GROUP THEORY

Manish Kumar, notes by Ramdas Singh

Third Semester

List of Symbols

Placeholder

Contents

1 INTRODUCTION TO GROUP THEORY 1
- 1.1 Set Theory . . . 1
- 1.2 Groups . . . 4
  - 1.2.1 The S_n Group . . . 5
- 1.3 Subgroups . . . 6
  - 1.3.1 Generation . . . 7

2 COSETS AND MORPHISMS 9
- 2.1 Cosets . . . 9
- 2.2 Mappings . . . 10
  - 2.2.1 Properties . . . 10
  - 2.2.2 Kernel and Image . . . 12
- 2.3 Normal Subgroups and Quotient Groups . . . 12
  - 2.3.1 Centre . . . 14
- 2.4 The Isomorphism Theorems . . . 15
  - 2.4.1 First Isomorphism Theorem . . . 15
  - 2.4.2 Second and Third Isomorphism Theorems . . . 17

3 GROUP ACTIONS 19
- 3.1 An Overview . . . 19
- 3.2 Orbits and Stabilizers . . . 20
- 3.3 Conjugation . . . 22
- 3.4 Sylow's Theorems . . . 24
  - 3.4.1 Simple Groups . . . 25

4 PRESENTATION OF GROUPS 29
- 4.1 Free Groups . . . 29
- 4.2 Automorphisms . . . 31

Index 33

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

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

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 $\text{ord}(G)$. 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 $\text{supp}(\tau_1) = \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$. 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 $S_2' = \text{supp}(\tau_2)$. 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, $|\sigma| = \text{lcm}(|\tau_1|, |\tau_2|, \ldots, |\tau_k|)$.*

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 $\{\sigma \in S_4 \mid \sigma(\square) \text{ is still a } \square\}$. 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. ■

2.2 Mappings

August 5th.

We now study important mappings between groups and the types of mappings one can define.

Definition 2.4. A function $f : (G, *) \to (H, \circ)$, where $(G, *)$ and $(H, \circ)$ are groups, is said to be a (group) *homomorphism* if

$$f(x * y) = f(x) \circ f(y) \text{ for all } x, y \in G. \tag{2.6}$$

The following is a trivial example of a group homomorphism.

Example 2.5. For instance, the map $a \mapsto a$ in $(\mathbb{Z}, +) \to (\mathbb{Q}, +)$ is a group homomorphism, trivially. More generally, if $H \leqslant G$, then $a \mapsto a$, called the *inclusion map* is a group homomorphism.

Homomorphisms can be classified further if they inherit nicer properties.

Definition 2.6. The group homomorphism is also called an injective homomorphism, or a *monomorphism*, if the mapping is also injective. Similarly, it is also called a surjective homomorphism, or a *epimorphism*, if the mapping is also surjective. Finally, the group homomorpshim is termed an *isomorphism* if it is bijective.

Example 2.7.

1. The map $q : (\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ defined as $q(a) = [a]_n$ for $n \geq 1$ is a group homomorphism. Specifically, it is an epimorphism.
2. $f : (G, *) \to (\{e\}, \cdot)$ with $f(g) = e$ for all $g \in G$ is another epimorphism. This is also a trivial homomorphism.
3. The scaling map $a \mapsto \lambda a$ in $\mathbb{Z} \to \mathbb{Z}$ is a monomorphism for $\lambda \in Z_{\geq 1}$. Similarly, $[a] \mapsto [\lambda a]$ in $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is group homomorphism. If $\gcd(n, \lambda) = 1$, then the map is also an isomorphism in this case.
4. The scaling map $f : \mathbb{Q} \to \mathbb{Q}$ with $f(a) = ca$ with $c \in \mathbb{Q}^*$ is an isomorphism. For $c = 0$, we get the trivial homomorphism.
5. From linear algebra, the map $T : (\mathbb{Q}^n, +) \to (\mathbb{Q}^n, +)$ with $T \in M_n(\mathbb{Q})$ defined as $v \mapsto Tv$ is also a group homomorphism. If $T \in GL_n(\mathbb{Q}) \subseteq M_n(\mathbb{Q})$, the map is also an isomorphism.
6. Towards more non-trivial examples, one can confirm that the map $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ defined as $x \mapsto e^x$ is a group homomorphism.

2.2.1 Properties

Arising from these structure-preserving mappings are some useful properties.

Proposition 2.8. *Let $f : (G, *) \to (H, \circ)$ be a group homomorphism. Then*

1. *$f(e_G) = e_H$,*
2. *$f(a^n) = f(a)^n$, and*
3. *$f(a)^{-1} = f(a^{-1})$.*

Proof. 1. Simply work as

$$f(e_G) = f(e_G * e_G) = f(e_G) \circ f(e_G) \implies e_H = f(e_G)^{-1} \circ f(e_G) = f_{e_G}. \tag{2.7}$$

2. We show the base case, then induction may be applied.

$$f(a^2) = f(a * a) = f(a) \circ f(a) = f(a)^2. \tag{2.8}$$

3. Again,

$$f(a^{-1}) \circ f(a) = f(a^{-1} * a) = f(e_G) = e_H = f(a)^{-1} \circ f(a) \implies f(a^{-1}) = f(a)^{-1}. \tag{2.9}$$

■

We show further some properties of bijective homomorphisms.

Proposition 2.9. *Let $f : (G, *) \to (H, \cdot)$ be a group isomorphism. Then*

1. *$f^{-1} : H \to G$ is a group isomorphism,*
2. *$o(x) = o(f(x))$ for all $x \in G$,*
3. *$|G| = |H|$, and*
4. *G is abelian if and only if H is abelian.*

Proof. 1. Fix $a, b \in H$, and let $x = f^{-1}(a)$ and $y \in f^{-1}(b)$. We want to show that $f^{-1}(a \cdot b) = f^{-1}(a) * f^{-1}(b)$. To this end, we have

$$f(f^{-1}(a) * f^{-1}(b)) = f(x * y) \Rightarrow f(f^{-1}(a)) \cdot f(f^{-1}(b)) = a \cdot b = f(x * y) \Rightarrow f^{-1}(a \cdot b) = x * y. \tag{2.10}$$

2. Let $o(x) = n$, where $x^m \neq e_G$ for $1 \leq m < n$ and $x^n = e_G$. This shows that $f(x)^n = f(x^n) = e_H$. Also, since $x^m \neq e_G$ for $1 \leq m < n$, we must have $f(x^m) \neq e_H$ for $1 \leq m < n$ as f is bijective. Thus, $o(f(x)) = o(x)$. If $o(x)$ were not finite, then $x^n \neq e_G$ for all $n \geq 1$ implies $f(x)^n \neq e_H$ for all $n \geq 1$.

3. This is trivial.

4. If G is abelian then $a * b = b * a$ for all $a, b \in G$. Applying f, we get $f(a * b) = f(b * a) \Rightarrow f(a) \cdot f(b) = f(b) \cdot f(a)$ for all $a, b \in G$. If we take $a = f^{-1}(x)$ and $b = f^{-1}(y)$, we get $x \cdot y = y \cdot x$ for all $x, y \in H$. For the converse implication, simply consider the isomorphism f^{-1}.

■

Essentially, in group theory, we consider two groups the same if they are isomorphic. Thus, we are equipped to classify groups up to isomorphism seeing as they share basically the same struture and properties. If two groups G and H are isomorphic, we denote it as $G \cong H$.

Proposition 2.10. *Let $(G, \cdot)$ be a group of order p, where p is prime. Then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $x \in G$ be a non-identity element. Then $o(x) = p$ since $o(x) \mid p$ and $o(x) \neq 1$. Define the map $f : \mathbb{Z}/n\mathbb{Z} \to G$ as $f(a) = x^a$. We show that this mapping is an isomorphism. For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, we have

$$f(\overline{a} + \overline{b}) = f(\overline{a + b}) = x^{a+b} = x^a \cdot x^b = f(\overline{a}) \cdot f(\overline{b}) \tag{2.11}$$

showing f is a group homomorphism. Moreover, $G = \langle x \rangle$ as $o(x) = p$, so G is also surjective. Hence, f is an isomorphism as G is finite. ■

Example 2.11. We find all the groups of order 4 upto isomorphism. The only two possibilities are $\mathbb{Z}/4\mathbb{Z}$, and $(\mathbb{Z}/2\mathbb{Z})^2$ with component-wise addition.

Example 2.12. We list down all the groups of order 6 upto isomorphism. Again, the only two possibilities are $\mathbb{Z}/6\mathbb{Z}$ and S_3.

August 7th.

Example 2.13. For groups of order 8, we have $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_4, and Q_8, the quaternions.

The *quaternions* Q_8 is the group $\{\pm 1, \pm i, \pm j, \pm k\}$ equipped with the multiplication operation such that

$$i^2 = -1, \quad j^2 = -1, \quad k^2 = -1, \tag{2.12}$$
$$ij = k, \quad jk = i, \quad ki = j, \tag{2.13}$$
$$ji = -k, \quad kj = -i, \quad ik = -j. \tag{2.14}$$

2.2.2 Kernel and Image

Definition 2.14. For a group homomorphism $f : G \to H$, we define the *kernel* of f as $\ker f = \{g \in G \mid f(g) = e_H\}$. We also define the *image* of f as $f(G) = \operatorname{Im} f = \{f(g) \mid g \in G\}$.

The image and kernel are both subgroups; this is our proposition.

Proposition 2.15. *For a group homomorphism $f : G \to H$, $\ker f$ and $\operatorname{Im} f$ are subgroups of G and H respectively.*

Proof. Note that $\emptyset \neq \operatorname{Im} f \subseteq H$; let $a, b \in \operatorname{Im} f$. Then $f(x) = a$ and $f(y) = b$ for some $x, y \in G$. So, $ab = f(x)f(y) = f(xy) \in \operatorname{Im} f$, showing $ab \in \operatorname{Im} f$. Also, $a^{-1} = f(x)^{-1} = f(x^{-1}) \in \operatorname{Im} f$, showing $a^{-1} \in \operatorname{Im} f$. Thus, $\operatorname{Im} f \leqslant H$.

For the kernel, note that $e_g \in \ker f$ since $f(e_G) = e_H$. Let $x, y \in \ker f$. Then $f(x) = f(y) = e_H$ implying $f(xy^{-1}) = f(x)f(y)^{-1} = e_H e_H^{-1} = e_H$. Thus, $xy^{-1} \in \ker f$, showing $\ker f \leqslant H$. ∎

Remark 2.16. Let f be a group homomorphism.

1. If f is an isomorphism, then $\operatorname{Im} f = H$ and $\ker f = \{e_G\}$.
2. If f is a monomorphism, then $\ker f = \{e_G\}$.
3. If f is an epimorphism, then $\operatorname{Im} f = H$.

2.3 Normal Subgroups and Quotient Groups

Proposition 2.17. *Let G be a group and $H \leqslant G$ be a subgroup. Then the following are equivalent.*

1. *$gH \subseteq Hg$ for all $g \in G$,*
2. *$g^{-1}Hg \subseteq H$ for all $g \in G$,*
3. *$gH = Hg$ for all $g \in G$,*
4. *$g^{-1}Hg = H$ for all $g \in G$.*

Such a subgroup satisfying any (all) of the above conditions is termed a *normal subgroup* of G and is denoted by $H \trianglelefteq G$.

Proof. For 1. implies 2., we are given $g^{-1}H \subseteq Hg^{-1}$ for all $g \in G$. Let $x \in g^{-1}Hg$. Then $x = g^{-1}hg$ for some $h \in H$. Thus, $g^{-1}h \in g^{-1}H \subseteq Hg^{-1}$ which implies $g^{-1}h = h'g^{-1}$ for some $h' \in H$. But then $g^{-1}hg = h' \in H$, showing $x \in H$. Therefore, $g^{-1}Hg \subseteq H$.

For 2. implies 3., assume $g^{-1}Hg \subseteq H$ for all $g \in G$. Let $x \in gH$, that is, $x = gh$ for some $h \in H$. Write this as $x = ghg^{-1}g$. But $ghg^{-1} \in gHg^{-1} \subseteq H$, so $ghg^{-1} = h'$ for some $h' \in H$. Thus, $x = h'g \in Hg$. Similarly, if $x \in Hg$, then $x \in gH$. We conclude that $Hg = gH$ for all $g \in G$.

For 3. implies 4., we have $gH = Hg$ for all $g \in G$. Let $x \in g^{-1}Hg$, where $x = g^{-1}hg$ for some $h \in H$. Note that $hg = gh'$ for some $h' \in H$ since $gH = Hg$. Thus, $x = g^{-1}hg = g^{-1}(gh') = h' \in H$, giving us $g^{-1}Hg \subseteq H$.

Finally, for 4. implies 1., let $x \in gh$; there exists $h \in H$ such that $x = gh$. Thus, $x = ghg^{-1}g = h'g \in Hg$ since $gHg^{-1} = H$. Hence, $gH \subseteq Hg$. ■

Note that if G is abelian, then every subgroup is normal.

Proposition 2.18. *The following miscellaneous propositions hold true. Let G be a group.*

1. *If $g, h \in G$, then $\mathrm{ord}(ghg^{-1}) = \mathrm{ord}(h)$.*
2. *The mapping $\varphi_g : G \to G$ defined as $\varphi_h(h) = g^{-1}hg$ is an isomorphism for all $g \in G$. The inverse isomorphism is given by $\varphi_g^{-1} = \varphi_{g^{-1}}$.*
3. *Both G and $\{e\}$ are normal subgroups of G.*

Proof. The proofs of these are left as an exercise to the reader. ■

Proposition 2.19. *Let $f : G \to H$ be a group homomorphism. Then $\ker f \trianglelefteq G$.*

Proof. For $g \in G$, let $x \in g^{-1}\ker(f)g$; that is, $x = g^{-1}hg$ for some $h \in \ker f$. Then,

$$f(x) = f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g)^{-1}e_H f(g) = e_H. \tag{2.15}$$

Thus, $x \in \ker f$, showing $g^{-1}\ker(f)g \subseteq \ker f$ for all $g \in G$; $\ker f \trianglelefteq G$. ■

Proposition 2.20. *Let G be a group with $H \leqslant G$ a subgroup. Then $H \trianglelefteq G$ if and only if for all $\varphi_g : G \to G$, we have $\varphi_g|_H : H \to H$, an isomorphism.*

Note that an isomorphism from a group to itself is called an *automorphism*. Thus, the above proposition equates to φ_g still remaning an automorphism when restricted to H.

Proof. The statement is simply equivalent to saying $g^{-1}Hg = H$ for all $g \in G$. ■

One also defines the notion of *product of groups*. Let G_1, G_2 be two groups. Then

$$G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\} \tag{2.16}$$

is a group with the equipped operation defined as

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2'). \tag{2.17}$$

Here, the identity element is (e_{G_1}, e_{G_2}) and the inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}).

Let G be a group and H, K be subgroups of G. Let $HK = \{hk \mid h \in H, k \in K\}$. Then HK is a group if either H or K is a normal subgroup of G.

Proof. Let us assume $H \trianglelefteq G$. Take the elements $h_1k_1, h_2k_2 \in HK$. Since $H \trianglelefteq G$, $k_1H = Hk_1$. So, $k_1h_2 = h'k_1$ for some $h' \in H$ Thus,

$$h_1k_1h_2k_2 = h_1h'k_1k_2 \in HK. \tag{2.18}$$

Similarly, $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = h'k_1^{-1} \in HK$ for some $h' \in H$, since $H \trianglelefteq G$ and $k_1^{-1}H = Hk_1^{-1}$. ■

August 12th.

We now get familiar with quotient groups.

Definition 2.21. Let G be a group and $H \trianglelefteq G$ a normal subgroup. The *quotient group* is defined as $G/H = \{gH \mid g \in G\}$ with the operation defined as $gH * g'H := (gg')H$ for all $g, g' \in G$.

Of course, it still remains to verify that the groups axioms are not violated and the operation is indeed well-defined.

Proof. Let $gH = kH$ and $g'H = k'H$ for $k, k' \in G$. We wish to show that $gg'H = kk'H$. Since $gH = kH$, we have $k^{-1}g \in H$. Similarly, $k'^{-1}g' \in H$, and $k'^{-1}g'(k^{-1}g) \in H$. Thus, $(kg')^{-1}gg' \in H$ and $gg'H = kg'H$. Hence, the operation is well-defined. We verify the group axioms now.

1. *Associativity:* We have
$$(gH * hH) * (kH) = (ghH) * kH = (gh)kH = g(hk)H = gH * (hkH) = (gH) * (gH * kH). \quad (2.19)$$
2. *Existence of Identity:* The identity here is $e_{G/H} = H$ since
$$gH * H = (ge)H = gH = (eg)H = H * gH. \quad (2.20)$$
3. *Existence of Inverse:* For $gH \in G/H$, we have $(gH)^{-1} = g^{-1}H$ since
$$(gH) * (g^{-1}H) = (gg^{-1})H = H = (g^{-1}g)H = (g^{-1}H) * (gH). \quad (2.21)$$

■

Note that the map $q : G \to G/H$ defined as $g \mapsto gH$ is a group epimorphism, with $\ker q = H$. The proof of showing surjectivity and preservation of group structure is left as an exercise the reader.

Example 2.22.
- As a familiar example, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ is a normal subgroup, and the quotient group $\mathbb{Z}/n\mathbb{Z}$ is the group of integers modulo n.
- If one sets $H = \{e\} \trianglelefteq G$, then $G/H = \{\{g\} \mid g \in G\}$ is the group of singletons, and the quotient map $q : G \to G/H$ becomes an isomorphism.
- If $H = G \trianglelefteq G$, then $G/H = \{G\}$ is the trivial group.

2.3.1 Centre

Definition 2.23. The *centre of a group* G, denoted $Z(G)$, is the set of all elements in G that commute with every element of G:
$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}. \quad (2.22)$$

One can show that $Z(G) \leqslant G$ always holds true. In fact, the centre is a subgroup of G.

Example 2.24.
- Since $Z(G)$ is a normal subgroup, the quotient group makes sense. However, in general, $Z(G/Z(G))$ is not trivial.
- G is abelian if and only if $Z(G) = G$.
- $Z(GL_2(\mathbb{R})) = \{\lambda I \mid \lambda \in \mathbb{R}^*\}$, where I is the identity matrix.

One can also define a centre for individual elements and subsets in a group.

Definition 2.25. The *centre of a subset* $H \subseteq G$ is defined as
$$C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}. \quad (2.23)$$
Note that $Z(G) \subseteq C_G(H)$ and $C_G(G) = Z(G)$. For $g \in G$, we define the *centralizer* of g as

$C_G(g) := C_G(\{g\})$. Additionally, if $H \leqslant G$, then

$$N_G(H) = \{g \in G \mid gH = Hg\} \tag{2.24}$$

is termed the *normalizer* of H in G.

Remark 2.26. The following may be shown, for a subset $H \subseteq G$.

- $C_G(H) = \bigcap_{g \in H} C_G(g)$.
- $C_G(H) \leqslant G$ holds.

The following may be shown, for a subgroup $H \leqslant G$.

- $C_G(H) \subseteq N_G(H)$ holds.
- $H \trianglelefteq N_G(H)$ holds.
- $N_G(H) \leqslant G$ holds.

The proofs of the above are left as an exercise to the reader.

2.4 The Isomorphism Theorems

These are important theorems that hold regarding isomorphisms. In particular, they describe the relationships between different quotient groups and subgroups. Before we encounter the actual theorems, we establish a minor result.

Proposition 2.27. *Let $f : G \to H$ be a group homomorphism and let $K = \ker f$. Then $K \trianglelefteq G$. Moreover, $K = \{e\}$ if and only if f is injective.*

Proof. The first part follows from the fact that $g^{-1}Kg \subseteq K$ for all $g \in G$. For the second part, if f is injective, then $\ker f = \{e\}$ since $f(g) = e_H$ implies $g = e_G$. Conversely, suppose $K = \{e\}$ and let $f(g) = f(g')$ for some $g, g' \in G$. Then

$$f(g^{-1}g') = f(g^{-1})f(g') = f(g)^{-1}f(g) = e_H \implies g^{-1}g' = e_G \implies g' = g. \tag{2.25}$$

■

2.4.1 First Isomorphism Theorem

Theorem 2.28 (The *first isomorphism theorem*)**.** *Let $f : G \to H$ be a group homomorphism. Then the map $\tilde{f} : G/K \to \operatorname{Im} f$ sending $gK \mapsto f(g)$ is a well-defined isomorphism where $K = \ker f$. Bluntly,*

$$G/\ker f \cong \operatorname{Im} f. \tag{2.26}$$

Proof. We first show that $\tilde{f}$ is well-defined. Suppose $gK = g'K$ for some $g, g' \in G$. Then

$$g^{-1}g' \in K \implies f(g^{-1}g') = e_H \implies f(g) = f(g'). \tag{2.27}$$

To show $\tilde{f}$ is a homomorphism, let $aK, bK \in G/K$. Then

$$\tilde{f}(aK \cdot bK) = \tilde{f}((ab)K) = f(ab) = f(a)f(b) = \tilde{f}(aK) \cdot \tilde{f}(bK). \tag{2.28}$$

Finally, we show $\tilde{f}$ is bijective. Let $h \in \operatorname{Im} f$. Then there exists $g \in G$ such that $f(g) = h$. We claim that $\tilde{f}(gK) = h$. Indeed,

$$\tilde{f}(gK) = f(g) = h. \tag{2.29}$$

Thus, $\tilde{f}$ is surjective. To show injectivity, suppose $\tilde{f}(gK) = \tilde{f}(g'K)$ for some $g, g' \in G$. Then

$$f(g) = f(g') \implies g^{-1}g' \in K \implies gK = g'K. \tag{2.30}$$

Therefore, $\tilde{f}$ is injective. We conclude that $\tilde{f}$ is a bijection. ■

August 14th.

Example 2.29. We discuss the *Heisenberg group*

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}. \tag{2.31}$$

The group operation here is matrix multiplication, and one can see that $H \leqslant SL_3(\mathbb{R})$. Here, the center of H is precisely

$$Z(H) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}. \tag{2.32}$$

If we look at the map $f : H \to \mathbb{R}^2$ that sends

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, c) \tag{2.33}$$

then f is a group homomorphism since

$$f(AA') = (a + a', c + c') = (a, c) + (a', c') = f(A) + f(A'). \tag{2.34}$$

Moreover, $\operatorname{Im} f = \mathbb{R}^2$ and $\ker f = Z(H)$. Hence, by the first isomorphism theorem, we have

$$H/Z(H) \cong \mathbb{R}^2 \tag{2.35}$$

with the map $\tilde{f} : H/Z(H) \to \mathbb{R}^2$ given by $\tilde{f}(AZ(H)) = f(A)$. Note that $\mathbb{R}^2$ is an abelian group, and so is $H/Z(H)$. Hence, $Z(H/Z(H)) = H/Z(H)$.

Commutator Subgroup

Definition 2.30. Let G be a group. Then

$$(G : G) := \langle \{ ghg^{-1}h^{-1} \mid g, h \in G \} \rangle \tag{2.36}$$

is termed the *commutator subgroup* of G.

Of course, the name suggests that $(G : G)$ is a subgroup of G. In fact, it is actually a normal subgroup of G.

Proposition 2.31. *$(G : G)$ is a normal subgroup of G. Moreover $G/(G : G)$ is abelian. Let $f : G \to A$ be a group homomorphism with an abelian group A. Then $(G : G) \subseteq \ker f$ and there exists $\bar{f} : G/(G : G) \to A$ such that $f = \bar{f} \circ q$ where $q : G \to G/(G : G)$ is the quotient map.*

Proof. Let $x \in G$. Then we have

$$\begin{aligned} x^{-1}(ghg^{-1}h^{-1})x &= x^{-1}gxx^{-1}hxx^{-1}g^{-1}xx^{-1}h^{-1}x = (x^{-1}gx)(x^{-1}hx)(x^{-1}g^{-1}x)(x^{-1}h^{-1}x) \\ &= aba^{-1}b^{-1} \in (G : G) \text{ where } a = x^{-1}gx \text{ and } b = x^{-1}hx. \end{aligned} \tag{2.37}$$

Thus, if $S = \{ghg^{-1}h^{-1} \mid g, h \in G\}$, then $x^{-1}Sx \subseteq (G : G)$ for all $x \in G$. We now show that $(G : G)$ is a subgroup. Let $a \in (G : G)$. Then $a = b_1 \cdots b_n$, where $b_i \in S$, and

$$x^{-1}ax = x^{-1}b_1xx^{-1}b_2x \cdots x^{-1}b_nx \in (G : G) \tag{2.38}$$

since $x^{-1}b_ix \in (G : G)$ for all i. Thus, $x^{-1}(G : G)x \subseteq (G : G)$ for all $x \in G$, showing $(G : G) \trianglelefteq G$. Hereforth, in this example, let $C = (G : G)$. We now show G/C is abelian. This is simple enough since $ghg^{-1}h^{-1} = gh(hg)^{-1} \in C$ implies $gChC = ghC = hgC = hCgC$.

Now let $f : G \to A$ be a group homomorphism with A an abelian group. We then have

$$f(ghg^{-1}h^{-1}) = f(g)f(h)f(g^{-1})f(h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = e_A. \tag{2.39}$$

Thus, $S \subseteq \ker f$ implying $(G : G) \subseteq \ker f$. Finally, we show that $\bar{f} : G/C \to A$ defined as $gC \mapsto f(g)$ is an isomorphism. To show $\bar{f}$ is well-defined, we have $gC = hC \Leftrightarrow gh^{-1} \in C \subseteq \ker f$ showing $f(gh^{-1}) = e_A$ or $f(g) = f(h)$. To show a homomorphism, for $g, h \in G$, we have

$$\bar{f}(gChC) = f(gh) = f(g)f(h) = \bar{f}(gC)\bar{f}(hC). \tag{2.40}$$

Moreover, $\bar{f} \circ q(g) = \bar{f}(gC) = f(g)$ for all $g \in G$, so $\bar{f} \circ q = f$. ■

Remark 2.32. A few corollaries, we have

- If G is abelian then $(G : G) = \{e\}$.
- For H, the Heisenberg group, we have $(H : H) = Z(H)$.
- $(G/(G : G) : G/(G : G)) = \{e\}$.
- If $H \leqslant G$ then $|H| \mid |G|$. The *index* of H in G is defined as $[G : H] = |G/H|$. It is also equal to $\frac{|G|}{|H|}$ if $|G|$ is finite.

2.4.2 Second and Third Isomorphism Theorems

Theorem 2.33 (The *second ismorphism theorem*)**.** *Let G be a group and $A, B \leqslant G$ be subgroups such that $A \leqslant N_G(B)$. Then $AB \leqslant G$, $B \trianglelefteq AB$, and $A \cap B \trianglelefteq A$. Moreover,*

$$AB/B \cong A/(A \cap B). \tag{2.41}$$

Proof. Firstly, we have $A \leqslant N_G(B)$ and $B \trianglelefteq N_G(B) = \{g \in G \mid gB = Bg\}$. Thus, $AB \leqslant N_G(B)$. Of course, this also means $AB \leqslant G$. Also, $B \trianglelefteq AB$ since $B \trianglelefteq N_G(B)$ and $AB \subseteq N_G(B)$.

We now define a map $f : A \to AB/B$ that maps $a \mapsto aB$ since $a \in A \subseteq AB$. f is a group homomorphism. Thus, by the first isomorphism theorem,

$$\bar{f} : A/\ker f \to \operatorname{Im} f \tag{2.42}$$

is an isomorphism. It is enough to show that $\ker f = A \cap B$ and f is surjective. Again, simple to see since

$$\ker f = \{a \in A \mid aB = B\} = \{a \in A \mid a \in B\} = A \cap B; \tag{2.43}$$

for surjectivity, let $x \in AB/B$. Then $x = abB$ for some $a \in A$ and $b \in B$. But abB is simply aB so we simply have $abB = aB = f(a)$. ■

Corollary 2.34. *For G a group with $A, B \leqslant G$, we have $[AB : B] = [A : A \cap B]$.*

Finally, we move on to the third theorem.

Theorem 2.35 (The *third isomorphism theorem*)**.** *Let G be a group and let $H, K \trianglelefteq G$ such that*

$K \leqslant H$. Then $H/K \trianglelefteq G/K$ and

$$\frac{G/K}{H/K} \cong G/H. \tag{2.44}$$

Proof. We define a map $f : G/K \to G/H$ via $gK \mapsto gH$. This is well-defined since if $gK = g'K$, then $g^{-1}g' \in K \subseteq H$ and hence $gH = g'H$. We now show that f is a group homomorphism. For $gK, hK \in G/K$, we have

$$f(gKhK) = f(ghK) = ghH = gHhH = f(gK)f(hK). \tag{2.45}$$

f is also surjective as $gH = f(gK)$ for all $g \in G$. By the first isormorphism theorem, we have

$$\frac{G/K}{\ker f} \cong \operatorname{Im} f = G/H \tag{2.46}$$

where the isomorphism is given by the map $gK \ker f \mapsto gH$. Since $\ker f = \{gK \mid gH = H\} = \{gK \mid g \in H\} = H/K$, our proof is complete. ■

Chapter 3

GROUP ACTIONS

3.1 An Overview

Let G be a group and S be a set. A *(left) group action* or G-action on S is a function $\theta : G \times S \to S$ satisfying

1. $\theta(g_1 g_2, x) = \theta(g_1, \theta(g_2, x))$ for all $g_1, g_2 \in G$ and $x \in S$.
2. $\theta(e_G, x) = x$ for all $x \in S$.

In practice, we prefer to write θ simply as $(g, x) \mapsto gx$. Thus, the axioms are simply $g_1(g_2 x) = (g_1 g_2)x$ and $ex = x$ for all $g_1, g_2 \in G$ and $x \in S$. Unless there are multiple different group actions on S in context, we will stick with this notation instead. In this case, S is called a G-set.

August 19th.

Remark 3.1.
- Let $\varphi_g : S \to S$ sending $x \mapsto gx$ for all $g \in G$ and $x \in S$. Then φ_g is a bijection for each $g \in G$. This can be shown simply by considering the maps $\varphi_{g^{-1}} \circ \varphi_g$.
- Let G be a group and X be a G-set. Then the map $\psi_\theta : G \to \mathrm{Bij}(X)$ given by $g \mapsto \theta(g, *) = \varphi_g(*)$ is a group homomorphism. Here, $\mathrm{Bij}(X)$ denotes the set (group) of bijections from X to itself.
- Let $\psi : G \to \mathrm{Bij}(X)$ be a group homomorphism. Also let $\theta_\psi : G \times X \to X$ be a map defined as $\theta_\psi(g, x) = \psi(g)(x)$. Then θ is a G-action on X.

One can show that $\theta_{\psi_\theta} = \theta$ and $\psi_{\theta_\psi} = \psi$; if one starts with the action, the homomorphism can be obtained and vice versa.

$$\theta_{\psi_\theta}(g, x) = \psi_\theta(g)(x) = \theta(g, x) \text{ for all } g \in G, x \in X, \tag{3.1}$$
$$\psi_{\theta_\psi}(g)(x) = \theta_\psi(g, x) = \psi(g)(x) \text{ for all } g \in G, x \in X. \tag{3.2}$$

Example 3.2.
- Let $H \leqslant S_n$. Then H acts on $\{1, 2, \ldots, n\}$ as $(\sigma, i) \mapsto \sigma(i)$ for all $\sigma \in H$ and $i \in \{1, 2, \ldots, n\}$.
- Naturally, $GL_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$ acts as $(A, x) \mapsto Ax$ for all $A \in GL_n(\mathbb{R})$ and $x \in \mathbb{R}^n$.
- More generally, let $f : G \to GL_n(\mathbb{R})$ be a homomorphism of groups. Then the induced action of G on $\mathbb{R}^n$ is given by $(g, x) \mapsto f(g)(x)$ for all $g \in G$ and $x \in \mathbb{R}^n$.
- Let G be a group and $H \leqslant G$. Also let $X = G/H = \{gH \mid g \in G\}$ be the set of left cosets of H in G. Then G acts on X as $(g, g'H) \mapsto gg'H$ for all $g, g' \in G$.

3.2 Orbits and Stabilizers

Definition 3.3. Let G be a group and X a G-set. Then, for $x \in X$, the G-orbit (or *orbit*) of x is defined as

$$\mathcal{O}(x) = Gx := \{gx \mid g \in G\} = \{\theta(g, x) \mid g \in G\} \subseteq X. \tag{3.3}$$

If $Gx = X$ for some $x \in X$, then the G-action on X is said to be a *transitive action*.

For example, if $H \leqslant G$, then the G-action on G/H is transitive.

Proposition 3.4. *Let G be a group acting on a set X. For $x, y \in X$, we say $x \sim y$ if there exists $g \in G$ such that $gx = y$. Then $\sim$ is an equivalence relation on X, and the equivalence classes are simply the orbits;*

$$[x] = \{y \in X \mid y \sim x\} = Gx. \tag{3.4}$$

Proof. $g \sim g$ since $eg = g$. If $x \sim y$, then $gx = y$ for some $g \in G$ implies $x = g^{-1}y$ or $y \sim x$. If $x \sim y$ and $y \sim z$, then $gx = y$ and $hy = z$ for some $g, h \in G$, so $(hg)x = z$ showing $x \sim z$. ■

These orbits of G-action on X give a partition of X.

Definition 3.5. Let a group G act on a set X. For $x \in X$, the *stabilizer* of x in G is defined as

$$\mathrm{Stab}_G(x) = \mathrm{Stab}(x) := \{g \in G \mid gx = x\} = \{g \in G \mid \theta(g, x) = x\} \subseteq G. \tag{3.5}$$

Proposition 3.6. $\mathrm{Stab}_G(x) \leqslant G$ *for all* $x \in X$.

Proof. Clearly, $e_G \in \mathrm{Stab}_G(x)$ since $ex = x$. If $g, h \in \mathrm{Stab}_G(x)$, then $(gh)x = g(hx) = gx = x$, so $gh \in \mathrm{Stab}_G(x)$. Note that if $g \in \mathrm{Stab}_G(x)$, then $gx = x$ implies $x = g^{-1}x$, or $g^{-1} \in \mathrm{Stab}_G(x)$. $\mathrm{Stab}_G(x)$ is therefore a subgroup. ■

Example 3.7.

- If G acts on G/H, then $\mathrm{Stab}(H) = H$ and $\mathrm{Stab}(gH) = \{x \in G \mid xgH = gH\} = gHg^{-1}$.
- Regarding the group action S_n on $\{1, 2, \ldots, n\}$, $\mathrm{Stab}(n) = \{\sigma \in S_n \mid \sigma(n) = n\} = S_{n-1}$.

Proposition 3.8. *We state two results.*

1. *Let a group G act on a set X. For $x \in X$, the set $G/\mathrm{Stab}(x)$ is in bijection with Gx, the orbit of x.*
2. *Let $x, y \in X$ be in the same orbit. Then $\mathrm{Stab}_G(x) = g\,\mathrm{Stab}_G(y)g^{-1}$, where $g \in G$ is such that $x = gy$.*

Proof.

1. Let $H = \mathrm{Stab}(x)$. Let $gH \in G/H$. We show that the map $\psi : G/H \to Gx$ defined as $gH \mapsto gx$ is the required bijection. ψ is well=defined since if $gH = g'H$ for some $g, g' \in G$, then $g^{-1}g'x = x$ implies $g^{-1}g' \in H = \mathrm{Stab}(x)$, so $g'x = gx$. The converse argument is also true, showing ψ is well-defined and one-one. Also, for $y \in Gx$, there exists $g \in G$ such that $y = gx = \psi(gH)$; ψ is also onto.

2. Let x, y be in the same orbit; that is, there exists $g \in G$ such that $x = gy$. Suppose $h \in \mathrm{Stab}(x)$, or $hx = x$. This implies $hgy = gy \Rightarrow g^{-1}hgy = y$, so $g^{-1}hg \in \mathrm{Stab}(y)$, showing $h \in g\,\mathrm{Stab}(y)g^{-1}$. The converse argument also holds.

■

Corollary 3.9 (The *orbit-stabilizer theorem*)**.** $|G/\operatorname{Stab}(x)| = |Gx|$*, that is,* $|G| = |\operatorname{Stab}(x)| \cdot |Gx|$.

Definition 3.10. Let G be a group acting on a set X. The action is termed a *faithful action* if $\{g \in G \mid gx = x \text{ for all } x \in X\} = \{e_G\}$, that is, the only element of G that fixes every point in X is the identity element.

The above definition is equivalent to saying that the induced group homomorphism $G \to \operatorname{Bij}(X)$ is injective.

Definition 3.11. The *kernel of an action* G acting on X is defined as

$$K = \{g \in G \mid gx = x \text{ for all } x \in X\}. \tag{3.6}$$

Note that if the action is θ, then $K = \ker \psi_\theta$.

One may show that

$$K = \bigcap_{x \in X} \operatorname{Stab}_G(x). \tag{3.7}$$

For example, the kernel of G-action on G/H is $K = \bigcap_{g \in G} gHg^{-1} \trianglelefteq G$. Note that, here in this example, K is the largest subgroup of G contained in H.

August 21st.

Proposition 3.12. *Let G be a finite group. Let $H \leqslant G$ be a subgroup such that $[G : H]$ is the smallest prime dividing $|G|$. Then H is a normal subgroup of G.*

Proof. Suppose G acts on G/H via $(g, xH) \mapsto gxH$. Letting $p = [G : H]$, this induces a group homomorphism $\varphi : G \to \operatorname{Bij}(G/H) \cong S_p$. Also $K = \ker \varphi \subseteq H$ with $K \trianglelefteq G$. By the first isomorphism theorem, we work as

$$G/K \cong \operatorname{Im} \varphi \Rightarrow |\operatorname{Im} \varphi| = |G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = [G : H][H : K]. \tag{3.8}$$

But $|\operatorname{Im} \varphi|$ divides $|S_p| = p!$, so $p[H : K] \mid p! \implies [H : K] \mid (p-1)!$. Since p is the smallest prime dividing $|G|$, we must have $[H : K] = 1$, showing $K = H$. ∎

One can show a different proof for a proposition we studied earlier.

Proposition 3.13. *Let $\sigma \in S_n$. Then σ is a product of disjoint cycles.*

Proof. Let $H = \langle \sigma \rangle \subseteq S_n$. Then H acts on $\{1, 2, \ldots, n\}$. Let $O_1, \ldots, O_r$ be the orbits of H-action on $\{1, 2 \ldots, n\}$. We claim that $O_i = \{x_i, \sigma x_i, \sigma^2 x_i, \ldots, \sigma^{d_i - 1} x_i\}$, where $|O_i| = d_i$ for $1 \leq i \leq r$. If it so happens, then

$$\sigma = (x_1\ \sigma x_1\ \cdots\ \sigma^{d_1-1}x_1)(x_2\ \sigma x_2\ \cdots\ \sigma^{d_2-1}x_2)\cdots(x_r\ \sigma x_r\ \cdots\ \sigma^{d_r-1}x_r). \tag{3.9}$$

Note that $\{x_i, \sigma x_i, \ldots, \sigma^{d_i-1}x_i\} \subseteq O_i$; if $\sigma^a x_i \neq \sigma^b x_i$ for $a \neq b$, then the elements are distinct. Otherwise, $\sigma^a x_i = \sigma^b x_i$ implies $\sigma^{b-a} x_i = x_i$. Then $O_i = \{x_i, \sigma x_i, \ldots, \sigma^{b-a-1} x_i\}$ which contradicts $|O_i| = d_i$ and $\sigma^{d_i} x_i = x_i$. The disjoint cycle decomposition then follows since $\bigcup_{i=1}^n O_i = \{1, 2, \ldots, n\}$ and $O_i \cap O_j = \emptyset$ for $i \neq j$. ∎

3.3 Conjugation

The *conjugation action* of G on $\mathcal{P}(G)$, the power set of G, is defined as $G \times \mathcal{P}(G) \to \mathcal{P}(G)$ given by $(g, S) \mapsto gSg^{-1} = \{gsg^{-1} \mid s \in S\}$. This is, indeed, an action since

$$(g_1g_2) \cdot S = (g_1g_2)S(g_1g_2)^{-1} = g_1(g_2Sg_2^{-1})g_1^{-1} = g_1 \cdot (g_2Sg_2^{-1}) = g_1 \cdot (g_2 \cdot S) \text{ and } e_G \cdot S = S. \tag{3.10}$$

This action gives one an action on G on itself as

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1}. \tag{3.11}$$

Orbits of this action are termed *conjugacy classes*. For example, the conjugacy class of e_G is $\{e_G\}$. In general, the conjugacy class of $x \in G$ is $\{x\}$ if and only if $x \in Z(G)$, that is, it commutes with every element.

Example 3.14. In S_3, the conjugacy classes are as follows:

- The class of the identity: $\{e_{S_3}\}$.
- The class of the transpositions: $\{(1\ 2), (2\ 3), (1\ 3)\}$.
- The class of the 3-cycles: $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

Note that elements belonging to the same conjugacy class have the same order; this is always true for conjugacy classes of any group. A necessary, but not sufficient, condition for a subset to be a conjugacy class is that the cardinality of the subset must divide the order of the group by the orbit-stabilizer theorem.

Proposition 3.15. *Two permutations $\sigma, \tau \in S_n$ belong to the same conjugacy class if their disjoint cycle decompositions are of the same type; that is, they have the same number of cycles and they have the same cycle lengths.*

Proof. We may assume $\sigma = (1\ \cdots\ d_1)(d_1+1\ \cdots\ d_1+d_2)\cdots(d_1+\cdots+d_{r-1}+1\ \cdots\ n)$ and $\tau = (i_1\ \cdots\ i_{d_1})(i_{d_1+1}\ \cdots\ i_{d_1+d_2})\cdots(i_{d_1+\cdots+d_{r-1}+1}\ \cdots\ n)$, where $1 \le i_1, \ldots, i_n$ are distinct, and the cycle lengths in σ are $d_1, d_2, \ldots, d_r$ such that $d_1 + d_2 + \cdots + d_r = n$. Moreover, we may assume that $d_1 \le d_2 \le \cdots \le d_r$.

Let $g \in S$ such that $g(j) = i_j$ for all $1 \le j \le n$. Then

$$g\sigma g^{-1}(i_j) = g(\sigma(j)) = \begin{cases} g(j+1) & \text{if } j \notin \{d_1, d_1+d_2, \ldots, d_1+\cdots+d_{r-1}, n\}, \\ g(d_1+\cdots+d_{l-1}+1) & \text{if } j = d_1+\cdots+d_l \text{ for } l = 1, 2, \ldots, r. \end{cases} \tag{3.12}$$

The cases are essentially i_{j+1} and $i_{d_1+\cdots+d_{l-1}+1}$. But this is $\tau(i_j)$ for every i_j, showing $g\sigma g^{-1} = \tau$. ∎

Let G be a finite group. Then

$$|G| = |Z(G)| + \sum_{\substack{[g] \text{ non-trivial} \\ \text{conjugacy classes}}} [G : C_G(g)]. \tag{3.13}$$

This is known as the *class-equation*.

Proof. G acts on G via conjugacy. If $x \in Z(G)$, then the conjugacy class of x, $[x] = \{x\}$. If x is not in the centre, then $[x]$ is non-trivial. Moreover, by the orbit-stabilizer theorem, $|[x]| = [G : \mathrm{Stab}(x)]$. But $\mathrm{Stab}(x) = \{g \in G \mid gxg^{-1} = x\} = C_G(x)$, the centralizer of x in G. Thus, $|[x]| = [G : C_G(x)]$. The class equation follows by summing over all non-trivial conjugacy classes and adding the size of the centre. ∎

The above result seem very trivial and straightforward, but proves to be useful in various contexts.

Remark 3.16.
Let $H \leqslant G$; the normalizer is then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. If G acts on $\mathcal{P}(G)$ via

conjugation, then $N_G(H) = \text{Stab}(H)$ with respect to this action.

Recall that G acts on G trivially via $(g, x) \mapsto gx$. This is then a transitive action; moreover, it is also a faithful action. This leads to a very important theorem in group theory.

Theorem 3.17 (*Cayley's theorem*)**.** *Every finite group is isomorphic to a subgroup of S_n for some n.*

Proof. The above G-action on itself is faithful; hence, the group homomorphism $\psi : G \to \text{Bij}(G) \cong S_{|G|}$ is injective, and $G \cong \text{Im}\,\psi \cong H \leqslant S_{|G|}$. ■

Definition 3.18. Let p be a prime. A finite group G is called a *p-group* if $|G| = p^n$ for some $n \geq 0$.

Of course, for $n = 1$, G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. For $|G| = p^2$, G is also abelian.

Proposition 3.19. *If G is a p-group then $Z(G)$ is non-trivial.*

Proof. This follows immediately from the class-equation since if $Z(G)$ is trivial, then p divides $|G|$ and the summation, but $p \nmid |Z(G)| = 1$, contradicting the class-equation. ■

Thus, $Z(G)$ contains at least p elements for a p-group G. One can show that if $G/Z(G)$ is cyclic then G is abelian.

August 26th.

Proposition 3.20. *Let G be a group and $N \trianglelefteq G$. Then there is a natural bijection between subgroups of G/N and subgroups of G containing N.*

Proof. Define a map $q : G \to G/N$. Let $H \leqslant G$ such that $N \subseteq H$ and $q(H) \leqslant G/N$; subgroups of G containing N are mapped to subgroups of G/N. Let the image be $\bar{H} \leqslant G/N$. Then $q^{-1}(\bar{H}) = \{h \in G \mid q(h) \in \bar{H}\}$ is a subgroup of G containing $q^{-1}(e_{G/N}) = N$. Let $g, g' \in q^{-1}(\bar{H})$, that is, $q(g), q(g') \in \bar{H}$. Then $q(gg') = q(g)q(g') \in \bar{H}$, so $gg' \in q^{-1}(\bar{H})$. Also, if $g \in q^{-1}(\bar{H})$, then $q(g) \in \bar{H}$ implies $q(g^{-1}) = q(g)^{-1} \in \bar{H}$, so $g^{-1} \in q^{-1}(\bar{H})$. Thus, $q^{-1}(\bar{H})$ is a subgroup of G containing N. The maps $H \mapsto q(H)$ (denoted by ϕ) and $\bar{H} \mapsto q^{-1}(\bar{H})$ (denoted by ψ) are inverses of each other. To show this, let $N \subseteq H \leqslant G$. Then $\phi(H) = q(H)$, and $H \subseteq q^{-1}(q(H)) = \psi(q(H))$.

Conversely, let $\bar{H} \leqslant G/N$. Then $\psi(\bar{H}) = q^{-1}(\bar{H})$ is a subgroup of G containing N. Applying ϕ, we have $\phi(\psi(\bar{H})) = q(q^{-1}(\bar{H})) = \bar{H}$. Similarly, for $H \leqslant G$ containing N, $\psi(\phi(H)) = q^{-1}(q(H)) = H$. Thus, ϕ and ψ are inverses, establishing the bijection. ■

Theorem 3.21 (*Cauchy's theorem*)**.** *Let $p \mid |G|$ for a prime p. Then there exists $x \in G$ such that $|x| = p$.*

Proof. We perform induction on $|G|$. If G is abelian, pick a non-identity $x \in G$. If $|x|$ is mp for some m, then x^m has order p. If $|x|$ is not a multiple of p, then $H = \langle x \rangle \trianglelefteq G$ and $p \mid |G/H|$. By induction hypothesis, there exists $yH \in G/H$ such that $|yH| = p$. Thus, $(yH)^p = e_{G/H} = H$ or $y^pH = H$; y^p must belong in H. This tells us that $y^p = x^r$ for some r, and $m = |x^r|$ is coprime to p as $(|x|, p) = 1$. Thus, $(y^p)^m = e_G$. We claim that $p \mid |y|$. If not, then $y^r = e$ for some $p \nmid r$ and $(yH)^r = H$. But $|yH| = p$, a contradiction. Hence, $|y| = pn$ for some n, and $|y^n| = p$.

For the general case, let $Z(G) \trianglelefteq G$ be the centre of G. If $|(Z(G))| \neq 1$, then consider two cases; if $p \mid Z(G)$, then there exists $x \in Z(G) \subseteq G$ such that $|x| = p$. If $p \nmid |Z(G)|$, then $p \mid |G/Z(G)|$ and there exists $yZ(G) \in G/Z(G)$ such that $|yZ(G)| = p$ by induction hypothesis. The same argument as before works leading to the claim that $|y|$ is a multiple of p where y is such that $q(y) = yZ(G)$, and that $|y^n| = p$ for some n.

If $Z(G) = \{e\}$, the class equation gives $|G| = |Z(G)| + \sum_{[x]:[G:C_G(x)]\neq 1}[G : C_G(x)]$. SO there exists $x \in G$ such that $p \nmid [G : C_G(x)] > 1$ implying that $p \mid |C_G(x)| < |G|$ since $|G| = |C_G(x)|\,[G : C_G(x)]$. By induction hypothesis there exists $y \in C_G(x) \leqslant G$ such that $|y| = p$ ■

3.4 Sylow's Theorems

Definition 3.22. Let G be a finite group and p be a prime. Let $|G| = p^n m$ where $(m, p) = 1$ and $n \geq 0$. A subgroup $H \leqslant G$ is called a *p-Sylow subgroup* of G if $|H| = p^n$.

In fact, such a subgroup always exists.

Theorem 3.23 (*Sylow's first theorem*)**.** *Let G be a finite group and p be a prime. Then G has a p-Sylow subgroup.*

Proof. We work similar to the proof of Cauchy's theorem; perform induction on $|G|$. We may assume $n \geq 1$. If $p \nmid Z(G)$, the class equation tells us

$$|G| = |Z(G)| + \sum_{\substack{[x] \text{ non-trivial} \\ \text{conjugacy classes}}} [G : C_G(x)]. \tag{3.14}$$

So there must exists $x \in G$ such that $p \nmid [G : C_G(x)] > 1$ implying that $|C_G(x)| < |G|$. Also, $|C_G(x)| = p^n k$ for some k. By the induction hypothesis, there exists $P \leqslant C_G(x)$ such that $|P| = p^n$ and $P \leqslant G$.

If $P \mid |Z(G)|$, then there exists $H \leqslant Z(G)$ such that $|H| = p$. Then $H \trianglelefteq G$ since $H \subseteq Z(G)$, giving us $|G/H| = p^{n-1}m$. So by the induction hypothesis there exists subgroup $\overline{P} \leqslant G/H$ such that $\left|\overline{P}\right| = p^{n-1}$. Let $q : G \to G/H$ be the quotient map. Let $P = q^{-1}(\overline{P})$. then $|P| = |P/H|\,|H| = p^{n-1} \cdot p = p^n$. Thus, $P \leqslant G$ and $|P| = p^n$. ∎

Remark 3.24.

- Note that S_n acts on $\{1, 2, \ldots, n\}$ by permuting the elements. Any subgroup $H \leqslant S_n$ is termed a *transitive subgroup* if the action of H on $\{1, 2, \ldots, n\}$ is transitive. For example, $\langle (1\ 2\ 3) \rangle \leqslant S_3$ is transitive. H is termed a *2-transitive subgroup* if given any $1 \leq i, j \leq n$ with $i \neq j$, there exists a permutation $h \in H$ such that $h(1) = i$ and $h(2) = j$. Since there does not exists $\sigma \in \langle (1\ 2\ 3) \rangle$ such that $\sigma(1) = 1$ and $\sigma(2) = 3$, the subgroup is not 2-transitive.

  One can show that $H \leqslant S_n$ is 2-transitive if and only if $\mathrm{Stab}_H(i)$ acts transitively on $\{1, 2, \ldots, n\} \setminus \{i\}$ for all $i \in \{1, 2, \ldots, n\}$.

- Suppose H acts on $A := \{1, 2, \ldots, n\}$. A subset $B \subseteq A$ is called a *block* of for all $\sigma \in H$, we have either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Note that $\{i\}$ is a block for all $i \in A$. A is also a block. H is termed a *primitive subgroup* if $\{i\}$ and A are the only blocks. One can show that 2-transitive subgroups are primitive.

August 28th.

Theorem 3.25 (*Sylow's theorem*)**.** *Let G be a finite group and P be a p-Sylow subgroup of G for a prime p.*

- *Let H be a p-subgroup of G. Then there exists $g \in G$ such that $H \leqslant g^{-1}Pg$.*
- *All p-Sylow subgroups of G are conjugate to each other.*
- *Let n_p be the number of p-Sylow subgroups of G. Then $n_p \equiv 1 \mod p$ and $n_p \mid [G : P]$.*

Proof. Let $S = \{g^{-1}Pg \mid g \in G\}$. Then G acts on S via conjugation. H, being a subgroup of G, also acts on S. Let $Q \in S$. Then $\mathrm{Stab}_H(Q) \leqslant H$; if this stabilizer is equal to H, then $H \leqslant N_G(Q)$. Also $Q \leqslant N_G(Q)$. Noting $GQ = S$, the orbit stabilizer theorem gives us

$$|S|\,|\mathrm{Stab}_G(Q)| = |G| \implies |S| = [G : N_G(Q)] \implies |S| \mid [G : Q]\ ([G : Q] = [G : P] = m). \tag{3.15}$$

Suppose $\mathrm{Stab}_H(Q)$ were a proper subgroup of H for all $Q \in S$. Then p divides the order of $\{hQh^{-1} | h \in H\}$ since H is a p-subgroup. Since $|S|$ is co-prime to p, the above is not possible; there exists $P_0 \in S$ such that $\mathrm{Stab}_H(P_0) = H$. This shows $H \leqslant N_G(P_0)$ and $P_0 \leqslant N_G(P_0)$ (P_0 is a normal subgroup, in fact). Thus, $HP_0 \leqslant N_G(P_0) \leqslant G$. $[HP_0 : P_0]$ is co-prime to p, and $|H/(H \cap P_0)|$ is a power of p, and

$HP_0/P_0 \cong H/(H \cap P_0)$ leads us to conclude that $[HP_0 : P_0] = 1$. Thus, $H \subseteq P_0$, or $H \leqslant g^{-1}Pg$ for some $g \in G$. Second part follows from the first part by taking H to be a p-Sylow subgroup. In particular, S turns out to be the set of all p-Sylow subgroups.

$P \leqslant G$ acts on S via conjugation. $\{P\}$ is one of the orbits since $gPg^{-1} = P$ for all $g \in P$. Let $Q \in S$ and $Q \neq P$. If $gQg^{-1} = Q$ for all $g \in P$, then $P \leqslant N_G(Q)$ and $PQ \leqslant N_G(Q) \leqslant G$. $[PQ : Q]$ is co-prime to p and $PQ/Q \cong P/(P \cap Q)$. Since $P \neq Q$, $|P/P \cap Q| \neq 1$ which implies that $gQg^{-1} \neq Q$ for all $g \in P$ or $\mathrm{Stab}_P(Q)$ is a proper subgroup of P. Thus $|PQ| = \left|\{gQg^{-1} \mid q \in P\}\right|$ is a multiple of p. So 1 P-orbit is $\{P\}$ and P-orbits are of size multiple of p; thus the class equation gives us $n_p = \#S = \sum |\text{orbits}| \equiv 1 \mod p$. ■

3.4.1 Simple Groups

Definition 3.26. A group G is called a *simple group* if the only normal subgroups are G and $\{e_G\}$.

An example is $\mathbb{Z}/p\mathbb{Z}$ for a prime p. One can show that A_n is simple for $n \geq 5$.

Corollary 3.27. *Let G be a finite group and p a prime. If n_p, the number of p-Sylow subgroups of G, is unity, then $P \trianglelefteq G$ where P is a p-Sylow subgroup.*

p-groups different from $\mathbb{Z}/p\mathbb{Z}$ are not simple, since their center is non-trivial (and proper).

Example 3.28. Let G be a group of order 12. We show that G is not simple. For $p = 3$, the conditions of $n_p \equiv 1 \mod p$ and $n_p \mid [G : P]$ tell us that n_3 is 1 or 4. If $n_3 = 1$, then $P \trianglelefteq G$ where P is a 3-Sylow subgroup. If $n_3 = 4$, then P is a 3-group and the number of elements of order 3 in P is 2. So there are 8 elements of order 3. Then the 2-Sylow subgroup is of order 4 containing the remaining 4 elements. Calling this group Q, we have $Q \trianglelefteq G$.

Proposition 3.29. *Let G be a group of order pq or p^2q, where p and q are distinct primes. Then G is not simple.*

Proof. We may assume $p < q$. If $|G| = pq$, then $n_q \equiv 1 \mod q$ and $n_q \mid p$ implies $n_q = 1$. Thus, $Q \trianglelefteq G$ where Q is a q-Sylow subgroup. For $|G| = p^2q$, if $q < p$, the above can be used. If $p < q$, then n_q is one of $1, p, p^2$. If $n_q = 1$, we are done. n_q cannot be p since $n_q \equiv 1 \mod q$. The third case, where $n_q = p^2$, tells us that $q \mid (p^2 - 1)$ or $q \mid (p - 1)(p + 1)$. Since $q > p$, $q \mid (p + 1)$ or $q = p + 1$. The only such case is when $q = 3$ and $p = 2$. It follows from the previous example that a group G of order $p^2q = 12$ cannot be simple. ■

Proposition 3.30. *Let G be a group of order pqr, where p, q, and r are primes. Then G is not simple.*

Proof. We may assume they are distinct; if not, the above proposition works. So we may take $p < q < r$. For G to be simple, n_p, n_q, n_r must be different from 1. The possibilities, thus, for n_r are p, q, or pq. But $n_r \equiv 1 \mod r$ implies that $n_r = pq$. If R and R' are r-Sylow subgroups, then $R = R'$ or $R \cap R' = \{e\}$. Thus the number of elements of order r in G is at least $pq(r - 1)$. Also, n_q is either r or pr since $p < q$. By the same argument, the number of elements of order q in G is at least $(q - 1)r$. Similarly, the number of elements of order p in G is at least $(p - 1)q$. Summing up (and a 1 for the identity), we get

$$pqr - pq + qr - r + pq - q + 1 = pqr + qr - r - q + 1 > pqr \tag{3.16}$$

which is a contradiction to the fact that $|G| = pqr$. Hence, (at least) one of n_p,n_q, or n_r must be 1, showing G is not simple. ■

Example 3.31. For $|G| = 24$, G is not simple. Let P be a 2-Sylow subgroup of G. Then P has order 8 and n_2 is either 1 or 3. If $n_2 = 1$, we are done, so let us take $n_2 = 3$ and $n_3 = 4$. 8 elements have order 3. Let P_1, P_2, and P_3 be distinct. Then $|P_1 \cap P_2| \leq 4$ and $|P_1 \cup P_2| \geq 12$. G acts trasitively on

$A = \{P_1, P_2, P_3\}$ via conjugation. This gives a group homomorphism via $\phi : G \to S_3$ and $\operatorname{Im}\phi \neq \{e\}$. Thus $\ker\phi$ is not the entirety of G and it's non-trivial. So G is not simple.

September 2nd.

Recall that the alternating groups A_n are simple for $n \geq 5$; this is a group of order $n!/2$, or 60 and above. One can show that any group of order less than 60 is simple if and only if it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p. If the order of G is pqr, pq, or p^n, then G is not simple. We use this to show that the previous statement.

If $|G| = 2^3 \cdot 3 = 24$, then we have already shown G is not simple. If $|G| = 2^2 \cdot 3^2 = 36$, then n_3 is 1 or 4 and n_1 is 1, 3, or 9. For simplicity, assume both are non-unity. If $n_3 = 4$, then G acts on 3-Sylow subgroups transitively which produces a non-trivial group homomorphism $\phi : G \to S_4$, with $\ker\phi$ non-trivial and a proper subgroup of G, since $|S_4| = 24$ and $|G| = 36$. Thus, G cannot be simple.

If we then look at $|G| = 2^3 \cdot 5 = 40$, then $n_2 = 1, 5$ and $n_5 = 1$. Thus, G is not simple. For $|G| = 2^4 \cdot 3 = 48$, we have $n_2 = 1$ or 3. If $n_2 = 3$, we proceed as before showing G not simple. $|G| = 50, 51, 52, 54$ also involves casework. For $|G| = 2^3 \cdot 7 = 56$, $n_7 = 1$ or 8. If $n_7 = 8$, then the number of elements of order 7 in G is $8 \cdot 6 = 48$. This means that the 2-Sylow subgroup H is made of these remaining 8 elements, showing $n_2 = 1$.

Alternating Groups

Proposition 3.32. *Let $N \trianglelefteq G$. Then N is the union of conjugacy classes, that is, if C is a conjugacy class in G then $C \subseteq N$ or $C \cap N = \emptyset$.*

Proof. This is simple to see since $g^{-1}Ng = N$ for all $g \in G$. ∎

We show that A_n's are simple for $n \geq 5$ using the above proposition. For sake of completion, we note that A_n is defined to the subgroup of S_n containing all even permutations, where a permutation is deemed even if it can be written as the product of an even number of transpositions.

Proposition 3.33. *Let $\sigma \in S_n$ be a permutation. If $\sigma = \tau_1\tau_2\cdots\tau_r = \tau_1'\tau_2'\cdots\tau_s'$ are two different expressions of σ as a product of transpositions, then $r \equiv s$ modulo 2.*

By the above proposition, the sign of a permutation $\operatorname{sgn}(\sigma) = (-1)^r$ is well-defined.

Proof. Let $\Delta = \Delta(x_1, \ldots, x_n) = \prod_{1 \leq i < j \leq n}(x_i - x_j)$. For $\sigma \in S_n$, define

$$\sigma(\Delta) := \Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}). \tag{3.17}$$

Let $\tau = (1\ 2)$. Then $\tau(\Delta) = -\Delta$. Similarly, for any transposition τ, we have $\tau(\Delta) = -\Delta$. If $\sigma \in S_n$ with $\sigma = \tau_1\tau_2\cdots\tau_r = \tau_1'\tau_2'\cdots\tau_s'$, then we have

$$(-1)^r = \tau_1\cdots\tau_r(\Delta) = \sigma(\Delta) = \tau_1'\cdots\tau_s'(\Delta) = (-1)^s. \tag{3.18}$$

Thus, $r \equiv s$ modulo 2. ∎

Proposition 3.34. *A_n is generated by 3-cycles.*

Proof. If $\sigma \in A_n$, then $\sigma = \tau_1\tau_2\cdots\tau_{2r-1}\tau_{2r}$ for some r, where each τ_i is a transposition. If $\tau_1 = (1\ 2)$ and $\tau_2 = (1\ 3)$, then $\tau_1\tau_2 = (1\ 3\ 2)$. If $\tau_1 = (1\ 2)$ and $\tau_2 = (3\ 4)$, then $\tau_1\tau_2 = (1\ 2)(3\ 4) = ((1\ 2)(2\ 3))((2\ 3)(3\ 4))$, where each term is a 3-cycle. Thus, σ is a product of 3-cycles. ∎

Proposition 3.35. *For $n \geq 5$, 3-cycles in A_n form a conjugacy class in A_n.*

Proof. Let $\tau \in A_n$ be a 3-cycle. Then there exists a $\sigma \in S_n$ such that $\sigma^{-1}(1\ 2\ 3)\sigma = \tau$. If $\sigma \in A_n$, we are done. If not, let $\sigma' = (4\ 5)\sigma$. Then $\sigma' \in A_n$ and $\sigma'^{-1}(1\ 2\ 3)\sigma' = \tau$. ∎

Theorem 3.36. *A_5 is a simple group.*

Proof. Here, $|A_5| = 60$. If $N \trianglelefteq A_5$, then it is a union of conjugacy classes. The conjugacy classes in A_5 are $\{e\}$, the set of 3-cycles (of size 20), $[(1\ 2)(3\ 4)]$ (of size 15). Via the orbit-stabilizer theorem,

$$|\mathrm{Stab}_{S_5}((1\ 2)(3\ 4))| = \frac{5!}{15} = 8 \tag{3.19}$$

where S_n acts on itself via conjugation. A_n also acts on S_n via conjugation, and $\mathrm{Stab}_{A_5}((1\ 2)(3\ 4)) \leqslant \mathrm{Stab}_{S_5}((1\ 2)(3\ 4))$, A_5. Thus the stabilizer in A_5 can be of order 1 or 2 or 4 or 8. Since $|A_5(1\ 2)(3\ 4)| \leq 15$, the stabilizer cannot be 1 or 2, and since $|A_5| = 60$, the stabilizer cannot be 8. Thus the stabilizer in A_5 must be of order 4. Thus, $[(1\ 2)(3\ 4)]$ is a conjugacy class in A_5 of size 15.

The number of 5-cycles in A_5 is $4! = 24$. By a similar arguments, there are 2 conjugacy classes in A_n of size 12 each consisting of 5-cycles.

Now suppose $N \neq \{e\}$. If N contains the 3-cycles, then N must be A_5 (since 3-cycles generate A_5), so we let $N \cap$ 3-cycles $= \emptyset$. Let $(1\ 2)(3\ 4) \in N$. Then $(1\ 2)(3\ 5) \in N$ and $(1\ 2)(3\ 4)(1\ 2)(3\ 5) = (3\ 5\ 4) \in N$ implies N contains all 3-cycles and must be A_5. So we also let the intersection of N with this conjugacy class be empty. If N contains half of the 5-cycles, then $|N| = 13$ which is not possible since $|N| \mid 60$. If N contains all 5-cycles, then $|N| = 25$, which is again not possible. The only real possibility left is that A_5 must be simple. ∎

Theorem 3.37. *A_n is a simple group for $n \geq 5$.*

Proof. Let $n \geq 6$, and let $\{e\} \neq N \leqslant A_n$. It is enough to show that N must contain a 3-cycle. Let $\sigma \in N$ be a non-identity element. Suppose $\sigma = \tau_1 \cdots \tau_r$ where τ_i are disjoint cycles. We deal with cases.

Case I, where at least two disjoint cycles are transpositions. We can assume that $\tau_1 = (1\ 2)$ and $\tau_2 = (3\ 4)$, and $\sigma = (1\ 2)(3\ 4)\tau$ and τ does not contain any elment in $\{1, 2, 3, 4\}$. Then

$$N \ni (1\ 2\ 3)\sigma(3\ 2\ 1)\sigma^{-1} = (1\ 2\ 3)(1\ 2)(3\ 4)\tau(3\ 2\ 1)\tau^{-1}(1\ 2)(3\ 4) = (1\ 3)(2\ 4). \tag{3.20}$$

Conjugating by a 3-cycle, we get

$$N \ni (1\ 3\ 5)(1\ 3)(2\ 4)(5\ 3\ 1)(1\ 3)(2\ 4) = (2\ 4)(3\ 5)(1\ 3)(2\ 4) = (1\ 3\ 5). \tag{3.21}$$

Thus, N contains a 3-cycle, and it must be equal to A_n. Case II, where exactly one of the cycles is a transposition, say, τ_1. This implies that one of $\tau_1, \ldots, \tau_r$ has length at least 4. Thus, $\sigma = (1\ 2\ 3\ 4\ \cdots)\tau = \tau'\tau$ where τ does not contain any element from τ'. Thus,

$$N \ni (1\ 2\ 3)(1\ 2\ 3\ 4\ \cdots)\tau(3\ 2\ 1)\tau^{-1}(1\ 2\ 3\ 4\ \cdots)^{-1} = (1\ 2\ 3)(2\ 4\ 3) = (1\ 2\ 4). \tag{3.22}$$

N, again, contains a 3-cycle implying it must be A_n. Case III, where none of the τ_i's are transpositions. If one of the τ_i's has length at least 4, then the same argument in Case II works. So we may assume σ is a product of disjoint 3-cycles. If σ is a 3-cycle, we are done. Otherwise, let $\sigma = (1\ 2\ 3)(4\ 5\ 6)\tau$ where τ is disjoint from the previous cycles. Then

$$N \ni (1\ 4\ 5)(1\ 2\ 3)(4\ 5\ 6)\tau(5\ 4\ 1)\tau^{-1}(6\ 5\ 4)(3\ 2\ 1) = (1\ 4\ 5)(6\ 5\ 2) = (1\ 4\ 5\ 2\ 6). \tag{3.23}$$

The argument for Case II can now be applied, since we have a cycle of length more than 4 in N. ∎

Chapter 4

PRESENTATION OF GROUPS

4.1 Free Groups

September 16th.

Let $S = \{a_1, a_2, \ldots\}$ be a non-empty set of letters. Our objective is to define a (free) group on S. Note that S need not be finite or countable. Let $\bar{S} = \{a_1, a_2, \ldots\} \sqcup \{a_1^{-1}, a_2^{-1}, \ldots\} \sqcup \{\square\}$ be the set of letters and their formal inverses, and another 'null' element $\square$. An element of $\bar{S}$ is called a *letter*. A *word* on S is a finite sequence of letters from $\bar{S}$, i.e., an element of the set $\bigcup_{n=0}^{\infty} \bar{S}^n$, where $\bar{S}^0 = \{\square\}$. If Ω denotes the set of all words, then clearly

$$\Omega = \{\square\} \sqcup \bar{S} \sqcup \bar{S}^2 \sqcup \bar{S}^3 \sqcup \cdots = \bigcup_{n=0}^{\infty} \bar{S}^n = \{f : \mathbb{N} \to \bar{S} \mid f(i) = \square \text{ for all but finitely many } i\}. \tag{4.1}$$

A word $w \in \Omega$ is said to be a *reduced word* if the associated function $f : \mathbb{N} \to \bar{S}$ satisfies the following:

- if there exists k such that $f(k) = \square$, then $f(i) = \square$ for all $i > k$;
- for all i, if $f(i) = a_j$ for some j, then $f(i+1) \neq a_j^{-1}$, and vice versa.

Essentially, null characters do not appear in the middle of a reduced word, and no letter is immediately followed by its formal inverse. The set of all reduced words is denoted by $\bar{\Omega}$. For example, if $S = \{a, b\}$, then $ab^{-1}a^{-1}b$ is a reduced word, but $ab^{-1}\square a^{-1}b$ and $abb^{-1}a^{-1}$ are not. Note that $\square$ is a reduced word.

Now define a binary operation $* : \bar{\Omega} \times \bar{\Omega} \to \bar{\Omega}$, termed *concatenation*, as follows: for $u, v \in \bar{\Omega}$, let u and v have the associated functions $f, g : \mathbb{N} \to \bar{S}$ respectively. Let $k \in \mathbb{N}$ be the least integer such that $f(k+1) = \square$. Then define $u * v$ to be the reduced word whose associated function $h : \mathbb{N} \to \bar{S}$ is given by

$$h(i) = \begin{cases} f(i) & \text{if } 1 \leq i \leq k, \\ g(i-k) & \text{if } k < i \end{cases} \tag{4.2}$$

where h is reduced to ensure that $u * v \in \bar{\Omega}$; this reduction is ensured by the following lemma.

Lemma 4.1. *Given $w \in \Omega$, there exists a unique $w_{\text{red}} \in \bar{\Omega}$ such that w_{red} is obtained from w by repeatedly deleting adjacent pairs of the form $a_j a_j^{-1}$ or $a_j^{-1} a_j$, for some j, until no such pair exists, and deleting all occurrences of $\square$ if a non-$\square$ letter appears anywhere after it.*

Proof. Define a function $\text{red} : \Omega \to \Omega$ as follows: if $w \in \bar{\Omega}$ then $\text{red}(w) = w$. Otherwise let i_0 be the least integer such that $w(i) = \square$ or $(w(i_0), w(i_0+1)) \in \{(a, a^{-1}), (a^{-1}, a)\}$ for some $a \in S$. Then define

$$\text{red}(w)(j) = \begin{cases} w(j) & \text{if } 1 \leq j < i_0, \\ w(j+1) & \text{if } w(i_0) = \square,\ j \geq i_0, \\ w(j+2) & \text{if } (w(i_0), w(i_0+1)) \in \{(a, a^{-1}), (a^{-1}, a)\},\ j \geq i_0. \end{cases} \tag{4.3}$$

Given $w \in \Omega$, one can show that there exists $k \in N$ less than the length of w such that $\text{red}^k(w) \in \bar{\Omega}$. ∎

September 18th.

From the above, we can define a function $r : \Omega \to \bar{\Omega}$ by $r(w) = \text{red}^k(w)$, where k is the least integer such that $\text{red}^k(w) \in \bar{\Omega}$. Note that if $w \in \bar{\Omega}$, then $r(w) = w$. The uniqueness of w_{red} follows from the fact that any two sequences of deletions must lead to the same reduced word. This can be proved by induction on the length of w.

Proposition 4.2. *Let $w, w' \in \Omega$. Then $r(w * w') = r(r(w) * r(w'))$.*

Proof. The proof is left as an exercise to the reader. ■

We can now 'fix' our binary operator by defining $\bar{*} : \bar{\Omega} \times \bar{\Omega} \to \bar{\Omega}$ by $u \bar{*} v = r(u * v)$ for $u, v \in \bar{\Omega}$.

Theorem 4.3. *$(\bar{\Omega}, \bar{*}, e)$, where $e(i) = \square$ for all i, is a group.*

The above is termed a *free group* on the set S, and is denoted by F_S.

Proof. 1. Associativity: Let $u, v, w \in \bar{\Omega}$. Then

$$(u \bar{*} v) \bar{*} w = r(r(u * v) * w) = r(u * v * w) = r(u * r(v * w)) = u \bar{*} (v \bar{*} w). \tag{4.4}$$

2. Identity: Let $u \in \bar{\Omega}$. Then $e \bar{*} u = r(e * u) = r(u) = u = r(u * e) = u \bar{*} e$.

3. Inverses: Let $u \in \bar{\Omega}$, and let u have the associated function $f : \mathbb{N} \to \bar{S}$. Define $u^{-1} \in \bar{\Omega}$ to be the reduced word whose associated function $g : \mathbb{N} \to \bar{S}$ is given by $g(i) = f(k - i + 1)^{-1}$ if $f(k) \neq \square$ and $g(i) = \square$ if $f(k) = \square$, where k is the least integer such that $f(k + 1) = \square$. Then $u \bar{*} u^{-1} = r(u * u^{-1}) = e = r(u^{-1} * u) = u^{-1} \bar{*} u$.

■

Note that there is a natural mapping $i : S \to F_S$ given by $a \mapsto \bar{a}$ where $\bar{a}(1) = a$ and $\bar{a}(k) = \square$ for all $k > 1$.

Theorem 4.4. *Let G be a group, and $S = \{a_1, a_2, \ldots, a_n\}$ be a set. Let $g_1, g_2, \ldots, g_n \in G$. Then there exists a unique group homomorphism $\phi : F_S \to G$ such that $\phi(\bar{a}_i) = g_i$ for all i. Moreover, if S is arbitrary and $\theta : S \to G$ is a function, then there exists a unique mapping $\phi : F_S \to G$ such that $\theta = \phi \circ i$, or $\theta(a) = \phi(i(a))$ for all $a \in S$.*

Proof. We show the existence via a constructive proof. Let $w \in F_S$. Then $w = a_1^{i_1} \cdots a_n^{i_n}$ where $i_1, \ldots, i_n \in \{\pm 1\}$. Then $\phi(w) := g_1^{i_1} g_2^{i_2} \cdots g_n^{i_n}$. Note that $\phi(\text{red}(w)) = \phi(w)$ and $\phi(r(w)) = \phi(w)$, so ϕ is well-defined. This tells us, for $w, w' \in \bar{\Omega}$,

$$\phi(w \bar{*} w') = \phi(r(w * w')) = \phi(w * w') = \phi(w)\phi(w') \tag{4.5}$$

showing that ϕ is a group homomorphism. If we have another homomorphism $\psi : F_S \to G$ such that $\psi(i(a)) = \psi(i(a))$ for all $a \in S$, then ϕ and ψ agree on the generators of F_S since $i(S)$ generates F_S, and both are group homomorphisms showing that $\phi = \psi$. The second part of the theorem follows from the first part by taking $g_i = \theta(a_i)$ for all i. ■

Proposition 4.5. *Let S and T be sets of the same cardinality. Then $F_S \cong F_T$.*

Proof. Let $\tilde{\theta} : S \to T$ be a bijection, and $i_T : T \to F_T$ $i_S : S \to F_S$ be the natural mappings. Define $\theta : i \circ \tilde{\theta}$. Then by the above theorem, there exists a unique group homomorphism $\phi : F_S \to F_T$ such that $\theta = \phi \circ i_S$. Similarly, since $\tilde{\theta}^{-1} : T \to S$ is also a bijection, there exists a unique group homomorphism $\psi : F_T \to F_S$ such that $i_S \circ \tilde{\theta}^{-1} = \psi \circ i_T$. We claim that $\psi = \phi^{-1}$. We have

$$\psi \circ \phi(i_S(a)) = \psi \circ \theta(a) = \psi \circ i_T \circ \tilde{\theta}(a) = \theta^{-1} \circ \tilde{\theta}(a) = i_S \circ \tilde{\theta}^{-1} \circ \tilde{\theta}(a) = i_S(a) \tag{4.6}$$

showing $\psi \circ \phi|_{i(S)} = \text{id}_{i(S)}$ or $\psi \circ \phi = \text{id}_{F_S}$. Similarly, $\phi \circ \psi = \text{id}_{F_T}$. ■

4.2 Automorphisms

Recall that an automorphism of a group G is simply an isomorphism from G to itself. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$, which also forms a group under composition. Moreover, $\emptyset \neq \mathrm{Aut}(G) \leq \mathrm{Bij}(G)$, where $\mathrm{Bij}(G)$ is the group of all bijections from G to itself.

Example 4.6.
1. One may show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, the group of units in $\mathbb{Z}/n\mathbb{Z}$, by sending an automorphism ϕ to $\phi(\bar{1})$.
2. Let $G = (\mathbb{Z}/p\mathbb{Z})^n$, for a prime p. Then $\mathrm{Aut}(G) \cong GL_n(\mathbb{Z}/p\mathbb{Z})$, the group of invertible $n \times n$ matrices over $\mathbb{Z}/p\mathbb{Z}$ since G can be viewed as an n-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$, and any automorphism of G is a linear transformation.

Proposition 4.7. *Let G be a group and $H \trianglelefteq G$ a normal subgroup. Given $g \in G$, the map $\varphi_g : H \to H$ given by $\varphi_g(h) = ghg^{-1}$ is an automorphism of H. Moreover, the map $X : G \to \mathrm{Aut}(G)$ given by $g \mapsto \varphi_g$ is a group homomorphism. The kernel of X is $\ker X = C_G(H)$, the centraliser of H in G.*

Proof. The proof is left as an exercise to the reader. ■

Corollary 4.8. *Let $H \trianglelefteq G$. Then the map $G/C_G(H) \to \mathrm{Aut}(H)$ given by $gC_G(H) \mapsto \varphi_g$ is an injective group homomorphism.*

Proof. This is easy to see by the first isomorphism theorem applied on the previous proposition. Hence, the map $gC_G(H) \mapsto \varphi_g$ is an injective group homomorphism from $G/C_G(H)$ to $\mathrm{Aut}(H)$. ■

In particular, taking $H = G$, we obtain $G/Z(G) \to \mathrm{Aut}(G)$, an injective homomorphism, where $Z(G)$ is the centre of G.

Definition 4.9. Let G be a group. An automorphism of G given by φ_g for some $g \in G$ is called an *inner automorphism* of G. The set of all inner automorphisms of G is denoted by $\mathrm{Inn}(G)$.

This set is precisely the image of the map $X : G \to \mathrm{Aut}(G)$ defined in the previous proposition. Note that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Moreover, it is normal in $\mathrm{Aut}(G)$. An automorphism $\psi \in \mathrm{Aut}(G) \setminus \mathrm{Inn}(G)$ is called an *outer automorphism*. We define $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ to be the group of outer automorphisms of G. Note that if G is abelian, then $\mathrm{Inn}(G)$ is trivial, and $\mathrm{Out}(G) = \mathrm{Aut}(G)$.

Example 4.10.
1. For $n \geq 3$, $\mathrm{Inn}(S_n) \cong S_n$.
2. For the quaternions, $\mathrm{Inn}(Q_8) \cong (Z/2Z)^2$.
3. The dihedral group also gives $\mathrm{Inn}(D_8) \cong (Z/2Z)^2$.

Index

p-Sylow subgroup, 24
p-group, 23
(left) group action, 19
2-transitive subgroup, 24

abelian group, 4
alternating group, 8
antisymmetric, 2
associativity, 4
automorphism, 13
axiom of choice, 2

block, 24

Cauchy's theorem, 23
Cayley's theorem, 23
centralizer, 14
centre of a group, 14
centre of a subset, 14
chain, 2
class-equation, 22
commutator subgroup, 16
concatenation, 29
conforming subset, 3
conjugacy classes, 22
conjugation action, 22
cycle, 5
cyclic group, 7

dihedral group, 8
disjoint cycles, 5

empty set, 1
epimorphism, 10
equivalence class, 3
equivalence relation, 3

faithful action, 21
finite group, 4
first isomorphism theorem, 15
free group, 30

group, 4

Heisenberg group, 16
homomorphism, 10

identity element, 4
image, 12
inclusion map, 10
index, 17
infinite axiom, 1
inner automorphism, 31
inverse element, 4
isomorphism, 10

kernel, 12
kernel of an action, 21

Lagrange's theorem, 9
left coset, 9
letter, 29

maximal element, 2
monomorphism, 10

normal subgroup, 12
normalizer, 15

orbit, 20
orbit-stabilizer theorem, 21
order of a group, 4
order of an element, 5
outer automorphism, 31

partial order, 2
power set, 1
primitive subgroup, 24
principle of induction, 3
principle of transfinite induction, 3
product of groups, 13

quaternions, 12
quotient group, 14

reduced word, 29
reflexive, 2
relation, 1
right coset, 9

second ismorphism theorem, 17

simple group, 25
stabilizer, 20
subgroup, 6
subset, 1
support, 6
Sylow's first theorem, 24
Sylow's theorem, 24
symmetric, 2

third isomorphism theorem, 17
total order, 2
transitive, 2
transitive action, 20
transitive subgroup, 24
transposition, 5
trivial group, 4, 7

upper bound, 2

well-order, 2
well-ordering principle, 2
word, 29

Zorn's lemma, 2