Groups Introduction

Gudfit

Contents

0
Sets and Fundamentals

We begin by formalising the definitions and operations of set theory that serve as the foundation for group theory.

0.1 *Sets and Subsets*

Definition 0.1. ***Set.***
A **set** is a collection of distinct objects, referred to as **elements**. We denote sets by uppercase letters ($A, B, \dots$) and elements by lowercase letters ($a, b, \dots$).
· If an element a belongs to a set A, we write $a \in A$.
· If a does not belong to A, we write $a \notin A$.
A set may be defined by listing its elements or by specifying a property $P(x)$ satisfied by all members: $A = \{x \mid P(x)\}$. For example, the set of even integers is written as $\{a \in \mathbb{Z} \mid a \equiv 0 \pmod 2\}$.

定義

Definition 0.2. ***Subsets and Equality.***
Let A and B be sets.
1. A is a **subset** of B, denoted $A \subseteq B$ or $B \supseteq A$, if every element of A is also an element of B.
2. A and B are **equal**, denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$.
3. If $A \subseteq B$ but $A \neq B$, then A is a **proper subset** of B, denoted $A \subset B$ or $A \subsetneq B$.

定義

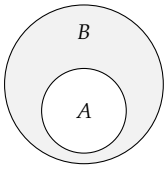


Figure 1: Visualisation of inclusion: $A \subseteq B$.

Two specific concepts regarding the size and emptiness of sets are essential.

Definition 0.3. ***Empty and Finite Sets.***
· The **empty set**, denoted $\varnothing$, is the set containing no elements. It is a subset of every set and a proper subset of every non-empty set.
· A set A is **finite** if it contains a finite number of elements. This number is called the **cardinality** or order of A, denoted $|A|$.
· If A is not finite, we define its order as $|A| = \infty$.

定義

Remark.

One may conceptualise these definitions through an analogy: a *Class* corresponds to a Set, the *Students* are the Elements, and a *Study Group* forms a Subset. The set of all classes constitutes a family of sets.

Definition 0.4. ***Power Set.***
The **power set** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

定義

Operations on Sets

We define the standard algebraic operations on sets. Let A and B be sets, and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I.

Definition 0.5. ***Intersection.***
The **intersection** of A and B is the set of elements common to both:

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}.$$

For an indexed family, the intersection is defined as:

$$\bigcap_{i\in I} A_i := \{x \mid x \in A_i \text{ for all } i \in I\}.$$

定義

Definition 0.6. ***Union.***
The **union** of A and B is the set of elements belonging to at least one of them:

$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}.$$

For an indexed family:

$$\bigcup_{i\in I} A_i := \{x \mid x \in A_i \text{ for some } i \in I\}.$$

If the sets A_i are pairwise disjoint (i.e., $A_i \cap A_j = \varnothing$ for $i \neq j$), their union is called a **disjoint union**, denoted $\bigsqcup_{i\in I} A_i$.

定義

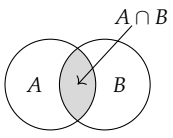


Figure 2: The intersection $A \cap B$.

Definition 0.7. ***Difference.***
Let U be a **universal set** (a fixed set containing all objects under discussion), and let A and B be subsets of U. The **difference** (or relative

complement) of B in A is:

$$A - B := \{x \mid x \in A \text{ and } x \notin B\}.$$

The **complement** of A in U is:

$$A^c := \{x \in U \mid x \notin A\}.$$

定義

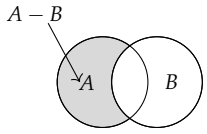


Figure 3: The set difference $A - B$.

It follows directly from the definitions that a set can be partitioned by any subset:

$$A = (A \cap B) \sqcup (A - B).$$

For finite sets, the sizes of unions and intersections are related by the Inclusion-Exclusion Principle. The base case for two sets is given by:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This generalises to arbitrary finite collections.

Proposition 0.1. ***Inclusion-Exclusion Principle.***
Let $A_1, \ldots, A_n$ be finite subsets of a set U. Then:

$$|A_1 \cup \cdots \cup A_n| = \sum_{j=1}^{n} (-1)^{j-1} \sum_{\{i_1,\ldots,i_j\} \subseteq \{1,\ldots,n\}} |A_{i_1} \cap \cdots \cap A_{i_j}|.$$

命題

Proof

We proceed by induction on n, the number of sets. The base case $n = 2$ is stated above. The inductive step involves applying the base case to the union of A_{n+1} and the set $S = \bigcup_{k=1}^{n} A_k$, then expanding using the inductive hypothesis.

■

The interaction between union, intersection, and complements is governed by De Morgan's laws.

Proposition 0.2. ***De Morgan's Laws.***
Let $\{A_i\}_{i \in I}$ be a family of subsets of U. Then:

$$\bigcap_{i \in I} A_i^c = \left(\bigcup_{i \in I} A_i \right)^c \quad \text{and} \quad \bigcup_{i \in I} A_i^c = \left(\bigcap_{i \in I} A_i \right)^c.$$

命題

Proof

We track the logical equivalence of element membership:

$$x \in \bigcap_{i\in I} A_i^c \iff \forall i \in I,\ x \in A_i^c \iff \forall i \in I,\ x \notin A_i \iff \neg(\exists i \in I,\ x \in A_i)$$

$$\iff x \notin \bigcup_{i\in I} A_i \iff x \in \left(\bigcup_{i\in I} A_i\right)^c.$$

■

Algebraic structures often involve pairs or tuples of elements.

Definition 0.8. ***Cartesian Product.***
The **Cartesian product** of two sets A and B is the set of all ordered pairs:

$$A \times B := \{(a,b) \mid a \in A, b \in B\}.$$

More generally, for a family $\{A_i\}_{i\in I}$, the product is the set of sequences (or functions $I \to \cup A_i$):

$$\prod_{i\in I} A_i := \{(a_i)_{i\in I} \mid a_i \in A_i\}.$$

定義

Throughout these notes, we adhere to the following standard notation for numerical sets:

- $\mathbb{Z}_+$: The set of positive integers.
- $\mathbb{N} = \mathbb{Z} \cup \{0\}$: The set of natural numbers.
- $\mathbb{Z}$: The set of integers.
- $\mathbb{Q}$: The set of rational numbers.
- $\mathbb{R}$: The set of real numbers.
- $F[X]$: The set of polynomials in variable X with coefficients in a field F.

0.2 *Mappings and Binary Operations*

The concept of a function, central to analysis, is generalised in algebra to the notion of a mapping between arbitrary sets.

Definition 0.9. ***Mapping.***
Let A and B be sets. A **mapping** (or map) $f : A \to B$ is a rule that assigns to every element $a \in A$ a unique element $b \in B$, denoted by $f(a) = b$.

- A is the **domain** of f.
- The set $f(A) = \{f(a) \mid a \in A\} \subseteq B$ is the **image** (or range) of f.
- If $f(a) = b$, then b is the image of a, and a is a **preimage** of b.

定義

Two mappings $f, g : A \to B$ are **equal**, denoted $f = g$, if $f(a) = g(a)$

for all $a \in A$.

Definition 0.10. ***Properties of Mappings.***
A mapping $f : A \to B$ is:
Injective (or one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$ for all $a_1, a_2 \in A$.
Surjective (or onto) if for every $b \in B$, there exists at least one $a \in A$ such that $f(a) = b$. Equivalently, $f(A) = B$.
Bijective (or a one-to-one correspondence) if it is both injective and surjective.

定義

Mappings can be combined sequentially.

Definition 0.11. ***Composition.***
Let $f : A \to B$ and $g : B \to C$ be mappings. The **composite mapping** $g \circ f : A \to C$ is defined by:

$$(g \circ f)(a) = g(f(a)) \quad \text{for all } a \in A.$$

定義

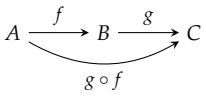


Figure 4: Composition of mappings.

While composition is not commutative in general (i.e., $g \circ f \neq f \circ g$), it satisfies a fundamental stability property known as associativity.

Proposition 0.3. ***Associativity of Composition.***
Let $f : A \to B$, $g : B \to C$, and $h : C \to D$ be mappings. Then:

$$(h \circ g) \circ f = h \circ (g \circ f).$$

命題

Proof

For any $a \in A$, we evaluate both sides:

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))).$$

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a))).$$

Since the mappings agree on every element of the domain, they are equal.

■

Algebraic structures are essentially sets equipped with operations that combine elements.

Definition 0.12. ***Binary Operation.***
Let X be a set. An **algebraic binary operation** (or composition law) on X is a function $T : X \times X \to X$. For every ordered pair $(a, b) \in X \times$

X, this map assigns a unique element $T(a, b) \in X$.

定義

Rather than writing $T(a, b)$, we typically use infix notation such as $a * b$, $a \circ b$, $a + b$, or simply ab. In group theory, we most frequently use multiplicative notation (ab) or additive notation ($a + b$).
A set X equipped with a specific binary operation $*$ is called an **algebraic structure** or algebraic system, denoted $(X, *)$. It is important to note that a single set can support multiple distinct operations. For instance, the integers $\mathbb{Z}$ form different structures under addition $(\mathbb{Z}, +)$ and multiplication $(\mathbb{Z}, \cdot)$. One could even define exotic operations like $n * m = n + m - nm$, creating yet another structure.
While one can define endless arbitrary operations, algebra focuses on those satisfying specific, powerful axioms. One such fundamental property is the existence of a neutral element.

Definition 0.13. ***Unit Element.***
An element $e \in X$ is called a **unit element** (or neutral element) relative to the operation $*$ if $e * x = x * e = x$ for all $x \in X$.

定義

It follows immediately that such an element, if it exists, is unique.

Proposition 0.4. ***Uniqueness of Unit Element.***
An algebraic structure $(X, *)$ possesses at most one unit element.

命題

Proof

Suppose e and e' are unit elements. By the defining property of e, we have $e * e' = e'$. By the defining property of e', we have $e * e' = e$. Thus $e = e'$.

■

Example 0.1. Arithmetic Operations. The standard operations of addition ($+$), subtraction ($-$), and multiplication ($\times$) are binary operations on $\mathbb{R}$. Division is not a binary operation on $\mathbb{R}$ because division by zero is undefined; however, it is a binary operation on the set of non-zero real numbers $\mathbb{R} \setminus \{0\}$.

範例

Example 0.2. Function Spaces. Let Σ_A be the set of all mappings from a set A to itself. The composition of mappings $\circ$ is a binary operation on Σ_A. Similarly, let S_A be the set of all bijections from A to itself. Since the composition of bijections is a bijection, $\circ$ is also a binary operation on S_A.

範例

Definition 0.14. ***Associativity and Commutativity.***
Let $*$ be a binary operation on S.
1. The operation is **associative** if for all $a, b, c \in S$:

$$(a * b) * c = a * (b * c).$$

2. The operation is **commutative** if for all $a, b \in S$:

$$a * b = b * a.$$

定義

0.3 *Equivalence Relations and Partitions*

In many contexts, we wish to treat distinct elements as "effectively equal" if they share a specific property (e.g., integers with the same parity). This leads to the concept of equivalence relations.

Definition 0.15. ***Relation.***
Let A and B be sets. A **relation** R from A to B is a subset of $A \times B$. If $A = B$, we say R is a relation on A. We write $a \, R \, b$ to mean $(a, b) \in R$.

定義

Definition 0.16. ***Equivalence Relation.***
A relation $\sim$ on a set A is an **equivalence relation** if it satisfies three axioms for all $a, b, c \in A$:
Reflexivity: $a \sim a$.
Symmetry: If $a \sim b$, then $b \sim a$.
Transitivity: If $a \sim b$ and $b \sim c$, then $a \sim c$.

定義

An equivalence relation allows us to group elements together.

Definition 0.17. ***Partition.***
A **partition** of a set A is a decomposition of A into a disjoint union of non-empty subsets. That is, $A = \bigsqcup_{i \in I} A_i$.

定義

These two concepts are mathematically dual. Given an equivalence relation $\sim$, we define the **equivalence class** of a as:

$$[a] = \{x \in A \mid x \sim a\}.$$

Lemma 0.1. ***Properties of Classes.***
For any $a, b \in A$, either $[a] = [b]$ (if $a \sim b$) or $[a] \cap [b] = \varnothing$ (if $a \nsim b$).

引理

Proof

If $x \in [a] \cap [b]$, then $x \sim a$ and $x \sim b$. By symmetry $a \sim x$, and by transitivity $a \sim b$. If $a \sim b$, let $y \in [a]$. Then $y \sim a$ and $a \sim b \implies y \sim b \implies y \in [b]$. Thus $[a] \subseteq [b]$. By symmetry, $[b] \subseteq [a]$, so $[a] = [b]$.

■

Consequently, the distinct equivalence classes form a partition of A:

$$A = \bigsqcup_{[a] \in A/\sim} [a].$$

Theorem 0.1. ***Equivalence and Partitions.***
There is a one-to-one correspondence between equivalence relations on a set A and partitions of A.
- Every equivalence relation induces a partition into equivalence classes.
- Conversely, given a partition $A = \bigsqcup_{i \in I} A_i$, the relation defined by "$a \sim b$ if a and b belong to the same subset A_i" is an equivalence relation.

定理

Example 0.3. Parity. Let $A = \mathbb{Z}$. We write $a \equiv b \pmod 2$ to mean $a - b = 2k$ for some $k \in \mathbb{Z}$. This relation is an equivalence relation. It partitions $\mathbb{Z}$ into two classes:
- $[0] = \{\dots, -2, 0, 2, \dots\}$ (the even integers).
- $[1] = \{\dots, -1, 1, 3, \dots\}$ (the odd integers).

範例

Partitions Induced by Mappings

A natural source of equivalence relations is the "fiber" structure of a mapping. Let $f : A \to B$ be a mapping. For any $b \in f(A)$, the **preimage** or fiber of b is:

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}.$$

Since every element $a \in A$ maps to exactly one image, the fibers are pairwise disjoint and cover A. Thus, we have the partition:

$$A = \bigsqcup_{b \in f(A)} f^{-1}(b).$$

The corresponding equivalence relation is defined by $a \sim a' \iff f(a) = f(a')$.

Example 0.4. Geometric Partition. Let $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = x - y$. For any real number $c \in \mathbb{R}$, the fiber $f^{-1}(c)$ is the set of points satisfying $x - y = c$, or $y = x - c$. Geometrically, this partitions the plane $\mathbb{R}^2$ into a family of parallel lines with slope 1 (see *figure 5*). Points are equivalent if they lie on the same line.

範例

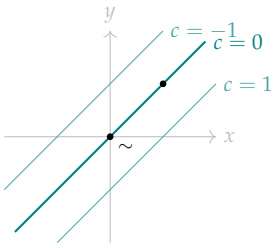


Figure 5: The equivalence classes of $f(x, y) = x - y$ form parallel lines.

0.4 *Exercises*

1. **Distributive Laws.** Let B and $\{A_i\}_{i \in I}$ be subsets of a universal set Ω. Prove:
   (a) $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.
   (b) $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$.

2. **Power Set Cardinality.** Let A be a finite set with n elements. Let $\mathcal{P}(A)$ be the set of all subsets of A. Prove that $|\mathcal{P}(A)| = 2^n$.

   Consider the correspondence between subsets and binary strings of length n.

3. **One-Sided Inverses.** Let $f : A \to B$ be a map with $A \neq \varnothing$. For any set X, we define the **identity map** $\mathrm{id}_X : X \to X$ by $\mathrm{id}_X(x) = x$.
   (a) Prove that f is injective if and only if there exists a left inverse $g : B \to A$ such that $g \circ f = \mathrm{id}_A$.
   (b) Prove that f is surjective if and only if there exists a right inverse $h : B \to A$ such that $f \circ h = \mathrm{id}_B$. For the direction $\Rightarrow$, you may assume the existence of a choice function that selects one preimage for each $b \in B$.

4. **Inverse of Composition.** Let $f : A \to B$ and $g : B \to C$ be bijections. If $h : X \to Y$ is a bijection, we define its **inverse** $h^{-1} : Y \to X$ as the unique map such that $h^{-1}(y) = x \iff h(x) = y$. Prove that $g \circ f$ is a bijection and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

5. **Counting Functions.** Let A and B be finite sets with $|A| = m$ and $|B| = n$.
   (a) How many distinct maps $f : A \to B$ exist?
   (b) How many distinct binary operations can be defined on A?

6. **Kernel Equivalence.** Let $f : A \to B$ be a map. Define a relation $\sim$ on A by $a \sim a'$ if and only if $f(a) = f(a')$. Prove that this is an equivalence relation. What are the equivalence classes?

7. **Independence of Axioms.** Prove that the three axioms of an equivalence relation (reflexivity, symmetry, transitivity) are independent. Specifically, for each axiom, construct a relation (i.e., a subset of $A \times A$) that fails that axiom but satisfies the other two.

   For example, find a relation that is symmetric and transitive but not reflexive.

1
Permutations

The study of permutations provides the necessary algebraic foundation for abstract algebra.

1.1 *The Symmetric Group*

We begin by formalising the concept of rearrangement as a function.

> **Definition 1.1.** ***Permutation.***
> Let X be a set. A **permutation** of X is a bijection $\alpha : X \to X$.
>
> 定義

When $X = \{1, 2, \ldots, n\}$, the set of all permutations of X is denoted by S_n. This set, equipped with function composition, forms a group. We will formalize the group axioms in *chapter 2*.

> *Remark.*
>
> At this stage, treat this as a preview: permutations are one of the first places where a single operation (composition) produces a rich algebraic structure. We will define the abstract notion of a *group* and its axioms later (in *chapter 2*); for now, we focus on concrete computations and structure in S_n.

> **Notation 1.1.** Symmetric Group The family of all permutations of X is called the **symmetric group** on X, denoted S_X. For the specific case where $X = \{1, \ldots, n\}$, we write S_n. The cardinality of S_n is $|S_n| = n!$.
>
> 記法

We initially represent elements of S_n using two-line notation. If $\alpha \in S_n$, we list the elements of the domain in the top row and their corresponding images in the bottom row:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}.$$

Since α is a bijection, the bottom row is a rearrangement of $\{1, \ldots, n\}$ with no repetitions.

1.2 *Cycle Notation*

The two-line notation, while explicit, obscures the structural properties of the permutation, such as its order or commutativity with other permutations. We introduce a more compact notation by tracking what happens to an element under repeated application of the permutation.

Definition 1.2. ***Cycle.***
Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, \ldots, n\}$. If $\alpha \in S_n$ satisfies:

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \ldots, \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1,$$

and $\alpha(x) = x$ for all $x \notin \{i_1, \ldots, i_r\}$, then α is called an ***r*-cycle** (or a cycle of length r). We denote this by $\alpha = (i_1\, i_2\, \ldots\, i_r)$.

定義

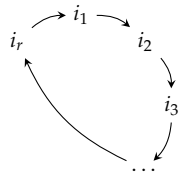


Figure 1.1: Visualisation of the r-cycle $(i_1\, i_2 \ldots i_r)$ as a clockwise rotation.

Remark.

A 1-cycle (i) is the identity map on the element i. Since 1-cycles fix every element, they represent the identity permutation ι. Often, 1-cycles are omitted from the notation. A 2-cycle $(i\, j)$ exchanges i and j and is called a **transposition**.

Because a cycle corresponds to a rotation of the indices (see *figure 1.1*), the notation is not unique:

$$(i_1\, i_2\, \ldots\, i_r) = (i_2\, i_3\, \ldots\, i_r\, i_1) = \cdots = (i_r\, i_1\, \ldots\, i_{r-1}).$$

Composition of Permutations

The operation in S_n is function composition. We adopt the convention of applying functions from right to left. That is, the product $\alpha\beta$ means $\alpha \circ \beta$, so $(\alpha\beta)(x) = \alpha(\beta(x))$.

Example 1.1. Cycle Decomposition Algorithm. Consider the permutation $\alpha \in S_9$:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}.$$

To factor α into cycles:

1. Start with 1. $\alpha(1) = 6$, $\alpha(6) = 1$. The sequence closes: $(1\,6)$.
2. The smallest uncovered number is 2. $\alpha(2) = 4$, $\alpha(4) = 2$. This closes: $(2\,4)$.
3. Next is 3. $3 \mapsto 7 \mapsto 8 \mapsto 9 \mapsto 3$. This gives $(3\,7\,8\,9)$.
4. Next is 5. $\alpha(5) = 5$. This is the 1-cycle (5).

Thus, $\alpha = (1\,6)(2\,4)(3\,7\,8\,9)(5)$.

範例

Example 1.2. Product of Cycles. Compute $\sigma = (12)(13425)(2513)$ in S_5. We evaluate the image of each element by tracing it through the cycles from right to left:

- $1 \xrightarrow{(2513)} 3 \xrightarrow{(13425)} 4 \xrightarrow{(12)} 4$. So $1 \mapsto 4$.
- $4 \to 4 \to 2 \to 1$. So $4 \mapsto 1$. This closes the cycle (14).
- $2 \to 5 \to 1 \to 2$. So $2 \mapsto 2$. This is a 1-cycle (2).
- $3 \to 2 \to 5 \to 5$. So $3 \mapsto 5$.
- $5 \to 1 \to 3 \to 3$. So $5 \mapsto 3$. This closes the cycle (53).

The disjoint cycle form is $\sigma = (14)(53)$.

範例

1.3 *Decomposition into Disjoint Cycles*

The factorisation observed in example 1.1 is not accidental. A fundamental property of permutations is that they can be decomposed into disjoint cycles.

Definition 1.3. ***Disjoint Permutations.***
Two permutations $\alpha, \beta \in S_n$ are **disjoint** if every i moved by one is fixed by the other. That is:

- If $\alpha(i) \neq i$, then $\beta(i) = i$.
- If $\beta(j) \neq j$, then $\alpha(j) = j$.

定義

Lemma 1.1. ***Commutativity of Disjoint Permutations.***
If $\alpha, \beta \in S_n$ are disjoint, then $\alpha\beta = \beta\alpha$.

引理

We show that $\alpha\beta(i) = \beta\alpha(i)$ for all $i \in \{1, \ldots, n\}$.

β moves i.

Let $\beta(i) = j \neq i$. Since β is a bijection and $\beta(i) \neq i$, β must also move j (otherwise $\beta(j) = j$ and $\beta(i) = j$ contradicts injectivity). Because α and β are disjoint, α fixes both i and j. Thus:

$$\alpha\beta(i) = \alpha(j) = j, \quad \text{and} \quad \beta\alpha(i) = \beta(i) = j.$$

証明終

α moves i.

By symmetry, the same logic applies.

証明終

Neither moves i.

Then $\alpha(i) = i$ and $\beta(i) = i$, so $\alpha\beta(i) = i = \beta\alpha(i)$.

証明終

In all cases, the functions agree.

Theorem 1.1. ***Cycle Decomposition.***
Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.

定理

We proceed by induction on k, the number of points moved by α.

Base Case ($k = 0$).

If α moves 0 points, it is the identity, which is a 1-cycle.

証明終

Inductive Step.

Assume the statement holds for all permutations moving fewer than k points. Let $k > 0$ and let i_1 be a point moved by α. Consider the sequence generated by iterating α:

$$i_1, \quad i_2 = \alpha(i_1), \quad i_3 = \alpha(i_2), \quad \dots$$

Since the set is finite, there exists a smallest r such that $\alpha(i_r) \in \{i_1, \dots, i_r\}$. Since α is injective and $\alpha(i_{j-1}) = i_j$ for $j > 1$, we must have $\alpha(i_r) = i_1$. Let $\sigma = (i_1\, i_2\, \dots\, i_r)$.

- If α fixes all other points (i.e., $k = r$), then $\alpha = \sigma$, and we are done.
- If $r < n$, let Y be the set of points not in $\{i_1, \dots, i_r\}$. Define α' such that $\alpha'(x) = \alpha(x)$ for $x \in Y$ and $\alpha'(x) = x$ otherwise. Then $\alpha = \sigma\alpha'$. Note that α' moves $k - r$ points. Since $r \geq 2$ (as α moves i_1), $k - r < k$. By the inductive hypothesis, α' is a product of disjoint cycles $\beta_1 \dots \beta_t$.

Since σ only moves points fixed by α' (and thus fixed by the β's), σ is disjoint from the β_j's. Therefore, $\alpha = \sigma\beta_1 \dots \beta_t$ is a product of disjoint cycles.

証明終

Note

The decomposition into disjoint cycles is unique up to the order of the factors (which commute) and the inclusion of 1-cycles.

Uniqueness of Decomposition

Earlier we suppressed 1-cycles (fixed points) for brevity; but to rigorously classify permutations, we must account for every element in the domain.

Definition 1.4. ***Complete Factorisation.***
A **complete factorisation** of a permutation $\alpha \in S_n$ is a decomposition into disjoint cycles that includes exactly one 1-cycle (i) for every element i fixed by α.

定義

For example, the 3-cycle $(1\,3\,5)$ in S_5 has the complete factorisation $(1\,3\,5)(2)(4)$.

Theorem 1.2. ***Uniqueness of Factorisation.***
Let $\alpha \in S_n$. The complete factorisation of α into disjoint cycles is unique up to the order of the factors.

定理

Proof

Since the complete factorisation explicitly lists every element of $\{1, \dots, n\}$, it suffices to consider factorisations into disjoint cycles of length $r \geq 2$. Suppose α has two such decompositions:

$$\alpha = \beta_1 \dots \beta_t = \gamma_1 \dots \gamma_s.$$

We proceed by induction on $m = \max(t, s)$. If $m = 0$, α is the identity, and the result holds. For the inductive step, let i be a specific element moved by β_t. The powers of β_t determine the iterates of i: $\beta_t^k(i) = \alpha^k(i)$. Since $\gamma_1 \dots \gamma_s$ represents the same function α, some cycle γ_j must also move i. Because disjoint cycles commute, we may reorder the γ's so that γ_s moves i. The cycle γ_s is determined entirely by the iterates of i under α. Thus, $\gamma_s = \beta_t$. Multiplying by β_t^{-1} (which equals γ_s^{-1}) yields $\beta_1 \dots \beta_{t-1} = \gamma_1 \dots \gamma_{s-1}$. By the inductive hypothesis, the remaining factors are identical up to order.

■

The cycle notation also simplifies the computation of inverses. Visually, if a cycle represents a clockwise rotation, its inverse is the counter-clockwise rotation.

Proposition 1.1. ***Inverses of Cycles.***

1. The inverse of a cycle $(i_1\, i_2\, \dots\, i_r)$ is $(i_r\, i_{r-1}\, \dots\, i_1)$.
2. If $\gamma = \beta_1 \dots \beta_k$ is a product of disjoint cycles, then $\gamma^{-1} = \beta_1^{-1} \dots \beta_k^{-1} = \beta_k^{-1} \dots \beta_1^{-1}$.

命題

Proof

For the first part, let $\sigma = (i_1\, i_2\, \ldots\, i_r)$ and $\tau = (i_r\, i_{r-1}\, \ldots\, i_1)$. We verify that $\tau\sigma = \iota$ by considering the action on each element (see *figure* 1.2). For any $j \in \{1, \ldots, r-1\}$, applying the functions from right to left gives:

$$\tau(\sigma(i_j)) = \tau(i_{j+1}) = i_j.$$

For the last element i_r, we have $\tau(\sigma(i_r)) = \tau(i_1) = i_r$. Any element $x \notin \{i_1, \ldots, i_r\}$ is fixed by both σ and τ, so $\tau(\sigma(x)) = x$. Thus $\tau\sigma = \iota$, which implies $\sigma^{-1} = \tau$.

For the second part, note that for permutations, $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ since

$$(\alpha\beta)(\beta^{-1}\alpha^{-1}) = \alpha(\beta\beta^{-1})\alpha^{-1} = \alpha\alpha^{-1} = \iota,$$

and similarly on the other side. By induction, $\gamma^{-1} = \beta_k^{-1} \ldots \beta_1^{-1}$. Since the cycles $\beta_1, \ldots, \beta_k$ are disjoint, they commute. It follows that their inverses also commute. Therefore, we may rearrange the factors in the product to obtain $\beta_1^{-1} \ldots \beta_k^{-1}$.

■

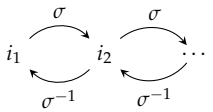


Figure 1.2: The inverse reverses the arrows.

Conjugacy

A natural question arises: when do two permutations "look the same"? In linear algebra, matrices representing the same linear transformation in different bases are similar. The analogous concept in group theory is conjugation.

Definition 1.5. ***Conjugate Permutations.***
Two permutations $\sigma, \gamma \in S_n$ are **conjugate** if there exists a permutation $\alpha \in S_n$ such that

$$\sigma = \alpha\gamma\alpha^{-1}.$$

定義

The geometric interpretation of $\alpha\gamma\alpha^{-1}$ is that we rename the elements of the set $\{1, \ldots, n\}$ according to α, apply γ, and then translate back via α^{-1}. This operation preserves the "shape" of the permutation, defined formally as follows.

Definition 1.6. ***Cycle Structure.***
Two permutations have the same **cycle structure** if their complete factorisations contain the same number of r-cycles for each length r.

定義

Example 1.3. Counting Cycle Structures. In S_4, the possible cycle structures partition the group into classes.

- Identity: 1^4 (one element).
- Transpositions (ab): $2^1 1^2$ (6 elements).
- 3-cycles (abc): $3^1 1^1$ (8 elements).
- 4-cycles $(abcd)$: 4^1 (6 elements).
- Double transpositions $(ab)(cd)$: 2^2 (3 elements).

Note the counting logic for $(ab)(cd)$: we choose 4 distinct elements in $\binom{4}{4}$ ways, partition them into pairs in 3 ways.

範例

Structure	Count
(1)	1
(1 2)	6
(1 2 3)	8
(1 2 3 4)	6
(1 2)(3 4)	3

Table 1.1: Distribution of permutations in S_4 by cycle structure.

The following lemma provides a powerful computational tool for conjugation: applying α to γ essentially "applies α to the symbols inside the cycle notation of γ".

Lemma 1.2. ***Conjugation Formula.***
Let $\gamma \in S_n$ have the complete factorisation containing the cycle $(i_1\, i_2\, \ldots\, i_r)$. Then the complete factorisation of $\alpha\gamma\alpha^{-1}$ contains the cycle

$$(\alpha(i_1)\, \alpha(i_2)\, \ldots\, \alpha(i_r)).$$

引理

Proof

Let $\sigma = \alpha\gamma\alpha^{-1}$. We track the image of an element $k = \alpha(i_j)$. Recall that we evaluate from right to left:

$$\sigma(k) = \sigma(\alpha(i_j)) = (\alpha \circ \gamma \circ \alpha^{-1})(\alpha(i_j)) = \alpha(\gamma(i_j)).$$

Since γ maps $i_j \mapsto i_{j+1}$ (where indices are taken modulo r), we have:

$$\sigma(\alpha(i_j)) = \alpha(i_{j+1}).$$

Thus, σ maps $\alpha(i_1) \to \alpha(i_2) \to \cdots \to \alpha(i_r) \to \alpha(i_1)$. If γ fixes an element x, i.e., (x) is a 1-cycle, then $\sigma(\alpha(x)) = \alpha(\gamma(x)) = \alpha(x)$, so $(\alpha(x))$ is a 1-cycle in σ. Since α is a bijection, every element in $\{1, \ldots, n\}$ is of the form $\alpha(x)$ for some x, so this describes the entire action of σ.

■

Example 1.4. Calculating Conjugates. Let $\gamma = (13)(247)(5)(6)$ and $\alpha = (256)(143)$ in S_7. Using *lemma 1.2*, we compute $\sigma =$

$\alpha\gamma\alpha^{-1}$ by applying α to the symbols in γ:

$$\begin{aligned}
1 &\mapsto \alpha(1) = 4 \\
3 &\mapsto \alpha(3) = 1 \\
2 &\mapsto \alpha(2) = 5 \\
4 &\mapsto \alpha(4) = 3 \\
7 &\mapsto \alpha(7) = 7 \quad \text{(fixed by } \alpha\text{)} \\
5 &\mapsto \alpha(5) = 6 \\
6 &\mapsto \alpha(6) = 2
\end{aligned}$$

Thus, $\sigma = (41)(537)(6)(2)$.

範例

This leads us to the fundamental classification theorem for the symmetric group.

Theorem 1.3. ***Conjugacy and Structure.***
Two permutations $\sigma, \gamma \in S_n$ are conjugate if and only if they have the same cycle structure.

定理

Proof

The "only if" direction is immediate from *lemma* 1.2: conjugation merely relabels the entries of the cycles, preserving their lengths. For the converse, suppose γ and σ have the same cycle structure. We construct the conjugating permutation α. List the disjoint cycles of γ and σ such that cycles of equal length are aligned vertically. For example:

$$\begin{aligned}
\gamma &= (i_1 \dots i_r)(j_1 \dots j_s)\dots \\
\sigma &= (k_1 \dots k_r)(l_1 \dots l_s)\dots
\end{aligned}$$

Define α by the "downward" mapping: $\alpha(i_m) = k_m$, $\alpha(j_m) = l_m$, and so on. Since the cycle structures match, every element of $\{1, \dots, n\}$ appears exactly once in the top row and exactly once in the bottom row. Thus, α is a well-defined bijection (a permutation). By construction and *lemma* 1.2:

$$\alpha\gamma\alpha^{-1} = (\alpha(i_1) \dots \alpha(i_r)) \cdots = (k_1 \dots k_r) \cdots = \sigma.$$

■

Example 1.5. Constructing the Conjugator. In S_5, let $\beta = (123)$ and $\gamma = (524)$. Both are 3-cycles, so they are conjugate. To find α

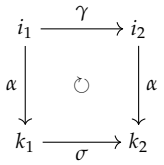


Figure 1.3: The commutative diagram for conjugation. If $\sigma = \alpha\gamma\alpha^{-1}$, then $\sigma \circ \alpha = \alpha \circ \gamma$. The "downward" map α transforms the cycle structure of γ into that of σ.

such that $\gamma = \alpha\beta\alpha^{-1}$, we align their complete factorisations:

$$\beta = (1\,2\,3)(4)(5)$$
$$\gamma = (5\,2\,4)(1)(3)$$

Define α by mapping the top to the bottom:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\,5\,3\,4).$$

Note that the alignment is not unique; we could rotate the cycles (e.g., writing γ as $(2\,4\,5)$) to find a different α.

範例

Decomposition into Transpositions

We conclude this chapter on permutations by examining their decomposition into the simplest building blocks: transpositions. While disjoint cycles provide a unique and structurally revealing factorisation, transpositions (2-cycles) offer a "atomic" view of permutations. Every rearrangement can be achieved by a sequence of swaps.

Proposition 1.2. ***Factorisation into Transpositions.***
If $n \geq 2$, every permutation $\alpha \in S_n$ is a product of transpositions.

命題

Proof

By *theorem* 1.1, α is a product of cycles. It suffices to show that any r-cycle can be written as a product of transpositions. We observe the identity:

$$(i_1\, i_2\, \ldots\, i_r) = (i_1\, i_r)(i_1\, i_{r-1}) \ldots (i_1\, i_3)(i_1\, i_2).$$

(Recall we multiply from right to left).

■

Unlike the disjoint cycle decomposition, factorisation into transpositions is far from unique.

Example 1.6. Non-uniqueness. Consider the cycle $(1\,2\,3) \in S_4$.

$$\begin{aligned}(1\,2\,3) &= (1\,3)(1\,2) \\ &= (2\,3)(1\,3) \\ &= (1\,3)(4\,2)(1\,2)(1\,4).\end{aligned}$$

Note that the number of factors varies (2 vs. 4), but the parity of the count remains invariant.

範例

Sign and Parity

The invariant hidden in the example above is the parity of the number of transpositions. To formalise this, we define the sign of a permutation based on its cycle structure.

Definition 1.7. ***Sign of a Permutation.***
Let $\alpha \in S_n$. Let t be the number of cycles in the **complete** factorisation of α (including 1-cycles). The **sign** (or signum) of α is defined as:

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}.$$

定義

This definition is well-defined by the uniqueness of the complete factorisation (*theorem 1.2*).

Example 1.7. Calculating Sign.

- Identity (1): n cycles ($t = n$). $\operatorname{sgn}(1) = (-1)^{n-n} = 1$.
- Transposition $\tau = (a\,b)$: Moves 2 elements, fixes $n-2$. Thus $t = 1 + (n-2) = n-1$.

$$\operatorname{sgn}(\tau) = (-1)^{n-(n-1)} = (-1)^1 = -1.$$

範例

The crucial property of the sign function is that it is a group homomorphism from S_n to the multiplicative group $\{1, -1\}$.

Theorem 1.4. ***Multiplicativity of Sign.***
For all $\alpha, \beta \in S_n$,

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

定理

Proof

We first establish how multiplication by a transposition $\tau = (a\,b)$ affects the number of cycles $t(\alpha)$.
Let a and b belong to cycles C_a and C_b in the decomposition of α.

a and b are in the same cycle. Let this cycle be $(a\,c_1 \dots c_k\,b\,d_1 \dots d_l)$.
Multiplying by $(a\,b)$ splits this into two:

$$(a\,b)(a\,c_1 \dots c_k\,b\,d_1 \dots d_l) = (a\,c_1 \dots c_k)(b\,d_1 \dots d_l).$$

The number of cycles increases by 1: $t(\tau\alpha) = t(\alpha) + 1$.

a and b are in different cycles. Let the cycles be $(a\,c_1 \dots c_k)$ and

$(b\, d_1 \dots d_l)$. Multiplying by $(a\, b)$ merges them:

$$(a\, b)(a\, c_1 \dots c_k)(b\, d_1 \dots d_l) = (a\, c_1 \dots c_k\, b\, d_1 \dots d_l).$$

The number of cycles decreases by 1: $t(\tau\alpha) = t(\alpha) - 1$.

In both cases, $n - t(\tau\alpha)$ differs from $n - t(\alpha)$ by an odd integer (± 1). Thus:

$$\operatorname{sgn}(\tau\alpha) = (-1)^{n-t(\tau\alpha)} = -(-1)^{n-t(\alpha)} = -\operatorname{sgn}(\alpha) = \operatorname{sgn}(\tau)\operatorname{sgn}(\alpha).$$

Since any permutation α is a product of transpositions $\tau_1 \dots \tau_m$, repeated application gives $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$.

■

This theorem allows us to rigorously define even and odd permutations based on their factors.

Definition 1.8. ***Parity.***
A permutation α is **even** if $\operatorname{sgn}(\alpha) = 1$ and **odd** if $\operatorname{sgn}(\alpha) = -1$.

定義

Theorem 1.5. ***Parity and Transpositions.***
A permutation is even if and only if it can be written as a product of an even number of transpositions. It is odd if and only if it is a product of an odd number of transpositions.

定理

Proof

Let $\alpha = \tau_1 \dots \tau_q$ be any factorisation into transpositions. By the multiplicativity of the sign:

$$\operatorname{sgn}(\alpha) = \operatorname{sgn}(\tau_1) \dots \operatorname{sgn}(\tau_q) = (-1)^q.$$

Thus, $\operatorname{sgn}(\alpha) = 1 \iff q$ is even, and $\operatorname{sgn}(\alpha) = -1 \iff q$ is odd. This implies that the parity of the number of factors q is invariant for a given α.

■

Corollary 1.1. *Parity Arithmetic.* The product of two even permutations is even. The product of two odd permutations is even. The product of an even and an odd permutation is odd.

推論

Proof

This follows directly from the rules of multiplication in $\{1, -1\}$: $1 \cdot 1 = 1$, $(-1)(-1) = 1$, and $1 \cdot (-1) = -1$.

■

1.4 Exercises

1. **Cycle Products.** Compute the following products in cycle notation. Remember to compute from right to left.
   (a) In S_5: $(123)(234)$.
   (b) In S_6: $(145)(23)(12)(56)$.
   (c) In S_8: α^2 where $\alpha = (12)(345)(678)$.
2. **Inverse Calculation.**
   (a) Find the inverse of $\sigma = (135)(24)$ in S_5. Verify that $\sigma\sigma^{-1} = \iota$.
   (b) Prove that for any permutation α and element i, $\alpha(i) \neq i$ if and only if $\alpha^{-1}(i) \neq i$.
3. **Disjoint Decomposition.** Write the following permutations as products of disjoint cycles:
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 5 & 9 & 8 & 1 & 6 \end{pmatrix}$.
   (b) $(12)(13)(14)(15)$ in S_5.
   (c) $(12)^2(34)$.
4. **Order of Permutations.** The **order** of a permutation α is the smallest positive integer k such that $\alpha^k = \iota$.
   (a) Prove that if α, β commute (i.e., $\alpha\beta = \beta\alpha$), then $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \in \mathbb{Z}$.
   (b) Prove that the order of an r-cycle is r.
   (c) Prove that if $\alpha = c_1 \dots c_m$ is a product of disjoint cycles of lengths $r_1, \dots, r_m$, then the order of α is $\operatorname{lcm}(r_1, \dots, r_m)$.
   (d) Find the maximum order of an element in S_7.
5. **Finding the Conjugator.** In S_6, let $\sigma = (13)(246)$ and $\tau = (36)(152)$.
   (a) Verify that σ and τ are conjugate.
   (b) Find a permutation $\alpha \in S_6$ such that $\alpha\sigma\alpha^{-1} = \tau$.
6. **Conjugacy Classes.** Determine the number of conjugacy classes in S_5. List a representative cycle structure for each class.
7. **Decomposition into Transpositions.** Write the permutation $\alpha = (12345)$ as:
   (a) A product of 4 transpositions.
   (b) A product of 6 transpositions.
8. **Sign Properties.**

(a) Prove that $\operatorname{sgn}(\alpha^{-1}) = \operatorname{sgn}(\alpha)$ for any $\alpha \in S_n$.

(b) Show that $\operatorname{sgn}(\alpha\beta\alpha^{-1}) = \operatorname{sgn}(\beta)$. Conclude that conjugate permutations have the same parity.

(c) If $\sigma \in S_n$ fixes some $j \in \{1, \ldots, n\}$, define $\sigma' \in S_{n-1}$ by restricting σ to the remaining $n-1$ elements. Prove that $\operatorname{sgn}(\sigma') = \operatorname{sgn}(\sigma)$.

> *Remark.*
>
> Compare the complete factorisations.

9. **Sign of an r-cycle.** Prove directly that the sign of an r-cycle is $(-1)^{r-1}$. Thus, an r-cycle is even if and only if its length r is odd.

10. **Adjacent Transpositions.** Prove that every permutation in S_n can be written as a product of adjacent transpositions $s_i = (i\ i+1)$.

11. **Generating the Symmetric Group.** Show that S_n is generated by the two elements $(1\,2)$ and $(1\,2\,\ldots\,n)$. That is, every permutation can be written as a product involving only these two and their powers.

2
Groups

The study of groups allows us to unify diverse mathematical objects (from number systems and matrices to geometric symmetries), under a single axiomatic framework.

2.1 *Axioms and Basic Properties*

We begin with the formal definition.

Definition 2.1. ***Group.***
A **group** is a set G equipped with a binary operation (usually denoted multiplicatively as ab) satisfying the following three axioms.

定義

Axiom 1. ***Associativity.***
For all $a, b, c \in G$, $(ab)c = a(bc)$.

公理

Axiom 2. ***Identity.***
There exists an element $1 \in G$ (often denoted e or 1_G) such that for all $a \in G$, $a \cdot 1 = 1 \cdot a = a$.

公理

Axiom 3. ***Inverses.***
For every $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = 1$. We denote the inverse of a by a^{-1}.

公理

The group is the pair $(G, \cdot)$.

Monoids and Semigroups

If we relax the axioms of a group, we obtain more general algebraic structures.

Definition 2.2. ***Semigroup and Monoid.***

1. A pair $(S, *)$ is called a **semigroup** if the operation is associative.
2. A pair $(M, *)$ is called a **monoid** if it is a semigroup and possesses a unit element.

定義

Example 2.1. Transformation Monoid. Let Ω be any set. Let $M(\Omega)$ be the set of all maps $f : \Omega \to \Omega$. Under function composition, $M(\Omega)$ is a monoid with the identity map id_Ω as its unit element. If $|\Omega| = n$, there are n^n such maps. Consider the case $n = 2$ with $\Omega = \{1, 2\}$. The set $M(\{1, 2\})$ contains $2^2 = 4$ elements: the identity e, and maps f, g, h. Their composition table is:

$\circ$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	g	g	g
h	h	h	h	h

(Note: The specific labels f, g, h correspond to the maps defined by their columns in the table). This monoid is non-commutative (e.g., $f \circ g \neq g \circ f$).

範例

Example 2.2. Power Set Monoids. Let $\mathcal{P}(\Omega)$ be the power set of Ω.

1. $(\mathcal{P}(\Omega), \cup, \emptyset)$ is a commutative monoid (unit is $\emptyset$).
2. $(\mathcal{P}(\Omega), \cap, \Omega)$ is a commutative monoid (unit is Ω).

範例

Example 2.3. Matrix Monoids. Let $M_n(\mathbb{R})$ be the set of $n \times n$ real matrices.

1. $(M_n(\mathbb{R}), +, 0)$ is a commutative monoid (unit is the zero matrix).
2. $(M_n(\mathbb{R}), \cdot, I_n)$ is a non-commutative monoid (unit is the identity matrix).

範例

Example 2.4. Integers Divisible by n. Let $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

1. $(n\mathbb{Z}, +, 0)$ is a commutative monoid.
2. $(n\mathbb{Z}, \cdot)$ is a commutative semigroup. If $n > 1$, it lacks a unit element and is not a monoid.

範例

Example 2.5. Stochastic Matrices. The set $P^n(\mathbb{R})$ of stochastic matrices (matrices where each row sums to 1) forms a monoid under matrix multiplication.

範例

Just as we study subgroups, we can define substructures for these systems.

Definition 2.3. ***Subsemigroup and Submonoid.***
Let $(S, *)$ be a semigroup. A subset $S' \subseteq S$ is a **subsemigroup** if it is closed under $*$, i.e., $x * y \in S'$ for all $x, y \in S'$. If $(M, *)$ is a monoid, a subset $M' \subseteq M$ is a **submonoid** if it is a subsemigroup and contains the unit element of M.

定義

Example 2.6. The Trivial Group. The set $G = \{1\}$ with the operation $1 \cdot 1 = 1$ is a group. It satisfies all axioms trivially.

範例

Although the axioms assert the existence of an identity and inverses, they do not explicitly state their uniqueness. This, however, is an immediate consequence.

Proposition 2.1. ***Elementary Properties.***
Let G be a group.
1. The identity element 1 is unique.
2. The inverse of any element $a \in G$ is unique.
3. **Cancellation Laws:** For any $a, b, c \in G$:

$$\text{If } ab = ac, \text{ then } b = c. \quad \text{If } ba = ca, \text{ then } b = c.$$

命題

Proof

1. This follows directly from *proposition* 0.4.
2. Suppose b and c are both inverses of a. Then:

$$b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c.$$

3. Suppose $ab = ac$. Multiply by a^{-1} on the left:

$$a^{-1}(ab) = a^{-1}(ac) \implies (a^{-1}a)b = (a^{-1}a)c \implies 1 \cdot b = 1 \cdot c \implies b = c.$$

The right cancellation follows similarly.

■

Definition 2.4. ***Abelian Group.***
A group G is called **Abelian** (or commutative) if the operation satis-

fies $ab = ba$ for all $a, b \in G$.

定義

Notation 2.1. For Abelian groups, we often use **additive notation**. The operation is denoted by $+$, the identity by 0, and the inverse of a by $-a$.

記法

Numerical Groups

The standard number systems provide familiar examples of infinite Abelian groups.

- The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ form Abelian groups under addition.
- The non-zero elements $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ (the multiplicative group of non-zero rationals), $\mathbb{R}^\times$ (the multiplicative group of non-zero reals), and $\mathbb{C}^\times$ (the multiplicative group of non-zero complex numbers) form Abelian groups under multiplication.

Modular Arithmetic

A crucial class of finite Abelian groups arises from modular arithmetic.

Example 2.7. Integers Modulo n. Let n be a positive integer. The set of residue classes modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$, consists of $\{0, 1, \ldots, n - 1\}$. Under addition modulo n, this forms a finite Abelian group of order n.

範例

When $n = p$ is a prime, the structure is richer. The set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (the finite field with p elements) forms a field. The non-zero elements $\mathbb{F}_p^\times = \{1, \ldots, p-1\}$ (the multiplicative group of non-zero elements of $\mathbb{F}_p$) form a multiplicative Abelian group of order $p - 1$. This relies on the number-theoretic result that for any $a \not\equiv 0 \pmod{p}$, there exists an integer b such that $ab \equiv 1 \pmod{p}$.

Roots of Unity

Consider the complex number $\zeta_n = \exp(2\pi i/n)$ (the primitive n-th root of unity). The set

$$\mu_n = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$$

consists of all n-th roots of unity (this is the group of n-th roots of unity under multiplication). Under complex multiplication, μ_n is a cyclic Abelian group of order n. Geometrically, these points form the vertices of a regular n-gon inscribed in the unit circle (see *figure* 2.1). Furthermore, the entire unit circle $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ (the unit circle in the complex plane) is an infinite multiplicative Abelian group.

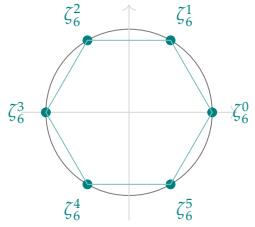


Figure 2.1: The group μ_6 of 6th roots of unity forms a regular hexagon in the complex plane.

The General Linear Group

We now turn to non-Abelian groups. A primary example comes from linear algebra.

Definition 2.5. ***General Linear Group.***
Let F be a field (such as $\mathbb{R}, \mathbb{C}$ or $\mathbb{F}_p$ where $\mathbb{F}_p$ is the finite field with p elements). The set of all $n \times n$ invertible matrices with entries in F is called the **general linear group**, denoted $\mathrm{GL}_n(F)$ or simply GL_n.

定義

The group operation is matrix multiplication. Since matrix multiplication is associative but generally not commutative (for $n \geq 2$), $\mathrm{GL}_n(F)$ is a non-Abelian group. The identity element is the identity matrix I_n.

Remark.

The set of all $n \times n$ matrices $M_n(F)$ under multiplication is a monoid, but not a group, as singular matrices lack inverses. Under addition, $M_n(F)$ is an Abelian group.

Example 2.8. Order of $\mathrm{GL}_n(\mathbb{F}_p)$. If $F = \mathbb{F}_p$ is a finite field with p elements, $\mathrm{GL}_n(\mathbb{F}_p)$ is a finite group. We determine its order by counting the number of valid bases for the vector space F^n.

範例

Solution

A matrix $A \in M_n(\mathbb{F}_p)$ is invertible if and only if its rows are linearly independent.

- The first row $\mathbf{r}_1$ can be any non-zero vector in F^n. There are $p^n - 1$ choices.
- The second row $\mathbf{r}_2$ must be linearly independent of $\mathbf{r}_1$. It cannot be a scalar multiple of $\mathbf{r}_1$. There are $p^n - p$ choices.
- The k-th row $\mathbf{r}_k$ must not lie in the subspace spanned by $\{\mathbf{r}_1, \ldots, \mathbf{r}_{k-1}\}$. This subspace has cardinality p^{k-1}. Thus, there are $p^n - p^{k-1}$ choices.

The total order is the product of these counts:

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

■

Symmetry and Rigid Motions

Groups naturally encode symmetry. As established in the previous chapter, the set of all bijections of a set X forms the symmetric group S_X. When $X = \{1, \ldots, n\}$, this is S_n.

Example 2.9. Symmetries of a Tetrahedron. Let T be a regular tetrahedron with vertices A, B, C, D. The set of rigid motions (rotations) that map T to itself forms a subgroup of the permutation group of the vertices S_4.

範例

Solution

We classify the rotations by their axes (see *figure 2.2*):

Identity. 1 rotation.

Vertex-Face axes. Axes passing through a vertex and the centre of the opposite face. There are 4 such axes. Each allows rotations by $2\pi/3$ and $4\pi/3$. Total: $4 \times 2 = 8$ rotations. These correspond to 3-cycles like $(B\,C\,D)$.

Edge-Edge axes. Axes connecting the midpoints of opposite edges (e.g., AB and CD). There are 3 such axes. A rotation by π about such an axis swaps $A \leftrightarrow B$ and $C \leftrightarrow D$. Total: 3 rotations. These correspond to double transpositions like $(A\,B)(C\,D)$.

The total number of rotational symmetries is $1 + 8 + 3 = 12$. This group is isomorphic to the alternating group A_4 (the subgroup of even permutations in S_4).

■

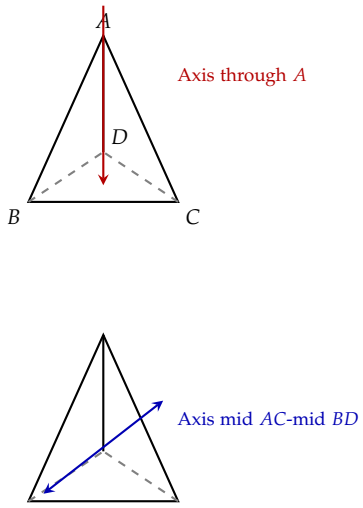


Figure 2.2: Rotational axes of a tetrahedron.

2.2 *Subgroups*

Just as a vector space may contain subspaces, a group may contain smaller subsets that are groups in their own right.

Definition 2.6. ***Subgroup.***
Let G be a group. A subset $H \subseteq G$ is called a **subgroup** of G, denoted $H \leq G$, if H itself forms a group under the binary operation of G. If $H \leq G$ and $H \neq G$, we call H a **proper subgroup**, denoted $H < G$.

定義

Example 2.10. Trivial Subgroups. For any group G, the singleton set $\{1\}$ containing only the identity is a subgroup, often called the trivial subgroup. The group G itself is also a subgroup.

範例

Example 2.11. Numerical Subgroups.

1. The set of even integers $2\mathbb{Z}$ is a subgroup of the additive group $\mathbb{Z}$. In general, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ for any $n \in \mathbb{Z}$.

2. The circle group $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is a subgroup of the multiplicative group $\mathbb{C}^\times$.
3. The group of n-th roots of unity μ_n is a subgroup of S^1, and thus also of $\mathbb{C}^\times$.

範例

To verify that a subset is a subgroup, one need not check all group axioms from scratch. Associativity is inherited from the parent group. We require only closure under the operation and the existence of inverses and the identity. This is efficiently summarised by the following criterion.

Proposition 2.2. ***Subgroup Criterion.***
A non-empty subset $H \subseteq G$ is a subgroup if and only if for all $a, b \in H$, the element ab^{-1} belongs to H.

命題

(⇒)

If $H \leq G$, then for any $b \in H$, its inverse b^{-1} must be in H. Since H is closed under multiplication, $a(b^{-1}) = ab^{-1} \in H$.

証明終

(⇐)

We assume $ab^{-1} \in H$ for all $a, b \in H$.

Identity: Since H is non-empty, take any $x \in H$. Then $1 = xx^{-1} \in H$.

Inverses: For any $x \in H$, since $1 \in H$, we have $x^{-1} = 1 \cdot x^{-1} \in H$.

Closure: Let $a, b \in H$. Since $b^{-1} \in H$, we have $ab = a(b^{-1})^{-1} \in H$.

Thus H satisfies the group axioms.

証明終

Remark.

For additive groups, the condition translates to: $H \leq G \iff \forall a, b \in H, a - b \in H$.

Example 2.12. Matrix Subgroup. Consider the set of upper triangular matrices with 1s on the diagonal:

$$H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \;\middle|\; a \in \mathbb{R} \right\} \subseteq \mathrm{GL}_2(\mathbb{R}).$$

範例

Solution

To check if this is a subgroup, let $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. The inverse of B is $\begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix}$. Then

$$AB^{-1} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a-b \\ 0 & 1 \end{bmatrix}.$$

Since $a - b \in \mathbb{R}$, the result lies in H. Thus $H \leq \mathrm{GL}_2(\mathbb{R})$.

■

The Dihedral Group

We previously discussed the symmetries of a tetrahedron. We now formalise the symmetries of a regular polygon in the plane.

Definition 2.7. ***Dihedral Group.***
Let P_n be a regular n-gon ($n \geq 3$) with vertices labelled $1, \ldots, n$. The **dihedral group**, denoted D_n, is the group of all rigid transformations (isometries) of the plane that map P_n to itself.

定義

The elements of D_n consist of:

1. **Rotations:** The n rotations by angles $2\pi k/n$ for $k = 0, \ldots, n-1$ about the centre of the polygon.
2. **Reflections:** The n reflections across axes of symmetry.

Thus, the order of D_n is $2n$. Since any symmetry permutes the vertices, D_n is naturally a subgroup of the symmetric group S_n.

Note

Notation for the dihedral group varies significantly across the literature. In these notes, D_n refers to the symmetries of a regular n-gon, which has order $2n$. Many algebraists (e.g., Dummit & Foote) denote this group as D_{2n} to emphasize its order. Conversely, some geometers use D_n to refer to the group of order n. Please always verify the convention when consulting external texts to avoid confusion between the number of sides and the order of the group.

Example 2.13. Symmetries of a Triangle. For $n = 3$, the group D_3 represents the symmetries of an equilateral triangle. It contains 3 rotations and 3 reflections. This group is isomorphic to S_3, as any permutation of the three vertices can be realised by a rigid motion. For $n \geq 3$, D_n is non-Abelian (rotations and reflections generally do not commute).

範例

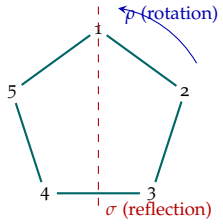


Figure 2.3: Symmetries of a regular pentagon ($n = 5$). The axis of reflection passes through a vertex and the midpoint of the opposite edge.

Direct Products

A standard method to construct larger groups from smaller ones is the direct product.

Definition 2.8. ***Direct Product.***
Let G_1 and G_2 be groups. The **direct product** $G = G_1 \times G_2$ is the set of ordered pairs $\{(g,h) \mid g \in G_1, h \in G_2\}$ equipped with the componentwise operation:

$$(g_1,h_1)\cdot(g_2,h_2) = (g_1g_2, h_1h_2).$$

定義

It is straightforward to verify that this forms a group:

- The identity is $1_G = (1_{G_1}, 1_{G_2})$.
- The inverse is $(g,h)^{-1} = (g^{-1}, h^{-1})$.
- The order is $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

Proposition 2.3. ***Subgroups of Products.***
If $H_1 \leq G_1$ and $H_2 \leq G_2$, then $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$. Note that not every subgroup of a product is of this form. In particular, $G_1 \times G_2$ always contains the subgroups $\{1_{G_1}\} \times G_2$ and $G_1 \times \{1_{G_2}\}$, which are isomorphic to G_2 and G_1 respectively.

命題

Proof

We verify the subgroup criterion. The set $H_1 \times H_2$ is non-empty because H_1, H_2 contain their respective identities. Let $x = (h_1,h_2)$ and $y = (k_1,k_2)$ be elements of $H_1 \times H_2$. The inverse of y in the direct product is $y^{-1} = (k_1^{-1}, k_2^{-1})$. Then

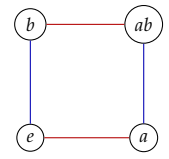
$$xy^{-1} = (h_1,h_2)(k_1^{-1},k_2^{-1}) = (h_1k_1^{-1}, h_2k_2^{-1}).$$

Since $H_1 \leq G_1$, we have $h_1k_1^{-1} \in H_1$. Similarly, $h_2k_2^{-1} \in H_2$. Thus $xy^{-1} \in H_1 \times H_2$, so $H_1 \times H_2 \leq G_1 \times G_2$.

■

Example 2.14. The Klein Four-Group. Let $C_2 = \{0,1\}$ be the cyclic group of order 2 (isomorphic to $\mathbb{Z}/2\mathbb{Z}$). The direct product $V_4 = C_2 \times C_2$ is called the **Klein Four-Group**. Its elements are $\{(0,0),(0,1),(1,0),(1,1)\}$. Since $x + x = 0$ for all $x \in C_2$, every non-identity element in V_4 has order 2. This distinguishes it from the cyclic group C_4, which contains elements of order 4.

範例



Cayley graph

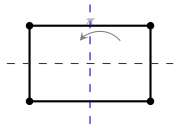

Rectangle symmetries

Figure 2.4: The Klein four-group V_4: Cayley graph (top) and as symmetries of a rectangle (bottom).

2.3 *Classical Groups*

Among the subgroups of the general linear group GL_n, certain families play a pivotal role in algebra, geometry, and physics. These are collectively known as the classical groups. They are typically defined as the groups of matrices that preserve specific geometric structures, such as volume, inner products, or bilinear forms.

The Special Linear Group

The most immediate subgroup of $\mathrm{GL}_n(F)$ arises from the determinant map. Since $\det(AB) = \det A \det B$, the determinant is a homomorphism from $\mathrm{GL}_n(F)$ to $F^\times$. The kernel of this map consists of matrices with unit determinant.

Definition 2.9. ***Special Linear Group.***
The **special linear group** of degree n over a field F is defined as

$$\mathrm{SL}_n(F) = \{A \in \mathrm{GL}_n(F) \mid \det A = 1\}.$$

定義

This group preserves the oriented volume in vector spaces. We can identify several other notable subgroups of $\mathrm{GL}_n(F)$ based on matrix structure:

$B_n(F)$: Invertible upper triangular matrices (the Borel subgroup).

$T_n(F)$: Upper triangular matrices with 1s on the diagonal (unipotent matrices).

$\mathrm{Diag}_n(F)$: Invertible diagonal matrices.

Observe that $T_n(F) \leq \mathrm{SL}_n(F)$ and $\mathrm{Diag}_n(F) \leq B_n(F)$.

Proof

The inclusion $\mathrm{Diag}_n(F) \leq B_n(F)$ is immediate, as every diagonal matrix is upper triangular. For the second inclusion, recall that the determinant of an upper triangular matrix is the product of its diagonal entries. Since $A \in T_n(F)$ implies $A_{ii} = 1$ for all $i \in \{1, \ldots, n\}$, we have $\det(A) = 1^n = 1$,so $A \in \mathrm{SL}_n(F)$.

■

The definition extends naturally to rings. For instance, $\mathrm{SL}_n(\mathbb{Z})$ consists of integer matrices with determinant 1. For a positive integer $N > 1$, we define the special linear group of degree 2 over $\mathbb{Z}/N\mathbb{Z}$ as:

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z}/N\mathbb{Z},\ ad - bc = 1 \right\}.$$

When the degree 2 is changed to a general n, we obtain the special linear groups over $\mathbb{Z}$ and $\mathbb{Z}/N\mathbb{Z}$.

Orthogonal Groups

When the vector space $\mathbb{R}^n$ is equipped with the standard Euclidean inner product $\langle X, Y\rangle = X^\top Y$, we consider the linear transformations that preserve lengths and angles.

Definition 2.10. ***Orthogonal Group.***
A matrix $A \in \mathrm{GL}_n(\mathbb{R})$ is **orthogonal** if it preserves the inner product, i.e., $\langle AX, AY\rangle = \langle X, Y\rangle$ for all X, Y. This condition is equivalent to $A^\top A = I$. The set of such matrices forms the **orthogonal group**:

$$O_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^\top A = I\}.$$

定義

Since $\det(A^\top A) = (\det A)^2 = 1$, the determinant of any orthogonal matrix is ± 1. The subgroup of rotations (orientation-preserving isometries) is:

$$\mathrm{SO}_n(\mathbb{R}) = O_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R}).$$

Example 2.15. The Case $n = 2$. The elements of $\mathrm{SO}_2(\mathbb{R})$ are rotation matrices:

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \;\middle|\; \theta \in \mathbb{R} \right\}.$$

The full orthogonal group $O_2(\mathbb{R})$ consists of rotations and reflections:

$$O_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}, \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \;\middle|\; \theta \in \mathbb{R} \right\}.$$

範例

More generally, if V is equipped with a non-degenerate symmetric bilinear form Q of signature (p, q) (where $p + q = n$), there exists a basis where the metric tensor is $J_{p,q} = \mathrm{diag}(I_p, -I_q)$. The group preserving this form is the **generalised orthogonal group**:

$$O_{p,q}(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^\top J_{p,q} A = J_{p,q}\}.$$

A prominent example is the Lorentz group $O_{3,1}(\mathbb{R})$ in special relativity.

Unitary Groups

For complex vector spaces $\mathbb{C}^n$, the natural structure is the Hermitian inner product $\langle X, Y \rangle = \bar{X}^\top Y$.

Definition 2.11. ***Unitary Group.***
A matrix $A \in \mathrm{GL}_n(\mathbb{C})$ is **unitary** if it preserves the Hermitian form, i.e., $\bar{A}^\top A = I$. The group of such matrices is denoted:

$$U(n) = \{A \in \mathrm{GL}_n(\mathbb{C}) \mid A^\dagger A = I\},$$

where $A^\dagger = \bar{A}^\top$.

定義

The intersection with the special linear group yields the **special unitary group**:

$$SU(n) = U(n) \cap \mathrm{SL}_n(\mathbb{C}).$$

Example 2.16. Low Dimensional Examples.

- $U(1)$ consists of complex numbers z with $|z|^2 = \bar{z}z = 1$. The group $U(1)$ is the unit circle S^1.
- $SU(2)$ consists of matrices $\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$ where $|\alpha|^2 + |\beta|^2 = 1$. This group is topologically equivalent to the 3-sphere S^3.

範例

Finally, we consider spaces equipped with a skew-symmetric bilinear form. Let V be a real vector space of even dimension $2n$. A standard non-degenerate skew-symmetric form Ω can be represented by the matrix $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$.

Definition 2.12. ***Symplectic Group.***
The **symplectic group** consists of matrices that preserve the form Ω:

$$\mathrm{Sp}_{2n}(\mathbb{R}) = \{A \in \mathrm{GL}_{2n}(\mathbb{R}) \mid A^\top J A = J\}.$$

定義

Unlike the orthogonal case, it is a non-trivial theorem that for any $A \in \mathrm{Sp}_{2n}(\mathbb{R})$, $\det A = 1$. Thus, there is no distinct "special symplectic group". These groups are fundamental in Hamiltonian mechanics.

2.4 *Homomorphisms and Isomorphisms*

To understand the structure of groups, we must study the relationships between them. Just as functions relate sets, specific mappings that preserve the algebraic structure relate groups.

Definition 2.13. ***Group Homomorphism.***
Let G_1 and G_2 be groups. A mapping $f : G_1 \to G_2$ is called a **group homomorphism** if it preserves the group operation. That is, for all $g, h \in G_1$:

$$f(gh) = f(g)f(h).$$

Note that the product gh is computed in G_1, while $f(g)f(h)$ is computed in G_2.

- If f is injective, it is called a **monomorphism**.
- If f is surjective, it is called an **epimorphism**.
- If f is bijective, it is called an **isomorphism**. In this case, we write $G_1 \cong G_2$.

定義

The structural preservation implies that the identity and inverses are mapped consistently.

Proposition 2.4. ***Preservation Properties.***
Let $f : G_1 \to G_2$ be a group homomorphism. Then:

1. f maps the identity of G_1 to the identity of G_2: $f(1_{G_1}) = 1_{G_2}$.
2. f maps inverses to inverses: for any $g \in G_1$, $f(g^{-1}) = f(g)^{-1}$.

命題

Proof

For the first property, observe that $1_{G_1} \cdot 1_{G_1} = 1_{G_1}$. Applying f:

$$f(1_{G_1}) = f(1_{G_1} \cdot 1_{G_1}) = f(1_{G_1})f(1_{G_1}).$$

Multiplying both sides by the inverse $f(1_{G_1})^{-1}$ in G_2, we obtain $1_{G_2} = f(1_{G_1})$.
For the second property, let $g \in G_1$. Then:

$$f(g)f(g^{-1}) = f(g \cdot g^{-1}) = f(1_{G_1}) = 1_{G_2}.$$

Similarly, $f(g^{-1})f(g) = 1_{G_2}$. By the uniqueness of inverses in G_2, $f(g^{-1}) = f(g)^{-1}$.

■

Examples of Homomorphisms

We provide several key examples that illustrate these concepts across number theory and linear algebra.

Example 2.17. Inclusion. If H is a subgroup of G, the inclusion map $i : H \to G$ defined by $i(h) = h$ is a homomorphism. Since it is injective, it is a monomorphism.

範例

Example 2.18. The Determinant. The determinant function $\det : \mathrm{GL}_n(F) \to F^\times$ satisfies $\det(AB) = \det(A)\det(B)$. Thus, it is a group homomorphism. Since any non-zero scalar can be the determinant of some matrix (e.g., a diagonal matrix), this map is an epimorphism.

範例

Example 2.19. Cyclic Groups. Consider the additive group of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$, and the group of n-th roots of unity, μ_n. Define the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mu_n$ by:

$$\varphi(m) = \zeta_n^m = e^{\frac{2\pi i m}{n}}.$$

This map is well-defined and bijective, satisfying $\varphi(a+b) = \zeta_n^{a+b} = \zeta_n^a \zeta_n^b = \varphi(a)\varphi(b)$. Thus, φ is an isomorphism.

範例

Example 2.20. Permutation Matrices. We can represent permutations as matrices. For each $\sigma \in S_n$, define a matrix $A_\sigma \in \mathrm{GL}_n$ by its action on the basis vectors. Specifically, for a vector $\mathbf{x} = (x_1, \ldots, x_n)^\top$, let:

$$A_\sigma \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} x_{\sigma^{-1}(1)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{bmatrix}.$$

The entries of the matrix $A_\sigma = (a_{ij})$ are given by:

$$a_{ij} = \begin{cases} 1 & \text{if } j = \sigma^{-1}(i) \iff \sigma(j) = i, \\ 0 & \text{otherwise.} \end{cases}$$

The mapping $\sigma \mapsto A_\sigma$ is a monomorphism $S_n \to \mathrm{GL}_n$. These A_σ are called **permutation matrices**. This allows us to view the symmetric group as a subgroup of the general linear group.

範例

Example 2.21. Rotations. The circle group $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ is isomorphic to the special orthogonal group $\mathrm{SO}_2(\mathbb{R})$. An explicit isomorphism is given by:

$$e^{i\theta} \mapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

範例

Example 2.22. Exponential and Logarithm. Let $\mathbb{R}$ be the additive group of real numbers, and let $\mathbb{R}_+^\times$ be the multiplicative group of positive real numbers. The exponential map:

$$\exp : \mathbb{R} \to \mathbb{R}_+^\times, \quad x \mapsto e^x$$

is an isomorphism, as $e^{x+y} = e^x e^y$. Its inverse is the natural logarithm:

$$\log : \mathbb{R}_+^\times \to \mathbb{R}, \quad y \mapsto \ln y,$$

which satisfies $\ln(xy) = \ln x + \ln y$.

範例

In group theory, we often treat isomorphic groups as identical. However, the ways in which a group can be isomorphic to itself — its symmetries — are of independent interest.

Definition 2.14. ***Automorphism.***
An isomorphism from a group G to itself is called an **automorphism**.

定義

Proposition 2.5. ***The Automorphism Group.***

1. The set of all automorphisms of a group G, denoted $\mathrm{Aut}(G)$, forms a group under function composition.
2. If $\varphi : G \to H$ is a fixed isomorphism, then the set of all isomorphisms from G to H is given by the coset $\varphi \,\mathrm{Aut}(G) = \{\varphi \circ f \mid f \in \mathrm{Aut}(G)\}$.

命題

Proof

1. The composition of two automorphisms is an automorphism, and the inverse of an automorphism is an automorphism. Associativity holds for function composition, and the identity map is the identity element.
2. Let $\psi : G \to H$ be any isomorphism. Then $\varphi^{-1} \circ \psi : G \to G$ is an automorphism, say f. Thus $\psi = \varphi \circ f$. Conversely, for any $f \in \mathrm{Aut}(G)$, the composite $\varphi \circ f$ is an isomorphism from G to H.

■

2.5 *Exercises*

1. **Function Space Group.** Let A be a set and G be a group. Let $\mathrm{Map}(A, G)$ be the set of all functions $f : A \to G$. Define the product fg pointwise: $(fg)(\alpha) = f(\alpha)g(\alpha)$ for all $\alpha \in A$. Prove that $\mathrm{Map}(A, G)$ forms a group.

2. **Isometry Group.** An isometry of the plane $\mathbb{R}^2$ is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ preserving distances: $|f(x) - f(y)| = |x - y|$. Prove that all isometries are bijections and that they form a group under composition.

3. **Solving Group Equations.** Let G be a group and fix $a, b \in G$.
   (a) Show that the equation $ax = b$ has a unique solution $x \in G$.
   (b) Show that the equation $ya = b$ has a unique solution $y \in G$.

4. **Matrix Groups.** Determine which of the following sets of 2×2 matrices form a group under matrix multiplication.
   (a) Matrices of the form $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ with $ac \neq b^2$.
   (b) Matrices of the form $\begin{bmatrix} a & b \\ c & a \end{bmatrix}$ with $a^2 \neq bc$.
   (c) Matrices of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ with $ac \neq 0$.
   (d) Integer matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc \neq 0$. (Check inverses!)

5. **Roots of Unity.** For a positive integer n, let $\mu_n = \{\zeta_n^k \mid k = 0, 1, \ldots, n-1\}$ where $\zeta_n = \exp(2\pi i/n)$ is the primitive n-th root of unity. These are the n-th roots of unity. Let $\mu_\infty = \bigcup_{n \geq 1} \mu_n$ be the set of all complex roots of unity of any order. Prove that μ_∞ is a group under multiplication.

6. **Product Subgroups.** If $A \leq G$ and $B \leq H$, prove that $A \times B \leq G \times H$. Find a subgroup of $\mathbb{Z} \times \mathbb{Z}$ that is not of the form $A \times B$ for subgroups $A, B \leq \mathbb{Z}$.

7. **Opposite Group.** Let $(G, \cdot)$ be a group. Define a new operation $\circ$ on G by $a \circ b = b \cdot a$. Prove that $(G, \circ)$ is a group (denoted G^{op}, called the opposite group of G).

8. **Group of Units.** Give an example of a monoid M where $M^\times$ is nontrivial. Compute $M^\times$ explicitly.

9. **Finite Subsequence Product.**

   Let G be a finite group of order n. Let $a_1, \ldots, a_n$ be any sequence of n elements in G. Prove there exist indices $1 \leq p \leq q \leq n$ such

that the product $a_p a_{p+1} \cdots a_q = 1$.

10. **Even Order Property.** Prove that in any finite group of even order, the number of elements satisfying $x^2 = 1$ is even. Deduce that there is at least one element of order 2.

11. **Classical Subgroups.** Verify the following subgroup inclusions in $\mathrm{GL}_n(F)$:
    (a) $O_n(\mathbb{R})$, $O_{p,q}(\mathbb{R})$, and $\mathrm{Sp}_{2n}(\mathbb{R})$ are subgroups of $\mathrm{GL}_n(\mathbb{R})$.
    (b) $U(n)$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$.

12. **Union of Subgroups.** Let $A, B \leq G$. Prove that $A \cup B$ is a subgroup if and only if $A \subseteq B$ or $B \subseteq A$. Use this to show a group cannot be the union of two proper subgroups.

13. **Product of Subgroups.** Let $A, B \leq G$. Let $AB = \{ab \mid a \in A, b \in B\}$. Prove that AB is a subgroup if and only if $AB = BA$.

14. **Large Subsets Product.** Let G be a finite group. Let $A, B \subseteq G$ be non-empty subsets such that $|A| + |B| > |G|$. Prove that $G = AB$. Specifically, if $|S| > |G|/2$, then every element is a product of two elements in S.

15. **Integer Subgroups.** Let $(G, \cdot)$ be a group and $g \in G$. The **cyclic subgroup generated by** g, denoted $\langle g \rangle$, is the subgroup consisting of all powers of g: $\{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\}$. If $G = \langle g \rangle$ for some element $g \in G$, then G is called a **cyclic group** generated by g.
    (a) Determine all subgroups of $\mathbb{Z}$ (under addition).

    > *Remark.*
    >
    > Show that any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \geq 0$, where $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.

    (b) Determine all subgroups of the finite cyclic group $\mathbb{Z}/n\mathbb{Z}$ (under addition modulo n).

    > *Remark.*
    >
    > Show that any subgroup of $\mathbb{Z}/n\mathbb{Z}$ is of the form $\langle \bar{d} \rangle$ where $\bar{d}$ is the residue class of d modulo n, and d divides n.

16. **Inversion Automorphism.** Prove that the map $x \mapsto x^{-1}$ is an automorphism of G if and only if G is Abelian.

17. **Product Isomorphisms.** Let G_1, G_2, G_3 be groups. Prove:
    (a) $G_1 \times G_2 \cong G_2 \times G_1$.
    (b) $(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$.

18. **Decomposition Check.** In each case, determine if $G \cong H \times K$:

(a) $G = \mathbb{R}^\times$, $H = \{\pm 1\}$, $K = \mathbb{R}_+^\times$.

(b) $G = B_n(F)$, $H = \mathrm{Diag}_n(F)$, $K = T_n(F)$.

> *Remark.*
> Do elements from H and K commute?

(c) $G = \mathbb{C}^\times$, $H = S^1$, $K = \mathbb{R}_+^\times$.

19. Q Structure. Prove that $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^\times, \cdot)$.

20. Affine Group. Let $G = \{(a, b) \in \mathbb{R}^2 \mid a \neq 0\}$ with operation $(a, b)(c, d) = (ac, ad + b)$.

(a) Prove G is a group.

(b) Show G is isomorphic to the group of matrices $\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \;\middle|\; a \neq 0 \right\}$.

21. Centralisers. Let G be a group and fix $a \in G$. Prove that the set $C_G(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G.

22. Centraliser in S_4. The centraliser of σ is the set $C(\sigma) = \{\alpha \in S_n \mid \alpha\sigma = \sigma\alpha\}$.

(a) Let $\sigma = (1\,2\,3)$ in S_4. Find all elements in $C(\sigma)$.

(b) Deduce the size of the conjugacy class of σ by counting directly or using the result from (a).

3
Cyclic Groups

In the preceding chapter, we introduced groups and subgroups. We now restrict our attention to the simplest class of groups: those generated by a single element. Despite their structural simplicity, cyclic groups serve as fundamental building blocks in the classification of finite Abelian groups and appear ubiquitously in number theory and cryptography.

3.1 Generated Subgroups

We begin by formalising the notion of a subgroup constructed from a specific subset of elements.

Definition 3.1. ***Generated Subgroup.***
Let G be a group.

1. Let $g \in G$. The **cyclic subgroup generated by** g, denoted $\langle g \rangle$, is the smallest subgroup of G containing g.
2. More generally, if $S \subseteq G$ is a subset, the **subgroup generated by** S, denoted $\langle S \rangle$, is the smallest subgroup of G containing S.

定義

Lemma 3.1. ***Intersection of Subgroups.***
Let $\{H_i\}_{i \in I}$ be a non-empty family of subgroups of G. Then $\bigcap_{i \in I} H_i$ is a subgroup of G.

引理

Proof

Let $H = \bigcap_{i \in I} H_i$. Since each H_i contains the identity, $1 \in H$. If $a, b \in H$, then $a, b \in H_i$ for every i, so $ab^{-1} \in H_i$ for every i, hence $ab^{-1} \in H$. Therefore H is a subgroup of G.

■

The term "smallest" is well-defined because the intersection of any collection of subgroups containing S is itself a subgroup containing S. Constructively, $\langle g \rangle$ consists of all possible powers of g.

Proposition 3.1. ***Structure of Cyclic Subgroups.***
For any $g \in G$,

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

命题

Proof

Let $H = \{g^k \mid k \in \mathbb{Z}\}$. First, we verify H is a subgroup.
Identity: $g^0 = 1 \in H$.
Closure: $g^i \cdot g^j = g^{i+j} \in H$ since $i + j \in \mathbb{Z}$.
Inverses: $(g^k)^{-1} = g^{-k} \in H$ since $-k \in \mathbb{Z}$.
Thus $H \leq G$. Since any subgroup containing g must contain all its integer powers by closure, H is necessarily the smallest such subgroup, so $\langle g \rangle = H$.

■

Definition 3.2. ***Cyclic Group.***
A group G is called **cyclic** if there exists an element $g \in G$ such that $G = \langle g \rangle$. Such an element g is called a **generator** of G.

定義

If a group is generated by a finite subset S, it is called a **finitely generated group**. Cyclic groups are the simplest finitely generated groups (generated by a singleton).

Note

Cyclic groups are necessarily Abelian, as $g^a g^b = g^{a+b} = g^{b+a} = g^b g^a$.

Order of an Element

The structure of the subgroup $\langle g \rangle$ depends entirely on the powers of g.

Definition 3.3. ***Order of an Element.***
The **order** of an element $g \in G$, denoted $|g|$ (some texts use $o(g)$), is the smallest positive integer k such that $g^k = 1$.
- If such a k exists, g has **finite order** k.
- If $g^k \neq 1$ for all integers $k \neq 0$, g has **infinite order**.

定義

The following lemma establishes the connection between the order of an element and modular arithmetic.

Lemma 3.2. ***Properties of Order.***
Let $g \in G$.
Finite Order: If $|g| = k$, then $g^n = 1$ if and only if $n \equiv 0 \pmod{k}$.
Consequently, $g^i = g^j \iff i \equiv j \pmod{k}$. The subgroup $\langle g \rangle$

contains exactly k distinct elements: $\{1, g, \ldots, g^{k-1}\}$.

Infinite Order: If g has infinite order, then $g^i = g^j \iff i = j$. The subgroup $\langle g \rangle$ is infinite.

引理

Proof

1. Suppose $|g| = k$. By the division algorithm, write $n = kq + r$ with $0 \leq r < k$. Then:

$$g^n = g^{kq+r} = (g^k)^q \cdot g^r = 1^q \cdot g^r = g^r.$$

   If $n \equiv 0 \pmod{k}$, then $r = 0$ and $g^n = 1$. Conversely, if $g^n = 1$, then $g^r = 1$. Since $0 \leq r < k$ and k is the *smallest* positive integer with $g^k = 1$, we must have $r = 0$. Thus $n \equiv 0 \pmod{k}$.
   For the second part, $g^i = g^j \iff g^{i-j} = 1 \iff i - j \equiv 0 \pmod{k} \iff i \equiv j \pmod{k}$. The distinct elements are therefore the residues modulo k, i.e., $\{g^0, \ldots, g^{k-1}\}$.
2. If g has infinite order, suppose $g^i = g^j$. Then $g^{i-j} = 1$. By definition, no non-zero power is the identity, so $i - j = 0$, implying $i = j$.

■

Classification of Cyclic Groups

Cyclic groups are completely classified by their order. Up to isomorphism, there is only one cyclic group of any given order n (finite or infinite).

Theorem 3.1. ***Classification of Cyclic Groups.***
Let $G = \langle g \rangle$ be a cyclic group.

1. If G is infinite, then $G \cong (\mathbb{Z}, +)$.
2. If G is finite of order n, then $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

定理

Proof

Consider the mapping $\varphi : \mathbb{Z} \to G$ defined by $\varphi(k) = g^k$. Since $g^k g^m = g^{k+m}$, this is a group homomorphism from the additive group of integers to G. Since G is generated by g, φ is surjective.
We examine the kernel:

Infinite Case: If G is infinite, g has infinite order. By *lemma 3.2*, $g^k = 1 \iff k = 0$. Thus $\ker \varphi = \{0\}$. The map is an isomorphism $\mathbb{Z} \cong G$.

Finite Case: If $|G| = n$, then $|g| = n$ (since $\langle g \rangle = G$). By *lemma 3.2*, $g^k = 1 \iff k \equiv 0 \pmod{n}$. Thus $\ker \varphi = n\mathbb{Z}$. The induced map $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G$ given by $k \pmod{n} \mapsto g^k$ is well-defined

and bijective. Thus $\mathbb{Z}/n\mathbb{Z} \cong G$.

■

This classification allows us to determine the generators and the automorphism group of any cyclic group by studying $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

Theorem 3.2. ***Structure of Generators and Automorphisms.*** Let $G = \langle g \rangle$ be a cyclic group.

Infinite Case: If G is infinite:

- The generators are g and g^{-1}.
- $\mathrm{Aut}(G) \cong \mathbb{Z}/2\mathbb{Z}$.

Finite Case: If $|G| = n$:

- The set of generators is $\{g^k \mid 1 \leq k < n, \gcd(k, n) = 1\}$.
- $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

定理

Generators.

An element $h = g^a$ generates G if and only if $g \in \langle h \rangle$. That is, there exists an integer b such that $h^b = g$, or $g^{ab} = g$.

- If G is infinite, $g^{ab} = g \implies g^{ab-1} = 1 \implies ab - 1 = 0 \implies ab = 1$. The only integer solutions are $a = \pm 1$. Thus generators are g^1 and g^{-1}.
- If $|G| = n$, $g^{ab} = g \implies ab \equiv 1 \pmod{n}$. This linear congruence has a solution for b if and only if $\gcd(a, n) = 1$.

証明終

Automorphisms.

Let $f \in \mathrm{Aut}(G)$. Since G is generated by g, f is completely determined by $f(g)$. Since f is surjective, $f(g)$ must be a generator of G.

- If G is infinite, $f(g)$ must be g or g^{-1}. Define $\psi : \mathrm{Aut}(G) \to \{1, -1\} \cong \mathbb{Z}/2\mathbb{Z}$ by $\psi(f) = 1$ if $f(g) = g$ and $\psi(f) = -1$ if $f(g) = g^{-1}$. This is an isomorphism.
- If $|G| = n$, $f(g) = g^a$ for some a with $\gcd(a, n) = 1$. Define $\psi : \mathrm{Aut}(G) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\psi(f) = a \pmod{n}$. Since $f_1(f_2(g)) = f_1(g^{a_2}) = (g^{a_1})^{a_2} = g^{a_1 a_2}$, we have $\psi(f_1 \circ f_2) = a_1 a_2 \pmod{n}$. This map is bijective and a homomorphism.

証明終

Discrete Logarithms

For a finite cyclic group G of order n with a fixed generator g, we have established an isomorphism $G \cong \mathbb{Z}/n\mathbb{Z}$. We define the inverse of the map $k \mapsto g^k$ explicitly.

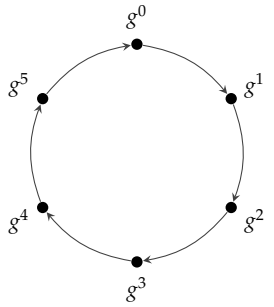


Figure 3.1: Visual representation of the cyclic group of order 6, generated by g.

Definition 3.4. ***Discrete Logarithm.***
Let $G = \langle g \rangle$ be a cyclic group of order n. For any $a \in G$, the unique integer $k \in \mathbb{Z}/n\mathbb{Z}$ such that $a = g^k$ is called the **discrete logarithm** of a with respect to g, denoted $\log_g a$.

定義

The map $\log_g : G \to \mathbb{Z}/n\mathbb{Z}$ is a group isomorphism:

$$\log_g(ab) = \log_g a + \log_g b \pmod{n}.$$

While computing g^k is computationally efficient (using repeated squaring), computing $\log_g a$ for large n is generally difficult. This asymmetry is the foundation of the **Discrete Logarithm Problem**, which underpins cryptographic protocols such as Diffie-Hellman key exchange and Elliptic Curve Cryptography.
We apply this framework to solve power equations in cyclic groups.

Proposition 3.2. ***Roots in Cyclic Groups.***
Let G be a cyclic group of order n generated by g. Let $a \in G$ and $k \in \mathbb{Z}$. The equation $x^k = a$ has solutions in G if and only if

$$\gcd(k, n) \mid \log_g a.$$

If this condition holds, there are exactly $\gcd(k, n)$ distinct solutions.

命題

Proof

Let $x = g^y$ for some unknown $y \in \mathbb{Z}/n\mathbb{Z}$. The equation $x^k = a$ becomes:

$$(g^y)^k = a \implies g^{yk} = g^{\log_g a}.$$

By *lemma 3.2*, this is equivalent to the linear congruence:

$$ky \equiv \log_g a \pmod{n}.$$

From elementary number theory, a linear congruence $Ay \equiv B \pmod{n}$ has solutions if and only if $d = \gcd(A, n)$ divides B. Here, $d = \gcd(k, n)$. Thus, solutions exist if and only if $d \mid \log_g a$.
If the condition is met, the congruence has exactly d solutions modulo n. Specifically, if y_0 is a particular solution, the set of solutions is:

$$\left\{ y_0 + t \cdot \frac{n}{d} \;\middle|\; t = 0, 1, \ldots, d-1 \right\}.$$

These correspond to d distinct elements g^y in G.

■

Example 3.1. Solving $x^k = a$. Consider $G = \mathbb{Z}/13\mathbb{Z}^\times$, which is cyclic of order $n = 12$. A generator is $g = 2$.

範例

Solution

We solve $x^3 = 5$ in G.

1. Compute discrete logs: We need $\log_2 5$. Powers of 2 mod 13 are: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 3, 2^5 = 6, 2^6 = 12, 2^7 = 11, 2^8 = 9, 2^9 = 5$. So $\log_2 5 = 9$.
2. Setup congruence: $3y \equiv 9 \pmod{12}$.
3. Check solvability: $\gcd(3, 12) = 3$. Since $3 \mid 9$, solutions exist. There are 3 solutions.
4. Solve: $3y = 9 + 12k \implies y = 3 + 4k$. The solutions modulo 12 are $y \in \{3, 7, 11\}$.
5. Map back to group: $x \in \{2^3, 2^7, 2^{11}\} \pmod{13} \implies x \in \{8, 11, 7\}$.

■

3.2 *Cosets and Lagrange's Theorem*

We now investigate the internal structure of groups by partitioning them relative to a subgroup. This decomposition leads to Lagrange's Theorem, a fundamental result connecting the order of a finite group to the orders of its subgroups.

Coset Decomposition

Let H be a subgroup of G. The group operation allows us to translate H by an element $g \in G$, generating a "shifted" version of the subgroup.

Definition 3.5. ***Cosets.***
Let $H \leq G$ and $g \in G$.

- The set $gH = \{gh \mid h \in H\}$ is called the **left coset** of H in G determined by g.
- The set $Hg = \{hg \mid h \in H\}$ is called the **right coset** of H in G determined by g.

定義

The element g is called a **representative** of the coset.

Lemma 3.3. ***Properties of Cosets.***
Let $H \leq G$.

1. Two left cosets aH and bH are either identical or disjoint.
2. $aH = bH$ if and only if $b^{-1}a \in H$.
3. There is a bijection between any two left cosets aH and bH. Thus, all cosets have the same cardinality as H.

Similar properties hold for right cosets, with the equality condition $ab^{-1} \in$

H.

引理

Proof

1. Suppose $aH \cap bH \neq \varnothing$. Let $x \in aH \cap bH$. Then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$. This implies $b^{-1}a = h_2 h_1^{-1} \in H$. For any element $ah \in aH$, we have

$$ah = b(b^{-1}a)h = b(h_2 h_1^{-1})h \in bH.$$

   Thus $aH \subseteq bH$. By symmetry, $bH \subseteq aH$, so $aH = bH$.
2. We just showed $aH \cap bH \neq \varnothing \implies b^{-1}a \in H \implies aH = bH$. Conversely, if $aH = bH$, then $a = a \cdot 1 \in aH = bH$, so $a = bh$ for some h, implying $b^{-1}a \in H$.
3. Define $f : aH \to bH$ by $f(ah) = bh$. Its inverse is $g : bH \to aH$ defined by $g(bh) = ah$. Thus $|aH| = |bH| = |H|$.

■

These properties imply that the left cosets of H form a partition of G.

$$G = \bigsqcup_{i \in I} g_i H.$$

The set of representatives $\{g_i\}_{i \in I}$ is called a **transversal** or a system of coset representatives.

Definition 3.6. ***Index of a Subgroup.***
The number of distinct left cosets of H in G is called the **index** of H in G, denoted $[G : H]$ or $(G : H)$.

定義

It is a standard result (see *lemma 3.4* below) that the number of left cosets equals the number of right cosets, so the index is well-defined regardless of the side chosen.

Lemma 3.4. ***Correspondence of Representatives.***
If $\{g_i\}_{i \in I}$ is a set of left coset representatives for H in G, then $\{g_i^{-1}\}_{i \in I}$ is a set of right coset representatives for H in G. Thus, $[G : H]$ is the same for left and right cosets.

引理

Proof

Consider the map $\psi : \{gH\} \to \{Hg^{-1}\}$ defined by $gH \mapsto (gH)^{-1} = Hg^{-1}$. This is a bijection because inversion is a bijection on G. Thus the cardinalities of the set of left cosets and the set of right cosets are equal.

■

Lagrange's Theorem

The partition of G into disjoint cosets of equal size yields one of the most important counting theorems in finite group theory.

Theorem 3.3. ***Lagrange's Theorem.***
If G is a finite group and $H \leq G$, then

$$|G| = |H| \cdot [G : H].$$

In particular, the order of a subgroup divides the order of the group.

定理

Proof

Let $k = [G : H]$. Let $g_1H, \ldots, g_kH$ be the distinct left cosets. Since these partition G:

$$G = \bigsqcup_{i=1}^{k} g_iH.$$

Since $|g_iH| = |H|$ for all i, we sum the cardinalities:

$$|G| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k \cdot |H|.$$

■

This theorem has immediate and powerful corollaries concerning the structure of finite groups.

Corollary 3.1. *Order of Elements.* Let G be a finite group. For any $g \in G$, the order $|g|$ divides $|G|$. Consequently, $g^{|G|} = 1$.

推論

Proof

The order of g is the order of the cyclic subgroup $\langle g \rangle$. By Lagrange's Theorem, $|\langle g \rangle|$ divides $|G|$. Thus $|G| = k \cdot |g|$ for some integer k, and $g^{|G|} = (g^{|g|})^k = 1^k = 1$.

■

Corollary 3.2. *Groups of Prime Order.* If $|G| = p$ where p is a prime number, then G is cyclic and $G \cong \mathbb{Z}/p\mathbb{Z}$. It has no non-trivial proper subgroups.

推論

Proof

Let $g \in G$ with $g \neq 1$. The order $|g|$ divides p. Since p is prime and $|g| > 1$, we must have $|g| = p$. Thus $\langle g \rangle$ contains p elements, so $\langle g \rangle = G$.

■

Corollary 3.3. *Fermat's Little Theorem.* Let p be a prime and a be an integer not divisible by p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

推論

Proof

Consider the multiplicative group of integers modulo p, denoted $(\mathbb{Z}/p\mathbb{Z})^\times$. This group has order $p - 1$. The residue class of a is an element of this group. By the corollary on element orders, $a^{|(\mathbb{Z}/p\mathbb{Z})^\times|} = 1$ in the group, which translates to $a^{p-1} \equiv 1 \pmod{p}$.

■

Lagrange's Theorem also helps classify subgroups of cyclic groups, providing a converse to the theorem for this specific case.

Corollary 3.4. *Subgroups of Cyclic Groups.* Let G be a cyclic group of order n. For every positive divisor $d \mid n$, there exists a unique subgroup of order d. This subgroup is cyclic.

推論

Let $G = \langle g \rangle$.

Existence.

Let $k = n/d$. Consider $h = g^k$. The order of h is $n/\gcd(k, n) = n/k = d$. Thus $\langle h \rangle$ is a subgroup of order d.

証明終

Uniqueness.

Let H be any subgroup of order d. Since G is cyclic, every subgroup of G is cyclic (proof below), so $H = \langle g^a \rangle$ for some a. The order of H is $n/\gcd(a, n) = d$, implying $\gcd(a, n) = n/d = k$. Since $k \mid a$, we have $g^a \in \langle g^k \rangle$, so $H \subseteq \langle g^k \rangle$. Since both have order d, they must be equal.

証明終

Lemma 3.5. ***Subgroups of Cyclic Groups Are Cyclic.*** Let $G = \langle g \rangle$ be a cyclic group and let $H \leq G$. If $H \neq \{1\}$, let m be the smallest positive integer such that $g^m \in H$. Then $H = \langle g^m \rangle$, so H is cyclic.

引理

Proof

Since H is non-empty, choose $h \in H$ with $h \neq 1$. Write $h = g^k$. By

the division algorithm, $k = qm + r$ with $0 \leq r < m$. Then

$$g^r = g^{k-qm} = g^k (g^m)^{-q} \in H.$$

By minimality of m, we must have $r = 0$, so $m \mid k$ and $g^k \in \langle g^m \rangle$. Hence $H \subseteq \langle g^m \rangle$, and the reverse inclusion is obvious.

■

This leads to a classic number-theoretic identity involving Euler's totient function φ.

Definition 3.7. ***Euler's Totient Function.***
For a positive integer n, the function $\varphi(n)$ denotes the number of integers in $\{1, 2, \ldots, n\}$ that are coprime to n.

定義

Corollary 3.5. *Totient Sum Identity.* For any positive integer n,

$$n = \sum_{d|n} \varphi(d).$$

推論

Proof

In a cyclic group of order n, every element generates a unique cyclic subgroup of some order d where $d \mid n$. The number of elements generating a specific subgroup of order d is $\varphi(d)$ (the number of generators of $\mathbb{Z}/d\mathbb{Z}$). Since every element belongs to exactly one such set of generators, summing $\varphi(d)$ over all divisors d counts every element in the group exactly once.

■

Index Multiplicativity

The index acts multiplicatively across chains of subgroups.

Theorem 3.4. ***Multiplicativity of the Index.***
Let $K \leq H \leq G$ be groups with finite indices. Then

$$[G : K] = [G : H] \cdot [H : K].$$

定理

Proof

Let $\{g_i\}_{i \in I}$ be coset representatives for H in G, so $G = \bigsqcup_{i \in I} g_i H$. Let $\{h_j\}_{j \in J}$ be coset representatives for K in H, so $H = \bigsqcup_{j \in J} h_j K$. Substi-

tuting the decomposition of H into that of G:

$$G = \bigsqcup_{i \in I} g_i \left(\bigsqcup_{j \in J} h_j K \right) = \bigcup_{(i,j) \in I \times J} g_i h_j K.$$

We verify these cosets are disjoint. Suppose $g_i h_j K = g_{i'} h_{j'} K$. Then $g_i h_j \in g_{i'} h_{j'} K \subseteq g_{i'} H$. Thus $g_i H \cap g_{i'} H \neq \varnothing$, which implies $i = i'$ (since g_i are distinct representatives). We cancel g_i to get $h_j K = h_{j'} K$, which implies $j = j'$. Thus, the set $\{g_i h_j\}$ is a transversal for K in G, and its size is $|I| \cdot |J| = [G : H] \cdot [H : K]$.

■

Product of Subgroups

We conclude with counting results for products of subgroups, which are not necessarily subgroups themselves.

Proposition 3.3. ***Order of Products.***
Let H and K be finite subgroups of G. The size of the set $HK = \{hk \mid h \in H, k \in K\}$ is given by:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

命題

Proof

Consider the map $f : H \times K \to HK$ defined by $(h, k) \mapsto hk$. This map is surjective. We determine the size of the fibre for any $x \in HK$. Let $x = h_0 k_0$. Suppose $hk = h_0 k_0$. Then $h_0^{-1} h = k_0 k^{-1}$. Let this element be u. Since $u \in H$ (LHS) and $u \in K$ (RHS), $u \in H \cap K$. Thus $h = h_0 u$ and $k = u^{-1} k_0$. Conversely, for any $u \in H \cap K$, $(h_0 u)(u^{-1} k_0) = h_0 k_0$. Therefore, every element in HK arises from exactly $|H \cap K|$ pairs in $H \times K$.

■

Theorem 3.5. ***Index Inequalities.***
Let $H, K \leq G$.

$$[G : H \cap K] \leq [G : H] \cdot [G : K].$$

Equality holds if and only if $HK = G$. If $[G : H]$ and $[G : K]$ are coprime, then $[G : H \cap K] = [G : H][G : K]$.

定理

Proof

By the index formula, $[G : H \cap K] = [G : H][H : H \cap K]$. We claim $[H : H \cap K] \leq [G : K]$. Consider the map $\varphi : h(H \cap$

$K) \mapsto hK$ from the left cosets of $H \cap K$ in H to the left cosets of K in G. If $h_1(H \cap K) = h_2(H \cap K)$, then $h_2^{-1}h_1 \in H \cap K \subseteq K$, so $h_1K = h_2K$. The map is well-defined and injective. Thus $[H : H \cap K] \leq [G : K]$. Multiplying by $[G : H]$ gives the result. Equality in the injection corresponds to surjectivity of cosets, which implies $HK = G$.

■

3.3 *Exercises*

1. **Order Calculation.** Let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ be matrices in $\mathrm{GL}_2(\mathbb{R})$.
   (a) Find the orders of A and B.
   (b) Compute the products AB and BA. Find their orders.
   (c) Observe that A and B have finite order, but their product may not. What does this imply about the set of elements of finite order in a non-Abelian group?
2. **Involutions.** Prove that an element $a \in G$ has order ≤ 2 if and only if $a = a^{-1}$.
3. **Commutativity via Order Relations.** Let $a, b \in G$. Suppose $|a| = 7$ and $a^3b = ba^3$. Prove that $ab = ba$.

   Note that $\gcd(3,7) = 1$. Can you express a as a power of a^3?
4. **Order Invariance.** Let $a, b \in G$. Prove:
   (a) $|a| = |a^{-1}|$.
   (b) $|ab| = |ba|$.
5. **Homomorphisms and Order.** Let $f : G \to H$ be a group homomorphism. If $g \in G$ has finite order, prove that $|f(g)|$ divides $|g|$.
6. **Product of Elements.**
   (a) Let G be a finite Abelian group. Prove that the product of all elements in G is equal to the product of all elements of order ≤ 2. Specifically:
   $$\prod_{g \in G} g = \prod_{a \in G, a^2 = 1} a.$$
   (b) Use this to prove **Wilson's Theorem**: If p is a prime, $(p-1)! \equiv -1 \pmod{p}$.
7. **Elements of Finite Order.**
   (a) Let G be an Abelian group. Let H be the set of elements of finite order. Prove that H is a subgroup of G (called the torsion subgroup).

(b) Show by counterexample that this is false for non-Abelian groups.

8. **Power Automorphisms.** Let G be a finite Abelian group of odd order. Consider the map $\varphi : G \to G$ defined by $\varphi(x) = x^2$.
   (a) Prove that φ is an automorphism.
   (b) Generalize: For which integers k is $x \mapsto x^k$ an automorphism?

9. **Function Group.** Let $f(x) = 1/x$ and $g(x) = (x-1)/x$ be functions on $\mathbb{R} \setminus \{0, 1\}$. Prove that the group generated by f and g under composition is isomorphic to S_3 (or D_3).

10. **Subgroups of $\mathbb{Q}$ and S^1.**
    (a) Let $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ be the unit circle in the complex plane, which forms a group under complex multiplication. Prove that every finite subgroup of S^1 is cyclic.
    (b) Prove that the additive group $\mathbb{Q}$ is not cyclic, but every finitely generated subgroup of it is cyclic.
    (c) For a fixed prime p, let $G = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \geq 0\}$ be the quasicyclic group (Prüfer p-group). This is the union of all cyclic groups μ_{p^n} of p^n-th roots of unity for $n \geq 0$. Prove that every proper subgroup of G is finite and cyclic.

11. **Product of Cyclic Subgroups.** Let $a, b \in G$ be commuting elements with orders n and m respectively. If $\gcd(n, m) = 1$, prove that $\langle ab \rangle$ is a cyclic subgroup of order mn.

12. **Uniqueness Implies Cyclicity.** Let G be a finite group of order n. Prove that if for every divisor $d \mid n$, there is at most one subgroup of order d, then G is cyclic.

13. **Index Properties.** Give an example of an infinite group where every non-trivial subgroup has finite index.

14. **Computing Automorphism Groups.**
    (a) Find $\mathrm{Aut}(\mathbb{Z})$.
    (b) Find the group $\mathrm{Aut}(\mathbb{Z}/20\mathbb{Z})$. List its elements.
    (c) Find $\mathrm{Aut}(V_4)$ where V_4 is the Klein four-group.
    (d) Find the set of endomorphisms $\mathrm{End}(\mathbb{Z}/20\mathbb{Z})$ and describe the structure of this set under pointwise addition and composition.

15. **Orders in Cyclic Groups.** Let G be cyclic of order n.
    (a) Show that for each divisor $d \mid n$, there are exactly $\varphi(d)$ elements of order d in G.
    (b) Use this to re-derive the identity $n = \sum_{d \mid n} \varphi(d)$.

16. **Coprime Intersection.** If $H, K \leq G$ have coprime orders $((|H|, |K|) =$

1), prove that $H \cap K = \{1\}$.

17. **Double Cosets.** Let $H, K \leq G$. The set $HgK = \{hgk \mid h \in H, k \in K\}$ is called a double coset. Prove that:

$$|HgK| = \frac{|H| \cdot |K|}{|g^{-1}Hg \cap K|}.$$

18. **Affine Solution Space.** Let W be the kernel of a linear map A (a subgroup of vector space V). Prove that the solution set to $Ax = b$ is a coset of W.

19. **Matrix Subgroups.**
    (a) Prove that the set of invertible diagonal matrices in $\mathrm{GL}_n(F)$ is a subgroup isomorphic to $(F^\times)^n$.
    (b) Prove that the set $T_n(F)$ of upper triangular matrices with 1s on the diagonal is a subgroup of $\mathrm{GL}_n(F)$.

4
Normal Subgroups and Quotient Groups

In the previous chapter, we analysed the structure of a group G by decomposing it into disjoint cosets relative to a subgroup H. We now investigate whether the set of these cosets, denoted G/H, inherits a group structure from G. This construction parallels the theory of vector spaces, where the quotient of a space V by a subspace W yields the quotient space V/W.

4.1 Normal Subgroups

Let H be a subgroup of G. We wish to define a binary operation on the set of left cosets $G/H = \{gH \mid g \in G\}$ using the operation of G. The natural candidate for the product of two cosets aH and bH is the coset containing the product of their representatives:

$$(aH) \cdot (bH) = (ab)H.$$

However, for this to be a well-defined operation on sets (where $A \cdot B = \{ab \mid a \in A, b \in B\}$), we require the set equality $aHbH = abH$. Expanding the set product, we require that for any $h_1, h_2 \in H$, there exists $h \in H$ such that

$$ah_1bh_2 = abh.$$

Simplifying, this implies $h_1 b = b(hh_2^{-1})$. Since h_1 and h_2 are arbitrary, this condition is equivalent to requiring $b^{-1}Hb \subseteq H$ for all $b \in G$. This motivates the following definitions regarding invariance under conjugation.

Definition 4.1. ***Conjugacy.***
Let G be a group.

1. Let $x, g \in G$. The element gxg^{-1} is called the **conjugate** of x by g.
2. Two elements x, y are conjugate if there exists $g \in G$ such that $y = gxg^{-1}$. This defines an equivalence relation on G.

定義

Definition 4.2. ***Normal Subgroup.***
A subgroup N of G is called a **normal subgroup**, denoted $N \trianglelefteq G$, if it is invariant under conjugation by any element of G. That is:

$$gNg^{-1} = N \quad \text{for all } g \in G.$$

定義

It follows immediately that $N \trianglelefteq G$ if and only if $gNg^{-1} \subseteq N$ for all $g \in G$, or equivalently, if $gN = Ng$ for all $g \in G$ (left cosets equal right cosets).

Example 4.1. Abelian Groups. If G is Abelian, then for any $g, x \in G$, we have $gxg^{-1} = xgg^{-1} = x$. Thus, every subgroup of an Abelian group is normal.

範例

Example 4.2. The Centre of a Group. The **centre** of a group G, denoted $Z(G)$, is the set of elements that commute with every element of G:

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

An element lies in the centre if and only if its conjugacy class contains only itself. $Z(G)$ is always a normal subgroup of G.

範例

A fundamental source of normal subgroups arises from group homomorphisms.

Definition 4.3. ***Kernel and Image.***
Let $\varphi : G \to H$ be a group homomorphism.
1. The **kernel** of φ is $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$.
2. The **image** of φ is $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\}$.

定義

Proposition 4.1. ***Normality of the Kernel.***
Let $\varphi : G \to H$ be a group homomorphism. Then $\ker \varphi$ is a normal subgroup of G, and $\operatorname{im} \varphi$ is a subgroup of H.

命題

Proof

We first verify the subgroup properties. Since $\varphi(1_G) = 1_H$, $1_G \in \ker \varphi$. Let $a, b \in \ker \varphi$. Then $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1_H \cdot 1_H^{-1} = 1_H$. Thus $ab^{-1} \in \ker \varphi$. To check normality, let $n \in \ker \varphi$ and $g \in G$. Then:

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g) \cdot 1_H \cdot \varphi(g)^{-1} = 1_H.$$

Thus $gng^{-1} \in \ker\varphi$, so $\ker\varphi \trianglelefteq G$. The proof that $\operatorname{im}\varphi \leq H$ follows directly from the homomorphism property $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1}$. ■

Example 4.3. Special Linear Group. The determinant map $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ is a homomorphism. Its kernel is the special linear group $\mathrm{SL}_n(\mathbb{C})$. Therefore, $\mathrm{SL}_n(\mathbb{C}) \trianglelefteq \mathrm{GL}_n(\mathbb{C})$.

範例

When N is a normal subgroup, the arithmetic of cosets becomes well-behaved.

Definition 4.4. ***Quotient Group.***
Let $N \trianglelefteq G$. The **quotient group** of G by N, denoted G/N, is the set of all cosets $\{gN \mid g \in G\}$ equipped with the operation:

$$(aN)(bN) = (ab)N.$$

定義

We denote the class aN by $\bar{a}$. The operation is then $\bar{a} \cdot \bar{b} = \overline{ab}$. The identity element of G/N is $\overline{1} = 1N = N$, and the inverse of $\bar{a}$ is $\overline{a^{-1}}$. Associated with any normal subgroup is the canonical projection map. Let $\pi : G \to G/N$ be defined by $\pi(g) = gN$. Then π is a surjective homomorphism with $\ker\pi = N$. This leads to a useful characterisation: normal subgroups are precisely the kernels of group homomorphisms.

Example 4.4. Projective Linear Groups.

1. The centre of the general linear group $\mathrm{GL}_n(F)$ consists of scalar matrices $Z = \{\lambda I_n \mid \lambda \in F^\times\}$. The quotient group

   $$\mathrm{PGL}_n(F) = \mathrm{GL}_n(F)/Z$$

   is called the **projective general linear group**.

2. Similarly, the centre of $\mathrm{SL}_2(\mathbb{Z})$ is $\{\pm I_2\}$. The quotient

   $$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I_2\}$$

   is the **modular group**, a central object in number theory and geometry.

範例

4.2 *The Isomorphism Theorems*

The relationship between homomorphisms, normal subgroups, and quotients is encapsulated in the Fundamental Homomorphism Theo-

rem (often called the First Isomorphism Theorem).

Theorem 4.1. ***Fundamental Homomorphism Theorem.***
Let $\varphi : G \to H$ be a group homomorphism. Then the map $\overline{\varphi} : G/\ker\varphi \to \operatorname{im}\varphi$ defined by

$$\overline{\varphi}(g\ker\varphi) = \varphi(g)$$

is a group isomorphism. Consequently,

$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

定理

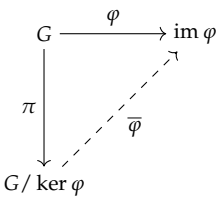


Figure 4.1: Commutative diagram for the Fundamental Homomorphism Theorem. The map φ factors through the quotient.

Let $K = \ker\varphi$.

Well-defined.

Suppose $\bar{g}_1 = \bar{g}_2$. Then $g_1K = g_2K$, implies $g_2 = g_1k$ for some $k \in K$.

$$\varphi(g_2) = \varphi(g_1k) = \varphi(g_1)\varphi(k) = \varphi(g_1)\cdot 1 = \varphi(g_1).$$

Thus the definition is independent of the representative.

証明終

Homomorphism.

$$\overline{\varphi}(\bar{g}_1\bar{g}_2) = \overline{\varphi}(\overline{g_1g_2}) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(\bar{g}_1)\overline{\varphi}(\bar{g}_2).$$

証明終

Injectivity.

$$\overline{\varphi}(\bar{g}) = 1_H \implies \varphi(g) = 1_H \implies g \in K \implies \bar{g} = K = 1_{G/K}.$$

Since the kernel of $\overline{\varphi}$ is trivial, it is injective.

証明終

Surjectivity.

By definition, for any $h \in \operatorname{im}\varphi$, there exists $g \in G$ such that $\varphi(g) = h$. Then $\overline{\varphi}(\bar{g}) = h$.

証明終

Corollary 4.1. *Criteria for Injectivity and Surjectivity.* Let $\varphi : G \to H$ be a homomorphism.

1. φ is injective if and only if $\ker\varphi = \{1\}$.
2. φ is surjective if and only if $G/\ker\varphi \cong H$.

推論

Example 4.5. The Circle Group. Consider the map $\varphi : (\mathbb{R}, +) \to S^1$ given by $x \mapsto e^{2\pi i x}$. This is a surjective homomorphism. The kernel is the set of integers $\mathbb{Z}$. By the Fundamental Homomorphism Theorem:

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

範例

Example 4.6. Principal Congruence Subgroups. Let N be a positive integer. The reduction homomorphism $\varphi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is given by:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a \bmod N & b \bmod N \\ c \bmod N & d \bmod N \end{bmatrix}.$$

This map is surjective (a non-trivial number-theoretic result). Its kernel is the **principal congruence subgroup** of level N:

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{array}{ll} a \equiv d \equiv 1 & (\mathrm{mod}\ N) \\ b \equiv c \equiv 0 & (\mathrm{mod}\ N) \end{array} \right\}.$$

Thus, $\Gamma(N) \trianglelefteq \mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Furthermore, for $N > 2$, the intersection of $\Gamma(N)$ with the centre $\{\pm I_2\}$ is trivial. Thus $\Gamma(N)$ embeds injectively into the modular group $\mathrm{PSL}_2(\mathbb{Z})$.

範例

The structure of the subgroups of a quotient group G/N is perfectly mirrored by the subgroups of G that contain N.

Theorem 4.2. ***Correspondence Theorem.***
Let $N \trianglelefteq G$. Let $\mathcal{M}$ be the set of subgroups of G containing N, and let $\overline{\mathcal{M}}$ be the set of subgroups of G/N. There is a one-to-one correspondence between $\mathcal{M}$ and $\overline{\mathcal{M}}$ given by:

$$M \mapsto M/N = \{mN \mid m \in M\}.$$

The inverse map is $\overline{M} \mapsto \{g \in G \mid gN \in \overline{M}\}$.

定理

Proof

Since $N \trianglelefteq G$, it is normal in any subgroup M containing it, so M/N is a well-defined subgroup of G/N. Conversely, if $\overline{M} \leq G/N$, let M be its preimage under the projection $\pi : G \to G/N$. Since π is a homomorphism, the preimage of a subgroup is a subgroup. Since $\overline{1} \in \overline{M}$, $N = \ker \pi \subseteq M$. The bijection follows from the definition of set preimages.

■

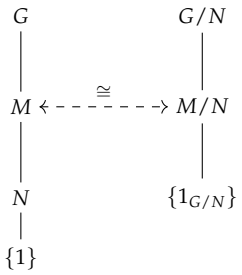


Figure 4.2: The Lattice Correspondence. Subgroups of G containing N correspond to subgroups of G/N.

We conclude with two isomorphism theorems that describe the interaction of subgroups with quotients.

Theorem 4.3. ***Second Isomorphism Theorem.***
Let $H \leq G$ and $N \trianglelefteq G$. Then $H \cap N \trianglelefteq H$, and

$$NH/N \cong H/(H \cap N).$$

定理

Proof

Note first that $NH = \{nh \mid n \in N, h \in H\}$ is a subgroup of G because N is normal (see previous chapter results on products NK). Also $N \trianglelefteq NH$. Define the homomorphism $\varphi : H \to NH/N$ by $\varphi(h) = hN$. This is surjective because any element of NH/N is of the form $nhN = hN = \varphi(h)$. The kernel is:

$$\ker \varphi = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N.$$

The result follows from the Fundamental Homomorphism Theorem.

■

Theorem 4.4. ***Third Isomorphism Theorem.***
Let N, M be normal subgroups of G with $N \leq M$. Then $M/N \trianglelefteq G/N$ and

$$(G/N)/(M/N) \cong G/M.$$

定理

Proof

Define $\varphi : G/N \to G/M$ by $\varphi(gN) = gM$. This is well-defined because $N \leq M$ (if $gN = g'N$, then $g^{-1}g' \in N \subseteq M$, so $gM = g'M$). The map is clearly a surjective homomorphism. The kernel is:

$$\ker \varphi = \{gN \in G/N \mid gM = M\} = \{gN \mid g \in M\} = M/N.$$

Applying the Fundamental Homomorphism Theorem yields the isomorphism.

■

4.3 *Exercises*

1. **Affine Group Quotient.** Let $G = \{(a, b) \mid a \in \mathbb{R}^\times, b \in \mathbb{R}\}$ with the operation $(a, b)(c, d) = (ac, ad + b)$. Let $K = \{(1, b) \mid b \in \mathbb{R}\}$.
   (a) Prove that K is a normal subgroup of G.
   (b) Prove that $G/K \cong \mathbb{R}^\times$.

2. **Positive Determinant Subgroup.** Let $H = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A > 0\}$. Prove that $H \trianglelefteq \mathrm{GL}_n(\mathbb{R})$. Identify the quotient group $\mathrm{GL}_n(\mathbb{R})/H$.

3. **Normality Transitivity.** Let $N \trianglelefteq M \trianglelefteq G$.
   (a) If $N \trianglelefteq G$, prove that $N \trianglelefteq M$ (trivial, but verify).
   (b) Is N necessarily normal in G? Provide a counterexample (e.g., in D_4 or S_4).

4. **Structural Properties.**
   (a) Prove that the center $Z(G)$ is always a normal subgroup of G.
   (b) Prove that any subgroup $H \leq G$ of index 2 (i.e., $[G : H] = 2$) is normal.

5. **Product Normality.** Let G, G' be groups. Prove that $G \times \{1\}$ is a normal subgroup of $G \times G'$, and $(G \times G')/(G \times \{1\}) \cong G'$.

6. **Cyclic Quotient Implies Abelian.** Prove that if $G/Z(G)$ is cyclic, then G is Abelian.

7. **Direct Product Centers.** Let $G = G_1 \times \cdots \times G_n$.
   (a) Prove that $Z(G) = Z(G_1) \times \cdots \times Z(G_n)$.
   (b) Prove that G is Abelian if and only if each factor G_i is Abelian.

8. **Inner Automorphisms.** For $x \in G$, define $\sigma_x : G \to G$ by $\sigma_x(g) = xgx^{-1}$.
   (a) Prove that σ_x is an automorphism of G (called an inner automorphism).
   (b) Let $\mathrm{Inn}(G) = \{\sigma_x \mid x \in G\}$. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.
   (c) Prove that $\mathrm{Inn}(G) \cong G/Z(G)$.

9. **Preimage of Image.** Let $f : G \to H$ be a homomorphism with kernel K. Let $M \leq G$. Prove that $f^{-1}(f(M)) = KM$.

10. **Commuting Normal Subgroups.** Let $M, N \trianglelefteq G$ such that $M \cap N = \{1\}$. Prove that for any $m \in M$ and $n \in N$, $mn = nm$.

    Consider $mnm^{-1}n^{-1}$ and which subgroup this belongs to.

11. **Coprime Order Element.** Let $N \trianglelefteq G$. Let $g \in G$ be an element whose order is finite and coprime to $|G/N|$. Prove that $g \in N$.

12. **Correspondence Theorem.** Let $\varphi : G \to G'$ be a surjective homomorphism. Prove that the mapping $H \mapsto \varphi(H)$ is a bijection between the set of subgroups of G containing $\ker \varphi$ and the set of subgroups of G'. Show that normal subgroups map to normal subgroups.

5
Group Actions and More Permutations

The structure of algebraic objects is often revealed through their interaction with other sets. From an algebraic point of view, the action of a group on a set is a fundamental method for studying both the group and the set.
We formalise the concept of a group 'moving' or permuting the elements of a set.

5.1 Group Actions

Definition 5.1. ***Group Action.***
Let X be a set and G be a group. A (left) **action** of G on X is a map

$$G \times X \to X, \quad (g, x) \mapsto g \cdot x,$$

satisfying the following two axioms.

定義

Axiom 4. ***Identity.***
For all $x \in X$, $1 \cdot x = x$.

公理

Axiom 5. ***Associativity.***
For all $x \in X$ and $g, h \in G$, $g \cdot (h \cdot x) = (gh) \cdot x$.

公理

A set X equipped with such an action is called a G**-set**.

The Symmetric Group Revisited

The most immediate example of a group action is the symmetric group acting on its index set. The symmetric group S_n acts naturally on $X_n = \{1, \ldots, n\}$ via function evaluation:

$$\sigma \cdot i = \sigma(i).$$

This action is fundamental; indeed, any action of a group G on a set X induces a homomorphism from G to the symmetric group S_X.

However, S_n also acts on itself in a manner distinct from simple multiplication: the action of **conjugation**. Defined by $g \cdot x = gxg^{-1}$, this action partitions the group into disjoint subsets called conjugacy classes.

Remark.

Recall from *chapter 1* that conjugation preserves cycle structure (*Lemma 1.2*), and that two permutations are conjugate in S_n if and only if they have the same cycle structure.

Visualising Conjugacy Classes

Cycle structure can be encoded by a partition of n (for example, the cycle structure $(1\,2\,3)(4)$ corresponds to $3+1$), and these partitions can be visualised using Young diagrams (or Ferrers diagrams).

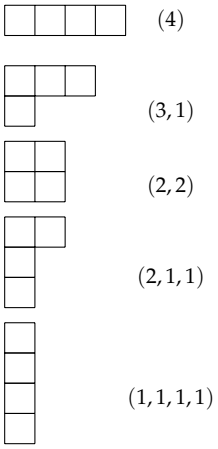


Figure 5.1: Young diagrams for the partitions of $n = 4$. Each diagram corresponds to one conjugacy class in S_4.

5.2 *Alternative Definition of Sign*

In *chapter 1* we developed the sign of a permutation from its cycle structure. Here is a different viewpoint: we recover the sign from an action of S_n on a polynomial ring.
Let $P_n = \mathbb{Z}[x_1, \ldots, x_n]$ be the set of polynomials in n variables with integer coefficients (equipped with standard addition and multiplication). We define an action of S_n on P_n by permuting the variables' indices. For $\sigma \in S_n$ and $f \in P_n$:

$$\sigma(f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Lemma 5.1. ***Action Properties.***
This operation defines a left group action of S_n on P_n. That is:

1. $1(f) = f$.
2. $\sigma(\tau(f)) = (\sigma\tau)(f)$ for all $\sigma, \tau \in S_n$.
3. It preserves algebraic structure: $\sigma(f+g) = \sigma(f) + \sigma(g)$ and $\sigma(fg) = \sigma(f)\sigma(g)$.

引理

Proof

1. The identity permutation does not change the variables, so $1(f)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$.
2. We verify the composition law. Let $g = \tau(f)$, so $g(y_1, \ldots, y_n) = f(y_{\tau(1)}, \ldots, y_{\tau(n)})$. Then

$$\sigma(g)(x_1, \ldots, x_n) = g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Let $y_i = x_{\sigma(i)}$. The k-th argument passed to f in the definition of g is $y_{\tau(k)}$, which equals $x_{\sigma(\tau(k))}$. Thus $\sigma(\tau(f))(x_\cdot) = f(x_{\sigma\tau(\cdot)})$,

which is exactly $(\sigma\tau)(f)$.

3. Both identities follow from substitution: replacing variables respects addition and multiplication in P_n.

■

Consider the **discriminant polynomial**:

$$\Delta(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

For any $\sigma \in S_n$, applying σ to Δ permutes the factors $(x_i - x_j)$. Since Δ is a product of distinct linear factors, $\sigma(\Delta)$ must be $\pm\Delta$.

Theorem 5.1. ***The Sign Homomorphism.***
There exists a unique group homomorphism $\varepsilon : S_n \to \{1, -1\}$ such that $\varepsilon(\tau) = -1$ for every transposition τ.

定理

Proof

Define $\varepsilon(\sigma) \in \{1, -1\}$ by the rule

$$\sigma(\Delta) = \varepsilon(\sigma)\Delta.$$

This is well-defined since $\sigma(\Delta)$ is obtained by permuting the factors of Δ and possibly changing the sign of some factors.
Now use the action law on Δ:

$$(\sigma\tau)(\Delta) = \sigma(\tau(\Delta)) = \sigma(\varepsilon(\tau)\Delta) = \varepsilon(\tau)\sigma(\Delta) = \varepsilon(\tau)\varepsilon(\sigma)\Delta.$$

By uniqueness of the coefficient of Δ, we get $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, so ε is a homomorphism.
Let $\tau = (k\,l)$ be a transposition. In $\tau(\Delta)$, every factor not involving x_k or x_l is unchanged. For each $m \notin \{k, l\}$, the pair of factors $(x_k - x_m)$ and $(x_l - x_m)$ is swapped; since multiplication in P_n is commutative, this swap does not change the product. The remaining factor $(x_k - x_l)$ becomes $(x_l - x_k) = -(x_k - x_l)$. Hence $\tau(\Delta) = -\Delta$, so $\varepsilon(\tau) = -1$.
For uniqueness, transpositions generate S_n, so a homomorphism is determined by its values on them.

■

The homomorphism ε agrees with the usual parity sign: by definition it sends each transposition to -1, and any permutation is a product of transpositions. Thus $\varepsilon(\sigma) = 1$ exactly for even permutations, and $\varepsilon(\sigma) = -1$ for odd permutations.

5.3 *The Alternating Group*

Since ε is a homomorphism, its kernel is a normal subgroup of S_n.
We write

$$A_n := \ker(\varepsilon) = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}.$$

In *chapter 2* we showed that kernels are normal; in *chapter 4* we also developed the fundamental homomorphism theorem, and one consequence is that $|S_n : A_n| = 2$ for $n \geq 2$, hence $|A_n| = n!/2$.
Just as S_n is generated by transpositions, A_n is generated by the simplest even permutations: 3-cycles.

Lemma 5.2. ***Generators of*** A_n**.**
For $n \geq 3$, the alternating group A_n is generated by 3-cycles.

引理

Proof

Any $\sigma \in A_n$ is a product of an even number of transpositions (see *chapter 1*). Group the transpositions into pairs. It suffices to show that the product of any two transpositions is a product of 3-cycles.
Let $\tau_1 = (a\,b)$ and $\tau_2 = (c\,d)$.
Case 1 (Disjoint). $\{a, b\} \cap \{c, d\} = \varnothing$.

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d).$$

Case 2 (Common element). $b = c$, but $a \neq d$.

$$(a\,b)(b\,d) = (a\,b\,d).$$

Case 3 (Identical). $(a\,b)(a\,b) = 1$.
Thus any pair reduces to 3-cycles.

■

Simplicity of the Alternating Group

We now address a fundamental structural question: does A_n contain any proper normal subgroups?

Definition 5.2. ***Simple Group.***
A group G is **simple** if its only normal subgroups are $\{1\}$ and G itself.

定義

Example 5.1. Abelian Simple Groups. If G is Abelian and simple, it must have no non-trivial proper subgroups. This implies G is finite of prime order p. Thus $C_p \cong \mathbb{Z}/p\mathbb{Z}$ are the only Abelian simple groups.

範例

For non-Abelian groups, the situation is more complex.

- $A_3 \cong C_3$ is simple (Abelian).
- A_4 is **not** simple. The Klein four-group $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4.

However, for $n \geq 5$, the structure stabilises.

Theorem 5.2. ***Simplicity of*** A_n**.**
For $n \geq 5$, the alternating group A_n is simple.

定理

The proof proceeds in two steps: first we show that 3-cycles behave uniformly in A_n, and then we show that any non-trivial normal subgroup must contain a 3-cycle.

Lemma 5.3. Conjugacy of 3-cycles Let $n \geq 5$. All 3-cycles are conjugate in A_n.

引理

Proof

Let $\sigma = (i\,j\,k)$ and $\sigma' = (i'\,j'\,k')$ be 3-cycles. Since 3-cycles have the same cycle structure, there exists $\gamma \in S_n$ such that $\gamma\sigma\gamma^{-1} = \sigma'$. If $\gamma \in A_n$, we are done. If $\gamma \notin A_n$, it is an odd permutation. Since $n \geq 5$, there exist distinct elements $r, s \in X_n \setminus \{i', j', k'\}$. Let $\tau = (r\,s)$. Then τ is odd, so $\gamma' = \tau\gamma$ is even (i.e., $\gamma' \in A_n$). Since τ is disjoint from σ', it commutes with it:

$$\gamma'\sigma(\gamma')^{-1} = \tau(\gamma\sigma\gamma^{-1})\tau^{-1} = \tau\sigma'\tau^{-1} = \sigma'.$$

Thus σ and σ' are conjugate in A_n.

■

Lemma 5.4. Normal Subgroups Contain 3-cycles Let $n \geq 5$ and let $N \trianglelefteq A_n$ be a non-trivial normal subgroup. Then N contains a 3-cycle.

引理

Choose $1 \neq \alpha \in N$ and write α as a product of disjoint cycles.

If α ***has a cycle of length*** ≥ 4***, then*** N ***contains a 3-cycle.***

Suppose α has a cycle $(a_1\,a_2\,a_3\,a_4\,\dots)$ of length at least 4. Let $\tau = (a_1\,a_2\,a_3) \in A_n$ and consider the element

$$\beta := \tau\alpha\tau^{-1}\alpha^{-1}.$$

Since N is normal in A_n and $\tau \in A_n$, we have $\tau\alpha\tau^{-1} \in N$; hence $\beta \in N$. To compute β, track three points in the cycle of α. Let a_r denote the element immediately preceding a_1 in that cycle, so $\alpha^{-1}(a_1) = a_r$ (and $a_r \notin \{a_1, a_2, a_3\}$ since the cycle has length ≥ 4).

Then

$$\beta(a_1) = \tau\alpha\tau^{-1}(\alpha^{-1}(a_1)) = \tau\alpha\tau^{-1}(a_r) = \tau\alpha(a_r) = \tau(a_1) = a_2.$$

Also $\alpha^{-1}(a_2) = a_1$ and $\tau^{-1}(a_1) = a_3$, so

$$\beta(a_2) = \tau\alpha\tau^{-1}(\alpha^{-1}(a_2)) = \tau\alpha\tau^{-1}(a_1) = \tau\alpha(a_3) = \tau(a_4) = a_4.$$

Finally $\alpha^{-1}(a_4) = a_3$ and $\tau^{-1}(a_3) = a_2$, so

$$\beta(a_4) = \tau\alpha\tau^{-1}(\alpha^{-1}(a_4)) = \tau\alpha\tau^{-1}(a_3) = \tau\alpha(a_2) = \tau(a_3) = a_1.$$

Thus β moves $a_1 \mapsto a_2 \mapsto a_4 \mapsto a_1$ and fixes every point outside the support of the original cycle, so $\beta = (a_1\, a_2\, a_4)$ is a 3-cycle in N.

証明終

Otherwise, α is a product of disjoint transpositions, and N contains a 5-cycle.

If α has no cycle of length ≥ 4 and $\alpha \neq 1$, then α must be a product of disjoint transpositions (and there are at least two of them because $\alpha \in A_n$). Pick two disjoint transpositions $(a\, b)(c\, d)$ occurring in α. Since $n \geq 5$, choose e distinct from a, b, c, d and set $\tau = (b\, c\, e) \in A_n$. Consider the element $\beta = \tau\alpha\tau^{-1}\alpha^{-1} \in N$. Using $\alpha^{-1} = \alpha$ and tracking the images of a, b, c, e, d (everything else is fixed), one finds:

$$\beta(a) = b, \quad \beta(b) = c, \quad \beta(c) = e, \quad \beta(e) = d, \quad \beta(d) = a,$$

so $\beta = (a\, b\, c\, e\, d)$ is a 5-cycle in N.

証明終

Now Step 1 applies to β (since it has length ≥ 4), and produces a 3-cycle in N. Now we prove *theorem 5.2*.

Proof for Simplicity of A_n

Let $N \trianglelefteq A_n$ be non-trivial. By the previous lemma, N contains a 3-cycle. By conjugacy of 3-cycles in A_n, normality forces N to contain *every* 3-cycle. Since A_n is generated by 3-cycles (*lemma 5.2*), we conclude $N = A_n$. Hence A_n is simple.

■

5.4 *Orbits and Stabilisers*

We recall the definition of a group action from the previous section. A group G acts on a set X via a map $G \times X \to X$, denoted $(g, x) \mapsto gx$, satisfying $1x = x$ and $g(hx) = (gh)x$.

Definition 5.3. ***Orbit and Transitivity.***
Let X be a G-set and let $x \in X$. The set

$$O_x = Gx = \{gx \mid g \in G\} \subseteq X$$

is called the **orbit** of x. If there exists an $x \in X$ such that $O_x = X$, we say the action of G on X is **transitive**.

定義

From the definition, distinct orbits are disjoint. The relation $x \sim y$ if $y \in O_x$ (i.e., $y = gx$ for some g) is an equivalence relation. Thus X is the disjoint union of its orbits. If $\{x_i\}_{i \in I}$ is a set of representatives from each orbit, we have:

$$X = \bigsqcup_{i \in I} O_{x_i}.$$

Definition 5.4. ***Stabiliser.***
Let $x \in X$. The set of elements in G that fix x,

$$G_x = \{g \in G \mid gx = x\},$$

is called the **stabiliser** of x.

定義

It is straightforward to verify that G_x is a subgroup of G.

Example 5.2. The Upper Half-Plane. Let $\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$. The group $G = \mathrm{SL}_2(\mathbb{R})$ acts on $\mathcal{H}$ via

$$\gamma z = \frac{az + b}{cz + d}, \quad \text{where } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

This action is transitive. The stabiliser of the point i consists of matrices satisfying $\frac{ai+b}{ci+d} = i$, which implies the stabiliser is $\mathrm{SO}_2(\mathbb{R})$.

範例

Example 5.3. Rigid Motions. Let M be the group of rigid motions of the plane. Elements of M are generated by translations, rotations, and reflections.
Rotation:

$$\rho_\theta \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Translation: $\tau_P \mathbf{v} = \mathbf{v} + \mathbf{v}_0$ where P corresponds to the vector $\mathbf{v}_0$.
Reflection:

$$r \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}.$$

M acts transitively on the set of points in the plane. The stabiliser of the origin O is the orthogonal group $O_2(\mathbb{R})$.

範例

Example 5.4. Coset Action. Let $H \leq G$ and let $G/H = \{aH \mid a \in G\}$ be the set of left cosets. The map

$$G \times G/H \to G/H, \quad (g, aH) \mapsto gaH$$

defines a transitive action of G on the set of cosets. For the specific coset H (the identity coset), the stabiliser is $\{g \in G \mid gH = H\} = H$.

範例

Example 5.5. Function Spaces. Let $G = \mathbb{R}$ (under addition) and let X be the set of continuous functions on $\mathbb{R}$. Define the action by shift:

$$(a \circ f)(x) = f(x + a).$$

The stabiliser reveals properties of f:

- $G_f = \mathbb{R}$ if and only if f is a constant function.
- $G_f = t\mathbb{Z}$ (with $t > 0$) if and only if f is periodic with minimum positive period t.
- $G_f = \{0\}$ if and only if f has no non-zero period.

範例

The relationship between the orbit of a point and its stabiliser is given by the following bijection.

Proposition 5.1. ***Orbit-Stabiliser Correspondence.***
Let X be a G-set and $x \in X$. Let $H = G_x$. There exists a natural bijection

$$\varphi : G/H \to O_x, \quad aH \mapsto ax.$$

This map is compatible with the action of G, meaning $\varphi(g(aH)) = g\varphi(aH)$.

命題

Proof

First, we check φ is well-defined. If $aH = bH$, then $a^{-1}b \in H = G_x$. Thus $a^{-1}bx = x$, which implies $bx = ax$. The definition is independent of the representative a. Compatibility is immediate: $\varphi(g \cdot aH) = \varphi(gaH) = gax = g(ax) = g\varphi(aH)$. Second, we check injectivity. If $ax = bx$, then $a^{-1}bx = x$, so $a^{-1}b \in G_x = H$. Thus $aH = bH$. Finally, since $O_x = \{ax \mid a \in G\}$, the map is clearly surjective. Thus φ is a bijection.

■

Corollary 5.1. *Counting Formula.* Let X be a G-set.
1. For any $x \in X$, $|O_x| = [G : G_x]$.
2. If X is finite, then

$$|X| = \sum_{x \in I} |O_x| = \sum_{x \in I} [G : G_x],$$

where I is a set of representatives for the distinct orbits.

推論

Proof

(1) follows directly from the bijection in the previous proposition.
(2) follows from the decomposition of X into disjoint orbits.

■

We can also describe the stabiliser of a point moved by the group.

Proposition 5.2. ***Conjugate Stabilisers.***
Let $x \in X$ and let $x' = ax \in O_x$. Then:
1. The set of elements mapping x to x' is the coset aG_x.
2. The stabiliser of x' is the conjugate of G_x:

$$G_{x'} = aG_x a^{-1} = \{aha^{-1} \mid h \in G_x\}.$$

命題

Proof

1. Note that $gx = x' = ax$ if and only if $a^{-1}gx = x$. This holds if and only if $a^{-1}g \in G_x$, which means $g \in aG_x$.
2. Similarly, $gx' = x'$ is equivalent to $g(ax) = ax$. Multiplying by a^{-1}, we get $(a^{-1}ga)x = x$. This occurs if and only if $a^{-1}ga \in G_x$, or $g \in aG_x a^{-1}$.

■

Example 5.6. Conjugate Symmetries. Returning to the rigid motions of the plane, if P is any point, the group of symmetries fixing P is

$$M_P = \tau_P M_O \tau_P^{-1} = \tau_P O_2(\mathbb{R}) \tau_{-P},$$

where τ_P is the translation mapping the origin O to P.

範例

Example 5.7. Order of the Dihedral Group. We use the counting formula to determine the order of D_n. D_n acts transitively on the n vertices of a regular n-gon. Let v be a vertex. The stabiliser $(D_n)_v$ contains exactly two elements: the identity and the reflection across the line connecting v to the center. Thus $|(D_n)_v| = 2$. By the

counting formula:

$$|D_n| = |O_v| \cdot |(D_n)_v| = n \cdot 2 = 2n.$$

範例

5.5 *Actions as Homomorphisms*

An action of a group G on a set X is mathematically equivalent to a homomorphism from G to the symmetric group S_X. This perspective allows us to "represent" abstract groups as concrete groups of permutations.
Let X be a G-set. For any fixed $g \in G$, define the map

$$\rho_g : X \to X, \quad x \mapsto g \cdot x.$$

Since $g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = 1 \cdot x = x$ and similarly $g^{-1} \cdot (g \cdot x) = x$, the map ρ_g is a bijection with inverse $\rho_{g^{-1}}$. Thus $\rho_g \in S_X$.
We can therefore define a map from the group to the symmetric group:

$$\rho : G \to S_X, \quad g \mapsto \rho_g.$$

The axiom $g \cdot (h \cdot x) = (gh) \cdot x$ translates directly to $\rho_g \circ \rho_h = \rho_{gh}$. Thus, ρ is a group homomorphism. We call this the **permutation representation** of G associated with the action.
Conversely, any homomorphism $\rho : G \to S_X$ defines an action by setting $g \cdot x = \rho(g)(x)$.

The Kernel of the Action

The kernel of the homomorphism ρ consists of those group elements that act trivially on every element of X.

$$\ker \rho = \{g \in G \mid \rho_g = \mathrm{id}_X\} = \{g \in G \mid \forall x \in X, g \cdot x = x\}.$$

In terms of stabilisers, an element fixes everything if it belongs to every stabiliser:

$$\ker \rho = \bigcap_{x \in X} G_x.$$

Since kernels are normal subgroups, this intersection is a normal subgroup of G. By the Fundamental Homomorphism Theorem, we obtain an embedding:

$$G/\ker \rho \hookrightarrow S_X.$$

If $\ker \rho = \{1\}$, the action is called **faithful**, and G is isomorphic to a subgroup of S_X.

Example 5.8. Kernel of the Coset Action. Let $H \leq G$. Consider the action of G on the left cosets G/H by left multiplication. The associated homomorphism is $\rho : G \to S_{G/H}$. The kernel is the set of g such that $g(aH) = aH$ for all $a \in G$. This is equivalent to $a^{-1}ga \in H$ for all a, or $g \in aHa^{-1}$. Thus:

$$\ker \rho = \bigcap_{a \in G} aHa^{-1}.$$

This subgroup is the largest normal subgroup of G contained in H, often called the **core** of H.

範例

Example 5.9. Isomorphism of Linear and Symmetric Groups. We use an action to prove an exceptional isomorphism: $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, where $\mathbb{F}_2$ is the finite field with 2 elements. Let $V = \mathbb{F}_2^2$ be the vector space of dimension 2 over the field with 2 elements. The elements of V are the zero vector $\mathbf{0}$ and three non-zero vectors: $e_1 = \binom{1}{0}$, $e_2 = \binom{0}{1}$, and $e_3 = e_1 + e_2 = \binom{1}{1}$. The general linear group $G = \mathrm{GL}_2(\mathbb{F}_2)$ acts on the set of non-zero vectors $X = \{e_1, e_2, e_3\}$ by matrix multiplication. This induces a homomorphism $\rho : G \to S_X \cong S_3$.

Injectivity: If $A \in \ker \rho$, then A fixes the basis vectors e_1 and e_2. Any linear map fixing a basis is the identity. Thus $\ker \rho = \{I\}$.

Surjectivity: Since ρ is injective, $|G| \leq |S_3| = 6$. By counting bases, $|\mathrm{GL}_2(\mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 3 \times 2 = 6$.

Since the orders match and the map is injective, ρ is an isomorphism.

範例

5.6 *Exercises*

1. **Reversal Permutation.** Let $\sigma \in S_n$ be defined by $\sigma(i) = n + 1 - i$. Determine the parity of σ as a function of n.

   Count the number of transpositions $(i, n+1-i)$.

2. **Counting by Type.** Let the cycle type of a permutation be denoted $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$.

   (a) Prove that the number of permutations of this type is

   $$n! / \prod_{i=1}^{n} (\lambda_i! i^{\lambda_i}).$$

(b) Use this to prove the identity

$$\sum \frac{1}{\prod_{i=1}^{n} \lambda_i!\, i^{\lambda_i}} = 1,$$

where the sum is over all tuples $(\lambda_1, \ldots, \lambda_n)$ of non-negative integers satisfying $\sum_{i=1}^{n} i\lambda_i = n$.

3. **Subgroups of A_4.** Prove that A_4 has no subgroup of order 6.

This is a counterexample to the converse of Lagrange's Theorem.

4. **Unique Index 2 Subgroup.** Prove that for $n \geq 2$, A_n is the unique subgroup of index 2 in S_n.

5. **Center of S_n.** The center of a group G is the set $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$. Prove that for $n \geq 3$, the center of S_n is trivial, i.e., $Z(S_n) = \{\iota\}$.

Show that if α commutes with every transposition $(i\,j)$, it must fix everything.

6. **Even/Odd Bijection.** Fix a transposition $\tau \in S_n$. Define $\Phi : A_n \to S_n \setminus A_n$ by $\Phi(\sigma) = \tau\sigma$.

Fix a transposition τ and use left-multiplication.

   (a) Prove that Φ is a bijection. Conclude that $|A_n| = \frac{n!}{2}$ for $n \geq 2$.
   (b) Deduce that the sign map $\operatorname{sgn} : S_n \to \{\pm 1\}$ is surjective for $n \geq 2$.

7. **Derangements.** Calculate the number of permutations in S_n that have no fixed points (derangements).

8. **Transitive Action Decomposition.** Let G act transitively on Σ. Let $N \trianglelefteq G$. Prove that all orbits of Σ under the restricted action of N have the same size.

9. **Small-Index Subgroups in Simple Groups.** Let G be a simple group. If there exists a proper subgroup $H < G$ such that $[G : H] \leq 4$, prove that $|G| \leq 3$.

10. **Finite Index Forces a Proper Normal Subgroup.** Let G be an infinite group and let H be a proper subgroup of finite index. Prove that G contains a proper normal subgroup of finite index.

11. **Function Scaling.** Let X be the set of functions $f : \mathbb{R} \to \mathbb{R}$. For $a \in \mathbb{R}^\times$, define $(a \cdot f)(x) = f(ax)$.

   (a) Verify this is a group action.
   (b) Find a function f whose stabiliser is $\mathbb{R}_+^\times$.

12. **Symmetry Groups.** Determine the symmetry groups of a square, a rectangle (non-square), a rhombus (non-square), and a circle.

13. **Burnside's Lemma.** Let G act on a finite set X. Let $X^g = \{x \in X \mid g \cdot x = x\}$ be the set of points fixed by g. Prove that the number of orbits of X under the action of G is

$$\frac{1}{|G|} \sum_{g \in G} |X^g|.$$

14. **Coloring Problems.** Let G be the rotational symmetry group of a regular tetrahedron acting on its 4 vertices. You may use that this action identifies G with a subgroup of S_4 isomorphic to A_4, and that (as permutations of the vertices) the elements of G consist of:

    (a) the identity (1 element),
    (b) 3-cycles (8 elements),
    (c) products of two disjoint transpositions (3 elements).

    Using Burnside's Lemma, find the number of distinct ways to color the vertices with 4 colors, up to rotational symmetry.

15. **Semidirect Product.** Let N, H be groups and $\varphi : H \to \mathrm{Aut}(N)$ a homomorphism. Define $G = N \times H$ with operation $(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2)$.

    (a) Prove G is a group, denoted $N \rtimes_\varphi H$.
    (b) Show that $N \times \{1\}$ is a normal subgroup of G and that $\{1\} \times H$ is a subgroup of G.
    (c) Prove that $G/(N \times \{1\}) \cong H$.
    (d) Prove that for $n \geq 3$, $S_n = A_n \rtimes \langle (1\,2) \rangle$.

16. **Automorphisms of S_3.** Determine $\mathrm{Aut}(S_3)$.

17. **Smallest Prime Normal Subgroup is Central.** Let p be the smallest prime factor of $|G|$. If a subgroup A of order p satisfies $A \trianglelefteq G$, prove that $A \leq Z(G)$.

6
The Sylow Theorems

Lagrange's Theorem (*Theorem 3.3*) imposes a strong constraint on the structure of finite groups: the order of any subgroup must divide the order of the group. However, the converse is false; if d divides $|G|$, G does not necessarily possess a subgroup of order d. A classical counterexample is the alternating group A_4 of order 12, which has no subgroup of order 6. The Sylow Theorems provide a partial converse.

6.1 *Sylow p-Subgroups*

Let G be a finite group of order n. Let p be a prime factor of n. We write $n = p^r m$, where p and m are coprime. A natural question arises: does G contain an element of order p? More generally, does G possess a subgroup of order p^r?

Definition 6.1. ***Sylow p-subgroup.***
A subgroup of G with order p^r is called a **Sylow p-subgroup** of G.

定義

We now proceed to prove the existence of such subgroups, their conjugacy properties, and formulae for their count.

Theorem 6.1. ***Sylow's First Theorem.***
Let G be a finite group of order $n = p^r m$ with $\gcd(p, m) = 1$. Then G contains a Sylow p-subgroup.

定理

Proof

Let X be the family of all subsets of G having exactly p^r elements:

$$X = \{U \subseteq G \mid |U| = p^r\}.$$

Its size is the binomial coefficient

$$N = |X| = \binom{n}{p^r} = \frac{mp^r(mp^r - 1)\cdots(mp^r - p^r + 1)}{1 \cdot 2 \cdots p^r}.$$

For $1 \leq i \leq p^r - 1$, write $i = p^t u$ with $p \nmid u$ (so t is the largest expo-

nent of p dividing i). Then

$$mp^r - i = p^t(p^{r-t}m - u),$$

and since $p \nmid u$, the largest power of p dividing $mp^r - i$ is p^t, the same as for i. Thus the p-power contributions of numerator and denominator factors cancel term-by-term (and the remaining factor m is coprime to p), so $p \nmid N$.
Let G act on X by left multiplication: $g \cdot U = \{gu \mid u \in U\}$. Since $p \nmid |X|$, there exists an orbit O_U with $|O_U|$ coprime to p. Let G_U be the stabiliser of U. By the orbit–stabiliser counting formula ($|G| = |O_U| \cdot |G_U|$),

$$|G_U| \cdot |O_U| = |G| = p^r m.$$

Hence $p^r \mid |G_U|$. On the other hand, for any $u \in U$ and $h \in G_U$, we have $hu \in hU = U$, so U is a union of left cosets of G_U. Therefore $|G_U| \mid |U| = p^r$. Since $|G_U|$ both divides and is divisible by p^r, we have $|G_U| = p^r$. Thus G_U is a Sylow p-subgroup of G.

■

Conjugacy

We now investigate the relationship between arbitrary subgroups and Sylow subgroups.

Theorem 6.2. ***Sylow's Second Theorem.***
Let K be a subgroup of G, and suppose p divides the order of K. Let H be a Sylow p-subgroup of G. Then there exists a conjugate $H' = gHg^{-1}$ such that $H' \cap K$ is a Sylow p-subgroup of K.

定理

Proof

Consider the set of left cosets $X = G/H = \{gH \mid g \in G\}$. The group G acts transitively on X by left multiplication. For an element $x = aH \in X$, the stabiliser is the conjugate subgroup:

$$G_x = aHa^{-1}.$$

We restrict the action of G on X to the subgroup K. Since $|X| = [G : H] = m$ and $\gcd(m, p) = 1$, the set X decomposes into orbits under K. Since the total size m is coprime to p, there exists at least one K-orbit O_x such that $|O_x|$ is coprime to p.
Let $x = aH$ be a representative of this orbit. The stabiliser of x in K is:

$$K_x = G_x \cap K = aHa^{-1} \cap K.$$

Since aHa^{-1} is a group of order p^r, its intersection with K is a p-group. Thus $|K_x|$ is a power of p. By the counting formula for the

action of K:

$$|O_x| \cdot |K_x| = |K|.$$

Since $|O_x|$ is coprime to p, the full power of p dividing $|K|$ must be contained in $|K_x|$. Therefore, K_x is a Sylow p-subgroup of K.

■

From this theorem, we deduce two fundamental properties.

Corollary 6.1. *Conjugacy and Containment.*

1. If $K \leq G$ is a p-group, then K is contained in some Sylow p-subgroup of G.
2. All Sylow p-subgroups of G are conjugate.

推論

Proof

1. Since K is a p-group, its maximal p-subgroup is K itself. Applying *theorem* 6.2, there exists a conjugate H' of a Sylow p-subgroup H such that $H' \cap K$ is a Sylow p-subgroup of K. Thus $H' \cap K = K$, which implies $K \leq H'$.
2. Let H and H_1 be two Sylow p-subgroups of G. By *theorem* 6.2 (applied with $K = H_1$), there exists $H' = gHg^{-1}$ such that $H' \cap H_1$ is a Sylow p-subgroup of H_1. Thus $H' \cap H_1 = H_1$, implying $H_1 \leq H'$. Since $|H_1| = |H| = |H'|$, we have $H_1 = H'$. Thus H_1 is conjugate to H.

■

The Number of Sylow Subgroups

Let $N(p)$ denote the number of Sylow p-subgroups of G. Since all Sylow p-subgroups are conjugate, $N(p)$ is the size of the set $X_H = \{aHa^{-1} \mid a \in G\}$, where H is a fixed Sylow p-subgroup.

Definition 6.2. ***Setwise Stabiliser of a Subgroup.***
For a subgroup $H \leq G$, define

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

This is the stabiliser of H under conjugation, and it is a subgroup of G containing H.

定義

Theorem 6.3. ***Sylow's Third Theorem.***
Let $N(p)$ be the number of Sylow p-subgroups of G. Then

$$N(p) \equiv 1 \pmod{p}.$$

定理

Proof

We know the conjugation action of G on X_H is transitive. By the counting formula, $N(p) = [G : N_G(H)]$, where $N_G(H)$ is the stabiliser of H under conjugation.
We decompose X_H into orbits under the conjugation action of the subgroup H. Suppose an orbit contains only one element H_i. Then $hH_ih^{-1} = H_i$ for all $h \in H$, which implies $H \leq N_G(H_i)$. However, H_i is a normal subgroup of $N_G(H_i)$ (by the definition of $N_G(H_i)$) and is therefore the unique Sylow p-subgroup of $N_G(H_i)$. Since H is a p-subgroup of $N_G(H_i)$ with the same maximal order, we must have $H = H_i$. Thus, the only orbit of size 1 is $\{H\}$.
For any other orbit O_{H_i} (where $H_i \neq H$), the counting formula gives:

$$|O_{H_i}| = [H : N_G(H_i) \cap H].$$

Since $H_i \neq H$, the intersection $N_G(H_i) \cap H$ is a proper subgroup of H. Therefore, the index is divisible by p. Thus, p divides the size of every orbit except the singleton $\{H\}$. Summing the orbit sizes:

$$N(p) = 1 + \sum |O_{H_i}| \equiv 1 \pmod{p}.$$

■

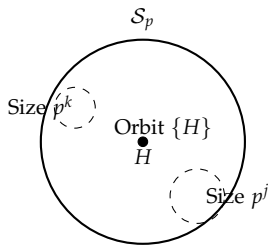


Figure 6.1: The decomposition of the set of Sylow p-subgroups under the conjugation action of H. There is exactly one fixed point.

We synthesise the preceding results into the standard statement of the Sylow Theorem.

Theorem 6.4. ***The Sylow Theorem.***
Let G be a finite group of order $p^r m$, where $\gcd(m, p) = 1$.
Existence: G contains a Sylow p-subgroup, i.e., a subgroup of order p^r.
Conjugacy: All Sylow p-subgroups of G are conjugate.
Counting: The number of Sylow p-subgroups, $N(p)$, satisfies:

$$N(p) \equiv 1 \pmod{p} \quad \text{and} \quad N(p) \mid m.$$

定理

Proof

Parts (1) and (2) are *theorem* 6.1 and *corollary* 6.1. For part (3), we established $N(p) \equiv 1 \pmod{p}$ in *theorem* 6.3. Additionally, since $N(p) = [G : N_G(H)]$ and $H \leq N_G(H)$, we have:

$$[G : H] = [G : N_G(H)] \cdot [N_G(H) : H].$$

Thus $N(p)$ divides $[G : H] = m$.

■

6.2 *Applications of the Sylow Theorems*

The Sylow theorems are nice tools for investigating the structure of finite groups. By counting the number of Sylow subgroups, we can often demonstrate the existence of a normal subgroup, thereby proving that a group is not simple. We begin with a structural lemma that allows us to decompose a group into a direct product of its normal subgroups.

Lemma 6.1. ***Direct Product Decomposition.***
Let H and K be normal subgroups of G such that $G = HK$ and $H \cap K = \{1\}$. Then $G \cong H \times K$.

引理

Proof

Let $h \in H$ and $k \in K$. Consider the element $x = khk^{-1}h^{-1}$. Since $H \trianglelefteq G$, we have $khk^{-1} \in H$, so $x = (khk^{-1})h^{-1} \in H$. Since $K \trianglelefteq G$, we have $hk^{-1}h^{-1} \in K$, so $x = k(hk^{-1}h^{-1}) \in K$. Thus $x \in H \cap K = \{1\}$, so $khk^{-1}h^{-1} = 1$, which implies $hk = kh$. Define the map $\varphi : H \times K \to G$ by $\varphi(h,k) = hk$.

Homomorphism: $\varphi((h_1,k_1)(h_2,k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. Since elements of H and K commute, $h_2k_1 = k_1h_2$, so this equals $h_1k_1h_2k_2 = \varphi(h_1,k_1)\varphi(h_2,k_2)$.

Surjectivity: Follows from the assumption $G = HK$.

Injectivity: If $\varphi(h,k) = 1$, then $hk = 1$, so $h = k^{-1}$. Since $h \in H$ and $k^{-1} \in K$, both lie in the intersection, so $h = 1$ and $k = 1$.

Thus φ is an isomorphism.

■

Criteria for Non-Simplicity

We apply the counting part of the Sylow Theorem to show that groups of specific orders cannot be simple.

Example 6.1. Group of Order 150. Let $|G| = 150 = 2 \cdot 3 \cdot 5^2$. We examine the number of Sylow 5-subgroups, n_5.

範例

Solution

By the Sylow Theorem, $n_5 \equiv 1 \pmod 5$ and n_5 divides 6. The only divisors of 6 satisfying the congruence are 1 and 6.

- If $n_5 = 1$, the unique Sylow 5-subgroup is normal, so G is not simple.

- If $n_5 = 6$, let X be the set of Sylow 5-subgroups. The conjugation action of G on X induces a homomorphism $\rho : G \to S_6$. Since $|G| = 150$ and $|S_6| = 720$, we observe that 150 does not divide 720 (as $720 = 150 \times 4.8$). By the First Isomorphism Theorem, $G/\ker\rho \cong \operatorname{im}\rho \leq S_6$. If ρ were injective (i.e., $\ker\rho = \{1\}$), then $|G|$ would divide $|S_6|$. Since it does not, $\ker\rho$ must be a non-trivial normal subgroup.

In either case, G is not simple.

■

We can extend this analysis to infinite families of groups.

Proposition 6.1. ***Groups of Order*** pq ***and*** p^2q**.**
Let p and q be distinct odd primes.
1. A group of order pq is not simple.
2. A group of order p^2q is not simple.

命題

Proof

Recall that p-groups have non-trivial centres (and thus are not simple if the order is a prime power $> p$). We assume $p \neq q$.

1. Assume $p < q$. Then $n_q \mid p$ and $n_q \equiv 1 \pmod q$. Since $p < q$, the only solution is $n_q = 1$. Thus the Sylow q-subgroup is normal.

2. Assume $p < q$. Then $n_q \mid p^2$ and $n_q \equiv 1 \pmod q$. Since $p < q$, $p \not\equiv 1 \pmod q$. Thus n_q cannot be p. This leaves $n_q = 1$ or $n_q = p^2$. If $n_q = 1$, the subgroup is normal. Suppose $n_q = p^2$. Then G contains p^2 distinct Sylow q-subgroups. Since q is prime, these subgroups are cyclic of order q, and any two intersect only at the identity. The number of elements of order q is therefore $p^2(q-1)$. The number of remaining elements is

$$p^2q - p^2(q-1) = p^2q - p^2q + p^2 = p^2.$$

These p^2 elements must constitute the unique (and thus normal) Sylow p-subgroup. If $p > q$, a similar argument on n_p shows $n_p = 1$.

■

The Smallest Non-Abelian Simple Group

It is a known fact that:
· Groups of prime order are cyclic (hence simple but Abelian).
· Groups of prime power order ($p^n, n \geq 2$) have non-trivial centres (hence not simple).

· Groups of order $2m$ where m is odd have a subgroup of index 2 (hence normal, so not simple).

Combining these facts with the results above, we can classify the simple groups of small order.

Theorem 6.5. ***Simplicity of*** A_5**.**
The smallest non-Abelian simple group is isomorphic to the alternating group A_5 (order 60).
1. If $|G| < 60$, G is not a non-Abelian simple group.
2. If $|G| = 60$ and G is a non-Abelian simple group, then $G \cong A_5$.

定理

Elimination of Orders < 60.

Excluding prime orders, prime powers, products pq, p^2q, and $2 \times$ odd, the only remaining candidates are $24, 36, 40, 48, 56$.

$|G| = 24 = 2^3 \cdot 3$. $n_2 \in \{1, 3\}$. If $n_2 = 3$, let H be a Sylow 2-subgroup. The action of G on the set of Sylow 2-subgroups induces a homomorphism $\rho : G \to S_3$. Since $|G| > |S_3|$, $\ker \rho$ is non-trivial.

$|G| = 36 = 2^2 \cdot 3^2$. $n_3 \in \{1, 4\}$. If $n_3 = 4$, the action induces $\rho : G \to S_4$. Since $36 > 24$, $\ker \rho \neq \{1\}$.

$|G| = 40 = 2^3 \cdot 5$. $n_5 \mid 8$ and $n_5 \equiv 1 \pmod 5 \implies n_5 = 1$.

$|G| = 48 = 2^4 \cdot 3$. Analogous to the case of 24. $n_2 \in \{1, 3\}$. Map to S_3 reveals a normal subgroup.

$|G| = 56 = 2^3 \cdot 7$. $n_7 \mid 8 \implies n_7 \in \{1, 8\}$. If $n_7 = 8$, there are $8 \times (7 - 1) = 48$ elements of order 7. The remaining $56 - 48 = 8$ elements must form the unique Sylow 2-subgroup. Thus either $n_7 = 1$ or $n_2 = 1$.

証明終

Structure of the Simple Group of Order 60.

Assume G is simple and $|G| = 60$.

No subgroup of small index. If G had a subgroup H of index $m \leq 4$, the action on cosets would yield $\rho : G \to S_m$. Since $60 \nmid m!$ for $m \leq 4$, the kernel would be non-trivial.

Existence of a subgroup of index 5. Consider the Sylow 2-subgroups ($|P| = 4$). n_2 divides 15 and is odd. $n_2 \in \{1, 3, 5, 15\}$. Since G is simple, $n_2 \neq 1$. By the index constraint, $n_2 \neq 3$ (since the normaliser would have index 3). Thus $n_2 \in \{5, 15\}$. If $n_2 = 5$, the normaliser of a Sylow 2-subgroup has index 5. If $n_2 = 15$, we count elements. $n_5 = 6$ (24 elements of order 5). $n_3 = 10$ (20 elements of order 3). Total so far: 44. This leaves 16 elements. If the 15 Sylow 2-subgroups were disjoint (except for 1), they would require $15 \times 3 = 45$ elements, which is too many. Thus,

there must exist Sylow 2-subgroups P_1, P_2 with non-trivial intersection $K = P_1 \cap P_2 \neq \{1\}$. Let H be the subgroup generated by P_1 and P_2. Since P_1, P_2 are Abelian (order 4), they normalise K. Thus $H \leq C_G(K)$ (strictly, H is in the normaliser, but for Abelian subgroups of this type, they centralise the intersection). Since G is simple, $C_G(K) \neq G$. Also $P_1 < H$, so $|H| > 4$. Since $|H|$ must be a multiple of 4 dividing 60, possible orders are 12, 20. Order 20 implies index 3 (impossible). Thus $|H| = 12$, which has index 5.

Isomorphism. The action of G on the cosets of a subgroup of index 5 gives a homomorphism $\rho : G \to S_5$. Since G is simple and the index is > 1, ρ is injective. Thus $G \cong \operatorname{im}\rho$, a subgroup of S_5 of order 60. The intersection $\operatorname{im}\rho \cap A_5$ is normal in $\operatorname{im}\rho$. Since $\operatorname{im}\rho$ is simple, the intersection is trivial or the whole group. It cannot be trivial (as $|S_5 : A_5| = 2$), so $\operatorname{im}\rho \leq A_5$. Since orders match, $G \cong A_5$.

証明終

6.3 *Exercises*

1. **Element of Order p.** If p is a prime factor of $|G|$, prove that G has an element of order p.
2. **Order Six.** Prove that the only non-Abelian group of order 6 is S_3.
3. **Sylow Subgroups in a Normal Subgroup.** Let $N \trianglelefteq G$ be finite. If $\gcd(p, |G/N|) = 1$, prove that N contains all Sylow p-subgroups of G.
4. **Sylow Subgroups and Quotients.** Let G be finite, $N \trianglelefteq G$, and let P be a Sylow p-subgroup of G. Prove:
   (1) $N \cap P$ is a Sylow p-subgroup of N.
   (2) PN/N is a Sylow p-subgroup of G/N.
   (3) $N_G(P)N/N \cong N_{G/N}(PN/N)$.
5. **Small Cofactor.** If $|G| = p^e a$ with $1 \leq a < p$ and $e \geq 1$, prove that G has a proper normal subgroup.
6. **Sylow Orbits in Permutation Groups.** Let G be a permutation group on a set Σ, and let P be a Sylow p-subgroup of G. For $a \in \Sigma$, prove that if p^m divides $|Ga|$, then p^m divides $|Pa|$.
7. **Stabiliser Action on Fixed Points.** Let G be a permutation group on a set Σ. For any $a \in \Sigma$, let P be a Sylow p-subgroup of the stabiliser G_a, and let Δ be the set of all fixed points of the orbit Ga under the action of P. Let $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$. Prove

that the action of $N_G(P)$ on Δ is transitive.

8. **No Simple Group of Order 224.** Prove that there is no simple group of order 224.

9. **Stabiliser Criterion.** Let P be a Sylow p-subgroup of G and suppose $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$ is normal in G. Prove that $P \trianglelefteq G$.

7
Free Groups and Presentations

In the previous chapters, we studied groups by examining their internal structure. Given an arbitrary set S, can we construct a "most general" group generated by S, imposing no constraints other than the group axioms? This leads to the concept of free groups, which serve as the universal prototypes for all groups.

7.1 Construction of Free Groups

We begin by viewing the elements of S as letters. Let $S^{-1} = \{s^{-1} \mid s \in S\}$ be a disjoint copy of S, with the formal rule $(s^{-1})^{-1} = s$. We define a **word** to be a string formed by concatenating elements from $S \cup S^{-1}$. However, to obtain a group structure on $F(S)$, we require three properties:

Multiplication: If $w_1 = x_1 \dots x_n$ and $w_2 = y_1 \dots y_m$, then the product $w_1 \cdot w_2$ is the concatenation $x_1 \dots x_n y_1 \dots y_m$.

Inverses: For every $x \in S$, there must exist an inverse $x^{-1} \in F(S)$. Consequently, we allow words to be formed from the alphabet $S \cup S^{-1}$.

Identity: There must be an empty word, denoted 1, such that concatenating it with any word w yields w.

Based on these requirements, we consider the set of all words:

$$W(S) = \{1\} \cup \{x_1 x_2 \dots x_n \mid x_i \in S \cup S^{-1}, 1 \leq i \leq n\}.$$

However, a direct set of strings is insufficient because it does not account for the group axioms, specifically the inverse property. By associativity, a subword of the form aa^{-1} or $a^{-1}a$ should cancel out. For instance, the word

$$w = \dots xaa^{-1}y \dots$$

should be equivalent to $w' = \dots xy \dots$. The elimination of such pairs is a simplification process.

A potential issue arises: a word might be reduced in multiple ways.

Consider

$$w = x^{-1}x(yy^{-1})x^{-1}yz.$$

One reduction path yields:

$$w \to x^{-1}(xx^{-1})yz \to x^{-1}yz.$$

Another path yields:

$$w = (x^{-1}x)yy^{-1}x^{-1}yz \to (yy^{-1})x^{-1}yz \to x^{-1}yz.$$

To formalise this, we introduce the notion of a reduced word.

Definition 7.1. ***Reduced Word.***
A word w is called a **reduced word** if w does not contain a string of the form $a^{-1}a$ or aa^{-1} for any $a \in S \cup S^{-1}$.

定義

It is natural to ask whether repeatedly applying reductions to a word always yields the same result.

Proposition 7.1. ***Uniqueness of Reduced Form.***
Every word w can be transformed into a unique reduced word by a finite sequence of elementary reductions.

命題

We proceed by induction on the length n of the word w.

Base Case.

If $n = 0$ or $n = 1$, the word is already reduced.

証明終

Inductive Step.

Suppose the result holds for all words of length less than n. Let w be a word of length n. If w is reduced, we are done. If not, we perform a reduction to obtain a word w' of length $n - 2$. By the induction hypothesis, w' has a unique reduced form w_0. We must ensure that the choice of the first reduction does not affect the final outcome. Suppose we can apply two distinct reductions to w, eliminating pairs at positions i and j (assume $i < j$).

Disjoint: If the pairs are disjoint (e.g., $w = \dots xx^{-1} \dots yy^{-1} \dots$), the order of reduction is irrelevant; performing both yields the same word of length $n - 4$.

Overlapping. If the pairs overlap, the subword must be of the form $xx^{-1}x$ or $x^{-1}xx^{-1}$. In the first case, reducing the first pair (xx^{-1}) leaves x; reducing the second pair $(x^{-1}x)$ also leaves x. The resulting words are identical.

証明終

Thus, all reduction paths converge to the same unique reduced word.

We define an equivalence relation $\sim$ on the set of all words: $w \sim u$ if they have the same reduced form.

Proposition 7.2. ***Multiplication of Reduced Words.***
If $w \sim w'$ and $u \sim u'$, then $wu \sim w'u'$.

命題

Proof

Let v be the unique reduced form of w (and w'), and z be the unique reduced form of u (and u'). The product wu reduces to the reduced form of vz. Similarly, $w'u'$ reduces to the reduced form of vz. By the uniqueness of the reduced form, $wu \sim w'u'$.

■

Definition 7.2. ***The Free Group.***
The **free group** generated by S, denoted $F(S)$, is the set of all reduced words on S (equivalently, $W(S)/\sim$). The binary operation is concatenation followed by reduction to the unique reduced form.

- The identity is the empty word 1.
- The inverse of $x_1 \dots x_n$ is $x_n^{-1} \dots x_1^{-1}$.

定義

Example 7.1. Examples of Free Groups.

1. If $S = \varnothing$, $F(S) = \{1\}$ is the trivial group.
2. If $S = \{a\}$, the reduced words are of the form a^n for $n \in \mathbb{Z}$. Thus $F(S) = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ ($F(\{a\}) \cong (\mathbb{Z}, +)$), which is an infinite cyclic group.
3. If $S = \{a, b\}$, $F(S)$ is an (infinite) non-Abelian group. The words ab and ba are distinct reduced words, so $ab \neq ba$. This group contains elements of infinite order and has a rich structure; for instance, $[a, b] = aba^{-1}b^{-1}$ is non-trivial since its reduced form has length 4.

範例

The Universal Property

Free groups are characterised by a universal property: any map from the set S to a group G extends uniquely to a homomorphism from $F(S)$ to G. This formalises the idea that there are "no relations" between the generators in $F(S)$ other than those required by group axioms.

Theorem 7.1. ***Universal Property of Free Groups.***
Let S be a set and G be a group. For any set map $f : S \to G$, there exists a unique group homomorphism $\varphi : F(S) \to G$ such that $\varphi(s) = f(s)$ for all $s \in S$.

定理

Proof

We construct φ explicitly on the reduced words. Let $w = x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \in F(S)$, where $x_i \in S$ and $\epsilon_i \in \{1, -1\}$. We define:

$$\varphi(w) = f(x_1)^{\epsilon_1} \dots f(x_n)^{\epsilon_n},$$

where $f(x)^{-1}$ denotes the inverse of $f(x)$ in G. Since f maps into a group, the operation preserves the cancellation of inverses (e.g., $f(x)f(x)^{-1} = 1_G$), so concatenation followed by reduction corresponds to multiplication in G. Thus φ is a homomorphism. Uniqueness follows because S generates $F(S)$; any homomorphism is determined by its values on the generators.

■

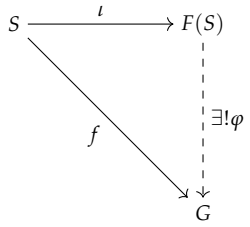


Figure 7.1: The universal property of the free group. The map ι is the natural inclusion of the generators.

This theorem implies that every group is a homomorphic image of a free group.

Theorem 7.2. ***Quotient Theorem.***
Every group G is isomorphic to a quotient of a free group. If G is finitely generated, it is a quotient of a free group of finite rank.

定理

Proof

Let S be a generating set for G (one can always take $S = G$). Let $f : S \to G$ be the inclusion map. By the universal property, there exists a homomorphism $\varphi : F(S) \to G$. Since S generates G, $\operatorname{im} \varphi$ contains S and thus equals G. By the First Isomorphism Theorem:

$$G \cong F(S) / \ker \varphi.$$

■

7.2 *Group Presentations*

Since every group is a quotient of a free group, we can describe any group by specifying a set of generators S and a set of relations describing the kernel $N = \ker \varphi$.

Definition 7.3. ***Presentation.***
A **presentation** of a group G, denoted $G = \langle S \mid R \rangle$, consists of:
· A set of generators S.
· A set of relations $R \subseteq F(S)$.
The group defined by this presentation is $F(S)/N$, where N is the smallest normal subgroup of $F(S)$ containing R.

定義

The notation $r = 1$ is often used for elements in R. For example, the relation $aba^{-1}b^{-1}$ is often written as $ab = ba$.

Example 7.2. Cyclic Groups. The cyclic group of order n has the presentation:

$$\mathbb{Z}/n\mathbb{Z} \cong \langle a \mid a^n = 1 \rangle.$$

Here $S = \{a\}$ and $R = \{a^n\}$. The normal subgroup generated by a^n in $F(\{a\}) \cong \mathbb{Z}$ is simply $n\mathbb{Z}$.

範例

Example 7.3. The Dihedral Group. We derived the structure of D_n geometrically in previous chapters. We can now define it algebraically via the presentation:

$$D_n = \langle \sigma, \tau \mid \sigma^n = 1,\ \tau^2 = 1,\ (\sigma\tau)^2 = 1 \rangle.$$

範例

Solution

Let G be the group defined by this presentation. Since D_n contains elements satisfying these relations (rotation and reflection), there is a surjective homomorphism $\varphi : G \twoheadrightarrow D_n$. To prove isomorphism, we show $|G| \leq 2n$. In G, the relation $(\sigma\tau)^2 = 1$ implies $\tau\sigma\tau = \sigma^{-1} = \sigma^{n-1}$. This allows us to move any τ to the right of any σ (using $\tau^2 = 1$). Any element can be written in the form $\sigma^i\tau^j$ with $0 \leq i < n$ and $0 \leq j < 2$. Thus $|G| \leq 2n$. Since $|D_n| = 2n$, the map φ is an isomorphism.

■

The Commutator Subgroup

Presentations allow us to systematically study the "Abelianisation" of a group.

Definition 7.4. ***Commutator.***
Let G be a group and $a, b \in G$. The **commutator** of a and b is the element

$$[a, b] = aba^{-1}b^{-1}.$$

定義

Note that $ab = [a, b]ba$. Thus a and b commute if and only if $[a, b] = 1$.

Definition 7.5. ***Commutator Subgroup.***
The **commutator subgroup** (or derived subgroup) of G, denoted G' or $[G, G]$, is the subgroup generated by all commutators $\{[a, b] \mid a, b \in G\}$.

定義

Proposition 7.3. ***Abelianisation.***

1. G' is a normal subgroup of G.
2. The quotient G/G' is an Abelian group, called the **Abelianisation** of G, denoted G^{ab}.
3. G/G' is the maximal Abelian quotient of G: if A is any Abelian group and $\varphi : G \to A$ is a homomorphism, then $G' \leq \ker \varphi$, and φ factors uniquely through G/G'.

命題

Proof

1. For any $g \in G$, a conjugate of a commutator is a commutator:

   $$g[a,b]g^{-1} = g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}].$$

   Since G' is generated by commutators, it is invariant under conjugation.
2. In the quotient G/G', we have $\overline{[a,b]} = \overline{1}$, which implies $\bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \overline{1}$, or $\bar{a}\bar{b} = \bar{b}\bar{a}$.
3. If A is Abelian, then for any $a, b \in G$, $\varphi([a,b]) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$. Since A is commutative, this product is 1_A. Thus generators of G' lie in $\ker \varphi$, so $G' \leq \ker \varphi$. The factorisation follows from the Fundamental Homomorphism Theorem.

■

The presentation of the Abelianisation is obtained simply by adding commutators to the relations.

Proposition 7.4. ***Presenting the Abelianisation.***
If $G = \langle S \mid R \rangle$, then

$$G/G' \cong \langle S \mid R \cup \{xy = yx \mid x, y \in S\} \rangle.$$

命題

Proof

Let $G = F(S)/N$ where N is the normal closure of R in $F(S)$. The quotient map $\pi : F(S) \to G$ induces a surjection $F(S) \twoheadrightarrow G/G'$. Its kernel contains N and also $F(S)'$, so it contains the normal closure of R together with all commutators. Hence the map factors through

$$F(S)/\langle\langle R,\ [x,y]\ (x,y \in S) \rangle\rangle.$$

The resulting quotient is Abelian and still satisfies the relations in R, so by the universal property of presentations it is isomorphic to G/G'.

■

In particular, the Abelianisation of the free group $F(S)$ is the free Abelian group on S, isomorphic to $\mathbb{Z}^{|S|}$ (if S is finite).

Proposition 7.5. ***Commutators of Free Groups.***
Let $\varphi : F(S) \to G$ be a surjective homomorphism. Then φ induces a surjective homomorphism

$$\overline{\varphi} : F(S)/F(S)' \to G/G', \quad \text{defined by } \overline{\varphi}(\overline{g}) = \overline{\varphi(g)}.$$

命題

Proof

Consider the composition of homomorphisms $\varphi : F(S) \to G \to G/G'$. Since G/G' is Abelian, the kernel of this composite map must contain $F(S)'$ (by the previous proposition). Thus the map factors through $F(S)/F(S)'$.

■

This proposition implies that if a group G has the presentation

$$G = \langle S \mid r_1 = \cdots = r_n = 1 \rangle,$$

then its maximal Abelian quotient G/G' has the presentation

$$G/G' = \langle S \mid r_1 = \cdots = r_n = 1,\ xy = yx \text{ for any } x, y \in S \rangle.$$

In particular, the group $F(S)/F(S)'$ has the presentation

$$F(S)/F(S)' = \langle S \mid xy = yx \text{ for any } x, y \in S \rangle.$$

Example 7.4. Abelianisation of D_n. For $D_n = \langle \sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$, the Abelianisation imposes $\sigma\tau = \tau\sigma$. The relation $\tau\sigma\tau = \sigma^{-1}$ becomes $\sigma\tau^2 = \sigma^{-1} \implies \sigma = \sigma^{-1} \implies \sigma^2 = 1$. Thus D_n^{ab} is generated by σ, τ with relations $\sigma^2 = 1, \tau^2 = 1, \sigma^n = 1, [\sigma, \tau] = 1$.

- If n is odd, $\sigma^2 = 1$ and $\sigma^n = 1$ imply $\sigma = 1$. Thus $D_n^{\text{ab}} \cong C_2$ (generated by τ).
- If n is even, $\sigma^2 = 1$ is compatible with $\sigma^n = 1$. Thus $D_n^{\text{ab}} \cong C_2 \times C_2$ (Klein four-group).

範例

7.3 *Finitely Generated Free Abelian Groups*

We now focus on a specific class of groups derived from the free group by imposing commutativity. These structures are the algebraic analogues of vector spaces over the ring of integers.

Definition 7.6. ***Free Abelian Group.***
Let S be a set. The **free Abelian group generated by** S, denoted $\mathbb{Z}(S)$, is the group defined by the presentation:

$$\mathbb{Z}(S) = F(S)/F(S)' = \langle S \mid xy = yx, \forall x, y \in S \rangle.$$

If S is a finite set, $\mathbb{Z}(S)$ is called a **finitely generated free Abelian group**.

定義

Unlike general free groups, the structure of free Abelian groups is remarkably simple. They are isomorphic to direct sums of the integers. From this point on, we use additive notation for Abelian groups.

Definition 7.7. ***Direct Sum of Integers.***
Let S be a set. The direct sum $\bigoplus_{x \in S} \mathbb{Z}$ is the set of sequences indexed by S:

$$\bigoplus_{x \in S} \mathbb{Z} = \{(a_x)_{x \in S} \mid a_x \in \mathbb{Z} \text{ and only finitely many } a_x \neq 0\}.$$

Under component-wise addition, this forms an Abelian group.

定義

If S is finite with $|S| = n$, this direct sum is isomorphic to $\mathbb{Z}^n$.
We now establish the fundamental isomorphism between the free Abelian group on S and this direct sum.

Theorem 7.3. ***Isomorphism Theorem for Free Abelian Groups.***

1. For any set S, $\mathbb{Z}(S) \cong \bigoplus_{x \in S} \mathbb{Z}$.
2. If $m \neq n$, then $\mathbb{Z}^m \ncong \mathbb{Z}^n$.

定理

Proof

1. Define a map $f : S \to \bigoplus_{x \in S} \mathbb{Z}$ by mapping x to the sequence e_x which has 1 at position x and 0 elsewhere. By the universal property of free groups, f extends uniquely to a surjective homomorphism $\varphi : F(S) \to \bigoplus_{x \in S} \mathbb{Z}$. Since the target group is Abelian, any commutator maps to the identity, so the kernel of φ contains the commutator subgroup $F(S)'$. Hence φ factors through the commutator quotient, inducing a surjective homomorphism:
$$\overline{\varphi} : \mathbb{Z}(S) \to \bigoplus_{x \in S} \mathbb{Z}.$$
In $\mathbb{Z}(S)$, the commutativity relations allow any word to be re-

ordered and combined, so every element has a normal form

$$x_1^{\alpha_1} \dots x_n^{\alpha_n}$$

with distinct $x_i \in S$ and $\alpha_i \in \mathbb{Z}$. The image of such an element is

$$\overline{\varphi}(x_1^{\alpha_1} \dots x_n^{\alpha_n}) = \alpha_1 e_{x_1} + \dots + \alpha_n e_{x_n}.$$

This sum is zero in the direct sum if and only if all coefficients α_i are zero, which implies the original element was the identity. Thus $\overline{\varphi}$ is injective and hence an isomorphism.

2. Suppose there exists an isomorphism $\tau : \mathbb{Z}^m \to \mathbb{Z}^n$. For any integer $k \geq 2$, the subgroup $k\mathbb{Z}^m$ maps to $k\mathbb{Z}^n$. Thus τ induces an isomorphism on the quotient groups:

$$\mathbb{Z}^m / k\mathbb{Z}^m \cong \mathbb{Z}^n / k\mathbb{Z}^n.$$

The order of the left group is k^m, while the order of the right group is k^n. For these to be equal, we must have $m = n$, which contradicts the assumption $m \neq n$.

■

This theorem justifies the classification of finitely generated free Abelian groups by a single integer invariant.

Corollary 7.1. *Uniqueness of Rank.* A finitely generated free Abelian group $\mathbb{Z}(S)$ is isomorphic to $\mathbb{Z}^{|S|}$. The integer $|S|$ is an invariant of the group.

推論

Proof

This is the content of *theorem 7.3*(2).

■

Definition 7.8. ***Basis and Rank.***
Let $G = \mathbb{Z}(S)$ be a finitely generated free Abelian group.

- The generating set S is called a **basis** of G.
- The size $|S|$ is called the **rank** of G, denoted $\operatorname{rank} G$.

定義

Remark.

Just as vector spaces have multiple bases, a free Abelian group possesses multiple bases. Let $S = \{x_1, \dots, x_n\}$ be a basis. Any element $g \in \mathbb{Z}(S)$ has a unique representation $g = x_1^{\alpha_1} \dots x_n^{\alpha_n}$. If $Y = \{y_1, \dots, y_n\}$ is another basis, we can express each basis in

terms of the other:

$$y_j = \prod_{i=1}^{n} x_i^{\alpha_{ij}} \quad \text{and} \quad x_j = \prod_{i=1}^{n} y_i^{\beta_{ij}}.$$

Defining matrices $A = (\alpha_{ij})$ and $B = (\beta_{ij})$ in $M_n(\mathbb{Z})$, the substitution of one basis into the other implies $AB = BA = I_n$. Thus, bases of $\mathbb{Z}^n$ are related by invertible integer matrices (matrices in $\mathrm{GL}_n(\mathbb{Z})$).

7.4 *Structure of Finitely Generated Abelian Groups*

We are now in a position to classify all finitely generated Abelian groups. The classification proceeds by showing that any such group is a direct sum of cyclic groups. The first step is to understand the structure of subgroups of free Abelian groups.

Lemma 7.1. ***Minimal Coefficient Lemma.***
Let G be free Abelian of rank n and $H \leq G$ non-zero. Define

$$I = \{s \in \mathbb{Z} \mid \exists \text{ basis } \{y_1, \ldots, y_n\} \text{ of } G \text{ and } \alpha \in H \text{ such that } \alpha = sy_1 + k_2y_2 + \cdots + k_ny_n\}.$$

Then I contains a smallest positive element d_1, and there exists a basis $\{x_1, \ldots, x_n\}$ of G and an element $\alpha \in H$ with $\alpha = d_1x_1$.

引理

Remark.

Swapping basis elements shows that any coordinate appearing in an expression for $\alpha \in H$ can be moved into the first position, so the same minimality argument applies to all coordinates.

Proof

If $s \in I$ and $t \in \mathbb{Z}$, then $ts \in I$ by replacing α with $t\alpha$. Since $H \neq 0$, I contains a positive integer; let d_1 be the smallest such. By definition, there exists a basis $\{y_1, \ldots, y_n\}$ and $\alpha \in H$ with

$$\alpha = d_1y_1 + k_2y_2 + \cdots + k_ny_n.$$

Write $k_i = q_id_1 + r_i$ with $0 \leq r_i < d_1$. Then

$$\alpha = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + r_2y_2 + \cdots + r_ny_n.$$

Let $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. Since $\{x_1, y_2, \ldots, y_n\}$ is a basis, each $r_i \in I$ (swap the coordinate containing r_i into the first slot). By minimality of d_1, all $r_i = 0$, so $\alpha = d_1x_1$.

■

Lemma 7.2. ***Coordinate Swap Lemma.***
Let G be free Abelian with basis $\{x_1, \dots, x_n\}$. If $dx_2 \in H$, then $d \in I$ (swap x_1 and x_2 in the basis).

引理

Proof

Replace the basis $\{x_1, x_2, \dots, x_n\}$ with $\{x_2, x_1, x_3, \dots, x_n\}$. Then dx_2 has coefficient d in the first position, so $d \in I$ by definition.

■

Lemma 7.3. ***Decomposition Lemma.***
Let G be free Abelian with basis $\{x_1, \dots, x_n\}$ and let $\alpha = d_1 x_1 \in H$. Set $G_1 = \langle x_2, \dots, x_n \rangle$. Then

$$H = \langle \alpha \rangle \oplus (H \cap G_1).$$

引理

Proof

Since $\langle x_1 \rangle \cap G_1 = \{0\}$, we have $\langle \alpha \rangle \cap (H \cap G_1) = \{0\}$. For any $h \in H$, write

$$h = k_1 x_1 + k_2 x_2 + \cdots + k_n x_n.$$

Since $k_1 \in I$, write $k_1 = q d_1 + r$ with $0 \le r < d_1$. By *lemma 7.2*, $r \in I$, so minimality gives $r = 0$ and $k_1 x_1 \in \langle \alpha \rangle$. Hence $h - k_1 x_1 \in H \cap G_1$, and the decomposition follows.

■

Theorem 7.4. ***Subgroups of Free Abelian Groups.***
Let G be a finitely generated free Abelian group of rank n. Let H be a non-zero subgroup of G. Then H is a free Abelian group of rank $r \le n$. Furthermore, there exists a basis $\{x_1, \dots, x_n\}$ of G and positive integers $d_1 \mid d_2 \mid \cdots \mid d_r$ such that $\{d_1 x_1, \dots, d_r x_r\}$ is a basis for H.

定理

We proceed by induction on $n = \operatorname{rank} G$.

Base case: $n = 1$.

Then $G \cong \mathbb{Z}$ and any non-zero subgroup is $d_1\mathbb{Z}$, which is free of rank 1 with basis $\{d_1\}$.

証明終

Inductive step.

Assume the result holds for rank $< n$. By *lemma 7.1*, there is a basis $\{x_1, \dots, x_n\}$ and $\alpha = d_1 x_1 \in H$. Let $G_1 = \langle x_2, \dots, x_n \rangle$. By *lemma 7.3*,

$$H = \langle d_1 x_1 \rangle \oplus (H \cap G_1).$$

If $H \cap G_1 = \{0\}$, we are done with $r = 1$. Otherwise, $H \cap G_1$ is

a non-zero subgroup of the free Abelian group G_1 of rank $n - 1$. By induction, there exist a basis $\{x_2, \ldots, x_n\}$ of G_1 and integers $d_2 \mid \cdots \mid d_r$ such that $\{d_2 x_2, \ldots, d_r x_r\}$ is a basis for $H \cap G_1$. Then $\{x_1, \ldots, x_n\}$ is a basis of G and $\{d_1 x_1, \ldots, d_r x_r\}$ is a basis of H. It remains to show $d_1 \mid d_2$. Since $d_2 \in I$, write $d_2 = q d_1 + r$ with $0 \leq r < d_1$. By *lemma 7.2*, swapping coordinates allows r to appear in the first slot, so $r \in I$, and minimality gives $r = 0$. Hence $d_1 \mid d_2$.

証明終

This theorem allows us to derive the invariant factor decomposition.

Theorem 7.5. ***Invariant Factor Decomposition.***
Let A be a finitely generated Abelian group. Then

$$A \cong \mathbb{Z}^k \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z},$$

where $k \geq 0$ is the rank, and $m_1 \mid m_2 \mid \cdots \mid m_s$ are integers greater than 1. These integers are uniquely determined by A and are called the **invariant factors**.

定理

Proof

Since A is finitely generated, there is a surjective homomorphism $\varphi : \mathbb{Z}^n \to A$ from a free Abelian group of rank n. Let $K = \ker \varphi$. By the previous theorem, there is a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{Z}^n$ and integers $d_1 \mid \cdots \mid d_r$ such that $\{d_1 x_1, \ldots, d_r x_r\}$ generates K. Then

$$A \cong \mathbb{Z}^n / K \cong \left(\bigoplus_{i=1}^{n} \mathbb{Z} x_i \right) \Big/ \left(\bigoplus_{j=1}^{r} \mathbb{Z} d_j x_j \right).$$

The quotient splits component-wise:

$$A \cong \left(\bigoplus_{j=1}^{r} \mathbb{Z} x_j / \mathbb{Z} d_j x_j \right) \oplus \left(\bigoplus_{i=r+1}^{n} \mathbb{Z} x_i \right).$$

The terms $\mathbb{Z}x_j / \mathbb{Z}d_j x_j$ are isomorphic to $\mathbb{Z}/d_j\mathbb{Z}$. If $d_j = 1$, the group is trivial and can be omitted. Let $m_1, \ldots, m_s$ be the values of $d_j > 1$. The free part has rank $k = n - r$.

■

We defer the uniqueness of the invariant factors to the proof of the elementary divisor theorem below.

Definition 7.9. ***Torsion Subgroup.***
The set of elements of finite order in an Abelian group A forms a subgroup called the **torsion subgroup**, denoted A_t:

$$A_t = \{a \in A \mid \exists n \in \mathbb{Z}^+, na = 0\}.$$

定義

In the decomposition above, $A_t \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z}$. The group A splits as $A \cong \mathbb{Z}^k \oplus A_t$.

Elementary Divisors

Alternatively, we can decompose the finite cyclic factors using the Chinese Remainder Theorem. If $m = p_1^{e_1} \dots p_k^{e_k}$, then $\mathbb{Z}/m\mathbb{Z} \cong \bigoplus \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. Applying this to each invariant factor m_j yields a decomposition into prime power orders.

Theorem 7.6. ***Elementary Divisor Decomposition.***
Any finitely generated Abelian group A is isomorphic to:

$$A \cong \mathbb{Z}^k \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/q_i\mathbb{Z},$$

where each q_i is a power of a prime $p_i^{e_i}$. The prime powers $\{q_1, \dots, q_t\}$ are uniquely determined and are called the **elementary divisors** of A.

定理

Proof

Write $A \cong \mathbb{Z}^k \oplus T$ with T finite, and apply the invariant factor decomposition to T:

$$T \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_s\mathbb{Z}, \quad m_1 \mid \cdots \mid m_s.$$

For each j, factor $m_j = \prod_p p^{e_{j,p}}$. By the Chinese Remainder Theorem,

$$\mathbb{Z}/m_j\mathbb{Z} \cong \bigoplus_p \mathbb{Z}/p^{e_{j,p}}\mathbb{Z}.$$

Collecting all prime power factors across the m_j gives the elementary divisor decomposition.
For uniqueness, fix a prime p and define

$$T[p^k] = \{t \in T \mid p^k t = 0\}.$$

Then each quotient $T[p^k]/T[p^{k-1}]$ is a vector space over $\mathbb{F}_p$ (the finite field with p elements), and its dimension depends only on T. If $T \cong \bigoplus_i \mathbb{Z}/p^{e_i}\mathbb{Z}$, then

$$\dim_{\mathbb{F}_p}\left(T[p^k]/T[p^{k-1}]\right) = \#\{i \mid e_i \geq k\}.$$

Hence the multiset $\{e_i\}$ is determined by T, so the multiset of elementary divisors is unique. Choose a prime $p \nmid |T|$. Then $T/pT = 0$ and

$$A/pA \cong (\mathbb{Z}/p\mathbb{Z})^k,$$

so $k = \dim_{\mathbb{F}_p}(A/pA)$ (dimension as a vector space over $\mathbb{F}_p$, the finite field with p elements) is uniquely determined. Thus the full decomposition is unique.

■

Theorem 7.7. ***Classification Theorem.***
Two finitely generated Abelian groups are isomorphic if and only if they have the same rank and the same set of elementary divisors (or equivalently, the same invariant factors).

定理

Proof

If two groups have the same rank and the same elementary divisors, their decompositions in the previous theorem are isomorphic term-by-term, so the groups are isomorphic. Conversely, isomorphic groups have the same rank and the same elementary divisors by uniqueness, so the invariants agree.

■

Example 7.5. Groups of Order 8. We classify Abelian groups of order 8. The partition of 8 into prime powers 2^k gives the elementary divisors.

1. 8: $A \cong \mathbb{Z}/8\mathbb{Z}$. Invariant factor: $\{8\}$.
2. $4+2$: $A \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Invariant factors: $2 \mid 4$.
3. $2+2+2$: $A \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Invariant factors: $2 \mid 2 \mid 2$.

There are exactly 3 isomorphism classes.

範例

Example 7.6. Order 1500. Let $|A| = 1500 = 2^2 \cdot 3^1 \cdot 5^3$. We determine the possible structures by partitioning the exponent of each prime.

Prime 2 (2^2): Partitions of 2: (2) or $(1,1)$. Possible factors: $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Prime 3 (3^1): Partitions of 1: (1). Possible factor: $\mathbb{Z}/3\mathbb{Z}$.

Prime 5 (5^3): Partitions of 3: (3), $(2,1)$, or $(1,1,1)$. Possible factors: $\mathbb{Z}/125\mathbb{Z}$, $\mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Thus the elementary divisors are:

$$\{2,2,3,5,5,5\}, \quad \{4,3,5,5,5\}, \quad \{2,2,3,5,25\}, \quad \{4,3,5,25\}, \quad \{2,2,3,125\}, \quad \{4,3,125\}.$$

Hence there are exactly 6 isomorphism classes of Abelian groups of order 1500.

範例

Example 7.7. Non-Abelian Groups of Order 8. Although not covered by the structure theorem, we can classify non-Abelian groups of order 8. If G is non-Abelian, it cannot have an element of order 8 (cyclic) or exponent 2 (Abelian). Thus elements have order 1, 2, 4. Let x be an element of order 4. $\langle x \rangle$ has index 2, so it is normal. Let $y \notin \langle x \rangle$. Then $y^2 \in \langle x \rangle$. Since $yxy^{-1} \in \langle x \rangle$ and has order 4, and x and y do not commute, $yxy^{-1} = x^{-1}$.

- If $y^2 = 1$, we get $D_4 = \langle x, y \mid x^4 = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$.
- If $y^2 = x^2$ (order 2), we get the Quaternion group $Q_8 = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$.

Using matrices:

$$Q_8 \cong \left\langle \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle \subset \mathrm{GL}_2(\mathbb{C}).$$

範例

7.5 *Exercises*

1. **Free Group Structure.** Let $F = F(x, y)$.
   (a) Prove that the subgroup generated by $u = x^2$ and $v = y^3$ is free on $\{u, v\}$.
   (b) Prove that the subgroup generated by $u = x^2, v = y^2, z = xy$ is free on $\{u, v, z\}$.
   (c) Prove or disprove: $F(x, y) \cong \mathbb{Z} \times \mathbb{Z}$.
2. **Dihedral Presentation.**
   (a) Verify that the dihedral group of a regular $2n$-gon is isomorphic to $D_n \times \mathbb{Z}/2\mathbb{Z}$ if n is odd.
   (b) Give a presentation for D_∞, the infinite dihedral group.
3. **Symmetric Group Presentation.** Show that S_n has the presentation:

   $$S_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i^2 = 1, (\sigma_i \sigma_{i+1})^3 = 1, (\sigma_i \sigma_j)^2 = 1 \text{ for } |i - j| > 1 \rangle.$$

4. **Isomorphism Check.** For $n \geq 3$, determine if $A_n \times \mathbb{Z}/2\mathbb{Z} \cong S_n$.
5. **Braid Group.** Define the 3-strand braid group B_3 geometrically (strings connecting points on two planes). Prove it has the presentation $\langle \sigma_1, \sigma_2 \mid \sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2 \rangle$.
6. **Product Structure.**
   (a) Is every subgroup of $G_1 \times \cdots \times G_n$ of the form $H_1 \times \cdots \times H_n$?
   (b) If $|G_i|$ are pairwise coprime, prove that every subgroup is a direct product of subgroups of the factors.

7. **Simple Factors.** Let G_1, G_2 be non-Abelian simple groups. Prove that the only non-trivial normal subgroups of $G_1 \times G_2$ are $G_1 \times \{1\}$ and $\{1\} \times G_2$.

8. **Rational Group.**
   (a) Prove $\mathbb{Q}$ is not a free Abelian group.
   (b) Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.
   (c) Prove $\mathbb{Q}^+$ (multiplicative) is free Abelian with basis the primes.

9. **Rank Inequality.** Let G be a finitely generated free Abelian group of rank r. If $g_1, \ldots, g_n$ generate G, prove $n \geq r$.

10. **Subgroup Existence.** Let A be a finite Abelian group.
    (a) For every divisor d of $|A|$, prove A has a subgroup of order d.
    (b) For every divisor d, prove A has a quotient of order d.

11. **Structure Theorem Practice.**
    (a) Classify Abelian groups of order 18 and 33.
    (b) Express the number of Abelian groups of order n in terms of the prime factorization of n and the partition function $p(k)$.
    (c) Determine the invariant factors of $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.
    (d) Find the elementary divisors of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/35\mathbb{Z}$.

12. **Vector Space Analogy.** Let $V = \mathbb{F}_p^n$ (the n-dimensional vector space over $\mathbb{F}_p$, the finite field with p elements).
    (a) Find the number of subgroups of order p^{n-1}.
    (b) Prove the number of subgroups of order p^k equals the number of subgroups of order p^{n-k} (duality).

13. **Non-Cyclic Property.** Prove that if a finite Abelian group A is not cyclic, it contains a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some prime p.

14. **Cyclic Order.** Prove that a group of order $5 \cdot 7 \cdot 13$ must be cyclic.