$ for all valid i. If $B_i = B$, we are done. Otherwise, let $x = \min(B \setminus B_i)$. Then $B_i = I(B, x)$, and $B_i \preceq B$. Thus, by Zorn's lemma, $\mathcal{C}$ has a maximal element— cal it $(M, \leq)$.

We now claim that $M = A$. If $M \subsetneq A$, then let $a \in A \setminus M$. If we let $\hat{M} = (M \cup \{a\}, \leq')$ where $x \leq' a$ for all $x \in M$, then $M = I(\hat{M}, a)$ but this is a contradiction to the fact that $(M, \leq)$ is a maximal element. Thus, $A = M$.

Next comes 1. implies 3. Let X be a partially ordered set such that every chain has an upper bound. Suppose X has no maximal element; we will utilise the axiom of choice to arise at a contradiction. For every chain T in X, there exists a strict upper bound c_T. Define a function f sending chains T in X to X as $f(T) = c_T \notin T$. Such a function f exists by the axiom of choice. A subset $A \subseteq X$ is called a *conforming subset* if A is well-ordered, with respect to order on X, and for all $x \in A$, $f(I(A, x)) = x$. We claim that if A and B are conforming subsets of X, then $A = B$ or one is the initial segment of the other. For now, let us take this claim to be true. We shall prove it later.

If $f(\emptyset) = x$ then $A = \{x\}$. Note that A is conforming. But $I(A, x) = \emptyset \implies f(I(A, x)) = x$. Let U be the union of all conforming subsets of X. Then U is conforming since if $x \in U$ then $x \in B$ for some B conforming and $x = f(I(B, x)) = f(I(U, x))$. Let $f(U) = w$. Define a new set $\tilde{U} = U \sqcup \{w\}$, which is well-ordered and conforming. Then $U = I(\tilde{U}, w)$, which is a contradiction.

Coming back to the claim, suppose $x \in A \setminus B$. We wish to show that $B = I(A, x)$ for some $x \in A$. Let $x = \min(A \setminus B)$. We claim that this x works. $I(A, x) \subseteq B$ holds since if $y \in A$ and $y < x$ then $y \in B$, or else $x \neq \min(A \setminus B)$. Suppose, now, that the equality does not hold. Take $y = \min(B \setminus I(A, x))$ and $z = \min(A \setminus I(B, y))$. We claim that $I(A, z) = I(B, y)$. Take $v \in I(A, z)$; then $v < z$ implies $v \in I(B, y)$ since $z = \min(A \setminus I(B, y))$. Taking $u \in I(B, y)$, we have $u \in I(A, x) \implies u < x$ since $y = \min(B \setminus I(A, x))$. If $z \leq u$, then $z \in I(A, x) \subseteq B \implies z \in I(B, y)$ contrading the fact that $z = \min(A \setminus I(B, y))$. Thus, $z > u$ and $y \in I(A, z)$. Finally, $z = f(I(A, z)) = f(I(B, y)) = y$ implies $z = x = y$. But this a contradiction since $x \in A \setminus B$ and $y \in B$. ■

Definition 1.17. A relation R on a set A is said to be an *equivalence relation* if it is reflexive, symmetric, and transitive. Let $x \in A$. Then $[x] = \{yRx \mid y \in A\} \subseteq A$ is called the *equivalence class* of x.

We note that $\bigcup_{x \in A} [x] = A$ and for $x, y \in A$, either $[x] \cap [y] = \emptyset$ or $[x] = [y]$. Thus, we get a partition of A into equivalence classes.

Let I be an indexing set, and let A_i be sets for all $i \in I$. Then the existence of $\mathrm{X}_{i \in I} A_i = \{f : I \to \dot{\bigsqcup} A_i \mid f(i) \in A_i \text{ for all } i \in I\}$ is another way of stating the axiom of choice.

Theorem 1.18 (The *principle of induction*)**.** *Let $S(n)$ be statements about the naturals $n \in \mathbb{N}$. Suppose $S(1)$ holds and for all $k \in \mathbb{N}$, $S(k) \Rightarrow S(k+1)$. Then $S(n)$ holds true for all $n \in \mathbb{N}$.*

Let I be a well-ordered set and let $S(i)$ be statements for all $i \in I$. Suppose that if $S(j)$ holds for all $j < i$, then $S(i)$ holds. Then $S(i)$ holds for all $i \in I$. This is the *principle of transfinite induction*, which is also equivalent to the axiom of choice. We now properly introduce the theory of groups.

1.2 Groups

We first define a group.

Definition 1.19. A *group* is a triple $(G, \cdot, e)$ where G is a set, $\cdot : G \times G \to G$ is a binary operation on G, and $e \in G$ is an element of G satisfying the following axioms:

- The property of *associativity*: For $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- The property of the *identity element*: For all $a \in G$, $a \cdot e = e \cdot a = a$. e is referred to as the identity element.
- The existence and property of the *inverse element*: For all $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

In addition, $(G, \cdot, e)$ is also termed an *abelian group* if for all $a, b \in G$, $a \cdot b = b \cdot a$, that is, commutativity holds.

A group may also be rewritten as $(G, \cdot)$, or just G. Some examples include $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$. The set $(\mathbb{Q}, \cdot)$ is not a group since 0 does not have an inverse. However, $(\mathbb{Q}^*, \cdot)$ is a group, where $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. All these groups are also abelian. An example of a non-abelian group is S_n, the set of all bijections from $\{1, 2, \ldots, n\}$ to itself, under the binary operation of composition of functions. Another non-abelian group is $(GL_n(\mathbb{R}), \cdot)$, for $n \geq 2$, the set of all invertible real $n \times n$ matrices.

July 24th.

From the axioms, arise basic properties related to groups.

Proposition 1.20. *Let $(G, \cdot, e)$ be a group.*

1. *Let $a \in G$ be such that $a \cdot b = b$ for all $b \in G$. Then $a = e$; the identity element is unique.*
2. *Each element $a \in G$ has a unique inverse. Thus, the inverse of a is then termed a^{-1}.*
3. *$(a^{-1})^{-1} = a$ holds for all $a \in G$.*
4. *For all $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*
5. *Let $a \in G$ be such that $a \cdot b = b$ for some $b \in G$. Then $a = e$.*

Proof.

1. Choose b to be e. Then $a \cdot e = e$ by hypothesis, and $a \cdot e = a$ by the property of the identity element. Thus, $a = e$.
2. Let $a \in G$ and $b \in G$ be such that $a \cdot b = b \cdot a = e$. Let $c \in G$ be also such that $c \cdot a = e$. Thus, $(c \cdot a) \cdot b = e \cdot b \Rightarrow c \cdot (a \cdot b) = e \cdot b \Rightarrow c \cdot e = b \Rightarrow c = b$.
3. Easy to see since $a^{-1} \cdot a = a \cdot a^{-1} = e$ which just means that the inverse of a^{-1} is a.
4. Also easy since $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$.
5. Finally, right multiplying b^{-1} leads to $a = a \cdot b \cdot b^{-1} = b \cdot b^{-1} = e$.

■

July 29th.

Definition 1.21. The *order of a group G* is the cardinality of the set G, and is denoted by $|G|$, $o(G)$, or $\mathrm{ord}(G)$. If $|G|$ is finite, we say G is a *finite group*.

We provide some examples.

Example 1.22.

- The *trivial group* is $G = \{e\}$, with $e \cdot e = e$. Here, $|G| = 1$, and it is the smallest possible finite group. Similarly, one can form a group with two elements as $G = \{e, a\}$, with $a \cdot a = e$ and $a \cdot e = e \cdot a = a$.

- Another important example is the set of all bijections of a set X, denoted by $S(X)$. It forms a group under composition. Here, if $f, g \in S(X)$, then $f \circ g \in S(X)$. Similarly, the bijection $\mathrm{id}_X(x) = x$ for all $x \in X$ is the identity element of $S(X)$. Associativity also holds, and the inverse of $f \in S(X)$ is simply the inverse mapping $f^{-1} \in S(X)$ to get $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$. If $X = \{1, 2, \ldots, n\}$, then $S(X)$ is also denoted by S_n, with $|S_n| = n!$. If the set X is infinite, then so is $S(X)$.
- The set ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ is a group when equipped with the binary operation of addition $(+)$. Here, $|{}^{\mathbb{Z}}/_{n\mathbb{Z}}| = n$.
- The set $\mu_n = \{e^{2\pi i m/n} \mid 1 \leq m \leq n\}$ is a group with respect to multiplication. Again, $|\mu_n| = n$.

Order is also defined for elements.

Definition 1.23. Let $(G, \cdot, e)$ be a group. The *order of an element* $a \in G$, denoted $o(a)$, $\mathrm{ord}(a)$, or $|a|$, is the least $n \geq 1$ such that $a^n = e$. If no such n exists, then we term $|a| = \infty$.

Examples follow.

Example 1.24.
- In μ_n, $o(e^{2\pi i/n}) = n$.
- Similarly, in ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$, $o([1]_n) = n$. For a general element $[a]_n \in {}^{\mathbb{Z}}/_{n\mathbb{Z}}$, the order is $o([a]_n) = \frac{n}{\gcd(a,n)}$.

Proposition 1.25. *Let G be a finite group. For all $a \in G$, $o(a)$ is finite.*

Proof. Let $a \in G$. We look at $a, a^2, a^3, \ldots \in G$. Since G is finite, not all are distinct; there exists $m > n$ such that $a^m = a^n$. Multiplying by a^{-n}, we have $a^{m-n} = a^{n-n} = e$, and the order of a is finite. ■

1.2.1 The S_n Group

To understand the order better, we look specifically at S_3.

Example 1.26. The elements in S_3 are

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}. \tag{1.3}$$

Alternatively, the elements may be (correspondingly) written as

$$e, \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \text{ and } \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}. \tag{1.4}$$

It is easy to see that the orders of $e, \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ are $1, 2, 3$, respectively. The elements $\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}$, and $\begin{pmatrix} 1 & 3 \end{pmatrix}$ are termed transpositions. In general, an element $\sigma \in S_n$ is called a *transposition* if there exists $1 \leq a \neq b \leq n$ such that $\sigma(a) = b$ and $\sigma(b) = a$, but $\sigma(x) = x$ for all $x \notin \{a, b\}$.
An element $\sigma \in S_n$ is called a *cycle* if there exists distinct $1 \leq a_1, a_2, \ldots, a_m \leq n$ such that $\sigma(a_i) = a_{i+1}$ for $1 \leq i \leq m-1$, $\sigma(a_m) = a_1$, and $\sigma(x) = x$ for all $x \notin \{a_1, a2, \ldots, a_m\}$. Thus, a transposition is really just a cycle of length 2. If σ is a cycle of length m, then $o(\sigma) = m$.
In the above, $\sigma^i(a_1) = a_{i+1}$ if $i < m$. Thus, $\sigma^i \neq e$ for $i < m$. But for m-times composition, we have $\sigma^m(a_i) = a_i$ for all $1 \leq i \leq m$. Hence, the order of σ is really m.

Note that S_3 is non-abelian since $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$, but $\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$.

Definition 1.27. Let $\sigma, \tau \in S_n$ be cycles. They are called *disjoint cycles* if $\sigma = (a_1, \ldots, a_m)$ and $\tau = (b_1, \ldots, b_k)$, and $\{a_1, \ldots, a_m\} \cap \{b_1, \ldots, b_k\} = \emptyset$.

If σ and τ are disjoint cycles then they commute; that is, $\sigma \circ \tau = \tau \circ \sigma$.

Proposition 1.28. *Every element of S_n can be written as a product of disjoint cycles.*

Proof. Let $\sigma \in S_n$, and let k be the least positive integer such that $\sigma^k(1) = 1$. Then let $\tau_1 = \begin{pmatrix} 1 & \sigma(1) & \sigma^2(1) & \cdots & \sigma^{k-1}(1) \end{pmatrix}$. Let S_1' be the *support* of τ_1, defined as $\mathrm{supp}(\tau_1) = \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$. If $S_1' = \{1, 2, \ldots, n\}$, we are done. Otherwise, let $a_2 = \min(\{1, 2, \ldots, n\} \setminus S_1')$. Let k_2 be the least positive integer such that $\sigma^{k_2}(a_2) = a_2$, and then let $\tau_2 = \begin{pmatrix} a_2 & \sigma(a_2) & \cdots & \sigma^{k_2-1}(a_2) \end{pmatrix}$. Then τ_2 is a cycle of length of k_2. Again, let $S_2' = \mathrm{supp}(\tau_2)$. We claim that $S_1' \cap S_2' = \emptyset$.

If $\sigma(a_2)$ were in S_1', then we would have $\sigma^i(i) = a_2 \in S_1'$, but a_2 was taken from $\{1, 2, \ldots, n\} \setminus S_1'$. Similarly, if $\sigma^j(a_2) \in S_1'$, then a similar problem arises. Thus, the sets have to be disjoint.

Continue this way to get $\tau_1, \tau_2, \ldots, \tau_l$ until $S_1' \cup S_2' \cup \cdots \cup S_k' = \{1, 2, \ldots, n\}$. The process stops since $S_1', S_2', \ldots, S_k'$ are non-empty. Thus, we conclude that $\tau_1 \circ \tau_2 \circ \cdots \circ \tau_l$ is the disjoint cycle decomposition of σ. ∎

For ease of notation, we will write $\sigma \circ \tau$ as $\sigma\tau$.

Proposition 1.29. *Let $\sigma \in S_n$ and $\sigma = \tau_1\tau_2 \cdots \tau_k$ be a disjoint cycle decomposition of σ. Then, $|\sigma| = \mathrm{lcm}(|\tau_1|, |\tau_2|, \ldots, |\tau_k|)$.*

Proof. The proof of this proposition is left as an exercise to the reader. ∎

1.3 Subgroups

We begin with the definition.

Definition 1.30. A non-empty subset H of a group $(G, \cdot)$ is called a *subgroup* if the following properties hold.

1. For all $a, b \in H$, $a \cdot b \in H$.
2. For all $a \in H$, $a^{-1} \in H$.

In such a scenario, we write $H \leqslant G$.

More properties of a subgroup can be inferred.

Proposition 1.31. *The following properties hold true for a subgroup $H \leqslant G$, where $(G, \cdot, e)$ is a group.*

1. *$e \in G$.*
2. *$(H, \cdot, e)$ is a group.*

Proof.
1. H is non-empty, so there exists $a \in G$ such that $a \in H$. From the definition, $a^{-1} \in H$ also. Since H is closed under the binary operation, we have $a \cdot a^{-1} = e \in H$.
2. We show that $(H, \cdot, e)$ satisfies the group axioms. From definition, $\cdot$ is an associative binary operaion on H. Also, e is the identity element in H. Again, from the definition, each $a \in H$ has an inverse $a^{-1} \in H$.

∎

Equivalently, H is a subgroup if the following holds.

Theorem 1.32. *Let G be a group and $H \subseteq G$ be non-empty. Then H is a subgroup of G if and only if $a \cdot b^{-1} \in H$ for all $a, b \in H$.*

Proof. The forward implication is left as an exercise to the reader. If $a \in H$ then $a \cdot a^{-1} \in H$ shows that $e \in H$. Since $e, a \in H$, $e \cdot a^{-1} = a^{-1} \in H$. If $a, b \in H$, then $a, b^{-1} \in H \implies a \cdot (b^{-1})^{-1} \in H \implies ab \in H$ ■

July 31st.

We look at some examples of subgroups.

Example 1.33.
- For any group G, $\{e\} \subseteq G$ is a subgroup. This is termed the *trivial group*.
- Any group G is a subgroup of itself.
- We have $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$. Similarly, $(\{\pm 1\}, \cdot) \leqslant (\mathbb{Q}^*, \cdot) \leqslant (\mathbb{R}^*, \cdot) \leqslant (\mathbb{C}^*, \cdot)$.
- If $H \leqslant G$ and $K \leqslant H$, then $K \leqslant G$.
- $\mu_n \leqslant (\mathbb{C}^*, \cdot)$ for all natural n.
- For $(\mathbb{Z}/6\mathbb{Z}, +) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, the only possible subgroups are $\{\bar{0}\}$, $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$, and $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

1.3.1 Generation

Definition 1.34. Let G be a group and $S \subseteq G$ be a subset. We say S generates a subgroup H if H is the smallest subgroup of G containing S. We denote this as $\langle S \rangle = H$.

Remark 1.35. Let $H_1, H_2 \leqslant G$. Then $H_1 \cap H_2 \leqslant G$.

Proof. Note that $e \in H_1, H_2$, so $H_1 \cap H_2 \neq \emptyset$. Also, if $x, y \in H_1 \cap H_2$, then $xy^{-1} \in H_1 \cap H_2$. We are done. ■

Proposition 1.36. *For $S \subseteq G$, $\langle S \rangle$ always exists and is unique.*

Proof. Let $\Omega = \{H \leqslant G \mid S \subseteq H\}$. Since $G \in \Omega$, it is non-empty. Thus, we simply take $\langle S \rangle = \cap_{H \in \Omega} H$, which is the smallest subgroup containing S. ■

The above proof is merely of existence, and will be a hassle for constructing the generated group. The following proposition simplifies the construction process.

Proposition 1.37. *Let G be a group and $S \subseteq G$ be a subset. Then*

$$\langle S \rangle = H = \{a_1 \cdots a_n \mid a_i \in S \text{ or } a_i^{-1} \in S \text{ for } n \geq 1\} \cup \{e\}. \tag{1.5}$$

Proof. Note that $S \subseteq H$, so H is non-empty. Let $x, y \in H$. Then, $x = a_1 \cdots a_n$ with $a_i \in S$ or $a_i^{-1} \in S$. Similarly, $y = b_1 \cdots b_m$ with $b_j \in S$ or $b_j^{-1} \in S$. We then have

$$a_1 \cdots a_n b_m^{-1} \cdots b_1^{-1} \text{ with } a_i \in S \text{ or } a_i^{-1} \in S, \text{ and } (b_j^{-1})^{-1} \in S \text{ or } b_j^{-1} \in S. \tag{1.6}$$

Thus, $xy^{-1} \in H$ and $\langle S \rangle \subseteq H$. For the converse inclusion, it is enough to show that if H' is a subgroup such that $S \subseteq H'$, then $H \leqslant H'$. Suppose H' is such a subgroup. Then $a_1 \cdots a_n \in H^{-1}$ for $a_i \in S$ or $a_i^{-1} \in S$ since $a_i \in S \subseteq H' \implies a_i^{-1} \in H'$ and $x, y \in H' \implies xy \in H$. Hence, $H \leqslant H'$. ■

Definition 1.38. A group G is termed a *cyclic group* if there exists $a \in G$ such that $\langle \{a\} \rangle = G$. Usually, we prefer to write it as $\langle a \rangle = G$.

Example 1.39. $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ for all natural n.

Proposition 1.40. *The group S_n is generated by transpositions, for all $n \geq 1$.*

Proof. From **Proposition 1.28**, every $\sigma \in S_n$ can be written as $\sigma = \tau_1 \cdots \tau_k$ where $\tau_i \in S_n$ are cycles. So it is enough to show that every cycle is a product of transpositions. Suppose $\begin{pmatrix} i_1 & i_2 & \cdots & i_l \end{pmatrix}$ is such a cycle with $i_1, \ldots, i_l$ begin distinct elements of $\{1, 2, \ldots, n\}$. This can be rewritten simply as

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_l \end{pmatrix} = \begin{pmatrix} i_1 & i_l \end{pmatrix} \begin{pmatrix} i_1 & i_{l-1} \end{pmatrix} \cdots \begin{pmatrix} i_1 & i_3 \end{pmatrix} \begin{pmatrix} i_1 & i_2 \end{pmatrix}. \tag{1.7}$$

■

Example 1.41. Let us look at $S_3 = \{e, \begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}\}$. Then the only possible subgroups are

- $\{e\}$,
- $\{e, \begin{pmatrix} 1 & 2 \end{pmatrix}\}$,
- $\{e, \begin{pmatrix} 2 & 3 \end{pmatrix}\}$,
- $\{e, \begin{pmatrix} 1 & 3 \end{pmatrix}\}$,
- $\{e, \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}\}$, and
- S_3.

An important subgroup of S_n is A_n, defined as the set of all permutations in S_n with even parity; all permutations that can be written as the product of even number of transpositions. A_n is termed the *alternating group*. Similarly, D_n is also defined. The *dihedral group* D_n is the group of symmetries of a n-regular polygon, which includes rotations and reflections. Labelling the vertices as 1 through n, the rotations and reflections can really be seen as those permutations in S_n that leave the n-regular polygon as itself after permutation. For example, D_4 is the group $\{\sigma \in S_4 \mid \sigma(\Box) \text{ is still a } \Box\}$. If n is even, we can write

$$D_n = \langle \begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}, \begin{pmatrix} 1 & n \end{pmatrix} \begin{pmatrix} 2 & n-1 \end{pmatrix} \cdots \begin{pmatrix} \frac{n}{2} & \frac{n}{2}+1 \end{pmatrix} \rangle. \tag{1.8}$$

If n is odd, we have

$$D_n = \langle \begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix}, \begin{pmatrix} 1 & n-1 \end{pmatrix} \begin{pmatrix} 2 & n-2 \end{pmatrix} \cdots \begin{pmatrix} \frac{n-1}{2} & \frac{n+1}{2} \end{pmatrix} \rangle. \tag{1.9}$$

Chapter 2

COSETS AND MORPHISMS

2.1 Cosets

We start with cosets.

Definition 2.1. Let $H \leqslant G$ and $x \in G$. A *left coset* of H generated by x is $xH = \{xh \mid h \in H\} \subseteq G$. The left coset need not be a subgroup of G. Similarly, a *right coset* of H generated by x is $Hx = \{hx \mid h \in H\} \subseteq G$. Again, the right coset need not be a subgroup

Let $H \leqslant G$. For $x, y \in G$, let us write $x \sim y$ if $x^{-1}y \in H$. Then $\sim$ is an equivalence relation. Moreover, $[x] = xH$ for all $x \in G$. Once we have proved, we will be able to partition our group.

Proof. Clearly, $\sim$ is reflexive since $x^{-1}x = e \in H$ for all $x \in G$. $\sim$ is symmetric since we have

$$x \sim y \implies x^{-1}y \in H \implies (x^{-1}y)^{-1}H \implies y^{-1}x \in H \implies y \sim x. \tag{2.1}$$

Finally, $\sim$ is also transitive since

$$x \sim y \text{ and } y \sim z \implies x^{-1}y, y^{-1}z \in H \implies x^{-1}y \cdot y^{-1}z = x^{-1}z \in H \implies x \sim z. \tag{2.2}$$

To show the latter result, we first have

$$y \in [x] \implies x \sim y \implies x^{-1}y \in H \implies xx^{-1}y = y \in xH \implies y \in xH. \tag{2.3}$$

So, $[x] \subseteq xH$. For the converse inclusion, we have

$$y \in xH \implies y = xh \text{ for some } h \in H \implies x^{-1}y = h \in H \implies y \in [x]. \tag{2.4}$$

Thus, $xH \subseteq [x]$ and $xH = [x]$. ■

The above results of cosets prove to be useful in the following theorem.

Theorem 2.2 (*Lagrange's theorem*)**.** *Let G be a finite group with $H \leqslant G$. Then $|H| \mid |G|$.*

Proof. For $x, y \in G$, if $xH \cap yH \neq \emptyset$, then we must have $xH = yH$. Also, $\bigcup_{x \in G} xH = G$. We now claim that $|xH| = |yH|$ for all $x, y \in G$. To show this, we let $f : xH \to yH$ be defined as $f(a) = yx^{-1}a$, and $g : yH \to xH$ be defined as $g(b) = xy^{-1}b$. Then f and g are inverses of each other since

$$(f \circ g)(b) = f(xy^{-1}b) = yx^{-1}xy^{-1}b = b \text{ and } (g \circ f)(a) = g(yx^{-1}a) = xy^{-1}yx^{-1}a = a. \tag{2.5}$$

Let $S = G/\sim$ (also denoted as G/H). Since $G = \bigcup_{A \in S} A$, we have $|A| = |H|$ for all $A \in S$, implying $|G| = |S|\,|H|$. ■

Corollary 2.3. *Let G be a finite group, with $a \in G$. Then $\o(a) \mid |G|$.*

Proof. If $o(a) = n$, then $\langle a \rangle = \{a, a,^2, \ldots, a^{n-1}, e\}$. Since this is a subgroup, we have $|\langle a \rangle| = n \mid |G|$ by Lagrange's theorem. ∎

Index