Bachelors with Mathematics as Major

5th Semester

MMT522J1: Mathematics/Applied Mathematics: Algebra-I

Credits: 3 THEORY + 1 TUTORIAL **Theory: 45 Hours & Tutorial: 15 Hours**

Course Objective: To introduce students towards basic concepts of algebraic structures, viz groups and rings. (ii) to identify various properties associated with the groups and rings. (iii) to expose students towards advanced mathematics, such as advanced abstract algebra and communtative ring theory.

Course Outcomes: After the completion of this course, students shall be able to (i) understand group through symmetries in nature and can identify patterns. (ii) shall be able to apply these concepts in linear classical groups to solve problems arising in physics, computer science, economics and engineering etc.

Theory: 3 Credits

Unit I

Binary composition, equivalence relation and equivalence class. Groups: Definition and examples, Finite & Infinite groups, abelian & non-abelian groups. Properties of groups: uniqueness of identity/ inverse and cancellation laws. Subgroups and Cosets. Criterion of subgroups, order of an element, Lagrange's theorem. Cyclic groups: Definition & examples, cyclic groups are abelian, order of a cyclic group is equal to the order of its generator.

Unit II

Normal subgroups: Definition & examples, criterion of normal subgroups, product of subgroups, Quotient groups. Homomorphism, kernel of a homomorphism, Fundamental theorem of homomorphism, Isomorphism theorems (statements only), Normalizer of an element, Centre of a group. Permutation groups and Cayley's theorem. Definitions and examples of symmetric groups and alternating groups.

Unit III

Rings: Definition & Examples, elementary properties of rings, rings with & without zero divisors, Integral domains & skew fields. Definitions & examples of Fields, Subrings, Ideals, Quotient rings and Boolean rings. A finite integral domain is a field. Ring homomorphism, fundamental theorem of homomorphism & ring isomorphism. Prime, Maximal and Principal ideals (Definitions & examples only).

Tutorial: 1 Credit

Unit IV

Examples of monoids, semigroups, abelian/non-abelian, cyclic/non-cyclic groups, computing generators in a cyclic group, Structure theorem for cyclic groups (statement only), concept of even and odd permutation. Examples of commutative & non-commutative rings, Left & right ideal of a ring, relation between ideals & subrings, sum & product of ideals.

Recommended Books:

1. I. N. Herstein, Topics in Algebra, John Wiley, 1975.
2. Joseph Gallian , Abstract Algebra, Narosa Publishers, New Delhi, 1999.
3. M. Artin, Algebra, Pearson Education India, 2011.
4. D. S. Dumit and R. M. Foote, Abstract Algebra, John Wiley, 2003
5. P.B. Bhattachariya, S.K. Jain, S. R. Nagpaul, Basic Abstract Algebra, Cambridge University Press, 1994
6. Surjeet singh and Qazi Zameeruddin, Modern Algebra, S Chand And Company Ltd, 2021

——Algebra I - (MMT522J1)—–

Author: Dr. Aijaz

Assistant Professor of Mathematics

JK Higher Education Department

All stuyd materials for UG Mathematics, PG Mathematics, Entrance Exams in Mathematics like NET-JRF/SET/GATE/PhD etc are avalaible at

Website: aijaz.vercel.app

Chapter 1

Groups and Subgroups

1.1 Preliminaries: Sets, Relations, and Compositions

Definition 1.1.1 (Binary Composition)**.** A **binary composition** (or **binary operation**) on a non-empty set S is a function $* : S \times S \to S$. For any pair of elements $(a, b) \in S \times S$, the element $*(a, b)$ is usually written as $a * b$. The crucial property is **closure**: for all $a, b \in S$, the result $a * b$ must also be an element of S.

Example 1.1.2.
1. Addition $(+)$ is a binary composition on the set of integers $\mathbb{Z}$. For any two integers $a, b \in \mathbb{Z}$, their sum $a + b$ is also a unique integer in $\mathbb{Z}$.

2. Multiplication $(\cdot)$ is a binary composition on the set of real numbers $\mathbb{R}$. For any $a, b \in \mathbb{R}$, the product $a \cdot b$ is also a unique real number.

3. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with real entries. Standard matrix multiplication is a binary composition on $M_2(\mathbb{R})$ because the product of two such matrices is another 2×2 matrix with real entries.

4. Subtraction $(-)$ is *not* a binary composition on the set of natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$. For example, $3 \in \mathbb{N}$ and $5 \in \mathbb{N}$, but $3 - 5 = -2 \notin \mathbb{N}$. The set is not closed under subtraction.

1.1.1 Equivalence Relations and Classes

The idea of 'equivalence' is a way to formalize the notion that different elements of a set can be considered 'the same' in a particular context.

Definition 1.1.3 (Equivalence Relation)**.** A relation $\sim$ on a non-empty set S is an **equivalence relation** if it satisfies the following three properties for all $a, b, c \in S$:

1. **Reflexivity:** $a \sim a$. (Every element is related to itself.)

2. **Symmetry:** If $a \sim b$, then $b \sim a$. (The order of relation does not matter.)

3. **Transitivity:** If $a \sim b$ and $b \sim c$, then $a \sim c$. (The relation can be chained.)

Example 1.1.4.
1. The usual equality $(=)$ on the set of real numbers $\mathbb{R}$ is an equivalence relation. It is reflexive $(a = a)$, symmetric (if $a = b$, then $b = a$), and transitive (if $a = b$ and $b = c$, then $a = c$).

2. **Congruence Modulo n.** Let n be a fixed positive integer. For two integers $a, b \in \mathbb{Z}$, we say a is congruent to b modulo n, written $a \equiv b \pmod{n}$, if n divides $(a - b)$. This is a fundamental equivalence relation in algebra.
   - **Reflexive:** $a \equiv a \pmod{n}$ because n divides $(a - a) = 0$.
   - **Symmetric:** If $a \equiv b \pmod{n}$, then n divides $(a - b)$. This implies n also divides $-(a - b) = (b - a)$, so $b \equiv a \pmod{n}$.
   - **Transitive:** If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then n divides $(a - b)$ and n divides $(b - c)$. Therefore, n must divide their sum, $(a - b) + (b - c) = a - c$. Thus, $a \equiv c \pmod{n}$.

3. The relation "is parallel to" $(\|)$ on the set of all lines in a plane is an equivalence relation (assuming a line is parallel to itself).

4. The relation $\leq$ on $\mathbb{R}$ is *not* an equivalence relation. It is reflexive $(a \leq a)$ and transitive (if $a \leq b$ and $b \leq c$, then $a \leq c$), but it is not symmetric (e.g., $3 \leq 5$ but $5 \not\leq 3$).

An equivalence relation on a set S naturally groups elements together into disjoint subsets, called equivalence classes.

Definition 1.1.5 (Equivalence Class)**.** Let $\sim$ be an equivalence relation on a non-empty set S. For any element $a \in S$, the **equivalence class** of a, denoted by $[a]$, is the set of all elements in S that are equivalent to a. That is,

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

Example 1.1.6. Consider the relation of congruence modulo 3 on the set of integers $\mathbb{Z}$.

- The equivalence class of 0 is $[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 3\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$. This is the set of all integers divisible by 3.
- The equivalence class of 1 is $[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$. This is the set of all integers which leave a remainder of 1 when divided by 3.
- The equivalence class of 2 is $[2] = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$.
- Note that $[3] = [0]$, $[4] = [1]$, and so on. There are only three distinct equivalence classes: $[0], [1]$, and $[2]$.

The following theorem is fundamental, as it shows that an equivalence relation on a set S slices S up into non-overlapping pieces.

Theorem 1.1.7. *Let $\sim$ be an equivalence relation on a set S. Then the set of equivalence classes forms a partition of S. That is:*

1. *The union of all equivalence classes is the entire set S.*
2. *For any two equivalence classes $[a]$ and $[b]$, either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

Proof. To prove the first point, we must show that every element of S belongs to some equivalence class. For any $a \in S$, we know $a \sim a$ by reflexivity. Therefore, $a \in [a]$, which means every element is in its own equivalence class at the very least. This ensures their union covers all of S.

For the second point, let $[a]$ and $[b]$ be two equivalence classes. Suppose their intersection is not empty, so there exists some element c such that $c \in [a]$ and $c \in [b]$. By definition of equivalence class, this means $c \sim a$ and $c \sim b$. By symmetry, we have $a \sim c$. Now, using transitivity on $a \sim c$ and $c \sim b$, we get $a \sim b$.

We now show that this implies $[a] = [b]$. First, let x be an arbitrary element in $[a]$, so $x \sim a$. Since we have $a \sim b$, by transitivity, $x \sim b$, which means $x \in [b]$. This proves $[a] \subseteq [b]$. Next, let y be an arbitrary element in $[b]$, so $y \sim b$. From $a \sim b$, we have $b \sim a$ by symmetry. By transitivity on $y \sim b$ and $b \sim a$, we get $y \sim a$, which means $y \in [a]$. This proves $[b] \subseteq [a]$. Since we have shown inclusion in both directions, we conclude that $[a] = [b]$.

Therefore, any two equivalence classes are either completely disjoint (if their intersection is empty) or identical (if their intersection is non-empty). This completes the proof. ■

1.2 Group

Definition 1.2.1 (Group)**.** A **group** is a pair $(G, *)$, where G is a non-empty set and $*$ is a binary composition on G, satisfying the following four axioms:

1. **Closure:** For all $a, b \in G$, the element $a * b$ is also in G. (This is inherent in the definition of a binary composition but is often stated for emphasis.)
2. **Associativity:** For all $a, b, c \in G$, we have $(a * b) * c = a * (b * c)$.
3. **Identity Element:** There exists an element $e \in G$, called the **identity element**, such that for all $a \in G$, $a * e = e * a = a$.
4. **Inverse Element:** For each element $a \in G$, there exists an element $a^{-1} \in G$, called the **inverse** of a, such that $a * a^{-1} = a^{-1} * a = e$.

1.2.1 Examples of Groups

The abstract definition of a group is illuminated by concrete examples.

Example 1.2.2.

1. **The Integers under Addition:** The pair $(\mathbb{Z}, +)$ is a group.
   - Closure: The sum of two integers is an integer.
   - Associativity: $(a + b) + c = a + (b + c)$ for all integers.
   - Identity: The identity element is 0, since $a + 0 = 0 + a = a$.
   - Inverse: For any integer a, its inverse is $-a$, since $a + (-a) = 0$.

2. **The Non-Zero Rational Numbers under Multiplication:** The pair $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group. Zero must be excluded because it does not have a multiplicative inverse.
    - Closure: The product of two non-zero rational numbers is a non-zero rational number.
    - Associativity: Multiplication of rational numbers is associative.
    - Identity: The identity element is 1.
    - Inverse: For any $p/q \in \mathbb{Q} \setminus \{0\}$, its inverse is q/p.
3. **The General Linear Group:** Let $GL_2(\mathbb{R})$ be the set of all 2×2 matrices with real entries and a non-zero determinant. The pair $(GL_2(\mathbb{R}), \times)$, where $\times$ is standard matrix multiplication, is a group.
    - Closure: If $A, B \in GL_2(\mathbb{R})$, then $\det(AB) = \det(A)\det(B) \neq 0$, so $AB \in GL_2(\mathbb{R})$.
    - Associativity: Matrix multiplication is associative.
    - Identity: The identity element is the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
    - Inverse: For any $A \in GL_2(\mathbb{R})$, since $\det(A) \neq 0$, its inverse matrix A^{-1} exists and has a non-zero determinant, so $A^{-1} \in GL_2(\mathbb{R})$.
4. **The Integers Modulo n:** Let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ be the set of equivalence classes modulo n. The pair $(\mathbb{Z}_n, +_n)$, where $+_n$ is addition modulo n (i.e., $[a] +_n [b] = [a+b]$), is a group.
    - Closure: The sum of two classes modulo n is another class modulo n.
    - Associativity: Inherited from the associativity of addition in $\mathbb{Z}$.
    - Identity: The identity element is $[0]$.
    - Inverse: The inverse of $[a]$ is $[n-a]$.

1.2.2 Finite and Infinite Groups

Groups can be classified based on the number of elements they contain.

Definition 1.2.3 (Finite and Infinite Groups)**.** A group $(G, *)$ is a **finite group** if the set G has a finite number of elements. The number of elements in G, denoted by $|G|$, is called the **order** of the group. If G has an infinite number of elements, it is called an **infinite group**.

Example 1.2.4.

- The groups $(\mathbb{Z}, +)$ and $(GL_2(\mathbb{R}), \times)$ are **infinite groups**.
- The group $(\mathbb{Z}_n, +_n)$ is a **finite group** of order n. For instance, $(\mathbb{Z}_4, +_4)$ has elements $\{[0], [1], [2], [3]\}$ and its order is $|Z_4| = 4$.

1.2.3 Abelian and Non-Abelian Groups

The order in which elements are combined can be a defining characteristic of a group.

Definition 1.2.5 (Abelian Group)**.** A group $(G, *)$ is said to be **abelian** (or **commutative**) if for all $a, b \in G$, the commutative law holds:

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

A group that is not abelian is called **non-abelian**.

Example 1.2.6.

1. All the additive groups like $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are abelian because standard addition is commutative. The group $(\mathbb{Z}_n, +_n)$ is also abelian.
2. The multiplicative group $(\mathbb{Q} \setminus \{0\}, \cdot)$ is abelian because multiplication of rational numbers is commutative.
3. The general linear group $(GL_2(\mathbb{R}), \times)$ is **non-abelian**. To see this, consider two matrices from the group:

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Their products are:

$$AB = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$$

Since $AB \neq BA$, the group is non-abelian.

1.2.4 Elementary Properties of Groups

Theorem 1.2.7 (Uniqueness of the Identity)**.** *In a group $(G, *)$, the identity element is unique.*

Proof. Suppose that both e and e' are identity elements in G. Since e is an identity, we have $e * e' = e'$. Since e' is an identity, we have $e * e' = e$. By comparing the two expressions, we see that $e = e'$, proving that the identity element must be unique. ■

Theorem 1.2.8 (Uniqueness of Inverses)**.** *In a group $(G, *)$, every element $a \in G$ has a unique inverse.*

Proof. Let a be an arbitrary element of G. Suppose that both b and c are inverses of a. This means $a * b = e$ and $a * c = e$. We can write $b = e * b$. Substituting $e = c * a$, we get $b = (c * a) * b$. By the associative property, this becomes $b = c * (a * b)$. Since b is an inverse of a, we know $a * b = e$. Thus, $b = c * e$. Finally, by the property of the identity element e, we have $b = c$. Therefore, the inverse of any element is unique. ■

The existence of unique inverses allows for a crucial property in solving equations within groups.

Theorem 1.2.9 (Cancellation Laws)**.** *Let $(G, *)$ be a group. For any $a, b, c \in G$:*

1. ***Left Cancellation:*** *If $a * b = a * c$, then $b = c$.*

2. ***Right Cancellation:*** *If $b * a = c * a$, then $b = c$.*

Proof. (1) Assume $a * b = a * c$. Since $a \in G$, its unique inverse a^{-1} exists in G. Multiplying the equation on the left by a^{-1} gives $a^{-1} * (a * b) = a^{-1} * (a * c)$. Using associativity, we get $(a^{-1} * a) * b = (a^{-1} * a) * c$. This simplifies to $e * b = e * c$, and by the identity property, $b = c$.

(2) The proof for right cancellation is analogous. Assume $b * a = c * a$. Multiplying on the right by a^{-1} yields $(b * a) * a^{-1} = (c * a) * a^{-1}$. By associativity, $b * (a * a^{-1}) = c * (a * a^{-1})$. This simplifies to $b * e = c * e$, which gives $b = c$. ■

Remark 1.2.10. It is important to note that in a non-abelian group, we cannot assume that $a * b = c * a$ implies $b = c$. The cancellation laws only apply when the common element is on the same side of the equation.

Finally, we establish a useful rule for finding the inverse of a product of two elements.

Theorem 1.2.11 (Socks-Shoes Property)**.** *For any two elements a, b in a group $(G, *)$, the inverse of their product is given by $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Proof. To prove that $b^{-1} * a^{-1}$ is the inverse of $(a * b)$, we must show that their product in both orders yields the identity element e. Consider the product $(a * b) * (b^{-1} * a^{-1})$. By associativity, we can regroup this as $a * (b * b^{-1}) * a^{-1}$. Since $b * b^{-1} = e$, this becomes $a * e * a^{-1}$, which simplifies to $a * a^{-1} = e$. Now consider the product in the other order: $(b^{-1} * a^{-1}) * (a * b)$. Regrouping gives $b^{-1} * (a^{-1} * a) * b$. Since $a^{-1} * a = e$, this becomes $b^{-1} * e * b$, which simplifies to $b^{-1} * b = e$. Since the result is e in both cases and inverses are unique, it must be that $(a * b)^{-1} = b^{-1} * a^{-1}$. ■

Remark 1.2.12. This property is humorously named the "socks-shoes property" because the order of operations is reversed, just like taking off your shoes and socks. You put your socks on first, then your shoes, but to undo it, you must take off your shoes first, then your socks.

1.3 Subgroups and Lagrange's Theorem

Within a group, it is often possible to find smaller sets that retain the group structure. These are called subgroups, and their relationship to the parent group is fundamental to understanding the group's overall structure.

1.3.1 Subgroups

Definition 1.3.1 (Subgroup)**.** Let $(G, *)$ be a group. A non-empty subset H of G is a **subgroup** of G if $(H, *)$ is itself a group under the same operation $*$ inherited from G. We denote this by $H \leq G$.

To check if a subset H is a subgroup, one could verify all the group axioms. However, a more efficient method exists, known as the subgroup criterion.

Theorem 1.3.2 (Subgroup Criterion)**.** *A non-empty subset H of a group G is a subgroup of G if and only if for every $a, b \in H$, the element $a * b^{-1}$ is also in H.*

Proof. First, assume H is a subgroup. If $a, b \in H$, then by the inverse property for H, $b^{-1} \in H$. By closure in H, $a * b^{-1} \in H$. This proves the condition is necessary.

Conversely, assume the condition holds for a non-empty subset H. We must show H is a group.

- **Identity:** Since H is non-empty, let $a \in H$. Applying the criterion with $b = a$, we have $a * a^{-1} = e \in H$. So H contains the identity.

- **Inverse:** Let $b \in H$. We know $e \in H$. Applying the criterion with $a = e$, we have $e * b^{-1} = b^{-1} \in H$. Thus, every element in H has its inverse in H.
- **Closure:** Let $a, b \in H$. We just showed that $b^{-1} \in H$. Applying the criterion to a and b^{-1}, we get $a * (b^{-1})^{-1} = a * b \in H$. So H is closed under the operation.
- **Associativity:** The operation is associative for all elements in G, so it is automatically associative for all elements in the subset H.

Thus, H is a subgroup of G. ■

Example 1.3.3.

1. The set of even integers $(2\mathbb{Z}, +)$ is a subgroup of the group of all integers $(\mathbb{Z}, +)$. If $a = 2k_1$ and $b = 2k_2$ are two even integers, then $a - b = 2(k_1 - k_2)$ is also an even integer, so the criterion holds.
2. The set $SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid \det(A) = 1\}$, known as the special linear group, is a subgroup of $GL_2(\mathbb{R})$. If $A, B \in SL_2(\mathbb{R})$, then $\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1 \cdot (\det(B))^{-1} = 1 \cdot 1^{-1} = 1$. So $AB^{-1} \in SL_2(\mathbb{R})$.
3. $\{[0], [2], [4]\}$ is a subgroup of $(\mathbb{Z}_6, +_6)$.

1.3.2 Order of an Element

Definition 1.3.4 (Order of an Element)**.** The **order** of an element a in a group G, denoted $|a|$, is the smallest positive integer n such that $a^n = e$. If no such integer exists, the order of a is said to be **infinite**. (Here a^n means $a * a * \cdots * a$, n times).

Example 1.3.5.

- In $(\mathbb{Z}_6, +_6)$, the order of $[2]$ is 3 because $[2]^1 = [2]$, $[2]^2 = [2] + [2] = [4]$, and $[2]^3 = [2] + [2] + [2] = [6] = [0]$. So $|[2]| = 3$.
- In $(\mathbb{Z}, +)$, every non-zero element has infinite order. For any $a \neq 0$, $na = a + \cdots + a$ can never be the identity element 0 for a positive integer n.
- In $(GL_2(\mathbb{R}), \times)$, the matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4, since $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$.

1.3.3 Cosets

Cosets are fundamental building blocks for partitioning a group based on one of its subgroups.

Definition 1.3.6 (Cosets)**.** Let H be a subgroup of a group G. For any element $a \in G$, the set

$$aH = \{ah \mid h \in H\}$$

is called the **left coset** of H in G containing a. Similarly, the **right coset** is $Ha = \{ha \mid h \in H\}$.

Remark 1.3.7. In an abelian group, the left and right cosets of a subgroup are always identical. For a non-abelian group, they may be different.

Example 1.3.8. Consider the group $G = \mathbb{Z}$ and the subgroup $H = 4\mathbb{Z} = \{\ldots, -4, 0, 4, 8, \ldots\}$. The distinct left cosets are:

- $0 + H = 4\mathbb{Z} = \{\ldots, -4, 0, 4, \ldots\}$
- $1 + H = \{1 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -3, 1, 5, \ldots\}$
- $2 + H = \{2 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -2, 2, 6, \ldots\}$
- $3 + H = \{3 + 4k \mid k \in \mathbb{Z}\} = \{\ldots, -1, 3, 7, \ldots\}$

Any other coset, like $4 + H$ or $5 + H$, will be identical to one of these. These four cosets form a partition of $\mathbb{Z}$.

A crucial property of cosets is that they all have the same size.

Theorem 1.3.9. *Let H be a subgroup of G. For any $a \in G$, there is a one-to-one correspondence between the elements of H and the elements of the coset aH. Thus, $|H| = |aH|$.*

Proof. Consider the map $\phi : H \to aH$ defined by $\phi(h) = ah$. This map is surjective by the definition of aH. To show it is injective, suppose $\phi(h_1) = \phi(h_2)$ for some $h_1, h_2 \in H$. This means $ah_1 = ah_2$. By the left cancellation law in G, we can cancel a to get $h_1 = h_2$. Thus, ϕ is a bijection, and the sets H and aH must have the same number of elements. ■

1.3.4 Lagrange's Theorem

We now arrive at one of the most important theorems in finite group theory, which elegantly connects the order of a subgroup to the order of the group.

Theorem 1.3.10 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. That is, $|H| \mid |G|$.*

Proof. Let $|G| = n$ and $|H| = m$. The set of left cosets of H in G forms a partition of G. This means that every element of G belongs to exactly one left coset of H. Let the distinct left cosets be $a_1H, a_2H, \ldots, a_kH$. Then $G = a_1H \cup a_2H \cup \cdots \cup a_kH$, and the union is disjoint. Taking the order of both sides, we get $|G| = |a_1H| + |a_2H| + \cdots + |a_kH|$. From the previous theorem, we know that $|a_iH| = |H| = m$ for all $i = 1, \ldots, k$. Therefore, $n = m + m + \cdots + m$ (k times), which gives $n = km$. This shows that m divides n, or $|H|$ divides $|G|$. ■

The number of distinct left cosets, k, is called the **index** of H in G, denoted $[G : H]$. From the proof, we have $|G| = [G : H]|H|$.

Lagrange's theorem has powerful consequences.

Corollary 1.3.11. *In a finite group G, the order of any element $a \in G$ must divide the order of the group.*

Proof. The order of the element a is the order of the cyclic subgroup generated by a, denoted $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. Since $\langle a \rangle$ is a subgroup of G, by Lagrange's Theorem, $|\langle a \rangle|$ must divide $|G|$. But $|\langle a \rangle|$ is precisely the order of the element a. ■

Corollary 1.3.12. *A group of prime order p has no non-trivial subgroups (its only subgroups are $\{e\}$ and the group itself).*

Proof. Let H be a subgroup of a group G with $|G| = p$. By Lagrange's theorem, $|H|$ must divide p. Since p is prime, its only positive divisors are 1 and p. Therefore, $|H| = 1$ (so $H = \{e\}$) or $|H| = p$ (so $H = G$). ■

1.3.5 Cyclic Groups

Among the simplest and most important types of groups are those whose entire structure can be described by a single element. These are known as cyclic groups.

Definition 1.3.13 (Cyclic Group)**.** A group G is called a **cyclic group** if there exists an element $a \in G$ such that every element of G can be expressed as a power of a. That is, for every $g \in G$, there is some integer k such that $g = a^k$. The element a is called a **generator** of the group, and we write $G = \langle a \rangle$.

Remark 1.3.14. In an additive group, the notation a^k corresponds to the multiple $ka = a + a + \cdots + a$ (k times), and a^{-k} corresponds to $(-k)a$.

Example 1.3.15.

1. The group of integers under addition, $(\mathbb{Z}, +)$, is an infinite cyclic group. It can be generated by 1 (since any integer k is $k \cdot 1$) or by -1 (since $k = (-k) \cdot (-1)$). So, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

2. The group of integers modulo n under addition, $(\mathbb{Z}_n, +_n)$, is a finite cyclic group of order n. It is generated by $[1]$, since any element $[k]$ can be obtained by adding $[1]$ to itself k times. For example, in $\mathbb{Z}_6$, we have $\mathbb{Z}_6 = \langle [1] \rangle$. Note that other elements can also be generators; in $\mathbb{Z}_6$, $[5]$ is also a generator, but $[2]$ is not as it only generates the subgroup $\{[0], [2], [4]\}$.

3. The group $U(10) = \{1, 3, 7, 9\}$ under multiplication modulo 10 is a cyclic group. It is generated by 3: $3^1 = 3$, $3^2 = 9$, $3^3 = 27 \equiv 7$, $3^4 = 81 \equiv 1$. So, $U(10) = \langle 3 \rangle$.

Cyclic groups have a beautifully simple structure, which leads to a very important property.

Theorem 1.3.16. *Every cyclic group is abelian.*

Proof. Let $G = \langle a \rangle$ be a cyclic group with generator a. Let x and y be any two elements in G. By the definition of a cyclic group, there exist integers m and n such that $x = a^m$ and $y = a^n$. Then, using the laws of exponents (which follow from associativity), we have:

$$x * y = a^m * a^n = a^{m+n}$$

And in the other order:

$$y * x = a^n * a^m = a^{n+m}$$

Since integer addition is commutative, $m + n = n + m$, so $a^{m+n} = a^{n+m}$. Therefore, $x * y = y * x$. As x and y were arbitrary, the group G is abelian. ■

Remark 1.3.17. The converse is not true. A group being abelian does not guarantee it is cyclic. For example, the Klein four-group $V_4 = \{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e$ and $ab = c, ba = c$, etc., is abelian but not cyclic, as no single element generates the entire group.

The order of a cyclic group is directly tied to the order of its generator, a fact which is central to their study.

Theorem 1.3.18. *The order of a finite cyclic group is equal to the order of its generator.*

Proof. Let $G = \langle a \rangle$ be a finite cyclic group and let the order of the generator a be n. By definition, n is the smallest positive integer such that $a^n = e$. Consider the set of elements $S = \{a^0, a^1, a^2, \dots, a^{n-1}\}$. These n elements are all distinct. If they were not, say $a^i = a^j$ for $0 \leq j < i < n$, then multiplying by $(a^j)^{-1} = a^{-j}$ would give $a^{i-j} = e$. But $0 < i - j < n$, which contradicts the fact that n is the smallest positive integer for which $a^n = e$. Thus, the set S contains exactly n distinct elements. We now show that S is the entire group G. Since G is cyclic with generator a, any element $g \in G$ can be written as $g = a^k$ for some integer k. By the division algorithm, we can write $k = qn + r$, where q is the quotient and r is the remainder with $0 \leq r < n$. Then $g = a^k = a^{qn+r} = (a^n)^q * a^r = e^q * a^r = e * a^r = a^r$. Since $0 \leq r < n$, the element a^r is in the set S. This shows that every element of G is in S, so $G = S$. Therefore, the number of elements in G is the number of elements in S, which is n. So, $|G| = n = |a|$. ■

Theorem 1.3.19 (Generators of $\mathbb{Z}_n$)**.** *An element $[k]$ is a generator of the cyclic group $(\mathbb{Z}_n, +_n)$ if and only if the greatest common divisor of k and n is 1. That is, $\mathbb{Z}_n = \langle [k] \rangle$ if and only if* $\gcd(k, n) = 1$.

Proof. We will prove this statement in two parts.

First, assume that $[k]$ is a generator of $\mathbb{Z}_n$. This means that every element in $\mathbb{Z}_n$ can be expressed as a multiple of $[k]$. In particular, the identity element of the parent group $(\mathbb{Z}, +)$, which is 1, must be generatable. So, the element $[1] \in \mathbb{Z}_n$ must be a multiple of $[k]$. This implies there exists an integer m such that $m \cdot [k] = [1]$. By the definition of addition modulo n, this is equivalent to the congruence relation $mk \equiv 1 \pmod{n}$. This congruence means that n divides $(mk - 1)$, so there exists an integer q such that $mk - 1 = qn$. Rearranging this equation gives $mk - qn = 1$. This is an integer linear combination of k and n that equals 1. By a fundamental result of number theory (Bézout's Identity), if such an integer solution $(m, -q)$ exists, the greatest common divisor of k and n must be 1. Thus, $\gcd(k, n) = 1$.

Conversely, assume that $\gcd(k, n) = 1$. By Bézout's Identity, we know there exist integers x and y such that $xk + yn = 1$. Considering this equation modulo n, we have $xk + yn \equiv 1 \pmod{n}$. Since yn is a multiple of n, $yn \equiv 0 \pmod{n}$. The equation thus simplifies to $xk \equiv 1 \pmod{n}$. In the language of the group $\mathbb{Z}_n$, this means $x \cdot [k] = [1]$. Now we can show that any element $[j] \in \mathbb{Z}_n$ can be generated by $[k]$. We can write any such element as $[j] = j \cdot [1]$. Substituting our expression for [1], we get:

$$[j] = j \cdot (x \cdot [k]) = (jx) \cdot [k]$$

Since j and x are integers, their product jx is also an integer. We have successfully expressed an arbitrary element $[j]$ as an integer multiple of $[k]$. Therefore, $[k]$ generates all of $\mathbb{Z}_n$. ■

Example 1.3.20. Consider the group $\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}$. The generators are the elements $[k]$ for which $\gcd(k, 8) = 1$.

- $\gcd(1, 8) = 1$, so [1] is a generator.
- $\gcd(2, 8) = 2 \neq 1$, so [2] is not a generator. ($\langle [2] \rangle = \{[0], [2], [4], [6]\}$)
- $\gcd(3, 8) = 1$, so [3] is a generator.
- $\gcd(4, 8) = 4 \neq 1$, so [4] is not a generator. ($\langle [4] \rangle = \{[0], [4]\}$)
- $\gcd(5, 8) = 1$, so [5] is a generator.
- $\gcd(6, 8) = 2 \neq 1$, so [6] is not a generator. ($\langle [6] \rangle = \{[0], [6], [4], [2]\}$)
- $\gcd(7, 8) = 1$, so [7] is a generator.

The set of generators for $\mathbb{Z}_8$ is $\{[1], [3], [5], [7]\}$.

Theorem 1.3.21 (Generators of an Infinite Cyclic Group)**.** *An infinite cyclic group has exactly two generators. If a is one generator, the only other generator is its inverse, a^{-1}.*

Proof. Let $G = \langle a \rangle$ be an infinite cyclic group.

First, we show that a^{-1} is indeed a generator. Let g be an arbitrary element of G. Since $G = \langle a \rangle$, there exists an integer k such that $g = a^k$. We can rewrite this expression as $g = (a^{-1})^{-k}$. Since $-k$ is an integer, any element $g \in G$ can be expressed as an integer power of a^{-1}. Therefore, a^{-1} is a generator of G.

Next, we show that these are the only two generators. Let b be any other generator of G. Since $b \in G$ and $G = \langle a \rangle$, we must have $b = a^k$ for some integer k. Since b is a generator, the original generator a must be a power of b. So, there exists an integer m such that $a = b^m$.

Substituting $b = a^k$ into the second equation, we get:

$$a = (a^k)^m = a^{km}$$

So, $a^1 = a^{km}$. Since G is an infinite group, the powers of the generator a are all distinct. That is, $a^i = a^j$ if and only if $i = j$. If this were not the case, say $a^i = a^j$ for $i > j$, then $a^{i-j} = e$, implying the group is finite, which is a contradiction.

From the equation $a^1 = a^{km}$, we can therefore conclude that $1 = km$. Since k and m are integers, the only possible solutions to this equation are $(k = 1, m = 1)$ or $(k = -1, m = -1)$.

- If $k = 1$, the generator b is $a^1 = a$.
- If $k = -1$, the generator b is a^{-1}.

This proves that any generator of G must be either a or a^{-1}. Thus, an infinite cyclic group has exactly two generators. ■

Example 1.3.22. The group of integers under addition, $(\mathbb{Z}, +)$, is the canonical example of an infinite cyclic group. As established, it can be generated by 1. The inverse of the element 1 in this additive group is -1. According to the theorem, the only generators of $\mathbb{Z}$ are 1 and -1, which is a well-known fact. Any other integer k (where $|k| > 1$) will only generate the subgroup $k\mathbb{Z}$, not all of $\mathbb{Z}$.

1.3.6 The Structure of Cyclic Groups

Cyclic groups are fundamental because their structure is completely understood. In fact, any cyclic group, no matter how it is presented, has the same essential structure as one of two very familiar groups: the integers under addition, or the integers modulo n. This is the content of the following landmark theorem.

Theorem 1.3.23 (Fundamental Theorem of Cyclic Groups)**.** *Every infinite cyclic group is isomorphic to the group of integers under addition, $(\mathbb{Z}, +)$. Every finite cyclic group of order n is isomorphic to the group of integers modulo n under addition, $(\mathbb{Z}_n, +_n)$.*

Proof. The proof is naturally divided into two cases.

Case 1: G is an infinite cyclic group. Let $G = \langle a \rangle$ be an infinite cyclic group with generator a. We want to show that $G \cong \mathbb{Z}$. To do this, we must construct a bijective homomorphism from $\mathbb{Z}$ to G.

Define the map $\phi : \mathbb{Z} \to G$ by the rule $\phi(k) = a^k$.

- **ϕ is a homomorphism:** Let $k, m \in \mathbb{Z}$. Then $\phi(k + m) = a^{k+m}$. By the laws of exponents, this is $a^k * a^m = \phi(k) * \phi(m)$. Thus, ϕ is a homomorphism.
- **ϕ is surjective:** By the definition of a cyclic group, every element $g \in G$ is of the form a^k for some integer k. This means for any $g \in G$, there exists a $k \in \mathbb{Z}$ such that $\phi(k) = g$. Thus, ϕ is surjective.
- **ϕ is injective:** Suppose $\phi(k) = \phi(m)$ for some integers k and m. This means $a^k = a^m$. Multiplying by $(a^m)^{-1} = a^{-m}$, we get $a^{k-m} = e$. Since G is an infinite group, its generator a must have infinite order. The only power of a that equals the identity is a^0. Therefore, it must be that $k - m = 0$, which implies $k = m$. Thus, ϕ is injective.

Since ϕ is a bijective homomorphism, we have established that $G \cong \mathbb{Z}$.

Case 2: G is a finite cyclic group of order n. Let $G = \langle a \rangle$ be a finite cyclic group with $|G| = n$. From a previous theorem, we know that the order of the generator a is also n. We want to show that $G \cong \mathbb{Z}_n$.

Define the map $\psi : \mathbb{Z}_n \to G$ by the rule $\psi([k]) = a^k$.

- **ψ is well-defined:** This is a crucial step. We must show that if $[k] = [j]$ in $\mathbb{Z}_n$, then $\psi([k]) = \psi([j])$. If $[k] = [j]$, then $k \equiv j \pmod{n}$, which means $k = j + qn$ for some integer q. Then $\psi([k]) = a^k = a^{j+qn} = a^j * a^{qn} = a^j * (a^n)^q$. Since $|a| = n$, we have $a^n = e$. So, $\psi([k]) = a^j * e^q = a^j * e = a^j = \psi([j])$. The map is therefore well-defined.
- **ψ is a homomorphism:** Let $[k], [j] \in \mathbb{Z}_n$. Then $\psi([k] + [j]) = \psi([k + j]) = a^{k+j}$. This is equal to $a^k * a^j = \psi([k]) * \psi([j])$. Thus, ψ is a homomorphism.
- **ψ is a bijection:** The domain $\mathbb{Z}_n$ has n elements, and the codomain G also has n elements. For finite sets of the same size, a map is bijective if it is either injective or surjective. We show it is surjective. By definition, any element $g \in G$ is of the form a^k for some integer k. This means $g = \psi([k])$. Thus, ψ is surjective. Since it is a surjective map between two finite sets of the same order, it must also be injective, and therefore is a bijection.

Since ψ is a well-defined bijective homomorphism, we have established that $G \cong \mathbb{Z}_n$. This completes the proof of the theorem. ■

Remark 1.3.24. This theorem is a powerful classification result. It tells us that no matter how a cyclic group is constructed—be it with matrices, numbers, or functions—its underlying structure is identical to that of either $\mathbb{Z}$ or $\mathbb{Z}_n$.

Chapter 2

Normal Subgroups and Homomorphisms

2.1 Normal Subgroups

Definition 2.1.1 (Normal Subgroup)**.** A subgroup H of a group G is said to be a **normal subgroup** of G if for every $g \in G$, its left coset gH is equal to its right coset Hg. That is,

$$gH = Hg \quad \forall g \in G$$

We denote this by $H \trianglelefteq G$. An equivalent condition is that the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is equal to H for all $g \in G$.

Example 2.1.2.

1. In any group G, the trivial subgroup $\{e\}$ and the group G itself are always normal subgroups. These are sometimes called the improper normal subgroups.

2. Every subgroup of an abelian group is normal. If G is abelian, then for any $h \in H$ and $g \in G$, we have $ghg^{-1} = gg^{-1}h = eh = h \in H$. Thus, $gHg^{-1} \subseteq H$, which is sufficient to prove normality (as shown in the criterion below).

3. The center of a group, $Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$, is a normal subgroup of G. For any $z \in Z(G)$ and $g \in G$, $gzg^{-1} = zgg^{-1} = z \in Z(G)$.

4. The alternating group A_n (the group of even permutations) is a normal subgroup of the symmetric group S_n. For example, $A_3 = \{e, (123), (132)\}$ is normal in S_3.

5. The subgroup $H = \{e, (12)\}$ in S_3 is not normal. For example, let $g = (13)$. Then the left coset is $gH = \{(13)e, (13)(12)\} = \{(13), (132)\}$, while the right coset is $Hg = \{e(13), (12)(13)\} = \{(13), (123)\}$. Since $gH \neq Hg$, H is not normal in S_3.

2.1.1 Criterion for a Normal Subgroup

The following theorem provides a more practical test for determining if a subgroup is normal.

Theorem 2.1.3 (Normal Subgroup Test)**.** *A subgroup H of a group G is a normal subgroup of G if and only if $ghg^{-1} \in H$ for all $h \in H$ and for all $g \in G$.*

Proof. First, assume $H \trianglelefteq G$. By definition, this means $gHg^{-1} = H$ for all $g \in G$. Then for any $h \in H$, it follows directly that the element ghg^{-1} belongs to the set gHg^{-1}, and therefore $ghg^{-1} \in H$.

Conversely, assume that $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$. This condition immediately implies that $gHg^{-1} \subseteq H$. We must now show the reverse inclusion, $H \subseteq gHg^{-1}$. Let h be an arbitrary element of H. We need to show that h can be written in the form gxg^{-1} for some $x \in H$. Let $k = g^{-1}$, which is also an element of G. By our assumption, $khk^{-1} \in H$. Substituting $k = g^{-1}$ gives $g^{-1}h(g^{-1})^{-1} = g^{-1}hg \in H$. Let $h' = g^{-1}hg$. Since $h' \in H$, we can write $h = g(g^{-1}hg)g^{-1} = gh'g^{-1}$. This shows that any element $h \in H$ is in the set gHg^{-1}, so $H \subseteq gHg^{-1}$. Since both inclusions $gHg^{-1} \subseteq H$ and $H \subseteq gHg^{-1}$ hold, we conclude that $gHg^{-1} = H$, and thus H is a normal subgroup of G. ■

Theorem 2.1.4. *Any subgroup of index two is a normal subgroup.*

Proof. Let H be a subgroup of a group G such that the index $[G : H] = 2$. This means there are exactly two distinct left cosets of H in G, and also exactly two distinct right cosets of H in G. We want to show that $gH = Hg$ for all $g \in G$.

We consider two cases for an element $g \in G$.

Case 1: If $g \in H$. Since H is a subgroup, it is closed under the group operation. Thus, $gH = \{gh \mid h \in H\} = H$. Similarly, $Hg = \{hg \mid h \in H\} = H$. Therefore, $gH = Hg$.

Case 2: If $g \notin H$. Since there are only two left cosets, one must be H itself and the other must be the set of all elements not in H. Because $g \notin H$, the left coset gH cannot be H (since $ge = g \in gH$). Therefore, gH must be the other coset, which is the complement of H in G. So, $gH = G \setminus H$. Similarly, the two right cosets are H and the complement

$G \setminus H$. Since $g \notin H$, the right coset Hg cannot be H. Thus, Hg must be the complement, $Hg = G \setminus H$. From this, we conclude that $gH = G \setminus H = Hg$.

Since the equality $gH = Hg$ holds for all $g \in H$ and for all $g \notin H$, it holds for every element $g \in G$. Therefore, H is a normal subgroup of G. ■

2.1.2 Quotient Groups

When a subgroup H of a group G is normal, we can form a new group whose elements are the cosets of H in G. This new group is called the quotient group or factor group. The normality of H is essential for the group operation to be well-defined.

Definition 2.1.5 (Quotient Group)**.** Let H be a normal subgroup of a group G. The set of all left (or right) cosets of H in G, denoted by G/H, is given by

$$G/H = \{gH \mid g \in G\}$$

We define a binary operation on the set G/H as follows:

$$(aH)(bH) = (ab)H \quad \text{for all } aH, bH \in G/H$$

Theorem 2.1.6. *Let H be a normal subgroup of G. The set G/H with the operation defined above forms a group.*

Proof. First, we show the operation is well-defined. Suppose $aH = a'H$ and $bH = b'H$. Then $a' = ah_1$ and $b' = bh_2$ for some $h_1, h_2 \in H$. We must show that $(a'b')H = (ab)H$. Consider the product $a'b' = (ah_1)(bh_2) = a(h_1b)h_2$. Since H is normal in G, $gH = Hg$ for all g, which implies $b^{-1}Hb = H$. Thus $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Substituting this, we get $a'b' = a(bh_3)h_2 = (ab)(h_3h_2)$. Since $h_3, h_2 \in H$, their product h_3h_2 is also in H. Thus, $a'b' \in (ab)H$, which implies $(a'b')H = (ab)H$. The operation is well-defined.

Now we verify the group axioms for G/H.

- **Closure:** For any $aH, bH \in G/H$, their product $(ab)H$ is by definition another coset of H in G, so it is in G/H.
- **Associativity:** For any $aH, bH, cH \in G/H$, we have

$$(aH)((bH)(cH)) = (aH)((bc)H) = (a(bc))H$$

$$((aH)(bH))(cH) = ((ab)H)(cH) = ((ab)c)H$$

  Since associativity holds in G, $a(bc) = (ab)c$, so the operation is associative.

- **Identity Element:** The coset $H = eH$ is the identity element in G/H, because for any $aH \in G/H$,

$$(aH)(eH) = (ae)H = aH \quad \text{and} \quad (eH)(aH) = (ea)H = aH$$

- **Inverse Element:** For any element $aH \in G/H$, the inverse is $a^{-1}H \in G/H$, since

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H \quad \text{and} \quad (a^{-1}H)(aH) = (a^{-1}a)H = eH = H$$

Since all axioms are satisfied, G/H is a group. The order of this group, if G is finite, is $|G/H| = [G : H] = |G|/|H|$. ■

Example 2.1.7.

1. Let $G = (\mathbb{Z}, +)$ and $H = 4\mathbb{Z} = \{..., -4, 0, 4, 8, ...\}$. Since $\mathbb{Z}$ is abelian, H is a normal subgroup. The quotient group is $\mathbb{Z}/4\mathbb{Z}$, which is the group of integers modulo 4. Its elements are the four cosets:

$$\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$$

   The operation is addition of cosets, for example, $(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = (2 + 3) + 4\mathbb{Z} = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$.

2. Let $G = S_3$ and $H = A_3 = \{e, (123), (132)\}$. Since $[S_3 : A_3] = 2$, A_3 is a normal subgroup. The quotient group S_3/A_3 has order 2. Its elements are the two cosets:

$$S_3/A_3 = \{A_3, (12)A_3\}$$

   Here, A_3 is the identity element, and $(12)A_3$ is the coset of odd permutations.

2.1.3 Homomorphism

A homomorphism is a map between two groups that preserves the group structure.

Definition 2.1.8 (Group Homomorphism)**.** Let $(G, *)$ and $(G', \cdot)$ be two groups. A mapping $\phi : G \to G'$ is called a **homomorphism** if for all $a, b \in G$, it satisfies the property:

$$\phi(a * b) = \phi(a) \cdot \phi(b)$$

Example 2.1.9.

1. The map $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +_n)$ defined by $\phi(x) = x \pmod n$ is a homomorphism.

2. The determinant map $\det : \mathrm{GL}(n, \mathbb{R}) \to (\mathbb{R}^*, \times)$ is a homomorphism, since $\det(AB) = \det(A)\det(B)$.

3. The map $\phi : G \to G'$ defined by $\phi(g) = e'$ for all $g \in G$ (where e' is the identity in G') is a homomorphism, known as the trivial homomorphism.

2.1.4 Kernel of a Homomorphism

The kernel is a fundamental concept associated with any homomorphism, which turns out to be a normal subgroup.

Definition 2.1.10 (Kernel)**.** Let $\phi : G \to G'$ be a group homomorphism. The **kernel** of ϕ, denoted by $\ker(\phi)$, is the set of all elements in G that are mapped to the identity element e' of G'.

$$\ker(\phi) = \{g \in G \mid \phi(g) = e'\}$$

Theorem 2.1.11. *If $\phi : G \to G'$ is a group homomorphism, then $\ker(\phi)$ is a normal subgroup of G.*

Proof. Let $K = \ker(\phi)$. First, we show K is a subgroup of G. Since $\phi(e) = e'$, $e \in K$, so K is non-empty. For any $a, b \in K$, $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = e'(e')^{-1} = e'$, so $ab^{-1} \in K$. Thus, K is a subgroup of G.

Next, we show K is normal in G. For any $k \in K$ and any $g \in G$, we must show that $gkg^{-1} \in K$.

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e'\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e'$$

Therefore, $gkg^{-1} \in \ker(\phi)$. This holds for all $g \in G$ and $k \in K$, so $\ker(\phi)$ is a normal subgroup of G. ■

Definition 2.1.12 (Image of a Homomorphism)**.** Let $\phi : G \to G'$ be a group homomorphism. The **image** of ϕ, denoted by $\phi(G)$ or $\mathrm{Im}(\phi)$, is the set of all elements in the codomain G' that are mapped to by some element of G.

$$\phi(G) = \{\phi(g) \mid g \in G\}$$

It is a subset of the codomain G'.

Theorem 2.1.13. *The image of a homomorphism $\phi : G \to G'$, $\phi(G)$, is a subgroup of G'.*

Proof. Let e and e' be the identity elements of G and G' respectively.

1. Since $\phi(e) = e'$, we have $e' \in \phi(G)$, so the image is non-empty.

2. Let $x, y \in \phi(G)$. Then there exist $a, b \in G$ such that $\phi(a) = x$ and $\phi(b) = y$. Their product is $xy = \phi(a)\phi(b) = \phi(ab)$. Since $ab \in G$, $xy \in \phi(G)$. Thus, $\phi(G)$ is closed under the operation of G'.

3. Let $x \in \phi(G)$, where $x = \phi(a)$ for some $a \in G$. The inverse of x in G' is $x^{-1} = (\phi(a))^{-1} = \phi(a^{-1})$. Since $a^{-1} \in G$, we have $x^{-1} \in \phi(G)$.

Therefore, $\phi(G)$ is a subgroup of G'. ■

2.1.5 Fundamental Theorem of Homomorphism

This theorem, also known as the First Isomorphism Theorem, establishes a fundamental relationship between a group, its quotient by a kernel, and the image of a homomorphism.

Theorem 2.1.14 (Fundamental Theorem of Homomorphism)**.** *Let $\phi : G \to G'$ be a group homomorphism. Then the image of ϕ, denoted $\phi(G)$, is a subgroup of G', and the quotient group $G/\ker(\phi)$ is isomorphic to $\phi(G)$.*

$$G/\ker(\phi) \cong \phi(G)$$

Proof. Let $K = \ker(\phi)$. We define a map $\psi : G/K \to \phi(G)$ by $\psi(gK) = \phi(g)$. First, we show ψ is well-defined. If $gK = hK$, then $h^{-1}g \in K$, so $\phi(h^{-1}g) = e'$. This means $\phi(h)^{-1}\phi(g) = e'$, which implies $\phi(g) = \phi(h)$. So, $\psi(gK) = \psi(hK)$.

Next, we show ψ is a homomorphism:

$$\psi((gK)(hK)) = \psi((gh)K) = \phi(gh) = \phi(g)\phi(h) = \psi(gK)\psi(hK)$$

The map ψ is surjective (onto) by its definition, as any element in the image $\phi(G)$ is of the form $\phi(g)$ for some $g \in G$, and is therefore the image of the coset gK.

Finally, we show ψ is injective (one-to-one). Suppose $\psi(gK) = \psi(hK)$. Then $\phi(g) = \phi(h)$, which implies $\phi(h)^{-1}\phi(g) = e'$, so $\phi(h^{-1}g) = e'$. This means $h^{-1}g \in K$, so $gK = hK$. Thus, ψ is injective. Since ψ is a well-defined, surjective, and injective homomorphism, it is an isomorphism. Therefore, $G/\ker(\phi) \cong \phi(G)$. ■

Example 2.1.15 (Applying the Fundamental Theorem of Homomorphism)**.** Let us illustrate the theorem by considering the homomorphism $\phi : (\mathbb{Z}, +) \to (\mathbb{Z}_4, +)$ defined by $\phi(x) = x \pmod 4$. This mapping preserves the group operation since $\phi(a + b) = (a + b) \pmod 4 = \phi(a) + \phi(b)$.

The kernel of this homomorphism, $\ker(\phi)$, is the set of all integers that map to the identity element $0 \in \mathbb{Z}_4$. An integer x has $x \pmod 4 = 0$ if and only if it is a multiple of 4. Therefore, the kernel is the subgroup $4\mathbb{Z} = \{..., -4, 0, 4, ...\}$. The image of the homomorphism, $\phi(\mathbb{Z})$, is the set of all possible output values in $\mathbb{Z}_4$. Since any integer's remainder upon division by 4 can be 0, 1, 2, or 3, the map is surjective, and its image is the entire group $\mathbb{Z}_4$.

The Fundamental Theorem of Homomorphism states that $G/\ker(\phi) \cong \phi(G)$. Applying this to our specific case, we substitute our findings for the kernel and the image:

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$$

This result confirms that the quotient group formed by the integers modulo the subgroup of multiples of 4 is structurally identical to the group of integers modulo 4. The elements of the quotient group $\mathbb{Z}/4\mathbb{Z}$ are the cosets $\{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$, which forms a cyclic group of order 4, just as $\mathbb{Z}_4$ does.

Isomorphism Theorems

Theorem 2.1.16 (Second Isomorphism Theorem)**.** *Let G be a group, S a subgroup of G, and N a normal subgroup of G. Then $SN = \{sn \mid s \in S, n \in N\}$ is a subgroup of G, $S \cap N$ is a normal subgroup of S, and*

$$(SN)/N \cong S/(S \cap N)$$

Theorem 2.1.17 (Third Isomorphism Theorem)**.** *Let G be a group and let H and K be normal subgroups of G with $H \subseteq K$. Then K/H is a normal subgroup of G/H and*

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

2.1.6 Normalizer of an Element

The normalizer of an element generalizes the idea of elements that commute with a specific, fixed element.

Definition 2.1.18 (Normalizer of an Element)**.** Let G be a group and let $a \in G$. The **normalizer** of a in G, denoted by $N(a)$, is the set of all elements in G that commute with a.

$$N(a) = \{g \in G \mid ga = ag\}$$

An equivalent definition is $N(a) = \{g \in G \mid gag^{-1} = a\}$.

Theorem 2.1.19. *For any $a \in G$, the normalizer $N(a)$ is a subgroup of G.*

Proof. First, $e \in N(a)$ because $ea = a = ae$, so $N(a)$ is non-empty. Let $g, h \in N(a)$. Then $ga = ag$ and $ha = ah$. From $ha = ah$, we get $a = h^{-1}ah$. Now consider the product gh: $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$, so $gh \in N(a)$. For the inverse, from $ga = ag$, we can write $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$, which simplifies to $ag^{-1} = g^{-1}a$. Thus, $g^{-1} \in N(a)$. By the subgroup test, $N(a)$ is a subgroup of G. ■

Example 2.1.20. In the symmetric group S_3, let's find the normalizer of the element $a = (12)$. We check which elements $g \in S_3$ satisfy $g(12)g^{-1} = (12)$.

- $e(12)e^{-1} = (12)$, so $e \in N((12))$.
- $(12)(12)(12)^{-1} = (12)$, so $(12) \in N((12))$.
- $(13)(12)(13)^{-1} = (23) \neq (12)$, so $(13) \notin N((12))$.
- $(123)(12)(123)^{-1} = (123)(12)(132) = (23) \neq (12)$, so $(123) \notin N((12))$.

The other elements also fail to commute. Thus, the normalizer is $N((12)) = \{e, (12)\}$.

2.1.7 Centre of a Group

The centre is the set of elements that commute with every element of the group.

Definition 2.1.21 (Centre of a Group)**.** The **centre** of a group G, denoted by $Z(G)$, is the set of elements in G that commute with all elements of G.

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

Theorem 2.1.22. *The centre $Z(G)$ is a normal subgroup of G.*

Proof. First, we show $Z(G)$ is a subgroup. It contains e since $eg = ge$ for all $g \in G$. If $z_1, z_2 \in Z(G)$, then for any $g \in G$, $(z_1z_2)g = z_1(z_2g) = z_1(gz_2) = (z_1g)z_2 = (gz_1)z_2 = g(z_1z_2)$, so $z_1z_2 \in Z(G)$. If $z \in Z(G)$, then $zg = gz$. Multiplying by z^{-1} on both sides gives $z^{-1}(zg)z^{-1} = z^{-1}(gz)z^{-1}$, which simplifies to $gz^{-1} = z^{-1}g$. So $z^{-1} \in Z(G)$. Thus, $Z(G)$ is a subgroup.

To show it is normal, let $z \in Z(G)$ and $g \in G$. We must show $gzg^{-1} \in Z(G)$. Since z is in the centre, it commutes with g, so $zg = gz$. Therefore,

$$gzg^{-1} = (gz)g^{-1} = (zg)g^{-1} = z(gg^{-1}) = ze = z$$

Since $z \in Z(G)$, we have shown $gzg^{-1} \in Z(G)$. Thus, $Z(G)$ is a normal subgroup of G. ■

Example 2.1.23.

1. A group G is abelian if and only if $Z(G) = G$.

2. The centre of the symmetric group S_n for $n \geq 3$ is the trivial subgroup $\{e\}$. For instance, $Z(S_3) = \{e\}$.

3. The centre of the general linear group $\mathrm{GL}(n, \mathbb{R})$ is the set of all non-zero scalar matrices, $\{cI_n \mid c \in \mathbb{R}, c \neq 0\}$.

Remark 2.1.24. The centre of a group G can be defined in terms of normalizers as the intersection of the normalizers of all elements in G: $Z(G) = \bigcap_{g \in G} N(g)$.

2.1.8 Permutation Groups

Definition 2.1.25 (Permutation Group)**.** Let S be a non-empty set. The set of all permutations of S, denoted by S_S, forms a group under the operation of function composition. A **permutation group** is any subgroup of S_S.

When the set S is finite, say $S = \{1, 2, ..., n\}$, we get the very important class of symmetric groups.

2.1.9 Symmetric Groups

Definition 2.1.26 (Symmetric Group)**.** The group of all permutations of the set $\{1, 2, ..., n\}$ is called the **symmetric group** of degree n and is denoted by S_n. The order of S_n is $n!$.

Elements of S_n are often written using cycle notation. A group G is non-abelian if its group operation is not commutative. For $n \geq 3$, S_n is non-abelian.

Example 2.1.27 (The Symmetric Group S_3)**.** The group S_3 consists of all permutations of the set $\{1, 2, 3\}$. Its order is $3! = 6$. The elements are:

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

where e is the identity permutation. To see that S_3 is non-abelian, consider the composition of two elements:

$$(12)(13) = (132) \quad \text{while} \quad (13)(12) = (123)$$

Since $(12)(13) \neq (13)(12)$, the group is not abelian.

Theorem 2.1.28. *Every permutation in S_n (for $n \geq 2$) can be written as a product of disjoint cycles.*

Proof. Let $\sigma \in S_n$ be a permutation on the set $X = \{1, 2, \ldots, n\}$. We can construct the cycle decomposition algorithmically. Pick any element $a_1 \in X$. Consider the sequence of its images under repeated application of σ: $a_1, \sigma(a_1), \sigma^2(a_1), \ldots$. Since X is finite, this sequence must eventually repeat. Let k be the smallest positive integer such that $\sigma^k(a_1) = \sigma^m(a_1)$ for some $m < k$. If $m > 0$, applying σ^{-1} yields $\sigma^{k-1}(a_1) = \sigma^{m-1}(a_1)$, contradicting the minimality of k. Thus, we must have $m = 0$, so $\sigma^k(a_1) = a_1$. This gives us our first cycle, $C_1 = (a_1 \ \sigma(a_1) \ \ldots \ \sigma^{k-1}(a_1))$. The permutation σ acts on the elements of C_1 exactly as the cycle C_1 does.

If the elements of C_1 comprise all of X, then $\sigma = C_1$ and we are done. If not, choose an element $b_1 \in X$ that is not in the set of elements of C_1. Repeat the same process to generate a second cycle, $C_2 = (b_1 \ \sigma(b_1) \ \ldots \ \sigma^{l-1}(b_1))$. The sets of elements in C_1 and C_2 are disjoint. If they were not, say $\sigma^i(a_1) = \sigma^j(b_1)$, then $b_1 = \sigma^{i-j}(a_1)$, which would imply b_1 is in the orbit of a_1, a contradiction.

We continue this process until all elements of X are exhausted. Since X is finite, this process must terminate. The permutation σ is then the product of the disjoint cycles constructed: $\sigma = C_1C_2 \ldots C_m$. ■

2nd Proof. Let $\sigma \in S_n$ be a permutation on the set $X = \{1, 2, \ldots, n\}$. The subgroup $\langle\sigma\rangle$ acts on X, partitioning it into a set of disjoint orbits $\{O_1, O_2, \ldots, O_m\}$. For any element $a \in O_i$, its orbit is $O_i = \{a, \sigma(a), \ldots, \sigma^{k-1}(a)\}$. The restriction of σ to O_i is precisely the cycle $\pi_i = (a\ \sigma(a)\ \ldots\ \sigma^{k-1}(a))$. Since the orbits are disjoint and their union is X, σ is the product of these disjoint cycles: $\sigma = \pi_1\pi_2 \ldots \pi_m$. ■

Theorem 2.1.29. *Disjoint cycles commute.*

Proof. Let α and β be disjoint cycles. Let A be the set of elements moved by α, and B be the set of elements moved by β, with $A \cap B = \emptyset$. Let x be any element. If $x \in A$, then $\beta(x) = x$. Thus $(\alpha\beta)(x) = \alpha(x)$. Also, since $\alpha(x) \in A$, β fixes it, so $(\beta\alpha)(x) = \beta(\alpha(x)) = \alpha(x)$. The result is the same. If $x \notin A$, $\alpha(x) = x$. Then $(\beta\alpha)(x) = \beta(x)$. Also, since β maps elements of B to B and fixes elements outside B, α will fix $\beta(x)$. Thus $(\alpha\beta)(x) = \alpha(\beta(x)) = \beta(x)$. In all cases, $(\alpha\beta)(x) = (\beta\alpha)(x)$, so $\alpha\beta = \beta\alpha$. ■

Theorem 2.1.30. *Every cycle can be written as a product of transpositions.*

Proof. A cycle $(a_1\ a_2\ \ldots\ a_k)$ can be expressed as the product $(a_1\ a_k)(a_1\ a_{k-1}) \ldots (a_1\ a_2)$. To verify, for any $i \in \{1, \ldots, k-1\}$, the first transposition on the right that moves a_i is $(a_1\ a_i)$, which sends $a_i \to a_1$. The next transposition, $(a_1\ a_{i+1})$, then sends $a_1 \to a_{i+1}$. Subsequent transpositions leave a_{i+1} untouched. The net effect is $a_i \to a_{i+1}$. For a_k, the only transposition that moves it is the leftmost, $(a_1\ a_k)$, sending $a_k \to a_1$. This matches the action of the original cycle. ■

2.1.10 Cayley's Theorem

Cayley's theorem is a fundamental result in group theory, showing that every group can be thought of as a group of permutations.

Theorem 2.1.31 (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations. More specifically, a finite group G of order n is isomorphic to a subgroup of the symmetric group S_n.*

Proof. Let G be an arbitrary group. Our goal is to find a group of permutations that is isomorphic to G. The set that will be permuted is the set of elements of G itself. Let S_G be the group of all permutations of the set G.

For each element $g \in G$, we define a map called the left regular representation of g, denoted $T_g : G \to G$, by the rule of left multiplication:

$$T_g(x) = gx \quad \text{for all } x \in G$$

First, we must show that each T_g is a permutation of G, meaning it is a bijection.

- **Injectivity:** Suppose $T_g(x_1) = T_g(x_2)$ for some $x_1, x_2 \in G$. By definition, this means $gx_1 = gx_2$. By the left cancellation law in G, we can conclude that $x_1 = x_2$. Thus, T_g is injective.
- **Surjectivity:** Let y be an arbitrary element in G. We need to find an element $x \in G$ such that $T_g(x) = y$. This requires solving $gx = y$ for x. The solution is $x = g^{-1}y$, which is an element of G. Therefore, T_g is surjective.

Since T_g is both injective and surjective for every $g \in G$, each T_g is a permutation of the set G and is an element of the group S_G.

Now, define a map $\phi : G \to S_G$ by $\phi(g) = T_g$. We will show that ϕ is an injective homomorphism.

- **ϕ is a homomorphism:** We must show that $\phi(gh) = \phi(g) \circ \phi(h)$. Let's evaluate the action of both sides on an arbitrary element $x \in G$. The left side is $\phi(gh) = T_{gh}$, so $T_{gh}(x) = (gh)x$. The right side is $\phi(g) \circ \phi(h) = T_g \circ T_h$, so $(T_g \circ T_h)(x) = T_g(T_h(x)) = T_g(hx) = g(hx)$. By the associative property in G, $(gh)x = g(hx)$. Thus, $T_{gh} = T_g \circ T_h$, and ϕ is a homomorphism.
- **ϕ is injective:** To show injectivity, we show that the kernel of ϕ is trivial. The identity element of S_G is the identity map I where $I(x) = x$ for all $x \in G$. Let $g \in \ker(\phi)$. This means $\phi(g)$ is the identity element of S_G.

  $$\phi(g) = I$$

  $$T_g = I$$

  By definition of the maps, this means $T_g(x) = I(x)$ for all $x \in G$.

  $$gx = x$$

  Choosing $x = e$ (the identity of G), we get $ge = e$, which implies $g = e$. Therefore, $\ker(\phi) = \{e\}$, and the homomorphism ϕ is injective.

Since $\phi : G \to S_G$ is an injective homomorphism, G is isomorphic to its image, $\phi(G)$. The image $\phi(G) = \{T_g \mid g \in G\}$ is a subgroup of S_G. Thus, G is isomorphic to a subgroup of S_G, which is a group of permutations.

If G is a finite group of order n, then the set G has n elements, and the group S_G is isomorphic to S_n. In this case, G is isomorphic to a subgroup of S_n. ■

Remark 2.1.32. The significance of Cayley's theorem is that it unifies the study of groups by showing that all abstract groups have a concrete representation as permutations. However, it is often more of theoretical importance than a practical computational tool, as S_n can be very large compared to the original group G.

2.1.11 Alternating Groups

Definition 2.1.33 (Even and Odd Permutations)**.** A permutation that can be expressed as a product of an even number of transpositions (2-cycles) is called an **even permutation**. A permutation that can be expressed as a product of an odd number of transpositions is called an **odd permutation**.

Definition 2.1.34 (Alternating Group)**.** The set of all even permutations in S_n forms a subgroup of S_n, called the **alternating group** of degree n, denoted by A_n. For $n \geq 2$, the order of A_n is $n!/2$.

Remark 2.1.35. The alternating group A_n is a normal subgroup of S_n. Since its index is $[S_n : A_n] = (n!)/(n!/2) = 2$, this is consistent with the theorem that any subgroup of index 2 is normal.

Example 2.1.36 (The Alternating Group A_3)**.** Consider the elements of S_3:

- e is even (product of 0 transpositions).
- $(12), (13), (23)$ are odd (each is 1 transposition).
- $(123) = (13)(12)$ is even (product of 2 transpositions).
- $(132) = (12)(13)$ is even (product of 2 transpositions).

The set of even permutations is $A_3 = \{e, (123), (132)\}$. The order is $|A_3| = 3$, which is $3!/2$.

Theorem 2.1.37. *The alternating group A_4 has no subgroup of order 6.*

Proof. The order of the alternating group A_4 is $|A_4| = \frac{4!}{2} = 12$. The number 6 is a divisor of 12. According to the converse of Lagrange's theorem, if it were true, A_4 should have a subgroup of order 6. We will prove by contradiction that no such subgroup exists.

Assume, for the sake of contradiction, that there exists a subgroup H of A_4 with $|H| = 6$. The index of this subgroup H in A_4 would be:

$$[A_4 : H] = \frac{|A_4|}{|H|} = \frac{12}{6} = 2$$

But any subgroup of index 2 is a normal subgroup. Therefore, if H exists, it must be a normal subgroup of A_4, i.e., $H \trianglelefteq A_4$.

Now, let us consider the elements of A_4. They are the even permutations of S_4.

- The identity element: e (1 element)
- The 3-cycles: $(123), (132), (124), (142), (134), (143), (234), (243)$ (8 elements)
- Products of two disjoint transpositions: $(12)(34), (13)(24), (14)(23)$ (3 elements)

All 3-cycles in A_4 have order 3.

Since H is a normal subgroup of A_4, we can form the quotient group A_4/H. The order of this quotient group is $|A_4/H| = [A_4 : H] = 2$. Any group of order 2 is isomorphic to $\mathbb{Z}_2$. A property of such a group is that for any element x, we have $x^2 = e$. In the context of our quotient group, this means that for any coset $gH \in A_4/H$, we must have $(gH)^2 = H$, where H is the identity element of A_4/H.

The operation in the quotient group gives $(gH)^2 = g^2H$. So, for any element $g \in A_4$, we must have $g^2H = H$. This is true if and only if $g^2 \in H$.

This is a very strong condition: the square of every element of A_4 must belong to the subgroup H. Let us test this condition with a 3-cycle, for example $g = (123) \in A_4$. The square of g is $g^2 = (123)^2 = (132)$. According to our deduction, (132) must be an element of H.

By the same logic, this must hold for all 8 of the 3-cycles in A_4. Let's see what their squares are:
$(123)^2 = (132)$ $(124)^2 = (142)$, $(134)^2 = (143)$, $(234)^2 = (243)$, $(132)^2 = (123)$, $(142)^2 = (124)$, $(143)^2 = (134)$, $(243)^2 = (234)$

This means that H must contain all 8 of the 3-cycles from A_4. If H contains these 8 elements, its order must be at least 8. This directly contradicts our initial assumption that H is a subgroup of order 6.

Therefore, our initial assumption must be false. There is no subgroup of order 6 in A_4. Since 6 divides 12 but there is no subgroup of order 6, A_4 serves as a counterexample to the converse of Lagrange's theorem. ■

Definition 2.1.38. The **Dihedral Group** D_4 is the group of symmetries of a regular square. It describes all the ways you can rotate or reflect a square so that it occupies the same physical space.

Order: The group D_4 has order $2n = 2 \times 4 = 8$.

Geometric Interpretation

Imagine a square with vertices labeled 1, 2, 3, 4 in counter-clockwise order. The 8 symmetries are:

1. **Four Rotations (forming a cyclic subgroup):**
   - R_0: Rotation by 0° (the identity).
   - R_{90}: Rotation by 90° counter-clockwise.
   - R_{180}: Rotation by 180°.
   - R_{270}: Rotation by 270°.
2. **Four Reflections (or flips):**
   - H: Reflection across the horizontal axis of symmetry.
   - V: Reflection across the vertical axis of symmetry.
   - D: Reflection across the main diagonal (through vertices 1 and 3).
   - D': Reflection across the anti-diagonal (through vertices 2 and 4).

Algebraic Representation

The group can be generated by two elements: a rotation r and a reflection s. Let $r = R_{90}$ and $s = H$. The entire group can be described by the relations:

$$r^4 = e, \quad s^2 = e, \quad sr = r^{-1}s = r^3s$$

The 8 elements are then:

$$\{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

These correspond to $\{R_0, R_{90}, R_{180}, R_{270}, H, D', V, D\}$ respectively.

Properties

- D_4 is **non-abelian**. The relation $sr = r^3s$ shows this directly. Performing a flip and then a 90° rotation is not the same as rotating first and then flipping.
- The subgroup of rotations $\{e, r, r^2, r^3\}$ is a cyclic, normal subgroup of order 4.
- All four reflections have order 2.

2.1.12 The Dihedral Group D_3

Definition 2.1.39. The **Dihedral Group** D_3 is the group of symmetries of an equilateral triangle.

Order The group D_3 has order $2n = 2 \times 3 = 6$.

Elements and Isomorphism to S_3

Let the vertices of the triangle be labeled 1, 2, 3. Each symmetry can be described as a permutation of these vertices, showing that D_3 is isomorphic to S_3.

1. **Three Rotations:**
   - R_0: Rotation by 0°. Corresponds to the identity permutation e.
   - R_{120}: Rotation by 120°. Corresponds to the cycle (1 2 3).
   - R_{240}: Rotation by 240°. Corresponds to the cycle (1 3 2).
2. **Three Reflections:**
   - S_1: Reflection through the axis passing through vertex 1. Swaps 2 and 3, corresponding to the transposition (2 3).
   - S_2: Reflection through the axis passing through vertex 2. Swaps 1 and 3, corresponding to (1 3).
   - S_3: Reflection through the axis passing through vertex 3. Swaps 1 and 2, corresponding to (1 2).

Properties

- D_3 is **non-abelian**, just like S_3.
- It is the smallest possible non-abelian group.
- Its algebraic representation is given by generators r (rotation by 120°) and s (any reflection) with relations:

$$r^3 = e, \quad s^2 = e, \quad sr = r^{-1}s = r^2s$$

Chapter 3

Rings and Homomorphisms

3.1 Rings and Homomorphisms

Definition 3.1.1 (Ring)**.** A **ring** is a non-empty set R equipped with two binary operations, usually called addition $(+)$ and multiplication $(\cdot)$, satisfying the following axioms:

1. $(R,+)$ is an abelian group.
   (a) (Closure) $a+b \in R$ for all $a,b \in R$.
   (b) (Associativity) $(a+b)+c = a+(b+c)$ for all $a,b,c \in R$.
   (c) (Identity) There exists an element $0 \in R$ such that $a+0 = 0+a = a$ for all $a \in R$.
   (d) (Inverse) For each $a \in R$, there exists an element $-a \in R$ such that $a+(-a) = (-a)+a = 0$.
   (e) (Commutativity) $a+b = b+a$ for all $a,b \in R$.
2. $(R,\cdot)$ is a semigroup.
   (a) (Closure) $a \cdot b \in R$ for all $a,b \in R$.
   (b) (Associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a,b,c \in R$.
3. Multiplication distributes over addition.
   (a) (Left Distributivity) $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ for all $a,b,c \in R$.
   (b) (Right Distributivity) $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a,b,c \in R$.

A ring is called a **commutative ring** if multiplication is commutative ($a \cdot b = b \cdot a$ for all $a,b \in R$). A ring is called a **ring with unity** (or identity) if there exists a multiplicative identity element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Example 3.1.2.

1. The set of integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ under usual addition and multiplication are all commutative rings with unity.
2. The ring of integers modulo n, $\mathbb{Z}_n = \{0,1,\dots,n-1\}$, with addition and multiplication modulo n, is a finite commutative ring with unity.
3. The set $M_n(\mathbb{R})$ of all $n \times n$ matrices with real entries is a ring under matrix addition and multiplication. It has a unity (the identity matrix I_n). If $n > 1$, this ring is non-commutative.
4. The set of even integers, $2\mathbb{Z}$, is a commutative ring under the usual operations. It does not have a unity.
5. The trivial ring is $\{0\}$, where $0+0=0$ and $0 \cdot 0 = 0$.

Elementary Properties of Rings

Theorem 3.1.3. *Let R be a ring and let 0 be the additive identity of R. For any elements $a,b \in R$, the following hold:*

1. $a \cdot 0 = 0 \cdot a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.
4. *If R has a unity 1, then* $(-1)a = -a$.

Proof. 1. We have $a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$. By the cancellation law in the additive group $(R,+)$, we get $a \cdot 0 = 0$. Similarly, $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$ implies $0 \cdot a = 0$.

2. To show $a(-b) = -(ab)$, we show that $a(-b)$ is the additive inverse of ab. By the distributive law, $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$. Thus, $a(-b) = -(ab)$. Similarly, $(-a)b = -(ab)$.

3. Using property (ii) twice, we get $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

4. Suppose R has a unity 1. Then $a + (-1)a = 1 \cdot a + (-1)a = (1 + (-1))a = 0 \cdot a = 0$. This shows that $(-1)a$ is the additive inverse of a, so $(-1)a = -a$.

■

Theorem 3.1.4. *If a ring R has a multiplicative identity, then it is unique.*

Proof. Suppose 1 and $1'$ are both multiplicative identities in a ring R. Since 1 is an identity, we can write $1 \cdot 1' = 1'$. Since $1'$ is an identity, we can write $1 \cdot 1' = 1$. Therefore, by transitivity, $1 = 1'$, proving the multiplicative identity is unique. ■

Theorem 3.1.5. *If an element of a ring R has a multiplicative inverse, then it must be unique.*

Proof. The existence of a multiplicative inverse for an element presupposes the existence of a multiplicative identity, let's call it 1, in the ring R. Let $a \in R$, and suppose that both b and c are multiplicative inverses of a. By definition, this means that $ab = ba = 1$ and $ac = ca = 1$. Now, consider the element b. We can write the following chain of equalities:

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

Thus, $b = c$, which shows that the multiplicative inverse of any element is unique. ■

Rings with and without Zero Divisors

Definition 3.1.6 (Zero Divisor)**.** Let R be a ring. A non-zero element $a \in R$ is called a **left zero divisor** if there exists a non-zero element $b \in R$ such that $ab = 0$. Similarly, a non-zero element $c \in R$ is a **right zero divisor** if there exists a non-zero $d \in R$ such that $dc = 0$.

A **zero divisor** is an element that is either a left or a right zero divisor. In commutative rings, the distinction between left and right zero divisors vanishes. A ring with no zero divisors is sometimes called a domain.

Example 3.1.7. 1. **Ring with Zero Divisors:** In the ring $\mathbb{Z}_6$, the element 2 is non-zero and 3 is non-zero, but $2 \cdot 3 = 6 \equiv 0 \pmod 6$. Thus, 2 and 3 are zero divisors in $\mathbb{Z}_6$.

2. **Ring with Zero Divisors:** In the ring of 2×2 matrices over $\mathbb{R}$, $M_2(\mathbb{R})$, consider the non-zero matrices $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Their product is $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, the zero matrix. Thus, both A and B are zero divisors.

3. **Ring without Zero Divisors:** The ring of integers $\mathbb{Z}$ has no zero divisors. If $a, b \in \mathbb{Z}$ and $ab = 0$, then it must be that either $a = 0$ or $b = 0$. The same is true for the rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

Integral Domains and Skew Fields

Definition 3.1.8 (Integral Domain)**.** An **integral domain** is a *commutative ring with unity* $(1 \neq 0)$ that has *no zero divisors.*

Equivalently, an integral domain is a commutative ring R with unity $1 \neq 0$ such that for any $a, b \in R$, if $ab = 0$, then either $a = 0$ or $b = 0$.

Theorem 3.1.9 (Cancellation Law)**.** *Let R be an integral domain. If $a, b, c \in R$ with $a \neq 0$ and $ab = ac$, then $b = c$.*

Proof. From $ab = ac$, we have $ab - ac = 0$, which implies $a(b - c) = 0$ by the distributive law. Since R is an integral domain and we are given that $a \neq 0$, the property of having no zero divisors forces the other factor to be zero. Thus, $b - c = 0$, which implies $b = c$. ■

Example 3.1.10. 1. The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all integral domains.

2. For any prime p, the ring of integers modulo p, $\mathbb{Z}_p$, is an integral domain.

3. The ring of polynomials with integer coefficients, $\mathbb{Z}[x]$, is an integral domain.

4. $\mathbb{Z}_6$ is not an integral domain because it has zero divisors $(2 \cdot 3 = 0)$. The ring of even integers $2\mathbb{Z}$ is not an integral domain because it lacks a multiplicative identity.

Definition 3.1.11 (Skew Field / Division Ring)**.** A **skew field** or **division ring** is a ring R with unity $(1 \neq 0)$ in which every non-zero element has a multiplicative inverse. In other words, the set of non-zero elements $R^* = R \setminus \{0\}$ forms a group under multiplication. A skew field need not be commutative.

Theorem 3.1.12. *Every skew field is a domain (has no zero divisors).*

Proof. Let R be a skew field and let $a, b \in R$ with $ab = 0$. Suppose $a \neq 0$. Then a has a multiplicative inverse a^{-1}. Multiplying the equation by a^{-1} on the left gives $a^{-1}(ab) = a^{-1}0$, which simplifies to $(a^{-1}a)b = 0$, so $1 \cdot b = 0$, which means $b = 0$. Thus, R has no zero divisors. ■

Fields

Definition 3.1.13 (Field)**.** A **field** is a *commutative ring* F with unity $(1 \neq 0)$ in which every non-zero element has a multiplicative inverse.

From the definitions, we can see that a field is simply a commutative skew field. Consequently, every field is an integral domain. The converse is not true; for example, $\mathbb{Z}$ is an integral domain but not a field.

Example 3.1.14.

1. The set of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are all fields.

2. The ring of integers modulo p, $\mathbb{Z}_p$, is a field if and only if p is a prime number. For example, $\mathbb{Z}_5$ is a field. Its non-zero elements are $\{1, 2, 3, 4\}$, and their inverses are $1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$.

3. The ring $\mathbb{Z}$ is an integral domain but not a field, as the only elements with multiplicative inverses in $\mathbb{Z}$ are 1 and -1. The element $2 \in \mathbb{Z}$ has no multiplicative inverse in $\mathbb{Z}$.

4. The ring $\mathbb{Z}_{12}$ is not a field because it is not an integral domain $(3 \cdot 4 = 0)$. Non-zero elements like 3 do not have multiplicative inverses.

Theorem 3.1.15. *A finite integral domain is a field.*

Proof. Let $R = \{x_1, x_2, \ldots, x_n\}$ be a finite non-zero integral domain. Clearly, $n \geq 2$ and let $x \in R$ be non-zero. Then $R = \{xx_1, xx_2, \ldots, xx_n\}$, since if $xx_k = xx_l$ for $k \neq l$, then **cancellation laws** imply $x_k = x_l$, a contradiction. Therefore, $x = xx_i$ for some i, $1 \leq i \leq n$. Now, let $y \in R$. Then $xy = (xx_i)y$, hence commutativity of R and **cancellation laws** give $y = x_i y = yx_i$. That is x_i is an identity element of R. Denote x_i by e. Then $e = xx_j = x_j x$ for some j, $1 \leq j \leq n$. So x_j is the inverse of x, that is, every non-zero element of R has an inverse. Hence R is a field. ■

Subrings

Definition 3.1.16 (Subring)**.** A non-empty subset S of a ring R is called a **subring** of R if S is itself a ring under the operations of addition and multiplication defined on R.

Theorem 3.1.17 (Subring Test)**.** *A non-empty subset S of a ring R is a subring of R if and only if for all $a, b \in S$:*

1. *$a - b \in S$ (closed under subtraction)*

2. *$ab \in S$ (closed under multiplication)*

Proof. If S is a subring, it is a ring, so it is an additive subgroup and is closed under multiplication. Thus (1) and (2) hold. Conversely, assume (1) and (2) hold. Since S is non-empty, let $a \in S$. Then by (1), $a - a = 0 \in S$. For any $s \in S$, $0 - s = -s \in S$. For any $s, t \in S$, we have $-t \in S$, so $s - (-t) = s + t \in S$. This shows $(S, +)$ is a subgroup of $(R, +)$. Since addition in R is commutative, it is commutative in S. The associativity of multiplication and the distributive laws are inherited from R. Condition (2) ensures closure of multiplication. Thus, S is a ring. ■

Example 3.1.18.

1. The set of integers $\mathbb{Z}$ is a subring of the ring of rational numbers $\mathbb{Q}$.

2. The set of even integers $2\mathbb{Z}$ is a subring of the ring of integers $\mathbb{Z}$.

3. For any ring R, the trivial set $\{0\}$ and the ring R itself are always subrings of R.

4. The set of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of the complex numbers $\mathbb{C}$.

Ideals

Definition 3.1.19 (Ideal)**.** A non-empty subset I of a ring R is called an **ideal** of R if:

1. For all $a, b \in I$, their difference $a - b \in I$ (i.e., I is an additive subgroup of R).

2. For all $a \in I$ and for all $r \in R$, both $ra \in I$ and $ar \in I$ (i.e., I "absorbs" products with elements of R).

Note: An ideal is always a subring, but a subring is not necessarily an ideal. For an ideal, the "absorption" property must hold for all elements $r \in R$, not just for $r \in I$. In a commutative ring, the conditions $ra \in I$ and $ar \in I$ are equivalent.

Example 3.1.20.

1. For any ring R, $\{0\}$ and R itself are ideals, called the trivial ideals.

2. In the ring of integers $\mathbb{Z}$, the set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is an ideal for any integer n.

3. The ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$, but it is not an ideal of $\mathbb{Q}$. For example, $1 \in \mathbb{Z}$ and $\frac{1}{2} \in \mathbb{Q}$, but their product $\frac{1}{2} \cdot 1 = \frac{1}{2}$ is not in $\mathbb{Z}$.

Quotient Rings

Let I be an ideal of a ring R. The ideal I allows us to define a new ring, called the quotient ring (or factor ring), denoted R/I.

Definition 3.1.21 (Quotient Ring)**.** Let I be an ideal of a ring R. The set of all cosets of I in R, denoted by R/I, is given by

$$R/I = \{r + I \mid r \in R\}$$

This set forms a ring under the operations defined below:

- **Addition**: $(a + I) + (b + I) = (a + b) + I$
- **Multiplication**: $(a + I)(b + I) = ab + I$

The zero element is $0 + I = I$, and the additive inverse of $a + I$ is $(-a) + I$. If R has unity 1, then R/I has unity $1 + I$. The fact that I is an ideal ensures that the multiplication is well-defined.

Example 3.1.22. 1. The quintessential example is the ring of integers modulo n. Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ consists of the cosets $\{0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$. This ring is isomorphic to the ring $\mathbb{Z}_n$.

2. Let $R = \mathbb{R}[x]$ be the ring of polynomials with real coefficients, and let I be the ideal generated by $x^2 + 1$, denoted $\langle x^2 + 1\rangle$. The quotient ring $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is isomorphic to the field of complex numbers $\mathbb{C}$. The coset $x + I$ behaves like the imaginary unit i, since $(x + I)^2 = x^2 + I = (x^2 + 1) - 1 + I = -1 + I$.

Boolean Rings

Definition 3.1.23 (Boolean Ring)**.** A ring R is called a **Boolean ring** if every element is idempotent, that is, if $x^2 = x$ for all $x \in R$.

Theorem 3.1.24. *Every Boolean ring R has the following properties:*

1. *It has characteristic 2, i.e., $x + x = 0$ for all $x \in R$.*
2. *It is commutative, i.e., $xy = yx$ for all $x, y \in R$.*

Proof. 1. For any $x \in R$, we have $x+x \in R$, so $(x+x)^2 = x+x$. Also, by distributivity, $(x+x)^2 = x^2+x^2+x^2+x^2 = x + x + x + x$. Thus $x + x = x + x + x + x$. By cancellation in the additive group $(R, +)$, we obtain $0 = x + x$.

2. For any $x, y \in R$, we have $x+y \in R$, so $(x+y)^2 = x+y$. Expanding the left side gives $(x+y)^2 = x^2+xy+yx+y^2 = x + xy + yx + y$. Therefore, $x + y = x + xy + yx + y$. By cancellation, $0 = xy + yx$. From property (1), $yx = -yx$. Thus $0 = xy - yx$, which implies $xy = yx$.

■

Example 3.1.25. 1. The ring $\mathbb{Z}_2 = \{0, 1\}$ is a Boolean ring, since $0^2 = 0$ and $1^2 = 1$.

2. Let S be any set. The power set of S, denoted $\mathcal{P}(S)$, forms a Boolean ring with unity. The operations are symmetric difference for addition ($A\Delta B$) and intersection for multiplication ($A\cap B$). For any subset $A \subseteq S$, we have $A\cap A = A$, so the idempotent property holds. The additive identity is the empty set $\emptyset$, and the multiplicative identity is the set S itself.

Theorem 3.1.26. *Let R be a ring with identity 1_R. If an ideal I of R contains a unit, then $I = R$.*

Proof. Let $u \in I$ be a unit. Then its inverse u^{-1} exists in R. Since I is an ideal, the product $u^{-1}u = 1_R$ must be in I. Now, for any element $r \in R$, the product $r \cdot 1_R = r$ must also be in I by the ideal absorption property. This shows that every element of R is in I, so $R \subseteq I$. As $I \subseteq R$ by definition, we have $I = R$. ■

Theorem 3.1.27. *If I and J are ideals of a ring R, then their sum $I + J = \{i + j \mid i \in I, j \in J\}$ is also an ideal of R.*

Proof. Let $x, y \in I + J$ and $r \in R$. Then $x = i_1 + j_1$ and $y = i_2 + j_2$ for some $i_1, i_2 \in I$ and $j_1, j_2 \in J$.

- **Closure under subtraction:** $x - y = (i_1 - i_2) + (j_1 - j_2)$. Since I and J are ideals, $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$. Thus, $x - y \in I + J$.
- **Absorption:** $rx = r(i_1 + j_1) = ri_1 + rj_1$. Since I, J are ideals, $ri_1 \in I$ and $rj_1 \in J$. Thus, $rx \in I + J$. Similarly, $xr = i_1r + j_1r \in I + J$.

Since $I + J$ is non-empty (as $0 = 0 + 0 \in I + J$) and satisfies the ideal test, it is an ideal of R. ■

Theorem 3.1.28. *Let I and J be ideals in a ring R. Then their product $IJ = \{\sum_{k=1}^{n} i_kj_k \mid i_k \in I, j_k \in J, n \in \mathbb{N}\}$ is also an ideal in R.*

Proof. Let $x = \sum i_kj_k$ and $y = \sum i'_lj'_l$ be elements of IJ, and let $r \in R$.

- **Closure under subtraction:** $x - y = \sum i_k j_k + \sum(-i'_l)j'_l$. Since I is an ideal, $-i'_l \in I$. Thus $x - y$ is also a finite sum of products of elements from I and J, so $x - y \in IJ$.
- **Absorption:** $rx = r(\sum i_k j_k) = \sum(ri_k)j_k$. Since I is an ideal, $ri_k \in I$, so $rx \in IJ$. Similarly, $xr = (\sum i_k j_k)r = \sum i_k(j_k r)$. Since J is an ideal, $j_k r \in J$, so $xr \in IJ$.

Since IJ is non-empty (as $0 \in IJ$) and satisfies the ideal test, it is an ideal of R. ■

3.2 Ring Homomorphism and Isomorphism

Ring Homomorphism

Definition 3.2.1 (Ring Homomorphism)**.** A **ring homomorphism** is a function $\phi : R \to S$ between two rings $(R, +, \cdot)$ and $(S, \oplus, \odot)$ that preserves the ring operations. That is, for all $a, b \in R$:

1. $\phi(a + b) = \phi(a) \oplus \phi(b)$
2. $\phi(a \cdot b) = \phi(a) \odot \phi(b)$

Definition 3.2.2 (Kernel of a Homomorphism)**.** The **kernel** of a ring homomorphism $\phi : R \to S$ is the set of elements in R that map to the zero element in S. It is denoted by $\ker(\phi)$.

$$\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$$

The kernel of a ring homomorphism is always an ideal of the domain ring R.

Fundamental Theorem of Homomorphism

Theorem 3.2.3 (Fundamental Theorem of Ring Homomorphism)**.** *Let $\phi : R \to S$ be a surjective ring homomorphism. Then the quotient ring $R/\ker(\phi)$ is isomorphic to the ring S.*

Proof. Let $I = \ker(\phi)$. We define a map $\psi : R/I \to S$ by $\psi(r+I) = \phi(r)$. This map is well-defined because if $r+I = r'+I$, then $r - r' \in I$, so $\phi(r - r') = 0_S$, which implies $\phi(r) = \phi(r')$. The map ψ is a homomorphism because it inherits the homomorphism properties of ϕ. For injectivity, suppose $\psi(r + I) = 0_S$. This means $\phi(r) = 0_S$, so $r \in I$, which makes $r+I = I$, the zero element of R/I. Thus, $\ker(\psi) = \{I\}$, and ψ is injective. The map ψ is surjective because ϕ is surjective. For any $s \in S$, there exists an $r \in R$ such that $\phi(r) = s$, and thus $\psi(r + I) = s$. Since ψ is a bijective homomorphism, it is an isomorphism, and $R/I \cong S$. ■

Ring Isomorphism

Definition 3.2.4 (Ring Isomorphism)**.** A **ring isomorphism** is a ring homomorphism $\phi : R \to S$ that is also a bijection (i.e., it is both one-to-one and onto). If such a map exists, we say that the rings R and S are **isomorphic**, and we write $R \cong S$.

3.3 Special Types of Ideals

Principal Ideals

Definition 3.3.1 (Principal Ideal)**.** An ideal I in a ring R is a **principal ideal** if it can be generated by a single element. That is, there exists an element $a \in R$ such that $I = \langle a \rangle$. In a commutative ring with unity, this is the set $\langle a \rangle = \{ra \mid r \in R\}$.

Example 3.3.2.

1. In the ring of integers $\mathbb{Z}$, every ideal is principal. The ideal of even integers is $\langle 2 \rangle = 2\mathbb{Z}$.
2. In any field F, the only ideals are $\{0\} = \langle 0 \rangle$ and the entire field $F = \langle 1 \rangle$. Both are principal.
3. In the ring of polynomials $\mathbb{Z}[x]$, the ideal $I = \langle 2, x \rangle = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ is not a principal ideal.

   A ring where every ideal is a principal ideal is called a **Principal Ideal Domain (PID)**.
4. **Polynomial Rings over a Field:** Any polynomial ring $F[x]$ where F is a field is a PID.
   - In the ring of polynomials with real coefficients, $\mathbb{R}[x]$, the ideal of all polynomials that have $x = 5$ as a root is the principal ideal $\langle x - 5 \rangle$.
   - In $\mathbb{Q}[x]$, the ideal of polynomials divisible by $x^2 - 2$ is the principal ideal $\langle x^2 - 2 \rangle$.
5. **A Non-Principal Ideal in $\mathbb{Z}[x]$:** The ring $\mathbb{Z}[x]$ is not a PID. The ideal $I = \langle 2, x \rangle$ consists of all polynomials whose constant term is an even integer. This ideal is not principal.

Proof Sketch. Suppose $I = \langle p(x) \rangle$ for some $p(x) \in \mathbb{Z}[x]$. Since $2 \in I$, we must have $2 = q(x)p(x)$ for some $q(x)$. This implies $p(x)$ must be a constant, specifically ± 1 or ± 2. If $p(x) = \pm 1$, then $I = \mathbb{Z}[x]$, which is false since $1 \notin I$. If $p(x) = \pm 2$, then $I = \langle 2 \rangle$. This is also false because $x \in I$ but x cannot be written as $2 \cdot g(x)$ for any $g(x) \in \mathbb{Z}[x]$. Therefore, no such $p(x)$ exists. ■

6. **A Non-Principal Ideal in $F[x, y]$:** The ring of polynomials in two variables over a field, $F[x, y]$, is not a PID. The ideal $I = \langle x, y \rangle$, which is the set of all polynomials with a zero constant term, is not a principal ideal.

7. **The Ring of Integers:** As mentioned before, $\mathbb{Z}$ is a classic example of a PID. Every ideal is of the form $n\mathbb{Z} = \langle n \rangle$ for some integer n.

Prime Ideals

Definition 3.3.3 (Prime Ideal)**.** Let R be a commutative ring. An ideal $P \subsetneq R$ is a **prime ideal** if for any elements $a, b \in R$, the condition $ab \in P$ implies that either $a \in P$ or $b \in P$. An equivalent condition is that the quotient ring R/P is an integral domain.

Example 3.3.4. 1. In $\mathbb{Z}$, an ideal $\langle n \rangle$ is prime if and only if n is a prime number or $n = 0$.

2. The ideal $\langle 6 \rangle$ in $\mathbb{Z}$ is not prime because $2 \cdot 3 = 6 \in \langle 6 \rangle$, but neither 2 nor 3 is in $\langle 6 \rangle$.

3. The ideal $\{0\}$ is a prime ideal in any integral domain.

4. **The Integers $\mathbb{Z}$:** An ideal $\langle n \rangle$ in $\mathbb{Z}$ is a prime ideal if and only if n is a prime number, or $n = 0$.

   - The ideal $\langle 5 \rangle = 5\mathbb{Z}$ is a prime ideal. If $ab \in \langle 5 \rangle$, then 5 divides ab. Since 5 is a prime number, Euclid's lemma implies that 5 must divide a or 5 must divide b. Thus, $a \in \langle 5 \rangle$ or $b \in \langle 5 \rangle$.
   - The ideal $\langle 6 \rangle$ is not a prime ideal. We have $2 \cdot 3 = 6 \in \langle 6 \rangle$, but neither $2 \in \langle 6 \rangle$ nor $3 \in \langle 6 \rangle$.
   - The zero ideal $\langle 0 \rangle = \{0\}$ is a prime ideal in $\mathbb{Z}$ because $\mathbb{Z}$ is an integral domain.

5. **The Zero Ideal $\langle 0 \rangle$:** In any commutative ring R, the zero ideal $\langle 0 \rangle$ is a prime ideal if and only if R is an integral domain. This follows directly from the definition: $ab \in \langle 0 \rangle$ means $ab = 0$, and the prime condition requires that this implies $a = 0$ or $b = 0$, which is the definition of an integral domain.

6. **Polynomial Rings:**

   - In the ring $\mathbb{Z}[x]$, the ideal $I = \langle x \rangle$ is a prime ideal. The quotient ring $\mathbb{Z}[x]/\langle x \rangle$ is isomorphic to $\mathbb{Z}$ (via the evaluation map $\phi(p(x)) = p(0)$). Since $\mathbb{Z}$ is an integral domain, the ideal $\langle x \rangle$ is prime.
   - In the ring $\mathbb{R}[x]$, the ideal $P = \langle x^2 + 4 \rangle$ is a prime ideal. This is because the polynomial $x^2 + 4$ is irreducible over the field of real numbers $\mathbb{R}$. The quotient ring $\mathbb{R}[x]/\langle x^2 + 4 \rangle$ is isomorphic to the field $\mathbb{C}$, which is an integral domain. In fact, since the quotient is a field, this ideal is also maximal.
   - The ideal $I = \langle 2 \rangle$ in $\mathbb{Z}[x]$ is also prime. The quotient ring $\mathbb{Z}[x]/\langle 2 \rangle$ is isomorphic to $\mathbb{Z}_2[x]$, the ring of polynomials with coefficients in $\mathbb{Z}_2$. Since $\mathbb{Z}_2$ is a field, $\mathbb{Z}_2[x]$ is an integral domain, and therefore $\langle 2 \rangle$ is a prime ideal.

7. **Product Rings:** Consider the ring $R = \mathbb{Z} \times \mathbb{Z}$.

   - The ideal $P_1 = \mathbb{Z} \times \{0\}$ is a prime ideal.

     Proof. Let (a, b) and (c, d) be elements of $\mathbb{Z} \times \mathbb{Z}$ such that their product $(ac, bd) \in P_1$. This means $bd = 0$. Since $\mathbb{Z}$ is an integral domain, this implies $b = 0$ or $d = 0$. If $b = 0$, then $(a, b) = (a, 0) \in P_1$. If $d = 0$, then $(c, d) = (c, 0) \in P_1$. Thus, one of the factors must be in P_1. ■

   - Similarly, $P_2 = \{0\} \times \mathbb{Z}$ is also a prime ideal.
   - Note that neither P_1 nor P_2 is a maximal ideal. For instance, $P_1 \subsetneq \mathbb{Z} \times 2\mathbb{Z} \subsetneq \mathbb{Z} \times \mathbb{Z}$.

Maximal Ideals

Definition 3.3.5 (Maximal Ideal)**.** Let R be a ring. An ideal $M \subsetneq R$ is a **maximal ideal** if there is no other ideal I of R such that $M \subsetneq I \subsetneq R$. In a commutative ring with unity, an ideal M is maximal if and only if the quotient ring R/M is a field.

Example 3.3.6. 1. In $\mathbb{Z}$, an ideal $\langle n \rangle$ is maximal if and only if n is a prime number.

2. The ideal $\langle 6 \rangle$ in $\mathbb{Z}$ is not maximal because $\langle 6 \rangle \subsetneq \langle 2 \rangle \subsetneq \mathbb{Z}$.

3. The ideal $\langle x \rangle$ in the polynomial ring $\mathbb{Z}[x]$ is prime but not maximal, since $\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$.

4. **Irreducible Polynomials in $F[x]$:** In the polynomial ring $F[x]$ over a field F, an ideal $\langle p(x) \rangle$ is maximal if and only if the polynomial $p(x)$ is irreducible over F.

- In $\mathbb{R}[x]$, the ideal $\langle x^2+1\rangle$ is maximal because x^2+1 has no real roots and is thus irreducible over $\mathbb{R}$. The quotient ring $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to the field of complex numbers $\mathbb{C}$.
- In contrast, the ideal $\langle x^2-1\rangle$ in $\mathbb{R}[x]$ is not maximal because $x^2-1=(x-1)(x+1)$ is reducible. Indeed, we have the proper containment $\langle x^2-1\rangle \subsetneq \langle x-1\rangle \subsetneq \mathbb{R}[x]$.

5. **Ideals in $F[x,y]$:** In the ring $F[x,y]$ over a field F, the ideal $M=\langle x-a, y-b\rangle$ for any $a,b\in F$ is a maximal ideal. The quotient ring $F[x,y]/M$ is isomorphic to the field F.

6. **Ring of Continuous Functions:** Let $C[0,1]$ be the ring of continuous real-valued functions on the interval $[0,1]$. For any point $c\in[0,1]$, the set
$$M_c=\{f\in C[0,1]\mid f(c)=0\}$$
is a maximal ideal. The quotient ring $C[0,1]/M_c$ is isomorphic to the field of real numbers $\mathbb{R}$.

7. **Ideals in a Finite Commutative Ring:** In the ring $\mathbb{Z}_{12}$, the ideal $\langle 2\rangle=\{0,2,4,6,8,10\}$ is a maximal ideal. This is because the quotient ring $\mathbb{Z}_{12}/\langle 2\rangle$ has order $12/6=2$ and is isomorphic to the field $\mathbb{Z}_2$. Similarly, $\langle 3\rangle$ is a maximal ideal because $\mathbb{Z}_{12}/\langle 3\rangle\cong\mathbb{Z}_3$. The ideal $\langle 4\rangle=\{0,4,8\}$ is not maximal because it is properly contained in the ideal $\langle 2\rangle$.

Chapter 4

Tutorial

Semigroups and Monoids

A **semigroup** is a non-empty set equipped with an associative binary operation. A **monoid** is a semigroup that also contains an identity element for the operation. Every monoid is a semigroup, but not every semigroup is a monoid.

Examples of Semigroups

1. The set of positive integers $(\mathbb{Z}^+, +)$ under addition is a semigroup. It is not a monoid because the identity element, 0, is not in the set.
2. The set of all $n \times n$ matrices $M_n(\mathbb{R})$ under matrix multiplication is a semigroup. It is also a monoid since the identity matrix I_n is in the set.
3. Let Σ be an alphabet (e.g., $\Sigma = \{a, b, c\}$). The set of all non-empty strings over Σ, with the operation of string concatenation, is a semigroup.

Examples of Monoids

1. The set of natural numbers including zero, $(\mathbb{N}_0, +)$, is a monoid with identity element 0.
2. The set of integers $(\mathbb{Z}, \cdot)$ under multiplication is a monoid with identity element 1. It is not a group because most elements (like 2) do not have a multiplicative inverse.
3. Let Σ be an alphabet. The set of all strings (including the empty string ϵ) over Σ is a monoid under concatenation, with ϵ as the identity element.

Abelian and Non-Abelian Groups

A group $(G, *)$ is **abelian** if its operation is commutative ($a * b = b * a$ for all $a, b \in G$). Otherwise, it is **non-abelian**.

Examples of Abelian Groups

1. The set of integers $(\mathbb{Z}, +)$ is an infinite abelian group.
2. The set of integers modulo n, $(\mathbb{Z}_n, +)$, is a finite abelian group of order n.
3. The set of non-zero rational numbers $(\mathbb{Q}^*, \cdot)$ is an infinite abelian group.
4. The Klein four-group $V_4 = \{e, a, b, c\}$ with relations $a^2 = b^2 = c^2 = e$ and $ab = c, ba = c$, etc., is a finite abelian group of order 4.

Examples of Non-Abelian Groups

1. The symmetric group S_3, the group of permutations of three elements, is the smallest non-abelian group. It has order $3! = 6$. For example, $(1\ 2)(1\ 3) = (1\ 3\ 2)$ while $(1\ 3)(1\ 2) = (1\ 2\ 3)$.
2. The general linear group $GL_2(\mathbb{R})$ of invertible 2×2 matrices with real entries is a non-abelian group under matrix multiplication.
3. The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a non-abelian group of order 8, where $ij = k$ but $ji = -k$.

Cyclic and Non-Cyclic Groups

A group G is **cyclic** if it can be generated by a single element. That is, there exists an element $g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Examples of Cyclic Groups

1. The group of integers $(\mathbb{Z}, +)$ is an infinite cyclic group, generated by either 1 or -1.
2. The group of integers modulo n, $(\mathbb{Z}_n, +)$, is a finite cyclic group of order n, generated by 1.
3. The group of n-th roots of unity in $\mathbb{C}$ under multiplication is a cyclic group of order n.

Examples of Non-Cyclic Groups

1. The Klein four-group V_4 is not cyclic. It is abelian, but every non-identity element has order 2, so no single element can generate the entire group of order 4.
2. The symmetric group S_3 is not cyclic. Its order is 6, but it contains no element of order 6.
3. The group of rational numbers $(\mathbb{Q}, +)$ is not cyclic.

Computing Generators in a Cyclic Group

Theorem 4.0.1. *An element $k \in \mathbb{Z}_n$ is a generator of the cyclic group $(\mathbb{Z}_n, +)$ if and only if the greatest common divisor of k and n is 1, i.e., $\gcd(k, n) = 1$.*

The number of generators of $\mathbb{Z}_n$ is given by $\phi(n)$, where ϕ is Euler's totient function.

Example 4.0.2 (Generators of $\mathbb{Z}_{12}$)**.** We want to find all integers k such that $1 \leq k < 12$ and $\gcd(k, 12) = 1$.

- $\gcd(1, 12) = 1$ (Generator)
- $\gcd(2, 12) = 2$
- $\gcd(3, 12) = 3$
- $\gcd(4, 12) = 4$
- $\gcd(5, 12) = 1$ (Generator)
- $\gcd(6, 12) = 6$
- $\gcd(7, 12) = 1$ (Generator)
- $\gcd(8, 12) = 4$
- $\gcd(9, 12) = 3$
- $\gcd(10, 12) = 2$
- $\gcd(11, 12) = 1$ (Generator)

The generators of $\mathbb{Z}_{12}$ are $\{1, 5, 7, 11\}$. There are $\phi(12) = 4$ generators.

Structure Theorem for Cyclic Groups (Statement Only)

This fundamental theorem classifies all cyclic groups up to isomorphism.

Theorem 4.0.3 (Structure Theorem for Cyclic Groups)**.** *Every cyclic group is isomorphic to exactly one of the following groups:*

1. *The additive group of integers $(\mathbb{Z}, +)$, if the cyclic group is infinite.*
2. *The additive group of integers modulo n, $(\mathbb{Z}_n, +)$, if the cyclic group is finite of order n.*

Even and Odd Permutation

A **transposition** is a permutation that swaps two elements and leaves all others fixed. It is a cycle of length 2, such as $(a\ b)$.

Theorem 4.0.4. *Every permutation in S_n (for $n \geq 2$) can be expressed as a product of transpositions.*

This decomposition is not unique in terms of the number of transpositions. However, for any given permutation, the number of transpositions in any decomposition is always either even or odd. This property is called the **parity** of the permutation.

Definition 4.0.5 (Even and Odd Permutation)**.** • A permutation is called **even** if it can be written as a product of an even number of transpositions.

- A permutation is called **odd** if it can be written as a product of an odd number of transpositions.

The identity permutation is considered even as it is a product of zero transpositions.

Example 4.0.6. 1. The permutation $\sigma = (1\ 3\ 2) \in S_3$ can be written as $(1\ 2)(1\ 3)$. This is a product of two transpositions, so σ is an even permutation.

2. A cycle of length k, $(a_1\ a_2\ \dots\ a_k)$, can be written as a product of $k-1$ transpositions: $(a_1\ a_k)(a_1\ a_{k-1})\dots(a_1\ a_2)$. Thus, a k-cycle is even if $k-1$ is even (i.e., k is odd), and odd if $k-1$ is odd (i.e., k is even).

3. The set of all even permutations in S_n forms a normal subgroup called the **Alternating Group**, denoted A_n.

Examples of Commutative & Non-Commutative Rings

Definition 4.0.7. A ring R is **commutative** if $ab = ba$ for all $a, b \in R$. Otherwise, it is **non-commutative**.

Commutative Rings

1. The ring of integers $(\mathbb{Z}, +, \cdot)$.
2. The fields of rational numbers $(\mathbb{Q})$, real numbers $(\mathbb{R})$, and complex numbers $(\mathbb{C})$.
3. The ring of integers modulo n, $(\mathbb{Z}_n, +, \cdot)$.
4. The ring of polynomials with real coefficients, $\mathbb{R}[x]$.

Non-Commutative Rings

1. The ring of $n \times n$ matrices over the real numbers, $M_n(\mathbb{R})$, for $n \geq 2$. For example, in $M_2(\mathbb{R})$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \quad \text{but} \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

2. The ring of Hamilton's Quaternions, $\mathbb{H}$. In this ring, i, j, k are elements such that $i^2 = j^2 = k^2 = ijk = -1$, which implies $ij = k$ but $ji = -k$.

Left & Right Ideal of a Ring

In non-commutative rings, we must distinguish between left, right, and two-sided ideals.

Definition 4.0.8. A subring I of a ring R is:

- a **left ideal** if for every $r \in R$ and $a \in I$, we have $ra \in I$.
- a **right ideal** if for every $r \in R$ and $a \in I$, we have $ar \in I$.
- a **two-sided ideal** (or simply an **ideal**) if it is both a left and a right ideal.

In a commutative ring, every left or right ideal is automatically a two-sided ideal.

Example 4.0.9. In the ring $R = M_2(\mathbb{R})$, consider the set $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$.

- I is a **left ideal**. Let $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in R$ and $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in I$. Their product is $\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ra + sb & 0 \\ ta + ub & 0 \end{pmatrix}$, which has the required form to be in I.
- I is **not a right ideal**. Consider the product in the other order: $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, which is not in I if a or b is non-zero.

Relation Between Ideals & Subrings

The relationship is simple and strict:

Every ideal is a subring, but not every subring is an ideal.

An ideal must satisfy the subring test ($a - b \in I$ and $ab \in I$), but it must also satisfy the stronger "absorption" property ($ra \in I$ and $ar \in I$ for all $r \in R$). The subring definition only requires closure for elements within the subring itself.

Example 4.0.10. The ring of integers $\mathbb{Z}$ is a subring of the ring of rational numbers $\mathbb{Q}$. However, $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$. To see why, take an element from the subring, $3 \in \mathbb{Z}$, and an element from the parent ring, $\frac{1}{2} \in \mathbb{Q}$. Their product is $3 \cdot \frac{1}{2} = \frac{3}{2}$, which is not in $\mathbb{Z}$. The absorption property fails.

Sum & Product of Ideals

Given two ideals I and J of a ring R, we can form new ideals.

Definition 4.0.11 (Sum of Ideals)**.** The **sum** of I and J is the set $I + J = \{i + j \mid i \in I, j \in J\}$. This set is the smallest ideal of R containing both I and J.

Definition 4.0.12 (Product of Ideals)**.** The **product** of I and J is the set of all finite sums of products of elements from I and J:

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \mid i_k \in I, j_k \in J, n \in \mathbb{N} \right\}$$

This set is also an ideal and is contained within the intersection $I \cap J$.

Example 4.0.13. In the ring $\mathbb{Z}$, let $I = \langle 4 \rangle = 4\mathbb{Z}$ and $J = \langle 6 \rangle = 6\mathbb{Z}$.

- **Sum:** $I + J = \langle 4 \rangle + \langle 6 \rangle = \langle \gcd(4, 6) \rangle = \langle 2 \rangle = 2\mathbb{Z}$.
- **Product:** $IJ = \langle 4 \rangle \langle 6 \rangle = \langle 4 \cdot 6 \rangle = \langle 24 \rangle = 24\mathbb{Z}$.