

Symmetry and Structure: From Groups to the Fundamental Theorem of Galois Theory

Prasanna Mahesh Pawar
AMMOC- An International Math Circle

Preface

Abstract algebra is a central area of mathematics that provides a systematic approach to understanding a wide range of mathematical concepts and structures. These notes are intended to provide a clear, systematic, and self-contained introduction to the fundamental ideas and core topics of abstract algebra. The main focus is on group theory, followed by ring and module theory, and finally field theory and Galois theory. The material is arranged so that the subject develops step by step, starting with basic definitions and examples and moving gradually toward more advanced and theoretical results.

The goal of these notes is to explain the main ideas of algebra in a way that is both clear and mathematically precise. Throughout the text, the emphasis is on understanding algebraic structures through their properties, examples, and relationships with one another. Abstract ideas are explained with easy-to-understand examples whenever possible, and important results are illustrated through relevant applications.

The first part of the text is devoted to group theory. It begins by fixing notation and reviewing binary operations and basic algebraic structures. The concept of a group is then introduced and studied in detail. The fundamental properties of groups are developed in a systematic way, with special attention given to important and well-known examples. Dihedral groups and symmetric groups are discussed early, since they provide concrete illustrations of the theory and play a key role in many areas of mathematics. The next chapter focuses on subgroups, which are essential for understanding the internal structure of groups. Subgroup tests are introduced, along with important constructions and examples. The ideas of centralizers and normalizers are used to study how elements and subsets behave inside a group. Cyclic groups and cyclic subgroups are examined in detail, as they are basic building blocks in group theory and appear frequently in applications.

Homomorphisms and isomorphisms are then introduced as maps that preserve algebraic structure. These concepts provide a powerful way to compare different groups. Cosets and Lagrange's theorem are used to study the relationship between a group and its subgroups. Quotient groups and the isomorphism theorems are developed to show how new groups can be formed from existing ones. The chapter ends with a discussion of simple groups, composition series, and the alternating group, emphasizing ideas of simplicity and decomposition.

Group actions connect abstract group theory with concrete examples. By looking at how groups act on sets, many important results can be understood in a clear and unified way. Topics such as Cayley's theorem, the class equation, and automorphisms are presented using this viewpoint. Sylow's theorems are introduced as a major application, providing strong tools for studying the structure of finite groups. The following part of the text deals with building new groups from known ones. Direct products and semidirect products are used to show how more complicated groups can be constructed from simpler pieces. Special attention is given to abelian groups, leading to the fundamental theorem of finitely generated abelian groups.

The scope of the notes is then expanded to include ring and module theory. Rings and their basic properties are introduced first, followed by ideals and factor rings. Modules over rings are presented as a generalization of vector spaces, allowing ideas from linear algebra to be applied in a wider setting. Topics such as homomorphisms, universal properties, integral domains, unique factorization, and finitely generated modules are included to build a strong algebraic foundation. The final chapter is devoted to field theory and Galois theory. It begins with fields and vector spaces and then develops the theory of field extensions and algebraic elements. Splitting fields and algebraically closed fields are introduced to study polynomial roots,

followed by separable extensions. The chapter concludes with Galois theory and the Fundamental Theorem of Galois Theory, which shows the deep connection between field extensions and groups of automorphisms.

These notes are intended for students formally studying a graduate course in abstract algebra. They provide systematic coverage of all the core topics of the subject and assume familiarity with linear algebra and basic proof techniques. The material is suitable both for classroom use in a graduate course and for independent study. Numerous examples are included to explain definitions and results, and the organization of the notes is designed to support both conceptual understanding and mathematical structure. It is hoped that these notes will serve not only as an introduction to modern abstract algebra, but also as a solid foundation for further study in algebra, number theory, geometry, and related areas of mathematics.

Acknowledgement

This project is the culmination of a year of directed reading under the guidance of my research mentor and teacher, Yaashaa Golovanov. I am infinitely indebted to him for believing in me in 2021, at a time when I had little faith in myself and had complete distaste for the subject of mathematics. Without his determination to guide and shape me as an aspiring mathematician, neither this project nor many aspects of my current life would have come to fruition. I am also thankful to the authors of several books which I used, as well as to the examination committee—Prof. Pradeep Das and Sridhar T. Sir—for their critical evaluation of my understanding of the material presented in this work.

Contents

Preface	5
Acknowledgement	7
	11
Chapter 1. Introduction to Group Theory	11
1. Notations	12
2. Binary Operations and Algebraic Structure	12
3. Groups	18
4. Properties of Groups	21
5. Dihedral Groups	24
6. Symmetric Groups	27
Chapter 2. Subgroups	31
1. Subgroups and Examples	31
2. Centralizers and Normalizers	35
3. Cyclic Groups and Cyclic Subgroups	37
Chapter 3. Group Isomorphisms and Quotient Groups	45
1. Homomorphisms and Isomorphisms	45
2. Normal Subgroups	51
3. Cosets and Lagrange's Theorem	54
4. Quotient Groups	61
5. The Isomorphism Theorems	64
6. Simple Groups and Composition Series	71
7. Transpositions and the Alternating Group	72
Chapter 4. Group Actions	75
1. Group Actions and Permutation Representations	75
2. Cayley's Theorem	79
3. The Class Equation	81
4. Automorphisms	84
5. Sylow's Theorem	87
Chapter 5. Direct and Semidirect Products, and Abelian Groups	91
1. Direct Products	91
2. The Fundamental Theorem of Finitely Generated Abelian Groups	95
3. Commutator Subgroups	96
Chapter 6. Ring and Module Theory	101
1. Rings and Examples	101
2. Ideals and Factor Rings	106
3. Modules over Rings and Examples	110
4. Ring and Module Homomorphisms	116
5. Universal Property	119

6. Integral Domains	125
7. Unique Factorization	128
8. Finitely Generated Modules	135
Chapter 7. Fields and Galois Theory	143
1. Fields and Examples	143
2. Vector Spaces	148
3. Field Extensions	152
4. Algebraic Elements	154
5. Splitting Fields and Algebraically Closed Fields	158
6. Separable Extensions	163
7. Galois Theory	167
8. The Fundamental Theorem of Galois Theory	177
Bibliography	183

CHAPTER 1

Introduction to Group Theory

“The mathematician’s patterns, like the painter’s or the poet’s must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics.”

— G. H. Hardy [4]

This chapter aims to provide a rigorous overview of group theory, including examples and fundamental results on groups, while also laying the groundwork for more detailed exploration in the chapters that follow.

Historical Note. As a formal mathematical discipline, group theory began to take shape in the 18th century. Around 1730, Euler and Lagrange began to explore ideas related to permutations and the structure of integers, laying the foundation for group theory. In 1824, Niels Henrik Abel used permutation groups in his proof that it was impossible to solve the general quintic equation by radicals. A decade later, Évariste Galois linked Galois groups to the solvability of algebraic equations, introducing important concepts such as normal subgroups and group order, forming the core of Galois theory.

In the mid-19th century, mathematicians such as Gauss, Cayley, and Jordan formalized group structures, with Cayley providing an abstract definition of a group as a set equipped with a binary operation. The late 19th century saw further refinement of group theory with Hölder’s work on quotient groups and Weber and Dyck’s formalization of abstract group definitions in 1882.

Group theory became an integral part of algebra in the 20th century, pioneered by Noether, Artin, and others advancing the theory. The completion of the classification of finite simple groups in 1982 marked a major milestone, characterizing all the basic building blocks of finite groups. Today, group theory continues to be a major area of research in mathematics, with applications extending to cryptography, quantum theory, and algebraic geometry.

In the 21st century, group theory continues to be a vibrant and expanding field of research with numerous branches of mathematics such as topology, Lie groups, and geometric group theory. These topics are very important to understand the symmetries of complex spaces and the structure of manifolds. Computational group theory has also developed, with the help of software such as GAP and Magma, allowing complex group calculations, especially on finite and permutation groups. In physics, groups play a fundamental role in quantum mechanics, gauge theory. More importantly, group theory is fundamental for cryptography, particularly in post-quantum cryptography, lattice-based and isogeny-based cryptography, which often involve group-theoretic structures on elliptic curves. Furthermore, higher-dimensional algebra and category theory have influenced modern group theory by generalizing group-like structures (e.g., groupoids and higher groups). Group theory continues to evolve with new insights, connections, and applications in pure and applied mathematics.

Group theory deals with the study of algebraic structures. **Algebraic Structures** are mathematical systems consisting of a set equipped with one or more operations. A **group** is a set equipped with a binary operation that satisfies the following properties: **associativity, the existence of an identity element, and the existence of inverses.** The study of symmetries of geometric objects is an important family of examples of groups. Beyond geometry, group theory plays a crucial role in number theory, physics,

cryptography, and even music theory. Also groups are the foundation for advanced algebraic structures such as rings, modules, and fields.

1. Notations

“To invent is to discern, to choose. But to choose, one must see clearly, and for that, good notation is indispensable.”

— Henri Poincaré [6]

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$	(Natural numbers)
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	(Integers)
$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$	(Rational numbers)
$\mathbb{R} = \{\text{All decimal expansions } \pm d_1 d_2 \dots d_n . a_1 a_2 a_3 \dots\}$	(Real numbers)
$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$	(Complex numbers)
$\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$	(Non-zero integers)
$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$	(Non-zero rational numbers)
$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$	(Non-zero real numbers)
$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$	(Non-zero complex numbers)
$\mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n > 0\}$	(Positive integers)
$\mathbb{Q}^+ = \left\{ \frac{p}{q} \in \mathbb{Q} \mid \frac{p}{q} > 0 \right\}$	(Positive rational numbers)
$\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$	(Positive real numbers)

2. Binary Operations and Algebraic Structure

“The ordinary operations of algebra suffice to resolve problems in the theory of curves.”

— Joseph-Louis Lagrange

In this section, we discuss **binary operations and algebraic structures**. Fundamental and important algebraic structures include groups, rings, and fields, each defined by specific combinations of operations. These structures form the foundation of abstract algebra, and they will be studied in the subsequent chapters in detail. Studying these algebraic structures allows mathematicians to generalize and identify patterns in arithmetic, geometry, and other areas of mathematics. Some of the examples and problems in this chapter are drawn from [1].

Question 2.1. Is it possible to associate every pair of elements of $\mathbb{Z}$ with an element in $\mathbb{Z}$?

Solution 2.1. Yes. Let (a, b) be an element in $\mathbb{Z} \times \mathbb{Z}$.

- (1) When we add two integers a and b , we perform the operation of **addition** to produce an integer, denoted by $a + b$.
- (2) Similarly, when we multiply a and b , we perform the operation of **multiplication** to produce an integer, denoted by $a \cdot b$ or ab .

Note that these operations are actually **functions from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$** .

Definition 2.1 (Binary operation). A **binary operation** $*$ on a non-empty set S is a function from $S \times S$ to S , that is, $*$ is a function that maps every ordered pair of elements of S to an element of S . Thus, $* : S \times S \rightarrow S$.

Example 2.1. (1) Addition and multiplication are binary operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}^+$ and $\mathbb{Q}^+$.

- (2) For the set $\mathbb{R}^*$ of non-zero real numbers, multiplication is a binary operation, but addition is not since $1 + (-1) = 0 \notin \mathbb{R}^*$.

- (3) Subtraction is a binary operation on $\mathbb{Z}$, but not on $\mathbb{N}$ (because the ordered pair $(5, 9)$ is mapped to $5 - 9 = -4$, which is not in $\mathbb{N}$).
- (4) Division is not a binary operation on $\mathbb{Z}$ and $\mathbb{N}$.
- (5) Division is a binary operation on the set of positive rational numbers, $\mathbb{Q}^+$, as the quotient of two positive rationals is a positive rational.

Example 2.2. Consider the set of all complex numbers $\mathbb{C}$.

- (1) We define addition $+$ on $\mathbb{C}$ by

$$(a + bi) + (c + id) = (a + c) + i(b + d)$$

for all $a + bi, c + id \in \mathbb{C}$. Then $+$ is a binary operation on $\mathbb{C}$.

- (2) We define multiplication $\cdot$ (we call complex multiplication) on $\mathbb{C}$ by

$$(a + bi) \cdot (c + id) = (ac - bd) + i(ad + bc)$$

for all $a + bi, c + id \in \mathbb{C}$. Then $\cdot$ is a binary operation on $\mathbb{C}$.

- Note 2.1.**
- (1) Suppose $*$ is a binary operation on a set. Then $a * b \in S$ for all $a, b \in S$.
 - (2) If T is a non-empty subset of S and $a, b \in T$, then $a * b \in S$ but **not necessarily** in T .
 - (3) A non-empty subset T of S is **closed** under $*$ if for all $a, b \in T$, $a * b \in T$.
 - (4) Subtraction is a binary operation on $\mathbb{Z}$, the subset $\mathbb{N}$ of $\mathbb{Z}$ is not closed under subtraction.

Example 2.3. The following sets are closed under the corresponding operations defined below.

- (1) **The set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ of integers modulo $n \geq 2$.**
 - For all $a, b \in \mathbb{Z}_n$, we define addition as $a + b = a + b \pmod{n}$.
 - For all $a, b \in \mathbb{Z}_n$, we define multiplication as $a \cdot b = ab \pmod{n}$.
- (2) **The set $M_2(\mathbb{R})$ of all 2×2 matrices over $\mathbb{R}$.** Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in M_2(\mathbb{R})$. Then we define
 - Matrix addition:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}.$$
 - Matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.$$
- (3) **The set $\mathcal{F}(\mathbb{R})$ of functions from $\mathbb{R}$ to $\mathbb{R}$ under function addition, multiplication, and composition are defined below.**
 - Function addition: $(f + g)(x) = f(x) + g(x)$.
 - Function multiplication: $(f \cdot g)(x) = f(x) \cdot g(x)$.
 - Function composition: $(f \circ g)(x) = f(g(x))$.
- (4) **The power set $P(A)$ of a set A under set operations are defined below.**
 - Set union: $A \cup B$.
 - Set intersection: $A \cap B$.
 - Set difference: $A \setminus B$.
- (5) For a more abstract example of a binary operation, let $S = \{a, b, c\}$. A binary operation $*$ on S is illustrated in the table below.

$*$	a	b	c
a	b	c	a
b	a	c	a
c	c	a	b

The binary operation of each pair of elements as follows.

- $a * a = b$
- $a * b = c$
- $a * c = a$

- $b * a = a$
- $b * b = c$
- $b * c = a$
- $c * a = c$
- $c * b = a$
- $c * c = b$

Since every element in the table belongs to S , indeed $*$ is a binary operation on S .

Result 1. For $a, b \in \mathbb{R} \setminus \{-2\}$, define the operation $a * b$ as

$$a * b = ab + 2a + 2b + 2,$$

where the operations indicated in $ab + 2a + 2b + 2$ are usual addition and multiplication in $\mathbb{R}$. Then $*$ is a binary operation on $\mathbb{R} \setminus \{-2\}$.

PROOF. Let $a, b \in \mathbb{R} \setminus \{-2\}$. We need to show that $a * b \in \mathbb{R} \setminus \{-2\}$. Suppose, for contradiction, that there exist $x, y \in \mathbb{R} \setminus \{-2\}$ such that $x * y = -2$. By definition of $*$, we have

$$x * y = xy + 2x + 2y + 2 = -2.$$

Rearranging, this gives

$$(x + 2)(y + 2) = 0.$$

Hence, either $x = -2$ or $y = -2$, which contradicts the assumption that $x, y \in \mathbb{R} \setminus \{-2\}$. Therefore, there are no such x, y exist, and it follows that $a * b \in \mathbb{R} \setminus \{-2\}$. Thus, $*$ is a binary operation on $\mathbb{R} \setminus \{-2\}$. $\square$

Definition 2.2 (Algebraic Structure). A non-empty set S with a binary operation $*$ is denoted by $(S, *)$. We refer to $(S, *)$ as an **algebraic structure** and $(S, *)$ may satisfies the following properties.

- **G1: Associative:** $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$.
- **G2: Identity:** There exists $e \in S$, called an identity element, such that $a * e = e * a = a$ for all $a \in S$.
- **G3: Inverses:** For each $a \in S$, there exists $s \in S$, called an inverse for a , such that $a * s = s * a = e$.
- **G4: Commutative:** $a * b = b * a$ for all $a, b \in S$.

Example 2.4. The following are examples of algebraic structures and their properties:

- (1) $(\mathbb{Z}, +)$:
 - Satisfies G1, G2, G3, G4.
 - Identity: 0, Inverse: $-n$ for $n \in \mathbb{Z}$.
- (2) $(\mathbb{R}, \cdot)$:
 - Satisfies G1, G2, G4.
 - Identity: 1.
 - Does not satisfies G3: 0 has no inverse.
- (3) $(\mathbb{R}^*, \cdot)$:
 - Satisfies G1, G2, G3, G4 (identity element is 1 and inverse of r is $\frac{1}{r}$)
- (4) $(\mathbb{C}^*, \cdot)$:
 - Satisfies G1, G2, G3, G4 (identity element is 1 and inverse of $a + ib$ is $\frac{1}{a + ib} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$).
- (5) $(\mathbb{Z}_n, +)$, $n \geq 2$:
 - Satisfies G1, G2, G3, G4.
 - Identity: $[0]$, Inverse: $[-a]$ for $[a] \in \mathbb{Z}_n$.
- (6) $(\mathbb{Z}_n, \cdot)$, $n \geq 2$:
 - Satisfies G1, G2, G4.
 - Identity: $[1]$.
 - Does not satisfies G3: $[0]$ has no inverse.
- (7) $(M_2(\mathbb{R}), +)$:
 - Satisfies G1, G2, G3, G4.
 - Identity: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

- Inverse: $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
- (8) $(M_2(\mathbb{R}), \cdot)$:
- Satisfies G1, G2.
 - Identity: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
 - Does not satisfies G3: Determinant must be non-zero for invertibility.
 - Does not satisfies G4: Matrix multiplication is not commutative.
- (9) $(S, *)$, where $S = \{a, b, c\}$ and $*$ defined on S as in Example 2.3 (5).
- Does not satisfies associative G1 since $b * (b * c) \neq (b * b) * c$.
 - Does not satisfies G2 since there is no $e \in S$ satisfies $e * x = x * e = x$.
 - Does not satisfies G4 since $a * c \neq c * a$.

Example 2.5. A binary operation $*$ is defined on the set $S = \{a, b, c\}$ by $x * y = x$ for all $x, y \in S$. Determine which of the properties G1-G4 are satisfied by $(S, *)$.

• **G1: Associativity:**

Let $x, y, z \in S$. We have:

$$x * (y * z) = x * y = x \quad \text{and} \quad (x * y) * z = x * z = x.$$

Thus, $(S, *)$ is associative.

• **G2: Identity:**

No identity exists in S since for any $e \in S$, we have $e * a = e * b = e$ and $e * a = a$, $e * b = b$, which is impossible.

• **G3: Inverses:**

Inverses of elements of S does not exists as $(S, *)$ has no identity.

• **G4: Commutativity:**

$(S, *)$ is not commutative because $a * b = a$, but $b * a = b$.

Example 2.6. Let $\mathbb{N}_0$ be the set of non-negative integers, and consider $(\mathbb{N}_0, *)$, where $*$ is the binary operation defined by $a * b = |a - b|$ for all $a, b \in \mathbb{N}_0$. Determine which of the properties G1-G4 are satisfied by $(\mathbb{N}_0, *)$.

• **G1: Associativity:**

Since $1 * (2 * 3) = 1 * |2 - 3| = 1 * 1 = |1 - 1| = 0$, while $(1 * 2) * 3 = |1 - 2| * 3 = 1 * 3 = |1 - 3| = 2$, it follows that

$$(1 * 2) * 3 \neq 1 * (2 * 3).$$

Thus, $(\mathbb{N}_0, *)$ is not associative.

• **G2: Identity:**

Let $a \in \mathbb{N}_0$. Since $a * 0 = 0 * a = |a| = a$, 0 is an identity for $(\mathbb{N}_0, *)$.

• **G3: Inverses:**

For each $a \in \mathbb{N}_0$, $a * a = |a - a| = 0$. Hence, every element $a \in \mathbb{N}_0$ is its own inverse.

• **G4: Commutativity:**

Since $|a - b| = |b - a|$, we have $a * b = b * a$. Thus, $(\mathbb{N}_0, *)$ is commutative.

Hence, $(\mathbb{N}_0, *)$ satisfies properties G2, G3 and G4.

Example 2.7. Let $*$ be the binary operation defined on $\mathbb{Z}$ by $a * b = a + b - 1$ for $a, b \in \mathbb{Z}$, where the operations indicated in $a + b - 1$ are ordinary addition and subtraction. Determine which of the four properties G1-G4 are satisfied by $(\mathbb{Z}, *)$.

• **G1: Associativity:**

For integers a, b, c , we have

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2,$$

and

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2.$$

Since $a * (b * c) = (a * b) * c$, we conclude that $(\mathbb{Z}, *)$ is associative.

- **G2: Identity:**

For any $a \in \mathbb{Z}$, $a * 1 = a + 1 - 1 = a$. Thus, 1 is an identity element for $(\mathbb{Z}, *)$.

- **G3: Inverses:**

For $a \in \mathbb{Z}$, let $b = -a + 2 \in \mathbb{Z}$. Then

$$a * b = a * (-a + 2) = a + (-a + 2) - 1 = 1.$$

Hence, b is an inverse of a , and every integer has an inverse.

- **G4: Commutativity:**

Since $a + b - 1 = b + a - 1$, it follows that $a * b = b * a$. Thus, $(\mathbb{Z}, *)$ is commutative.

Therefore, $(\mathbb{Z}, *)$ satisfies all four properties $G1$, $G2$, $G3$, and $G4$.

Problem 2.1. Suppose that $*$ is an associative binary operation on a set S . Let

$$T = \{a \in S : a * x = x * a \text{ for all } x \in S\}.$$

Prove that T is closed under $*$.

Solution 2.2. Let $a, b \in T$. We now prove that $a * b \in T$, that is,

$$(a * b) * x = x * (a * b) \quad \text{for all } x \in S.$$

Since $a, b \in T$, we have

$$a * x = x * a \quad \text{and} \quad b * x = x * b \quad \text{for all } x \in S.$$

We now consider

$$\begin{aligned} (a * b) * x &= a * (b * x) \quad (\text{by associativity of } *) \\ &= a * (x * b) \\ &= (a * x) * b \quad (\text{by associativity of } *) \\ &= (x * a) * b \\ &= x * (a * b) \quad (\text{by associativity of } *). \end{aligned}$$

Thus, $(a * b) * x = x * (a * b)$ for all $x \in S$ and so $a * b \in T$.

Problem 2.2. Suppose that $*$ is an associative and commutative binary operation on a set S . Let

$$T = \{a \in S : a * a = a\}.$$

Prove that T is closed under $*$.

Solution 2.3. Let $a, b \in T$. We now prove that

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

By the definition of T , we have

$$a * a = a \quad \text{and} \quad b * b = b.$$

We now use associativity and commutativity of $*$ and obtain

$$\begin{aligned} (a * b) * (a * b) &= a * (b * (a * b)) \\ &= a * ((b * a) * b) \\ &= a * ((a * b) * b) \\ &= (a * a) * (b * b) \\ &= a * b. \end{aligned}$$

Thus, $a * b \in T$ and so T is closed under $*$.

Problem 2.3. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in M_2(\mathbb{R}),$$

and define a binary operation $*$ on $M_2(\mathbb{R})$ by

$$A * B = \begin{bmatrix} a + e - 1 & b + f \\ c + g & d + h + 1 \end{bmatrix}.$$

Which of the properties G1-G4 are satisfied?

Solution 2.4. It is easy to see that the operation is closure, associativity and commutativity. An identity element of $M_2(\mathbb{R})$ is $E = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, since $A * E = E * A = A$ for all $A \in M_2(\mathbb{R})$. An inverse of

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{R}) \text{ is}$$

$$A^{-1} = \begin{bmatrix} 2 - a & -b \\ -c & -d - 2 \end{bmatrix},$$

since $A * A^{-1} = A^{-1} * A = E$. Thus, the operation $*$ will satisfy all the properties G1-G4.

Problem 2.4. For $n \geq 2$ and $[a], [b] \in \mathbb{Z}_n$, the binary operation $*$ is defined on $\mathbb{Z}_n$ by

$$[a] * [b] = [a + b + 1].$$

Which of the properties G1-G4 are satisfied?

Solution 2.5. The operation $*$ satisfies the closure property since $[a + b + 1] \in \mathbb{Z}_n$. Note that

$$([a] * [b]) * [c] = [a + b + 1] * [c] = [a + b + c + 2]$$

and

$$[a] * ([b] * [c]) = [a] * [b + c + 1] = [a + b + c + 2].$$

Thus, $*$ is associative. Next, we find an identity element. Suppose $[e]$ is an identity element. Then $[a + e + 1] = [a]$. This implies that $[e + 1] = [0]$ and so $e \equiv -1 \pmod{n}$. So $[e] = [n - 1]$. To verify this, consider

$$[a] * [n - 1] = [a + n - 1 + 1] = [a + n] = [a]$$

and

$$[n - 1] * [a] = [n - 1 + a + 1] = [a + n] = [a].$$

Thus, $[n - 1]$ is an identity. Similarly, we can prove that an inverse of $[a]$ is $[n - 2 - a]$. Finally, we check the commutative property. Since

$$[a] * [b] = [a + b + 1] = [b + a + 1] = [b] * [a],$$

we conclude that $*$ satisfies the commutative property. Thus, the operation $*$ will satisfy all the properties G1-G4.

Problem 2.5. Let

$$T = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}.$$

Is T closed under

- (a) matrix addition?
- (b) matrix multiplication?

Solution 2.6. (a) **Matrix Addition:**

Let

$$A = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \in T.$$

Then

$$A + B = \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix} \in T.$$

Thus, T is closed under matrix addition.

(b) **Matrix Multiplication:**

Let

$$A = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}, \quad B = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \in T.$$

Then

$$AB = \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + b_1a_2) \\ b_1a_2 + b_1a_2 & a_1a_2 - b_1b_2 \end{bmatrix} \in T.$$

Thus, T is closed under matrix multiplication.

3. Groups

"As long as algebra and geometry have been separated, their progress have been slow and their uses limited; but when these two sciences have been united, they have lent each mutual forces, and have marched together towards perfection."

— Joseph-Louis Lagrange

Definition 3.1 (Semi-group). A **semi-group** is a non-empty set G with respect to a binary operation $*$ that satisfies the property **G1**.

Definition 3.2 (Monoid). A **monoid** is a non-empty set G with respect to a binary operation $*$ that satisfies the properties **G1** and **G2**.

Definition 3.3 (Group). A **group** is a non-empty set G with respect to a binary operation $*$ that satisfies the properties **G1**, **G2** and **G3**.

Definition 3.4 (Abelian group). A group $(G, *)$ is called an **abelian** (or **commutative**) if it satisfies the property **G4**.

Example 3.1. From Example 2.4 we can prove the following.

- (1) The non-empty sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are abelian groups with respect to the binary operation addition $+$.
- (2) The non-empty sets $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ are abelian groups with respect to the binary operation multiplication $\times$.
- (3) $(\mathbb{Z}_n, +_n)$ is an abelian group.
- (4) $(M_2(G), +)$ is an abelian group, where $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}_n$.

Example 3.2. The subset $\{1, -1, i, -i\}$ of $\mathbb{C}$ is an abelian group with respect to complex multiplication (-1 has self inverse, i has inverse $-i$ and $-i$ has inverse i).

Remark 3.1. $\mathbb{Z}^*$ is not a group under multiplication because every non-zero integer except ± 1 does not have an inverse in $\mathbb{Z}^*$. But it is a monoid.

Example 3.3. The set $\mathbb{R}^n = \{(a_1, a_2, \dots, a_n) \mid a_1, a_2, \dots, a_n \in \mathbb{R}\}$ is a group under component-wise addition, that is,

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n).$$

Here, $\mathbb{R}^n$ has identify element $(0, 0, \dots, 0)$ and inverse of $(a_1, a_2, \dots, a_n)$ is $(-a_1, -a_2, \dots, -a_n)$.

Example 3.4. For a fixed point $(a, b) \in \mathbb{R}^2$, we define a function $T_{a,b} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ by

$$T_{a,b}(x, y) = (x + a, y + b).$$

Let

$$G = \{T_{a,b} \mid a, b \in \mathbb{R}\}.$$

Then G forms a group under function composition. Note that

$$T_{a,b} \circ T_{c,d} = T_{a+c, b+d}.$$

This implies that G is closed under composition, $T_{0,0}$ is the identity element, and the inverse of $T_{a,b}$ is $T_{-a,-b}$. Thus, G is an abelian group since function composition is always associative. The elements of G are called *translations*.

Example 3.5 (Klein 4-Group). The **Klein 4-group**

$$V_4 = \langle a, b \mid a^2 = b^2 = e, ab = ba \rangle = \{e, a, b, ab\}$$

is an abelian group of order 4.

Example 3.6 (Quaternion Group). The **quaternion group**, denoted by Q_8 , is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with the operation is quaternion multiplication, and the elements satisfy the following

$$i^2 = j^2 = k^2 = ijk = -1.$$

From these identities, we have the following relations

$$ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j.$$

Problem 3.1. Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. For $x, y \in G$, define

$$x * y := \text{frac}(x + y) = x + y - \lfloor x + y \rfloor,$$

where $\lfloor a \rfloor$ denotes the greatest integer less than or equal to a . Prove that $*$ is a well-defined binary operation on G , and that G is an abelian group under $*$ (called the real numbers mod 1).

Solution 3.1. First, we prove the operation $*$ is well-defined. Let $x, y \in G$. Then $0 \leq x < 1$ and $0 \leq y < 1$. This implies that $0 \leq x + y < 2$ and so

$$\lfloor x + y \rfloor = \begin{cases} 0 & \text{if } x + y < 1, \\ 1 & \text{if } x + y \geq 1. \end{cases}$$

Therefore,

$$x * y = x + y - \lfloor x + y \rfloor \in [0, 1).$$

Thus, $*$ satisfies the closure property.

Let $x, y, z \in G$. Define $\text{frac}(a) = a - \lfloor a \rfloor$. Then we obtain

$$(x * y) * z = \text{frac}(\text{frac}(x + y) + z) = \text{frac}(x + y + z)$$

and

$$x * (y * z) = \text{frac}(x + \text{frac}(y + z)) = \text{frac}(x + y + z).$$

Thus,

$$(x * y) * z = x * (y * z)$$

and conclude that $*$ is associative.

Next, we prove that $0 \in G$ is the identity. Let $x \in G$. Then we have

$$x * 0 = \text{frac}(x + 0) = \text{frac}(x) = x$$

and

$$0 * x = \text{frac}(0 + x) = \text{frac}(x) = x.$$

Thus, 0 is the identity element.

Finally, we prove the existence of inverse of elements of G . Let $x \in G$, define $y = 1 - x$ if $x > 0$, and $y = 0$ if $x = 0$. Then $0 \leq y < 1$. This shows that $y \in G$, and hence

$$x * y = \text{frac}(x + y) = 0.$$

Thus, $y = 1 - x$ is the inverse of x in G .

Let $x, y \in G$. Then we have

$$x * y = \text{frac}(x + y) = \text{frac}(y + x) = y * x.$$

Thus, $*$ is commutative and conclude that $(G, *)$ is an abelian group.

Problem 3.2. Let

$$G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}.$$

- (a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).
- (b) Prove that G is not a group under addition.

Solution 3.2. (a) It is clear that, G is closed under multiplication and satisfies the associative property. Note that the element $1 \in G$ is the identity element. The inverse of $z \in G$ is $\frac{1}{z}$. Thus, G is a group under multiplication.

- (b) Note that, $1 \in G$ and $-1 \in G$, but $1 - 1 = 0 \notin G$. Thus, G is not a group under addition.

Problem 3.3. Let

$$G = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}.$$

Then

- (a) G is a group under addition.
- (b) the non-zero elements of G form a group under multiplication.

Solution 3.3. (a) First, we prove that G is a group under addition.

- **Closure:** Let $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in G$, where $a, b, c, d \in \mathbb{Q}$. Then

$$x + y = (a + c) + (b + d)\sqrt{2}.$$

Thus, $x + y \in G$.

- **Associativity:** It is clear that associativity holds in G since $G \subset \mathbb{R}$.
- **Identity:** The additive identity of G is 0 since $a + b\sqrt{2} = 0 + a + b\sqrt{2} = a + b\sqrt{2}$ for all $a + b\sqrt{2} \in G$.
- **Inverses:** The additive inverse of $x = a + b\sqrt{2}$ is $-x = -a - b\sqrt{2}$.

Thus, G is a group under addition.

- (b) Next, we prove that non-zero elements of G form a group under multiplication. Denote $G^\times$ the set of all non-zero elements of G .

$$G^\times = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}, a + b\sqrt{2} \neq 0\}.$$

- **Closure:** Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ be in $G^\times$. Then we have

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2},$$

where $ac + 2bd \in \mathbb{Q}$ and $ad + bc \in \mathbb{Q}$. Thus, $xy \in G^\times$ as x, y are non-zero.

- **Associativity:** Associativity follows from associativity of real numbers under multiplication.
- **Identity:** The multiplicative identity of $G^\times$ is 1.
- **Inverses:** Let $x = a + b\sqrt{2} \in G^\times$, with $a, b \in \mathbb{Q}$ and $x \neq 0$. Then the inverse of x is

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}$$

since $a^2 - 2b^2 \neq 0$.

Thus, the set $G^\times$ is a group under multiplication.

Problem 3.4. Let

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \mid a, b \in \mathbb{R}, a \neq 0 \right\}.$$

Prove or disprove: G is a group under matrix multiplication.

Solution 3.4. We have to check whether G is a group under matrix multiplication.

1. **Closure:** Let

$$A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \quad A' = \begin{bmatrix} a' & b' \\ 0 & 0 \end{bmatrix} \in G.$$

Then

$$AA' = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a' & b' \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} aa' & ab' \\ 0 & 0 \end{bmatrix} \in G.$$

Thus, G is closed under multiplication.

2. Associativity: It is clear that the operation is associative.

3. Identity: Identity element does not exist in G .

4. Inverses: Inverse property is not true as identity element does not exist in G .

4. Properties of Groups

“Algebra is but written geometry and geometry is but figured algebra.”

— Sophie Germain

We call G a group, which means it is a group with respect to $*$. Also we write ab for $a * b$.

Proposition 4.1 (Cancellation Laws). Let G be a group and $a, b, c \in G$.

(1) If $a * b = a * c$, then $b = c$ (The Left Cancellation Law).

(2) If $b * a = c * a$, then $b = c$ (The Right Cancellation Law).

PROOF. Assume that $a * b = a * c$. Let s be an inverse of a . Then

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

By the associativity law, we have

$$s * (a * b) = (s * a) * b = e * b = b$$

and

$$s * (a * c) = (s * a) * c = e * c = c.$$

Thus, $b = c$.

Similarly, we can prove the right cancellation law. □

Proposition 4.2 (Uniqueness of Identity and Inverse). Let G be a group. Then

(a) G has a unique identity element.

(b) Each element in G has a unique inverse.

PROOF. Assume that e and e' are two identity elements in G . Since e is an identity, $ee' = e'$, and since e' is an identity, $ee' = e$. Thus, $e = ee' = e'$. This proves part (a).

Next, we prove the uniqueness of inverses. Let $g \in G$. Suppose that s and t are both inverses of g . Then $gs = sg = e$ and $gt = tg = e$. Since $gs = gt$ and by the Left Cancellation Law, we have $s = t$. This proves part (b). □

Proposition 4.3. Let G be a group and $a \in G$. Then $(a^{-1})^{-1} = a$.

PROOF. Note that $aa^{-1} = a^{-1}a = e$, where a^{-1} is the inverse of a . This implies that a is the inverse of a^{-1} (replacing a by a^{-1}). That is, $(a^{-1})^{-1} = a$. □

Proposition 4.4. Let G be a group and $a, b \in G$. Then

$$(ab)^{-1} = b^{-1}a^{-1}.$$

PROOF. To prove $b^{-1}a^{-1}$ is the inverse of ab , it enough to verify that

$$(ab)(b^{-1}a^{-1}) = e \quad \text{and} \quad (b^{-1}a^{-1})(ab) = e.$$

Consider

$$\begin{aligned}
 (ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \\
 &= (a(bb^{-1}))a^{-1} \\
 &= (ae)a^{-1} \\
 &= aa^{-1} \\
 &= e.
 \end{aligned}$$

Similarly, we can prove $(b^{-1}a^{-1})(ab) = e$. □

Definition 4.1 (Order of a Group). The number of elements of a group G (finite or infinite) is called the *order* of G . We use $|G|$ to denote the order of the group G .

Definition 4.2 (Order of an Element). The **order** of an element G in a group G is the smallest positive integer K such that

$$g^K = e.$$

(In additive notation, this would be $kg = 0$.) If no such integer exists, we say that G has **infinite order**. The order of an element $g \in G$ is denoted by $|g|$.

Problem 4.1. Suppose that G is a finite abelian group of order n , say $G = \{g_1, g_2, \dots, g_n\}$. Let

$$g = g_1g_2 \cdots g_n \cdot g_1g_2 \cdots g_n.$$

What is g ?

Solution 4.1. Let $a = g_1g_2 \cdots g_n$. Then $g = a^2$. As G is abelian, the product a does not depend on the order of multiplication. We now pair each element $g_i \in G$ with its inverse g_i^{-1} . If $g_i \neq g_i^{-1}$, then the product $g_i g_i^{-1} = e$. If $g_i = g_i^{-1}$, then $g_i^2 = e$. Next, we use the commutative property and obtain that

$$a = \prod_{g_i \in G, g_i = g_i^{-1}} g_i.$$

This implies that

$$g = a^2 = \prod_{g_i \in G, g_i = g_i^{-1}} g_i^2 = e.$$

Problem 4.2. Let $x \in G$ and $|x| = n < \infty$. If $n = st$ for some $s, t \in \mathbb{N}$, then prove that $|x^s| = t$.

Solution 4.2. Let $x \in G$ with $|x| = n$. Let $n = st$. Then

$$(x^s)^t = x^{st} = x^n = e.$$

This implies that $(x^s)^t = e$. That is, $|x^s|$ divides t . Suppose that $|x^s| = d < t$. Then

$$(x^s)^d = x^{sd} = e.$$

This implies that $x^{sd} = e$. Thus, $n \mid sd$. Since $n = st$, we have $t \mid d$. This is a contradiction to $d < t$ and $d, t \in \mathbb{Z}^+$. Thus, we conclude that $|x^s| = t$.

Problem 4.3. Let G be a group with $x^2 = 1$ for all $x \in G$. Then G is abelian.

Solution 4.3. Note that $x^2 = 1$ implies that x is its own inverse. Let $a, b \in G$. We now prove that $ab = ba$. Consider $aba^{-1}b^{-1} = abab$ as $a^{-1} = a$ and $b^{-1} = b$. Since $(ab)^2 = 1$, we have $abab = 1$. Therefore, $ab = b^{-1}a^{-1} = ba$. Thus, $ab = ba$ for all $a, b \in G$, and therefore G is abelian.

Problem 4.4. Let G be a finite group of even order. Then G contains an element of order 2.

Solution 4.4. Let G be a finite group with $|G|$ even. Let $e \in G$ be the identity element. Then $|G \setminus \{e\}|$ is odd. We now consider every element $g \in G \setminus \{e\}$ and its inverse g^{-1} . Note that, if $g \neq g^{-1}$, then G and g^{-1} are distinct and can be paired. Otherwise, we have $g = g^{-1}$, which implies that $g^2 = e$. Therefore, $|g| = 2$.

Suppose that there is no element $x \neq e$ in G of order 2. Then $g \in G \setminus \{e\}$ satisfies $g \neq g^{-1}$ for all $x \in G \setminus \{e\}$. Also every element in $G \setminus \{e\}$ can be paired off with its distinct inverses. Hence, $|G \setminus \{e\}|$ is even. This is a contradiction to $|G \setminus \{e\}|$ is odd. Therefore, there exists $g \in G \setminus \{e\}$ such that $g = g^{-1}$. This implies that $g^2 = e$, where $g \neq e$. Thus, the order of G is 2.

Problem 4.5. Let x be an element of finite order n in a group G . Use the Division Algorithm to show that any integral power of x equals one of the elements in the set

$$\{1, x, x^2, \dots, x^{n-1}\}.$$

Solution 4.5. Let $x \in G$ be an element of finite order n , and $m \in \mathbb{Z}$. By the division algorithm, there exist unique integers q and R such that

$$m = nq + r, \quad \text{where } 0 \leq r < n.$$

Consider

$$x^m = x^{nq+r} = x^{nq} \cdot x^r = (x^n)^q \cdot x^r = 1^q \cdot x^r = x^r.$$

Since $0 \leq r < n$, we conclude that $x^m \in \{1, x, x^2, \dots, x^{n-1}\}$.

Problem 4.6. Let a and b be two elements in a group G . Prove that if a and b commute, then a^{-1} and b^{-1} commute.

Solution 4.6. Assume that $ab = ba$. Then

$$\begin{aligned} (ab)^{-1} &= (ba)^{-1} \\ b^{-1}a^{-1} &= a^{-1}b^{-1}. \end{aligned}$$

Thus, a^{-1} and b^{-1} commute.

Problem 4.7. Let $(G, *)$ be a group and let $a, b, c \in G$. Prove that each of the following equations has a unique solution for x in G and determine the solution.

- (a) $a * x * b = c$
- (b) $a * b * x = c$

Solution 4.7. (a) Consider the equation $a * x * b = c$. By multiplying a^{-1} on both sides (on the left), we obtain

$$a^{-1} * (a * x * b) = a^{-1} * c.$$

Using associativity and the identity $a^{-1} * a = e$, we obtain $(e * x) * b = a^{-1} * c$ and so $x * b = a^{-1} * c$.

We now multiply both sides on the right by b^{-1} and get

$$(x * b) * b^{-1} = (a^{-1} * c) * b^{-1}.$$

This implies that $x * (b * b^{-1}) = a^{-1} * c * b^{-1}$ and so

$$x = a^{-1} * c * b^{-1}.$$

Uniqueness: Suppose x_1 and x_2 are two solutions such that

$$a * x_1 * b = c \quad \text{and} \quad a * x_2 * b = c.$$

Then $a * x_1 * b = a * x_2 * b$. Multiply both sides on the left by a^{-1} and on the right by b^{-1} , we get

$$a^{-1} * (a * x_1 * b) * b^{-1} = a^{-1} * (a * x_2 * b) * b^{-1}$$

Using associativity and the inverse properties, we obtain

$$x_1 = x_2.$$

Thus, the solution is unique.

(b) Consider the equation

$$a * b * x = c.$$

By multiplying $(a * b)^{-1}$ on both sides (on the left), we get

$$(a * b)^{-1} * (a * b * x) = (a * b)^{-1} * c.$$

Using associativity and the identity $(a * b)^{-1} * (a * b) = e$, we obtain

$$e * x = (a * b)^{-1} * c \quad \text{and so} \quad x = (a * b)^{-1} * c.$$

Uniqueness: Suppose x_1 and x_2 are two solutions such that

$$a * b * x_1 = c \quad \text{and} \quad a * b * x_2 = c.$$

Then $a * b * x_1 = a * b * x_2$. Multiply both sides on the left by $(a * b)^{-1}$, we get

$$(a * b)^{-1} * (a * b * x_1) = (a * b)^{-1} * (a * b * x_2).$$

Using associativity and the inverse properties, we obtain

$$x_1 = x_2.$$

Thus, the solution is unique.

Problem 4.8. Let $a, b \in G$ with $ab = ba$. Then prove that $(ab)^n = a^n b^n$ for every $n \in \mathbb{Z}$.

Solution 4.8. *Case 1:* For $n = 0$, we have $(ab)^0 = e = a^0 b^0$.

Case 2: Assume that $n > 0$. In this case, we prove this by induction on n . For $n = 1$, we have $(ab)^1 = ab = a^1 b^1$.

Inductive step: Assume $(ab)^k = a^k b^k$ for some $k \geq 1$. Then

$$(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab.$$

Since a and b are commuting elements of G , we have

$$a^k b^k ab = a^k ab^k b = a^{k+1} b^{k+1}.$$

Thus, $(ab)^{k+1} = a^{k+1} b^{k+1}$ for all $n \in \mathbb{N}$.

Case 3: Assume that $n < 0$. Let $n = -m$, where $m > 0$. Then

$$(ab)^n = (ab)^{-m} = ((ab)^m)^{-1}.$$

From case 2, we have $(ab)^m = a^m b^m$ and so $(ab)^{-m} = (a^m b^m)^{-1}$. Since $(xy)^{-1} = y^{-1} x^{-1}$, we get

$$(a^m b^m)^{-1} = (b^m)^{-1} (a^m)^{-1} = b^{-m} a^{-m}.$$

As a and b commute, their inverses also commute. Therefore,

$$b^{-m} a^{-m} = a^{-m} b^{-m} = a^n b^n.$$

Therefore, $(ab)^n = a^n b^n$ for all $n < 0$. Thus, for all $n \in \mathbb{Z}$, we have $(ab)^n = a^n b^n$.

5. Dihedral Groups

“Algebra is but written geometry and geometry is but figured algebra.”

— Sophie Germain

Historical notes: Dihedral groups show how ideas from geometry developed into modern abstract algebra. Around 300 BC, the Greek mathematician Euclid studied regular polygons and their symmetries in his *Elements*, giving early ideas of rotations and reflections. In the eighteenth century, especially between 1730 and 1780, mathematicians such as Euler and Lagrange studied symmetries through permutations while working on algebraic equations. A major change came in the nineteenth century with Évariste Galois, who between 1830 and 1832 introduced the concept of a group to describe symmetry in algebraic terms. Soon after, Augustin–Louis Cauchy made significant contributions to permutation groups between 1815 and 1845. In 1854, Arthur Cayley gave an abstract definition of groups, independent of geometry. Dihedral groups then became standard examples of finite groups that are not commutative. They helped clarify ideas such as generators and relations. By the late nineteenth century, around 1880–1900, they were widely used in group theory texts. Today, dihedral groups connect geometric symmetry with abstract algebra and play an important role in learning group theory.

One of the most important families of examples of groups is given by symmetries of geometric objects. In particular, the symmetries of a regular n -gon provide one of the simplest and most natural examples of a group. With composition as the operation, these symmetries form a group consisting of rotations and reflections, known as the dihedral group.

Constructions: Let $n \geq 3$ be an integer. Define D_{2n} as the symmetry set of a regular n -gon (here symmetry refers to rotation or reflection) that maps the n -gon onto itself. To describe the symmetries, we label the n vertices of the n -gon with the set $\{1, 2, 3, \dots, n\}$. Note that any symmetry $s \in D_{2n}$ induces a permutation σ on these vertices as follows: if a vertex i is moved to the position originally occupied by vertex j , then $\sigma(i) = j$. For example, a rotation by $\frac{2\pi}{n}$ radians clockwise maps $i \mapsto i + 1$ for $1 \leq i \leq n - 1$, and $n \mapsto 1$.

The set D_{2n} is a group under composition of functions. For any symmetries $s, t \in D_{2n}$, the composition st means applying t first, then s . That is, if s and t correspond to permutations σ and τ , then st corresponds to $\sigma \circ \tau$. Note that this operation is associative since function composition is associative. Also D_{2n} with respect to the operation composition satisfies the following properties.

- **G2:** The identity element of D_{2n} is the identity symmetry, which fixes all vertices. We denote the identity by 1.
- **G3:** The inverse of a symmetry s is the symmetry that exactly reverses the effect of s . That is, if s induces permutation σ , then its inverse induces σ^{-1} .

We now prove that the order of D_{2n} is equal to $2n$. For this, given any vertex i , there is a symmetry which maps 1 to position i . Note that vertex 2 is adjacent to vertex 1, it must map to either $i + 1$ or $i - 1$ (modulo n). Therefore, there are $n \cdot 2 = 2n$ distinct positions for the ordered pair $(1, 2)$, each corresponding to a unique symmetry. Since rigid motions are completely determined by the images of two adjacent vertices, we have exactly $2n$ symmetries.

More precisely, the $2n$ symmetries are as follows:

- **n rotations** by angles $\frac{2\pi i}{n}$ for $0 \leq i \leq n - 1$,
- **n reflections** across symmetry axes:
 - (a) Suppose n is odd. Then for each axis passes through a vertex and the midpoint of the opposite side.
 - (b) Suppose n is even. Then there are $\frac{n}{2}$ axes through pairs of opposite vertices and $\frac{n}{2}$ axes bisecting pairs of opposite sides.

Definition 5.1 (Dihedral Group). The set D_{2n} is called the **dihedral group** of order $2n$. Some authors denote this group as D_n .

Fix a regular n -gon centred at $(0, 0)$ in the xy plane. We label the n vertices from 1 to n (consecutively) in a clockwise direction. Let r denote the rotation about the origin in the clockwise direction through an angle of $\frac{2\pi}{n}$ radians. Let s be represent the reflection across the line of symmetry that passes through vertex 1 and the $(0, 0)$. Then

- (1) the elements $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$. Thus, $|r| = n$.
- (2) $|s| = 2$.
- (3) $s \neq r^i$ for any i .
- (4) $sr^i \neq sr^j$ for every $0 \leq i, j \leq n - 1$ with $i \neq j$. Therefore,

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

- (5) $rs = sr^{-1}$.
- (6) $r^i s = sr^{-i}$ for all $0 \leq i \leq n$.

From the above relations, we can write

$$D_{2n} = \{r, s \mid r^n = s^2 = e, rs = sr^{-1}\}.$$

Problem 5.1. If $n = 4$, then describe in pictures or words the elements of D_{2n} (symmetries of an equilateral triangle).

Solution 5.1. The group D_{2n} is the group of symmetries of a regular n -gon. For $n = 4$, D_8 is the symmetry group of a square. The elements of D_8 are 4 rotations and 4 reflections as below.

(1) **4 rotations:**

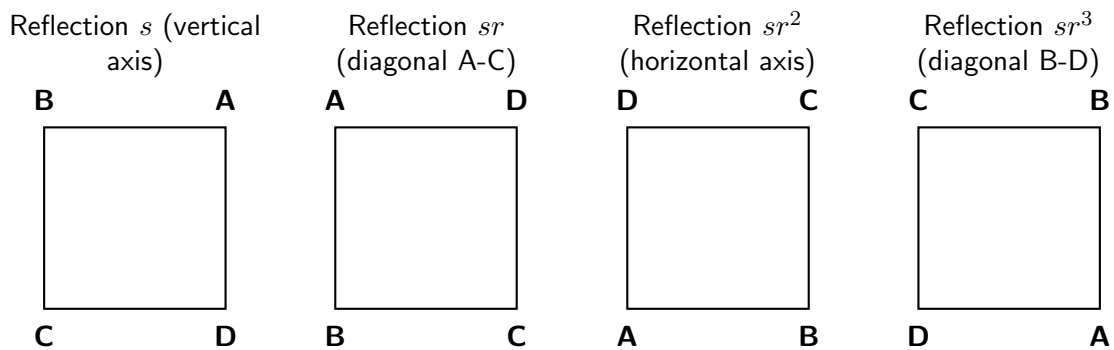
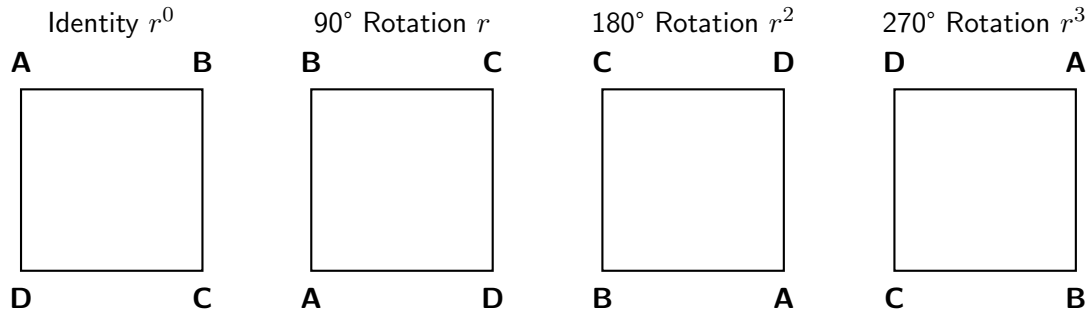
- $r^0 = id$: identity element
- R : rotation by 90°
- r^2 : rotation by 180°
- r^3 : rotation by 270°

(2) **4 reflections:**

- S : reflection over the vertical axis
- sr : reflection over the diagonal from top-left to bottom-right
- sr^2 : reflection over the horizontal axis
- sr^3 : reflection over the diagonal from top-right to bottom-left

Note that these elements satisfy the relations $r^4 = e$, $s^2 = e$, $sr = r^{-1}s$.

Geometric interpretations:

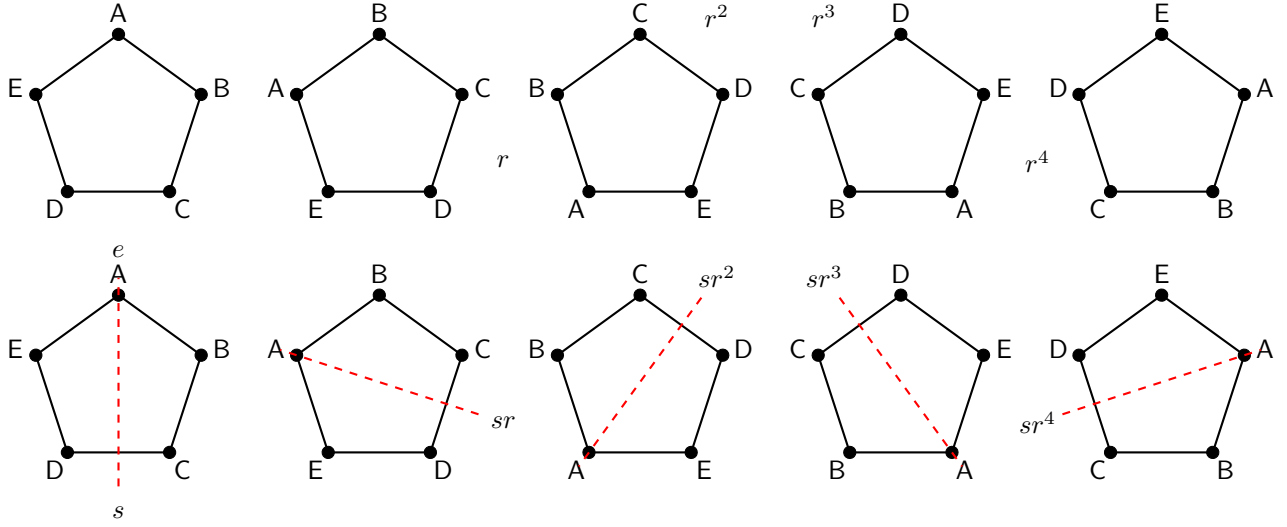


Problem 5.2. If $n = 5$, then describe in pictures or words the elements of D_{2n} (symmetries of a regular pentagon).

Solution 5.2. The group D_{10} of order 10 describes the symmetries of a regular pentagon as below.

- (1) **Rotations:** The rotations are $e = \text{identity}$, $r = \text{rotation by } 72^\circ$, $r^2 = \text{rotation by } 144^\circ$, $r^3 = \text{rotation by } 216^\circ$, $r^4 = \text{rotation by } 288^\circ$ and $r^5 = e$.
- (2) **Reflections:** The Reflections are s, sr, sr^2, sr^3, sr^4 , where $s^2 = e$ and $srs = r^{-1}$.

Geometric interpretations:



Problem 5.3. If r_1, r_2 , and r_3 represent rotations from D_{2n} and s_1, s_2 , and s_3 represent reflections from D_{2n} , determine whether $r_1 r_2 s_1 r_3 s_2 s_3 r_3$ is a rotation or a reflection.

Solution 5.3. We use the following properties of the dihedral group D_{2n} to find $r_1 r_2 s_1 r_3 s_2 s_3 r_3$.

- The product of two rotations is again a rotation.
- The product of two reflections is a rotation.
- The product of a rotation and a reflection (in either order) is a reflection.

We now consider $r_1 r_2 s_1 r_3 s_2 s_3 r_3$. Note that

$$\begin{aligned}
 r_1 r_2 &= \text{rotation} \\
 (\text{rotation}) \cdot s_1 &= \text{reflection} \\
 (\text{reflection}) \cdot r_3 &= \text{reflection} \\
 (\text{reflection}) \cdot s_2 &= \text{rotation} \\
 (\text{rotation}) \cdot s_3 &= \text{reflection} \\
 (\text{reflection}) \cdot r_3 &= \text{reflection}.
 \end{aligned}$$

Hence, the element $r_1 r_2 s_1 r_3 s_2 s_3 r_3$ is a reflection.

6. Symmetric Groups

"Symmetry, as wide or as narrow as you may define its meaning, is one idea by which man through the ages has tried to comprehend and create order, beauty, and perfection."

— Hermann Weyl [7]

In this section, we study a particular class of groups known as **permutation groups**, which consist of functions from a non-empty set A to itself, and the operation is the composition of functions.

Historical note: During the early and mid-19th century, mathematicians primarily studied permutation groups, because these were the only examples known at the time. The concept of abstract group was first introduced by Cayley around 1850, but it took almost 25 years for the abstract group theory to become widely accepted in mathematics.

Let A be any non-empty set and S_A be the collection of all bijections (permutations) from A to A . The set S_A satisfies the following properties with respect to the operation function composition.

- Function composition is a binary operation on S_A because the composition of two bijections is also a bijection.
- Function composition is associative. That is, $(f \circ g) \circ h = f \circ (g \circ h)$ for all $f, g, h \in S_A$.

- The identity element in S_A is the identity permutation id , where $id(a) = a$ for all $a \in A$.
- Every permutation $\sigma \in S_A$ has the inverse σ^{-1} as $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$.

Thus, $(S_n, \circ)$ satisfies all group axioms and forms a group under function composition. The group S_A is called the **symmetric group (or permutation group)** on the set A .

We now consider the special case when $A = \{1, 2, 3, \dots, n\}$. The symmetric group on A is denoted by S_n and we call S_n as the **symmetric group of degree n** .

6.1. Finding the order of S_A : Consider the permutations of the set $A = \{1, 2, 3, \dots, n\}$. It is enough to count the number of injective functions from A to itself, as A is a finite set. The number of injective functions can be counted as follows.

- The element 1 can be map to any of the n elements.
- 2 can be map to the remaining $n - 1$ elements.
- 3 can be map to the remaining $n - 2$ elements, and so on.

This implies that the total number of permutations is

$$n \cdot (n - 1) \cdot (n - 2) \dots 2 \cdot 1 = n!$$

Thus, $|S_n| = n!$.

6.2. Cycle Decomposition: For every element $\sigma \in S_n$, we write σ in the cycle notation. A *cycle* is a string of integers that represents a permutation which cyclically permutes these integers while leaving all other integers fixed. For example, the cycle $(1 \ 3 \ 4 \ 5)$ is the permutation that maps $1 \rightarrow 3$, $3 \rightarrow 4$, $4 \rightarrow 5$, and $5 \rightarrow 1$. In general, the cycle $(a_1 \ a_2 \ \dots \ a_k)$ represents the permutation that sends a_i to a_{i+1} for $1 \leq i \leq k - 1$, and sends a_k to a_1 . Note that every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. This product of is called the *cycle decomposition* of σ .

6.3. Finding Inverse of Cycle Decomposition: For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by reversing the order of the numbers in each cycle of the cycle decomposition of σ . For example, if

$$\sigma = (1 \ 2 \ 8 \ 10 \ 4)(2 \ 1 \ 3)(5 \ 1 \ 7)(6 \ 9),$$

then

$$\sigma^{-1} = (4 \ 10 \ 8 \ 1 \ 2)(1 \ 3 \ 2)(7 \ 1 \ 5)(9 \ 6).$$

6.4. Computing Products in S_A : To compute the product (here the operation is composition) $\sigma \circ \tau$ of permutations σ and τ in S_n , to an element $i \in \{1, 2, \dots, n\}$ we calculate from right to left. That is, we calculate $\tau(i)$ and then calculate $\sigma(\tau(i))$. For example,

$$(1 \ 2)(1 \ 3) = (1 \ 3 \ 2) \quad \text{and} \quad (1 \ 3)(1 \ 2) = (1 \ 2 \ 3).$$

Remark 6.1. The above calculations show that S_A is a non-abelian group for every $n \geq 3$.

Note 6.1. (1) A permutation in S_A may be written in many ways as a product of cycles, but the cycle decomposition of each permutation is unique (up to rearranging the cycles and cyclically permuting the elements within each cycle).

- (2) The **order of a permutation** σ is the least common multiple *l.c.m* of the lengths of the cycles in its cycle decomposition.

Proposition 6.1. Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decomposition

$$(a_1 \ a_2 \ \dots \ a_{k_1}) \ (b_1 \ b_2 \ \dots \ b_{k_2}) \ \dots$$

Then $\tau \sigma \tau^{-1}$ has cycle decomposition

$$(\tau(a_1) \ \tau(a_2) \ \dots \ \tau(a_{k_1})) \ (\tau(b_1) \ \tau(b_2) \ \dots \ \tau(b_{k_2})) \ \dots$$

PROOF. Note that $\sigma(i) = j$ implies that

$$\tau\sigma\tau^{-1}(\tau(i)) = \tau(\sigma(i)) = \tau(j).$$

Therefore, if (i, j) appears in the cycle decomposition of σ , then $(\tau(i), \tau(j))$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This implies that $\tau\sigma\tau^{-1}$ is obtained by applying τ to each element in the cycles of σ . $\square$

Problem 6.1. Let σ be the permutation defined by

$$\begin{array}{ccccc} 1 \mapsto 13, & 2 \mapsto 2, & 3 \mapsto 15, & 4 \mapsto 14, & 5 \mapsto 10, \\ 6 \mapsto 6, & 7 \mapsto 12, & 8 \mapsto 3, & 9 \mapsto 4, & 10 \mapsto 1, \\ 11 \mapsto 7, & 12 \mapsto 9, & 13 \mapsto 5, & 14 \mapsto 11, & 15 \mapsto 8, \end{array}$$

and let τ be the permutation defined by

$$\begin{array}{ccccc} 1 \mapsto 14, & 2 \mapsto 9, & 3 \mapsto 10, & 4 \mapsto 2, & 5 \mapsto 12, \\ 6 \mapsto 6, & 7 \mapsto 5, & 8 \mapsto 11, & 9 \mapsto 15, & 10 \mapsto 3, \\ 11 \mapsto 8, & 12 \mapsto 7, & 13 \mapsto 4, & 14 \mapsto 1, & 15 \mapsto 13. \end{array}$$

Then find the cycle decompositions of σ , τ , σ^2 , $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

Solution 6.1. Note that

$$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)(2)(6) \quad \text{and} \quad \tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)(6).$$

Then we have

$$\begin{aligned} \sigma^2 &= (1\ 5)(13\ 10)(3\ 8\ 15)(4\ 11\ 12)(14\ 7\ 9)(2)(6), \\ \sigma\tau &= (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)(6)(12), \\ \tau\sigma &= (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)(6)(7), \\ \tau^2\sigma &= (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)(6)(9). \end{aligned}$$

Problem 6.2. Let σ be the m -cycle $(1\ 2\ \dots\ m)$. Show that σ^i is also an m -cycle if and only if i is relatively prime to m .

Solution 6.2. Let $\sigma = (1\ 2\ \dots\ m)$. Then we consider the map σ maps $k \mapsto k+1 \pmod{m}$. This implies that

$$\sigma^i(k) = k + i \pmod{m}.$$

Assume that σ^i is an m -cycle. Then the elements

$$1, \sigma^i(1), \sigma^{2i}(1), \dots, \sigma^{(m-1)i}(1)$$

are distinct. This is only possible if the values $i, 2i, \dots, mi$ modulo m are all distinct. Thus, $\gcd(i, m) = 1$.

Conversely, assume that $\gcd(i, m) = 1$. Then the map $k \mapsto k + i \pmod{m}$ generates all residues modulo m . Thus, σ^i is a single m -cycle.

Problem 6.3. Prove that the order of an element in S_n is equal to the least common multiple of the lengths of each cycle in its cycle decomposition.

Solution 6.3. Let $\sigma \in S_n$. Assume that $\sigma = \gamma_1\gamma_2\cdots\gamma_k$, where each γ_i is a disjoint cycle of length ℓ_i . Then σ has disjoint cycle decomposition. Since disjoint cycles commute, we have

$$\sigma^m = (\gamma_1\gamma_2\cdots\gamma_k)^m = \gamma_1^m\gamma_2^m\cdots\gamma_k^m$$

Since each cycle γ_i has order ℓ_i , we have $\gamma_i^m = id$ if and only if $\ell_i \mid m$. Therefore, $\sigma^m = id$ if and only if m is a common multiple of all ℓ_i . Thus,

$$|\sigma| = \text{lcm}(\ell_1, \ell_2, \dots, \ell_k).$$

Problem 6.4. Find the order of the permutation $(11\ 2\ 8\ 10\ 4)(21\ 3)(5\ 11\ 7)(6\ 9)$.

Solution 6.4. Let $\sigma = (11\ 2\ 8\ 10\ 4)(21\ 3)(5\ 11\ 7)(6\ 9)$. We now compute the disjoint cycle decomposition of the permutation

$$\sigma = (2\ 8\ 10\ 4\ 7\ 5\ 11)(3\ 21)(6\ 9).$$

We now find the order of the permutation, which is the least common multiple of the lengths of the disjoint cycles. Thus, the order of σ given by

$$|\sigma| = \text{lcm}(7, 2, 2) = 14.$$

Problem 6.5. Show that if $n \geq 4$, then the number of permutations in S_n which are the product of two disjoint 2-cycles is

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

Solution 6.5. Note that the permutation is of the form $(a\ b)(c\ d)$, where a, b, c, d are distinct, are disjoint 2-cycles. Therefore, we have the following possibility

- First, the possibility of choosing 4 distinct elements out of n is $\binom{n}{4}$.
- Then count the number of ways to partition the 4 elements into two disjoint 2-cycles. There are

$$\frac{1}{2} \cdot \binom{4}{2} = \frac{1}{2} \cdot 6 = 3$$

such ways (we divide by 2 to account for the fact that the order of the two 2-cycles doesn't matter).

Thus, the number of permutations in S_n which are the product of two disjoint 2-cycles is

$$\binom{n}{4} \cdot 3 = \frac{n(n-1)(n-2)(n-3)}{24} \cdot 3 = \frac{n(n-1)(n-2)(n-3)}{8}.$$

CHAPTER 2

Subgroups

“Mathematics, rightly viewed, possesses not only truth but supreme beauty ”

— Bertrand Russell

In this chapter, we study and explore subgroups of a group, which are subsets that themselves form groups under the same operation. Also we study the concepts of generator of a group, cyclic groups, Centralizers and Normalizers, Stabilizers and Kernels. A selection of examples and exercises in this chapter is based on material from [3].

1. Subgroups and Examples

Definition 1.1 (Subgroup). Let G be a group and H be a subset of G . If H is a group under the operation of G , then H is called a subgroup of G and denote it by $H \leq G$.

Example 1.1. Any group G has two subgroups $H = G$ and $H = \{e\}$, where e is the identity element of G . If $H = \{e\}$ is called the *trivial subgroup*. If $H \neq G$ is a subgroup of G , then H is called a *proper subgroup* or *non-trivial subgroup* of G and denote it by $H < G$.

Example 1.2. (a) The group $(2\mathbb{Z}, +)$ of even integers under addition is a subgroup of $(\mathbb{Z}, +)$. That is, $(2\mathbb{Z}, +) < (\mathbb{Z}, +)$.
(b) The group $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$ and $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$. That is, $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$.

Note 1.1. The relation “is a subgroup of” is transitive: if $H \leq G$ and $K \leq H$, then $K \leq G$. Thus, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

Proposition 1.1 (The Subgroup Test). Let G be a group and H be a subset of G . Then H is a subgroup of G if and only if

- (a) $H \neq \emptyset$, and
- (b) $xy^{-1} \in H$ for all $x, y \in H$.

Furthermore, if H is a finite set, then it is enough to check that H is non-empty and closed under the same operation on G .

PROOF. Assume that H is a subgroup of G . Then it is clear that (a) and (b) hold true.

Conversely, assume that $H \leq G$ satisfies conditions (a) and (b). Let $x \in H$ as $H \neq \emptyset$. Take $y = x$ in (b), then

$$xx^{-1} = e \in H.$$

This shows that the identity element $e \in H$. Let $x \in H$. By (b) with $y = e \in H$, we get

$$xe^{-1} = x \in H,$$

and with $x = e, y = x$, we obtain

$$e \cdot x^{-1} = x^{-1} \in H.$$

Next, let $x, y \in H$. Since $y^{-1} \in H$ and by (b), we obtain

$$x(y^{-1})^{-1} = xy \in H.$$

Hence, H is closed under multiplication. Clearly, the associative property holds true in H . Thus, H is a subgroup of G .

Let H be a finite subset of G which is closed under multiplication and $x \in H$. Note that the sequence $x, x^2, x^3, \dots$ must eventually repeat. So there exist integers $a < b$ such that $x^a = x^b$. Take $n = b - a$, then $x^n = e$ and $x^{n-1} = x^{-1} \in H$. Thus, every element of H has an inverse in H , and hence H is also closed under inverses and is a subgroup of G . $\square$

Problem 1.1. Let

$$H = \left\{ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} : a, b, c \in \mathbb{R} \right\}.$$

Then $(H, +)$ is a subgroup of $(M_2(\mathbb{R}), +)$.

Solution 1.1. From the subgroup test, it is enough to show that $H \neq \emptyset$ and for all $A, B \in H$, $A - B \in H$. It is clear that $H \neq \emptyset$ as $a, b, c \in \mathbb{R} \neq \emptyset$.

Let

$$A = \begin{bmatrix} a_1 & a_2 \\ a_3 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} b_1 & b_2 \\ b_3 & 0 \end{bmatrix},$$

where $a_i, b_i \in \mathbb{R}$ for $1 \leq i \leq 3$. Then

$$A + B = \begin{bmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & 0 \end{bmatrix} \in H$$

and the inverse of A under addition is

$$-A = \begin{bmatrix} -a_1 & -a_2 \\ -a_3 & 0 \end{bmatrix} \in H.$$

Thus, by the subgroup test, H is a subgroup of $M_2(\mathbb{R})$.

Problem 1.2. Let G be an abelian group with identity element e . Define

$$H = \{x \in G \mid x^2 = e\}.$$

Then H is a subgroup of G .

Solution 1.2. Note that $e^2 = e \cdot e = e$, so $e \in H$ and H is non-empty. Now let $a, b \in H$. Then $a^2 = e$ and $b^2 = e$. We now prove that $ab^{-1} \in H$. That is,

$$(ab^{-1})^2 = e.$$

Since G is abelian, we have

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1}.$$

As $a^2 = e$ and $b^2 = e$, we have

$$a^2(b^2)^{-1} = e \cdot e^{-1} = e.$$

Thus, $ab^{-1} \in H$, and by the subgroup test, H is a subgroup of G .

Problem 1.3. Prove that the following subset is not a subgroup of the given group.

- (a) For $n \geq 3$, the set of 2-cycles in S_n .
- (b) For $n \geq 3$, the set of reflections in D_{2n} .
- (c) Given a composite integer $n > 1$ and G a group containing an element of order n , the set

$$\{x \in G \mid |x| = n\} \cup \{1\}.$$

- (d) The set of odd integers (both positive and negative integers) in $\mathbb{Z}$ with 0.
- (e) The set of real numbers whose square is a rational number (under addition).

Solution 1.3. (a) The set of all 2-cycles is not a subgroup of S_n since $(1\ 2)$ and $(2\ 3)$ are 2-cycle but $(1\ 2)(2\ 3) = (1\ 2\ 3)$ is not a 2-cycle. Thus, the set is not closed under composition, and so it is not a subgroup.

(b) Note that the product of two reflections in D_{2n} is a rotation (not a reflection) unless the reflections are the same. Thus, the set of all reflections is not a subgroup of D_{2n} .

(c) Let $n = ab$ and x be an element of G with $|x| = n$. Then $x^a \neq 1$, and $|x^a| = b < n$, so $x^a \notin \{x \in G \mid |x| = n\} \cup \{1\}$. Thus, it is not a subgroup as it is not closed.

(d) Clearly, it is not a subgroup of $\mathbb{Z}$ as 1 and 3 are odd integers but $1 + 3 = 4$ is even. Thus, the set is not closed under addition and is not a subgroup.

(e) We prove that the set $\{x \in \mathbb{R} \mid x^2 \in \mathbb{Q}\}$ is not a subgroup of $\mathbb{R}$ under addition. Let $x = \sqrt{2}$ and $y = \sqrt{3}$. Then $x^2 = 2 \in \mathbb{Q}$ and $y^2 = 3 \in \mathbb{Q}$. This implies that

$$(x + y)^2 = x^2 + 2xy + y^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$$

is irrational. Therefore, $x + y$ is not in the set. Thus, the set is not a subgroup of $\mathbb{R}$ under addition.

Problem 1.4. Let G be an abelian group. Then prove that the set $\{g \in G \mid |g| < \infty\}$ is a subgroup of G . This subgroup H of H is called the *torsion subgroup* of G . Give an explicit example where this set is not a subgroup when G is non-abelian.

Solution 1.4. It is clear that the identity element $e \in T(G)$. Let $g \in T(G)$ with $|g| = n$ for some $n \in \mathbb{N}$. Then $g^n = e$ and $(g^{-1})^n = (g^n)^{-1} = e^{-1} = e$. Thus, g^{-1} has finite order and $g^{-1} \in T(G)$.

Next, let $g, h \in T(G)$ with $|g| = m$ and $|h| = n$. Since G is abelian, we can write

$$(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = e^n e^m = e.$$

Therefore, gh has finite order dividing mn and $gh \in T(G)$. Thus, $T(G)$ is a subgroup of G by the subgroup test.

Counterexample when G is non-abelian. Consider the non-abelian group $G = \text{GL}_2(\mathbb{Q})$. Let

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Then the order of A is 4, and the order of B is 3. But the product $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order.

Problem 1.5. Let H and K be subgroups of G . Prove that $H \cup K$ is a subgroup if and only if either $H \leq K$ or $K \leq H$.

Solution 1.5. Assume that $H \cup K \leq G$. Suppose that neither $H \subseteq K$ nor $K \subseteq H$. Then there exist elements $h \in H \setminus K$ and $k \in K \setminus H$. As $h, k \in H \cup K$ and $H \cup K$ is a subgroup, it follows that $hk \in H \cup K$. If $hk \in H$, then $k = h^{-1}(hk) \in H$ as $h^{-1} \in H$, which is a contradiction to $k \notin H$. If $hk \in K$, then $h = (hk)k^{-1} \in K$ as $k^{-1} \in K$, which is a contradiction to $h \notin K$. Therefore, we conclude that $H \subseteq K$ or $K \subseteq H$.

Conversely, assume that $H \subseteq K$. Then $H \cup K = K$ is a subgroup. Similarly, if $K \subseteq H$, then $H \cup K = H$ is also a subgroup.

Problem 1.6. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$.

- $\{(a, 1) \mid a \in A\}$.
- $\{(1, b) \mid b \in B\}$.
- $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the diagonal subgroup).

Solution 1.6. Let A and B be groups. We use the subgroup test to prove that the above subsets of $A \times B$ are subgroups.

(a) Let $H = \{(a, 1) \mid a \in A\}$. Then

- The identity $(1, 1) \in H$.
- If $(a_1, 1), (a_2, 1) \in H$, then $(a_1, 1)(a_2, 1) = (a_1 a_2, 1) \in H$.
- The inverse of $(a, 1)$ is $(a^{-1}, 1) \in H$.

Thus, H is a subgroup of $A \times B$.

(b) Let $K = \{(1, b) \mid b \in B\}$. Then

- The identity $(1, 1) \in K$.
- If $(1, b_1), (1, b_2) \in K$, then $(1, b_1)(1, b_2) = (1, b_1 b_2) \in K$.
- The inverse of $(1, b)$ is $(1, b^{-1}) \in K$.

Thus, K is a subgroup of $A \times B$.

(c) Let $A = B$ and $S = \{(a, a) \mid a \in A\}$. Then

- The identity $(1, 1) \in S$.
- If $(a_1, a_1), (a_2, a_2) \in S$, then $(a_1, a_1)(a_2, a_2) = (a_1 a_2, a_1 a_2) \in S$.
- The inverse of (a, a) is $(a^{-1}, a^{-1}) \in S$.

Thus, S is a subgroup of $A \times A$.

Problem 1.7. Let $H_1 \leq H_2 \leq \dots$ be an ascending chain of subgroups of G . Prove that $\bigcup_{i=1}^{\infty} H_i$ is a subgroup of G .

Solution 1.7. Let $H_1 \leq H_2 \leq \dots$ be an ascending chain of subgroups of G . Define

$$H = \bigcup_{i=1}^{\infty} H_i.$$

We prove that H is a subgroup of G . Since each H_i is a subgroup, it contains the identity element e of G . Thus, $e \in H_i$ for all i , and therefore $e \in H$. Hence, $H \neq \emptyset$. Let $a, b \in H$. Then there exist $m, n \in \mathbb{N}$ such that $a \in H_m$ and $b \in H_n$. Without loss of generality, assume $m \leq n$. Since the chain is ascending, we have

$$H_m \subseteq H_n.$$

This implies that $a, b \in H_n$. As H_n is a subgroup, it follows that $ab \in H_n \subseteq H$.

Let $a \in H$. Then $a \in H_m$ for some $m \in \mathbb{N}$. Since H_m is a subgroup, we have $a^{-1} \in H_m \subseteq H$. Thus, H is a subgroup of G by the subgroup test.

Problem 1.8. Let $G = \text{GL}_n(F)$, where $F = \mathbb{R}$ or $\mathbb{C}$. Define

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

(called the special linear group). Prove that $\text{SL}_n(F) \leq \text{GL}_n(F)$.

Solution 1.8. It is clear that, $\text{SL}_n(F) \neq \emptyset$ as the identity matrix $I \in \text{SL}_n(F)$.

Let $A, B \in \text{SL}_n(F)$. Then

$$\det(AB) = \det(A) \det(B) = 1 \cdot 1 = 1.$$

This implies that $AB \in \text{SL}_n(F)$.

Let $A \in \text{SL}_n(F)$. Then $\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$ and so $A^{-1} \in \text{SL}_n(F)$. Therefore, $\text{SL}_n(F)$ is a subgroup of $\text{GL}_n(F)$ by the subgroup test.

Problem 1.9. Let $n \in \mathbb{Z}^+$ and let $F = \mathbb{R}$ or $\mathbb{C}$. Prove that the set

$$\{(a_{ij}) \in \text{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$$

is a subgroup of $\text{GL}_n(F)$ (called the group of upper triangular matrices).

Solution 1.9. Let $F = \mathbb{R}$ or $\mathbb{C}$ and $n \in \mathbb{Z}^+$. Define

$$U_n(F) = \{A = (a_{ij}) \in \text{GL}_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}.$$

Since the identity matrix $I_n \in \text{GL}_n(F)$ is upper triangular, we have $I_n \in U_n(F)$.

Let $A = (a_{ij}), B = (b_{ij}) \in U_n(F)$. Consider $C = AB = (c_{ij})$, where

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}.$$

Let $i > j$. If $k < i$, then $a_{ik} = 0$, since A is upper triangular. If $k > j$, then $b_{kj} = 0$ since B is upper triangular. This implies that $a_{ik} b_{kj} = 0$ and $c_{ij} = 0$ when $i > j$. Therefore, C is upper triangular. Since $\text{GL}_n(F)$ is closed under multiplication, $C \in \text{GL}_n(F)$. Thus, $AB \in U_n(F)$.

Let $A \in U_n(F)$. Then A is invertible and upper triangular. Note that the inverse of an invertible upper triangular matrix is also upper triangular. Hence, $A^{-1} \in U_n(F)$. Thus, $U_n(F)$ is a subgroup of $\text{GL}_n(F)$ by the subgroup test.

2. Centralizers and Normalizers

Let G be a group and A be a non-empty subset G .

Definition 2.1 (Centralizer). The subset

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$$

of G is called the *centralizer* of A in G . Note that $gag^{-1} = a$ if and only if $ga = ag$.

Let a be a fixed element of a group G . Then the set

$$C_G(a) = \{g \in G \mid gag^{-1} = a\}$$

is called the centralizer of a in G .

Proposition 2.1. The subset $C_G(A)$ is a subgroup of G .

PROOF. Since $ea = ae$ for all $a \in G$, we have $e \in C_G(A)$ and so $C_G(A) \neq \emptyset$. Let $x, y \in C_G(A)$. Then $xax^{-1} = a$ and $yay^{-1} = a$ for all $a \in A$.

This implies that $a = y^{-1}ay$ and $y^{-1} \in C_G(A)$. Next, we consider

$$\begin{aligned} (xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \quad (\text{by the associative law}) \\ &= xax^{-1} \quad (\text{since } y \in C_G(A)) \\ &= a \quad (\text{since } x \in C_G(A)). \end{aligned}$$

Thus, $xy \in C_G(A)$, and conclude that $C_G(A)$ is a subgroup of G by the subgroup test. $\square$

Note 2.1. (a) If $A = \{a\}$, then we write $C_G(\{a\})$ for $C_G(a)$, and $a^n \in C_G(a)$ for every $n \in \mathbb{Z}$.
(b) If G is an abelian group, then $C_G(A) = G$ for all subsets A of G .

Definition 2.2 (Center of a group). Define

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

This subset of G is called the *center* of G .

Note 2.2. It is clear that $Z(G) = C_G(G)$. From Proposition 2.1, $Z(G)$ is a subgroup of G . If G is an abelian group, then $Z(G) = G$.

Definition 2.3 (Normalizer). The subset

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

of G is called the *normalizer* of A in G . Recall that $gAg^{-1} = \{gag^{-1} \mid a \in A\}$.

Note 2.3. Suppose $g \in C_G(A)$. Then $gag^{-1} = a \in A$ for all $a \in A$. Thus, $C_G(A) \leq N_G(A)$. Note that if G is an abelian group, then $C_G(A) = N_G(A) = G$ for every subset A of G .

Problem 2.1. Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Solution 2.1. Recall that the center of a group G

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

and the centralizer of a subset A of G

$$C_G(A) = \{g \in G \mid ga = ag \text{ for all } a \in A\}.$$

Note that for all $g \in G$ and $z \in Z(G)$, we have $gz = zg$. This implies that

$$g \in C_G(Z(G)) \quad \text{for all } g \in G.$$

Therefore, $C_G(Z(G)) = G$.

Next, we consider $N_G(Z(G)) = \{g \in G \mid gZ(G)g^{-1} = Z(G)\}$. Note that for all $g \in G$, we have $gZ(G)g^{-1} = Z(G)$ and so $g \in N_G(Z(G))$. Thus, we conclude that $N_G(Z(G)) = G$.

Problem 2.2. Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution 2.2. Assume that $A \subseteq B$. If $g \in C_G(B)$, then $gb = bg$ for all $b \in B$, and in particular, for all $a \in A$. Hence, $g \in C_G(A)$. Therefore, $C_G(B) \subseteq C_G(A)$. Since both $C_G(B)$ and $C_G(A)$ are subgroups of G and $C_G(B) \subseteq C_G(A)$, it follows that

$$C_G(B) \leq C_G(A).$$

Problem 2.3. Let H be a subgroup of the group G .

- (a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.
- (b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Solution 2.3. (a) Let $h \in H$. As H is a subgroup, we have $hHh^{-1} = \{h x h^{-1} \mid x \in H\} \subseteq H$. For every $y \in H$, we have $y = h^{-1}(h y h^{-1})h \in h^{-1}Hh \subseteq H$ as $h^{-1} \in H$. This implies that $hHh^{-1} = H$ and hence $h \in N_G(H)$. Thus, $H \leq N_G(H)$.

Counter-example when H is not a subgroup. Let $G = S_3$ and $H = \{(12), (13)\}$. Then the product $(12)(13) = (132) \notin H$ and so H is not a subgroup. Note that $(12) \in H$, but $(12)((13))(12)^{-1} = (23) \notin H$. This implies that $(12) \notin N_G(H)$ and hence $H \not\leq N_G(H)$.

(b) Assume that $H \leq C_G(H)$. Then for any $a, b \in H$ we have $ab = ba$ as $a \in C_G(H)$. Thus, H is abelian. Conversely, if H is abelian, then every $h \in H$ commutes with every element of H . Hence, $h \in C_G(H)$ and $H \leq C_G(H)$.

Problem 2.4. Let $n \in \mathbb{Z}$ with $n \geq 3$. Then prove the following statements.

- (a) $Z(D_{2n}) = \{1\}$ if n is odd.
- (b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$.

Solution 2.4. Recall the the dihedral group D_{2n} is the group of symmetries of a regular n -gon and we write

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle.$$

The elements of D_{2n} are of the form r^i and sr^i for $0 \leq i < n$.

(a) We prove that $Z(D_{2n}) = \{1\}$ if n is odd. Let $z \in Z(D_{2n})$. Since z must commute with both r and s , we consider the possible forms of z . Suppose that $z = r^k$. Then

$$sr^k = r^k s \iff sr^k s = r^k \iff r^{-k} = r^k \iff r^{2k} = 1.$$

Since n is odd, we have $k \equiv 0 \pmod{n}$. Thus, $r^k = 1$.

Next, we assume that $z = sr^k$. Then we consider

$$zr = sr^k r = sr^{k+1} \quad \text{and} \quad rz = r sr^k = sr^{-k} r = sr^{-(k-1)}.$$

This implies that $zr \neq rz$ and $z = sr^k \notin Z(D_{2n})$. Thus, $Z(D_{2n}) = \{1\}$.

(b) We prove that $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$ is even. Let $n = 2k$. Then consider the element r^k and we have the following observations

- r^k clearly commutes with all powers of r since $r^k r^i = r^i r^k$.
- Since $srs = r^{-1}$, we have $sr^k s = r^{-k}$ and $sr^k = r^{-k} s$. This implies that $sr^k = r^{-k} s$ and $sr^k = r^k s$. Therefore, $r^{-k} = r^k$ and so $r^{2k} = r^n = 1$. Hence, r^k commutes with s .

Thus, $1, r^k \in Z(D_{2n})$.

Next, suppose $z = sr^m$. Then

$$zr = sr^m r = sr^{m+1}, \quad rz = r sr^m = sr^{-m+1}.$$

This implies that $zr \neq rz$ and sr^m is in the center. Thus, we conclude that

$$Z(D_{2n}) = \{1, r^k\}.$$

3. Cyclic Groups and Cyclic Subgroups

“Theory attracts practice as the magnet attracts iron.”

— Carl Friedrich Gauss

Let a be an element of a group G . Define

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

Proposition 3.1. $\langle a \rangle$ is a subgroup of G .

PROOF. Since $a \in \langle a \rangle$, the set $\langle a \rangle \neq \emptyset$. Let $a^n, a^m \in \langle a \rangle$, where $n, m \in \mathbb{Z}$. Then $-m, n - m \in \mathbb{Z}$, $(a^m)^{-1} = a^{-m} \in \langle a \rangle$ and

$$a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle.$$

From the subgroup test, we conclude that $\langle a \rangle$ is a subgroup of G . $\square$

Definition 3.1. The subgroup $\langle a \rangle$ is called the *cyclic subgroup* of G generated by a .

Definition 3.2 (Cyclic group). A group G is called a *cyclic group* if $G = \langle a \rangle$ for some $a \in G$. We call a is a generator of G .

Note 3.1. A cyclic group G may have many generators.

Remark 3.1. Let G be a cyclic group generated by $g \in G$. If g has order n , then $G = \langle g \rangle$ is cyclic of order n . If $g \in G$ has infinite order, then $G = \langle g \rangle$ is an infinite cyclic group.

Problem 3.1. Prove that $(\mathbb{Z}, +)$ is a cyclic group and has two generators 1 and -1 .

Solution 3.1. Let $1 \in \mathbb{Z}$. Then

$$\langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \mathbb{Z}.$$

Therefore, 1 is a generator of $\mathbb{Z}$ under addition. Similarly, we see that $-1 \in \mathbb{Z}$ generates $\mathbb{Z}$ as

$$\langle -1 \rangle = \{n \cdot (-1) \mid n \in \mathbb{Z}\} = \mathbb{Z}.$$

Problem 3.2. Prove that $(\mathbb{Z}_n, +_n)$ is a cyclic group.

Solution 3.2. It is clear that, $1 \in \mathbb{Z}_n$ and $\langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} = \mathbb{Z}_n$.

Problem 3.3. Prove or disprove: $(\mathbb{Q}^*, \cdot)$ is a cyclic group.

Solution 3.3. Assume that the group $(\mathbb{Q}^*, \cdot)$ is cyclic with generator $g = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $a \neq 0$, $b > 0$, and $\gcd(a, b) = 1$. Then every element $h \in \mathbb{Q}^*$ of the form $h = g^n = \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$ for some integer n .

Consider the element $\frac{1}{2} \in \mathbb{Q}^*$. If $\frac{1}{2} = \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$, then:

$$\frac{a^n}{b^n} = \frac{1}{2} \implies a^n = \frac{b^n}{2} \implies 2a^n = b^n.$$

Note that a^n and b^n are integers. So b^n must be divisible by 2, which implies that b has 2 as a prime factor. Similarly, consider $\frac{1}{3} \in \mathbb{Q}^*$. If $\frac{1}{3} = \left(\frac{a}{b}\right)^m = \frac{a^m}{b^m}$, then

$$\frac{a^m}{b^m} = \frac{1}{3} \implies a^m = \frac{b^m}{3} \implies 3a^m = b^m.$$

Thus, b must be divisible by 3. Continuing this argument, for any prime p we get

$$\frac{1}{p} = \left(\frac{a}{b}\right)^k = \frac{a^k}{b^k} \implies a^k = \frac{b^k}{p} \implies pa^k = b^k.$$

This implies b is divisible by p . Thus, there are infinitely many primes p that divide b , which contradicts that b is a finite integer.

Problem 3.4. Find different examples of finite non-cyclic groups.

Solution 3.4. (1) The Klein four-group has order 4 and all non-identity elements have order 2, so it cannot be cyclic.

- (2) The symmetric group S_3 has order 6 and is non-abelian. Since cyclic groups are abelian, S_3 is not cyclic.
- (3) The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ has order 8 and is non-abelian, and there is no generator in this group. Thus, Q_8 is not cyclic.
- (4) The group $\mathbb{Z}_2 \times \mathbb{Z}_4$ has order 8 and the maximum order of any element is 4. Thus, it is not cyclic.
- (5) The alternating group A_4 has order 12 and is non-abelian, and there is no element of order 12. Thus, it is not cyclic.
- (6) The group $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic. Suppose $\mathbb{Z} \times \mathbb{Z}_2$ is cyclic, generated by (a, b) where $a \in \mathbb{Z}_2$, $b \in \mathbb{Z}$. Since $\mathbb{Z}$ is infinite cyclic, the subgroup generated by (a, b) is infinite cyclic. But $(0, 1)$ is an element of order 2 not in the infinite cyclic subgroup generated by (a, b) , because infinite cyclic groups have no non-trivial finite order elements. Therefore, $\mathbb{Z} \times \mathbb{Z}_2$ is not cyclic.
- (7) The group $(\mathbb{R}^*, \cdot)$ is not cyclic. If $(\mathbb{R}^*, \cdot)$ is cyclic generated by r , then the subgroup generated by r is countable, since it consists of all integer powers of r . But $\mathbb{R}^*$ is uncountable. Thus, $(\mathbb{R}^*, \cdot)$ is not cyclic.

Theorem 3.1. Let G be a group and $g \in G$.

- (a) If g has infinite order, then $g^i = g^j$ if and only if $i = j$.
- (b) If g has finite order, say n , then $\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$, and $g^i = g^j$ if and only if n divides $i - j$.

PROOF. (a). If g has infinite order, then $g^n \neq e$ (the identity element) for all $n \in \mathbb{N}$. We assume that $g^i = g^j$. This implies that $g^{i-j} = e$. Thus, $i - j = 0$ and so $i = j$.

The converse is trivial since $i = j$ implies that $g^i = g^j$.

(b) Assume that $|g| = n$, i.e., the order of g is n . Clearly, the elements $e, g, g^2, \dots, g^{n-1}$ are in $\langle g \rangle$. Suppose that g^k is an arbitrary member of $\langle g \rangle$. By the division algorithm, there exist integers q and r such that

$$k = qn + r \quad \text{with} \quad 0 \leq r < n.$$

Then we can write

$$g^k = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Thus, $g^k \in \{e, g, g^2, \dots, g^{n-1}\}$ and

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}.$$

We assume that $g^i = g^j$. Then $g^{i-j} = e$. By the division algorithm, there exist integers q and r such that

$$i - j = qn + r \quad \text{with} \quad 0 \leq r < n.$$

Therefore,

$$g^{i-j} = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r.$$

Since $g^n = e$ and n is the smallest positive integer such that $g^n = e$, we must have $r = 0$. Thus, n divides $i - j$.

Conversely, if n divides $i - j$, then $i - j = nq$ for some $q \in \mathbb{Z}$. Therefore,

$$g^{i-j} = g^{nq} = (g^n)^q = e^q = e.$$

Thus, $g^i = g^j$. □

Corollary 3.1. Let G be a group and $g \in G$. Then $|g| = |\langle g \rangle|$.

Corollary 3.2. Let G be a group and a be an element of order n in G . If $a^k = e$, then n divides k .

Theorem 3.2. Let g be an element of order n in a group, and k be a positive integer. Then $\langle g^k \rangle = \langle g^{\gcd(n,k)} \rangle$ and $|g^k| = \frac{n}{\gcd(n,k)}$.

PROOF. Let $d = \gcd(n, k)$. We can write $k = dr$ for some integer r as d divides k . Since $g^k = (g^d)^r$, we have $\langle g^k \rangle \leq \langle g^d \rangle$.

By Bézout's identity, there exist integers s and t such that

$$d = ns + kt.$$

This implies that

$$g^d = g^{ns+kt} = g^{ns}g^{kt} = (g^n)^s(g^k)^t = e(g^k)^t = (g^k)^t \in \langle g^k \rangle.$$

Therefore, $\langle g^d \rangle \leq \langle g^k \rangle$. Thus,

$$\langle g^k \rangle = \langle g^{\gcd(n,k)} \rangle.$$

Next, we prove that $|g^k| = \frac{n}{\gcd(n,k)}$. For this, we first show that $|g^d| = \frac{n}{d}$ for any divisor d of n . Clearly,

$$(g^d)^{n/d} = g^n = e,$$

which implies that $|g^d| \leq n/d$. On the other hand, if i is a positive integer less than n/d , then $(g^d)^i \neq e$ by the definition of $|g^d|$. This implies that $n/d \leq |g^d|$. Therefore, $|g^d| = n/d$ for all divisors d of n . In particular, we have $|g^{\gcd(n,k)}| = \frac{n}{\gcd(n,k)}$ since $\gcd(n, k)$ divides n .

Thus,

$$|g^k| = |\langle g^k \rangle| = |\langle g^{\gcd(n,k)} \rangle| = |g^{\gcd(n,k)}| = \frac{n}{\gcd(n,k)}.$$

□

Corollary 3.3. In a finite cyclic group, the order of an element divides the order of the group.

Corollary 3.4. Let $|a| = n$. Then

- (a) $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$.
- (b) $|a^i| = |a^j|$ if and only if $\gcd(n, i) = \gcd(n, j)$.

Corollary 3.5. Let $|a| = n$. Then

- (a) $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$.
- (b) $|a| = |\langle a^j \rangle|$ if and only if $\gcd(n, j) = 1$.

Corollary 3.6. An integer $k \in \mathbb{Z}$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

Theorem 3.3 (Fundamental Theorem of Cyclic Groups). Let $G = \langle g \rangle$ be a cyclic group.

- (a) Every subgroup of G is cyclic.
- (b) If $|G| = n$, then the order of any subgroup of G divides n .
- (c) If $|G| = n$, then for any $k \mid n$, the subgroup $\langle g^{n/k} \rangle$ is the unique subgroup of order k .

PROOF. (a) Let H be a subgroup of G . If $H = \{e\}$, then $H = \langle e \rangle$ is a cyclic group. Suppose that $H \neq \{e\}$. Then choose the element $g^m \in H$ with the smallest positive exponent $m \in \mathbb{Z}^+$, using the well-ordering principle. Clearly, $\langle g^m \rangle \leq H$.

Now assume that $g^k \in H$. By the division algorithm, we can write

$$k = qm + r, \quad \text{where } 0 \leq r < m.$$

This implies that

$$r = k - qm.$$

Since $g^k \in H$ and $g^m \in H$, it follows that

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

By the minimality of m , we must have $r = 0$, which implies $g^k = (g^m)^q$ and $g^k \in \langle g^m \rangle$. Thus, $H = \langle g^m \rangle$ is a cyclic group.

(b) Let H be a subgroup of G . By part (a), H is cyclic, so we can write $H = \langle g^m \rangle$, where $m \in \mathbb{Z}^+$ is minimal by the well-ordering principle.

By the division algorithm, there exist two integers q and r such that

$$n = qm + r, \quad \text{where } 0 \leq r < m.$$

This implies that

$$r = n - qm.$$

Since $g^n \in H$ and $g^m \in H$, it follows that

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

By the minimality of m , we must have $r = 0$, which implies

$$n = qm.$$

Therefore, the order of H is given by

$$|H| = |\langle g^m \rangle| = |g^m| = \frac{n}{\gcd(n, m)} = \frac{n}{m}.$$

Thus, the order of H divides n .

(c) Let $G = \langle g \rangle$ be a cyclic group of order n . For any $k \mid n$, we have

$$|\langle g^{n/k} \rangle| = |g^{n/k}| = \frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

Thus, $\langle g^{n/k} \rangle$ is a subgroup of order k .

Next, we prove the uniqueness. Let $H \leq G$ be a subgroup with $|H| = k$, where $k \mid n$. Since $H \leq G$ and G is a cyclic group, it follows from (a) and (b) that H is cyclic. Thus, we can write

$$H = \langle g^m \rangle$$

for some m dividing n . Then we have

$$k = |H| = |\langle g^m \rangle| = |g^m| = \frac{n}{\gcd(n, m)} = \frac{n}{m}.$$

Therefore,

$$H = \langle g^m \rangle = \langle g^{n/k} \rangle.$$

Thus, $\langle g^{n/k} \rangle$ is the unique subgroup of order k . □

Corollary 3.7. For each positive divisor k of n , the set $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k . Moreover, these are the only subgroups of $\mathbb{Z}_n$.

Problem 3.5. Find all subgroups of $\mathbb{Z}_{45}$ and find a generator for each. Describe the containment between these subgroups.

Solution 3.5. Note that $\mathbb{Z}_{45}$ is a cyclic group of order 45. Every subgroup of a cyclic group is also cyclic. Therefore, the number of subgroups of $\mathbb{Z}_{45}$ corresponds to the number of positive divisors of 45. Since the set of all positive divisors of 45 is

$$\{1, 3, 5, 9, 15, 45\}$$

For each divisor d of 45, there is a unique subgroup of order d , generated by an element K such that $\gcd(k, 45) = \frac{45}{d}$. Thus, the subgroups and their generators are as follows.

- Order 1: $\langle 0 \rangle = \{0\}$
- Order 3: $\langle 15 \rangle = \{0, 15, 30\}$ since $\gcd(15, 45) = 15 = \frac{45}{3}$
- Order 5: $\langle 9 \rangle = \{0, 9, 18, 27, 36\}$ since $\gcd(9, 45) = 9 = \frac{45}{5}$
- Order 9: $\langle 5 \rangle = \{0, 5, 10, 15, 20, 25, 30, 35, 40\}$
- Order 15: $\langle 3 \rangle = \{0, 3, 6, 9, \dots, 42\}$
- Order 45: $\langle 1 \rangle = \mathbb{Z}_{45}$

Note that the subgroup of order d is contained in the subgroup of order k if $d \mid k$. Therefore, we conclude that

$$\langle 0 \rangle \leq \langle 15 \rangle \leq \langle 5 \rangle \leq \langle 3 \rangle \leq \mathbb{Z}_{45} = \langle 1 \rangle.$$

Problem 3.6. If g is an element of the finite group G and $|g| = |G|$, prove that $G = \langle g \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Solution 3.6. Let $g \in G$ be an element of a finite group G with $|g| = |G|$. Since $|\langle g \rangle| = |g|$ and $|g| = |G|$ it follows that $|\langle g \rangle| = |G|$. Thus, $\langle g \rangle = G$ since $\langle g \rangle \subseteq G$.

Counterexample: Consider the infinite group $(\mathbb{Z} \times \mathbb{Z}, +)$ and the element $g = (1, 0)$. Note that the order of g and G are infinite, but

$$\langle g \rangle = \{(n, 0) \mid n \in \mathbb{Z}\} \neq \mathbb{Z} \times \mathbb{Z} = G.$$

Hence, the result need not be true in the infinite case.

Definition 3.3 (Euler's totient function). Euler's totient function denoted by $\varphi(n)$, is defined as the number of positive integers less than or equal to n that are relatively prime to n . That is,

$$\varphi(n) = |\{k \in \mathbb{Z}^+ \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|.$$

Theorem 3.4. If d is a positive divisor of n , the number of elements of order d in a cyclic group of order n is $\varphi(d)$.

PROOF. Let G be a group of order n and d be a divisor of n . By Theorem 3.3, the group G has exactly one subgroup $\langle a^{n/d} \rangle$ of order d . Then every element of order d also generates the subgroup $\langle a^d \rangle$.

By Corollary 3.5, an element a^k generates $\langle a^d \rangle$ if and only if $\gcd(k, d) = 1$. Thus, the number of such elements is precisely $\varphi(d)$. $\square$

Corollary 3.8. Let G be a finite group. Then the number of elements of order d in G is a multiple of $\varphi(d)$.

PROOF. If a finite group G has no elements of order d , then the statement is trivially true since $\varphi(d)$ divides 0. We assume that there exists an element $a \in G$ with $|a| = d$. By Theorem 3.4, the subgroup $\langle a \rangle$ has exactly $\varphi(d)$ elements of order d . If all elements of order d in G are in $\langle a \rangle$, then we are done.

Now suppose there exists an element $b \in G$ of order d such that $b \notin \langle a \rangle$. Then the subgroup $\langle b \rangle$ also has $\varphi(d)$ elements of order d . Thus, we have found $2\varphi(d)$ elements of order d if $\langle a \rangle$ and $\langle b \rangle$ have no common elements of order d . If there exists an element c of order d belonging to both $\langle a \rangle$ and $\langle b \rangle$, then $\langle a \rangle = \langle c \rangle = \langle b \rangle$. This implies that $b \in \langle a \rangle$, which is a contradiction.

Continuing in this way, we conclude that the number of elements of order d in a finite group is a multiple of $\varphi(d)$. $\square$

Problem 3.7. Let p be a prime and n be a positive integer. Show that if g is an element of the group G such that $g^{p^n} = 1$, then $|g| = p^m$ for some $m \leq n$.

Solution 3.7. Let $|g| = d$. Since $g^{p^n} = 1$, the order d divides p^n . The positive divisors of p^n are $d = p^m$ for some integer m with $0 \leq m \leq n$. Since $d > 0$, it follows that

$$|g| = p^m \quad \text{for some } m \leq n.$$

Problem 3.8. Let p be an odd prime, and let n be a positive integer. Use the Binomial Theorem to show that

$$(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$$

but

$$(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}.$$

Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution 3.8. Let p be an odd prime and $n \geq 1$. Using the Binomial Theorem, we expand

$$(1 + p)^{p^{n-1}} = 1 + \binom{p^{n-1}}{1}p + \binom{p^{n-1}}{2}p^2 + \cdots + p^{p^{n-1}}.$$

Note that $\binom{p^{n-1}}{1}p = p^{n-1} \cdot p = p^n$ is divisible by p^n . For $k \geq 2$, $\binom{p^{n-1}}{k}p^k$ is divisible by p^{n+1} . Therefore,

$$(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}.$$

Next, consider

$$(1+p)^{p^{n-2}} = 1 + \binom{p^{n-2}}{1}p + \text{terms divisible by } p^n.$$

The second term is $\binom{p^{n-2}}{1}p = p^{n-2} \cdot p = p^{n-1}$, which is not divisible by p^n . Hence,

$$(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}.$$

Thus, the order of $1+p$ modulo p^n is p^{n-1} .

Problem 3.9. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.

Solution 3.9. Consider the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ for $n \geq 3$. Note that the element -1 has order 2 since $(-1)^2 = 1$. Also

$$(2^{n-1} - 1)^2 = (2^{n-1})^2 - 2 \cdot 2^{n-1} + 1 = 2^{2n-2} - 2^n + 1.$$

By taking modulo 2^n , we get

$$(2^{n-1} - 1)^2 \equiv 1 \pmod{2^n}.$$

Hence, $2^{n-1} - 1$ also has order 2. Recall that for $n \geq 3$, $|(\mathbb{Z}/2^n\mathbb{Z})^\times| = \varphi(2^n) = 2^{n-1}$ and a cyclic group of order m has a unique subgroup of order d for each divisor d of m . But we have two distinct subgroups $\langle -1 \rangle$ and $\langle 2^{n-1} - 1 \rangle$ of order 2 as $-1 \not\equiv 2^{n-1} - 1 \pmod{2^n}$. This is not possible. Thus, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$.

Problem 3.10. Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute, i.e., $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n . Need this be true if x and y do not commute? Give an example of commuting elements x, y such that the order of xy is not equal to $\text{lcm}(|x|, |y|)$.

Solution 3.10. Assume that $|x| = n$, $|y| = m$ and $xy = yx$. Then we have

$$(xy)^{\text{lcm}(m,n)} = x^{\text{lcm}(m,n)} y^{\text{lcm}(m,n)}.$$

Since $|x| = n$ and $\text{lcm}(m, n)$ is a multiple of n , we get $x^{\text{lcm}(m,n)} = e$. Similarly, $y^{\text{lcm}(m,n)} = e$ since $\text{lcm}(m, n)$ is a multiple of m . Therefore,

$$(xy)^{\text{lcm}(m,n)} = e \cdot e = e.$$

Thus, the order of xy divides $\text{lcm}(m, n)$.

This need not hold if $xy \neq yx$. For example, we consider the group $\mathbb{Z}_4 \times \mathbb{Z}_2$. Let

$$x = (1, 0), \quad y = (1, 1).$$

Then we have

$$|x| = 4, \quad |y| = 4, \quad \text{lcm}(4, 4) = 4,$$

but $x + y = (2, 1)$ has order 2. Hence, $|x + y| = 2 \neq \text{lcm}(|x|, |y|) = 4$.

Problem 3.11. Prove that for elements x and y in any group G , we have $|x| = |yxy^{-1}|$.

Solution 3.11. Let G be a group and let $x, y \in G$. Consider the element yxy^{-1} . For any positive integer n ,

$$(yxy^{-1})^n = yx^ny^{-1}.$$

If $(yxy^{-1})^n = e$, then $yx^ny^{-1} = e$ and so $x^n = y^{-1}ey = e$. Therefore, $(yxy^{-1})^n = e$ if and only if $x^n = e$. Thus, $|yxy^{-1}| = |x|$.

3.1. Subgroups generated by sets. The process of constructing cyclic subgroups of a group G is a particular case of constructing a subgroup from a subset $A \subseteq G$. As we know, cyclic subgroups are generated by a single element in the group. In the general case, for any subset A of a group G , the subset generated by A is the smallest subgroup of G containing all elements of A . This is achieved by taking all finite products of elements of A . This idea parallels constructions in other mathematical structures, such as vector spaces, where the smallest subspace containing a set of vectors is their span. The general theme is to construct a minimal subspace containing the subset by closing it under the corresponding functions.

Proposition 3.2. If $\mathcal{A}$ is any non-empty collection of subgroups of G , then the intersection of all members of $\mathcal{A}$ is also a subgroup of G .

PROOF. Let

$$K = \bigcap_{H \in \mathcal{A}} H.$$

We want to prove that K is a subgroup of G . Since each $H \in \mathcal{A}$ is a subgroup, we have $e \in H$ and so $e \in K$. That is, $K \neq \emptyset$. Let $a, b \in K$. Then $a, b \in H$ for all $H \in \mathcal{A}$. Since each H is a group, $ab^{-1} \in H$ for all H , hence $ab^{-1} \in K$. By the subgroup test, we conclude that K is a subgroup of G . $\square$

Definition 3.4. Let A be any subset of a group G . Then the *subgroup of G generated by A* is defined by

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H.$$

Note that $\langle A \rangle$ is the intersection of all subgroups of G containing A . Also $G \in \mathcal{A}$. Therefore, $\langle A \rangle$ is a subgroup of G by Proposition 3.2 (here, $\mathcal{A} = \{H \leq G \mid A \subseteq H\}$). Since $A \subseteq H$ for all $H \in \mathcal{A}$, we have $A \subseteq \langle A \rangle$. Thus, $\langle A \rangle$ is the unique minimal element of $\mathcal{A}$ which contains A and is contained in every element of $\mathcal{A}$.

CHAPTER 3

Group Isomorphisms and Quotient Groups

"The basis for poetry and scientific discovery is the ability to comprehend the unlike in the like and the like in the unlike. "

— Jacob Bronowski

Historical notes: The ideas of group isomorphism and quotient groups developed gradually during the nineteenth century as mathematicians moved from concrete symmetries to abstract algebraic structures. Évariste Galois first recognized that different permutation groups could share the same underlying structure, anticipating the modern concept of group isomorphism. Later, Arthur Cayley formalized abstract groups and showed that every group is isomorphic to a permutation group, firmly establishing isomorphism as the correct notion of "sameness" in group theory. The concept of quotient groups emerged more slowly, beginning with Camille Jordan and later Otto Hölder, who used factor-like constructions in studying group decompositions. The recognition that only certain subgroups, now called normal subgroups, permit cosets to inherit a group structure was clarified toward the end of the century through the work of Heinrich Weber and others. By the early twentieth century, quotient groups had become a central tool in algebra, topology, and number theory, providing a systematic way to simplify groups while preserving essential structural information.

1. Homomorphisms and Isomorphisms

In this section, we formalize the idea of when two groups 'look the same', that is, when they share the same group structure. This motivates the concept of an *isomorphism* between groups. To develop this concept, we first introduce the notion of a *group homomorphism*.

Definition 1.1 (Group homomorphism). Let G and H be two groups. A *group homomorphism* is a map f from G to H that preserves the group operation, that is,

$$f(ab) = f(a)f(b) \quad \text{for all } a, b \in G.$$

Definition 1.2 (Kernel of a Homomorphism). The *kernel* of a group homomorphism $f : G \rightarrow H$ is the set

$$\ker f = \{x \in G \mid f(x) = e_H\}.$$

The kernel of f is denoted by $\ker f$.

Problem 1.1. The determinant mapping

$$\det : GL(2, \mathbb{R}) \rightarrow \mathbb{R}^*, \quad A \mapsto \det(A)$$

is a group homomorphism. The kernel of the determinant map is $SL(2, \mathbb{R})$.

Solution 1.1. Let $A, B \in GL(2, \mathbb{R})$. Note that $\det(AB) = \det(A)\det(B)$. This implies that the determinant map preserves the group operations. Thus, $\det$ is a group homomorphism.

Next, we consider the *kernel* of the determinant map

$$\ker(\det) = \{A \in GL(2, \mathbb{R}) \mid \det(A) = 1\}.$$

It is clear that, $\ker(\det) = SL(2, \mathbb{R})$.

Problem 1.2. Let $f : \mathbb{R}^* \rightarrow \mathbb{R}^*$ be a map defined by $f(x) = |x|$. Then f is a homomorphism and $\ker f = \{1, -1\}$.

Solution 1.2. Let $x, y \in \mathbb{R}^*$. Then

$$f(xy) = |xy| = |x||y| = f(x)f(y).$$

Thus, f is a group homomorphism. Note that

$$\ker f = \{x \in \mathbb{R}^* \mid |x| = 1\} = \{1, -1\}.$$

Problem 1.3. The map $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ defined by $f(m) = m \pmod{n}$ is a group homomorphism with $\ker f = n\mathbb{Z}$.

Solution 1.3. Let $m_1, m_2 \in \mathbb{Z}$. Then

$$f(m_1 + m_2) = (m_1 + m_2) \pmod{n} = (m_1 \pmod{n} + m_2 \pmod{n}) = f(m_1) + f(m_2).$$

Therefore, f is a group homomorphism. The kernel of f is

$$\ker f = \{m \in \mathbb{Z} \mid f(m) = 0 \pmod{n}\}.$$

Consider $f(m) = 0 \pmod{n}$, which implies $m \equiv 0 \pmod{n}$, that is, $m = kn$ for some $k \in \mathbb{Z}$. Thus,

$$\ker f = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}.$$

1.1. Properties of Homomorphisms.

Theorem 1.1. Let $f : G \rightarrow G'$ be a group homomorphism and g be an element of G . Then

- (1) $f(e) = e'$, where e and e' are the identity element of G and G' , respectively.
- (2) $f(g^n) = (f(g))^n$ for every $n \in \mathbb{Z}$.
- (3) Suppose $|g|$ is finite. Then $|f(g)| \mid |g|$.
- (4) $\ker f$ is a subgroup of G .
- (5) $\text{Im } f = \{f(g) \mid g \in G\}$ is a subgroup of G' .

PROOF. (1) Let e be the identity element of G and e' be the identity element of G' . Since f is a homomorphism, we have

$$f(eg) = f(e)f(g)$$

for each $g \in G$. Since $e \in G$ is the identity, we have $eg = g$ and

$$f(g) = f(e)f(g).$$

Using the group cancellation in G' , canceling $f(g)$ from both sides, we get

$$f(e) = e'.$$

Therefore, f maps the identity of G to the identity of G' .

(2) *Case i: $n > 0$*

We prove this by induction on n . For $n = 0$, we have $g^0 = e$. So, $f(g^0) = f(e) = e' = (f(g))^0$, where e' is the identity in G' .

Inductive step: Assume that $f(g^m) = (f(g))^m$ for some $m \geq 0$. Then

$$f(g^{m+1}) = f(g^m g) = f(g^m)f(g) = (f(g))^m f(g) = (f(g))^{m+1}.$$

Therefore, by induction, the property holds for all $n \in \mathbb{N} \cup \{0\}$.

Case ii: $n < 0$

Let $n = -m$ for some $m > 0$. Then

$$f(g^n) = f(g^{-m}) = f((g^{-1})^m) = (f(g^{-1}))^m.$$

Since f is a homomorphism and $f(g^{-1}) = (f(g))^{-1}$, we have

$$(f(g^{-1}))^m = ((f(g))^{-1})^m = (f(g))^{-m} = (f(g))^n.$$

Thus, $f(g^n) = (f(g))^n$ for all $n \in \mathbb{Z}$.

(3) From Property (1) and (2) and $g^n = e$, we have

$$e' = f(e) = f(g^n) = (f(g))^n.$$

Therefore, $|f(g)|$ divides n .

(4) Clearly, $\ker f$ is non-empty as $e \in \ker f$. Assume $a, b \in \ker f$. We have to show that $ab^{-1} \in \ker f$. Since $f(a) = e$ and $f(b) = e$, we have

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = ee^{-1} = e.$$

Therefore, $ab^{-1} \in \ker f$. Hence, $\ker f$ is a subgroup of G by the subgroup test.

(5) Clearly, $\text{Im } f$ is non-empty by Property (1). Let $a, b \in \text{Im } f$. Then there exist $g_1, g_2 \in G$ such that $a = f(g_1)$ and $b = f(g_2)$. We now prove that $ab^{-1} \in \text{Im } f$. Since f is a homomorphism, we have

$$ab^{-1} = f(g_1)(f(g_2))^{-1} = f(g_1)f(g_2^{-1}) = f(g_1g_2^{-1}).$$

This implies that $ab^{-1} \in \text{Im } f$ as $g_1g_2^{-1} \in G$. By the subgroup test, $\text{Im } f$ is a subgroup of G' . $\square$

Definition 1.3 (Group Isomorphism). Let G and G' be two groups. A bijective homomorphism $f : G \rightarrow G'$ is called an isomorphism. We say G and G' are isomorphic if there is an isomorphism from G to G' , and write $G \cong G'$.

Example 1.1. Let $G = (\mathbb{R}, +)$ and $G' = (\mathbb{R}^+, \cdot)$. Then $G \cong G'$ under the mapping $f(x) = 2^x$. Next, we prove f is a one-to-one map. Let $2^x = 2^y$. Then

$$\log_2 2^x = \log_2 2^y,$$

and $x = y$. To prove f is onto, we have to prove for any $y \in \mathbb{R}^+$ there exists $x \in \mathbb{R}$ such that $f(x) = y$, that is,

$$2^x = y.$$

Solving for x gives $\log_2 y$. Note that

$$f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x)f(y)$$

for all x and y in $\mathbb{R}$. This proves f is a homomorphism. Thus, f is an isomorphism.

Example 1.2. Prove that there is no isomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Q}^*, \cdot)$.

PROOF. Assume that $f : \mathbb{Q} \rightarrow \mathbb{Q}^*$ is an isomorphism. Then there exists a $a \in \mathbb{Q}$ such that $f(a) = -1$. This implies that

$$-1 = f(a) = f\left(\frac{a}{2} + \frac{a}{2}\right) = f\left(\frac{a}{2}\right)f\left(\frac{a}{2}\right) = \left[f\left(\frac{a}{2}\right)\right]^2.$$

This is not possible. Hence, there is no isomorphism from $(\mathbb{Q}, +)$ to $(\mathbb{Q}^*, \cdot)$. $\square$

Example 1.3. Let $G = \text{SL}(2, \mathbb{R})$, the group of 2×2 real matrices with determinant 1. Prove that there is an isomorphism from $\text{SL}(2, \mathbb{R})$ to itself.

PROOF. Let m be any 2×2 real matrix with determinant 1. Then we define a map $f : G \rightarrow G$ by

$$f_M(A) = MAM^{-1} \quad \text{for all } A \in G.$$

We now prove that f is one-to-one. Suppose that $f(A) = f(B)$. Then

$$MAM^{-1} = MBM^{-1}$$

and, by left and right cancellation, $A = B$. Next, we prove that f is onto. Let $B \in G$. We have to find $A \in G$ such that $f_M(A) = B$. Choose $A = M^{-1}BM$. Then $f(A) = MAM^{-1} = M(M^{-1}BM)M^{-1} = B$.

Finally, we prove f is a homomorphism. Let $A, B \in G$. Then

$$f(AB) = M(AB)M^{-1} = MA(M^{-1}M)BM^{-1} = (MAM^{-1})(MBM^{-1}) = f_M(A)f_M(B).$$

Thus, f is an isomorphism. $\square$

Definition 1.4 (Automorphism). An isomorphism from a group G onto itself is called an automorphism of G . Denote $\text{Aut}(G)$ is the set of all automorphisms of G .

Example 1.4. Consider the function $f : (\mathbb{C}, +) \rightarrow (\mathbb{C}, +)$ by $f(a + bi) = a - bi$ is an automorphism.

Example 1.5. Let $\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$. Then the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by $f(a, b) = (b, a)$ is an automorphism. Geometrically, f reflection about the line $y = x$. Note that every reflection across a line passing through $(0, 0)$ or any rotation of the plane about $(0, 0)$ is an automorphism of $\mathbb{R}^2$.

Definition 1.5 (Inner Automorphism). Let G be a group, and let $a \in G$. The function f_a defined by

$$f_a(x) = axa^{-1} \quad \text{for all } x \in G$$

is called the inner automorphism of G induced by a .

Example 1.6. The action of the inner automorphism of D induced by R_{90} is given in the following table

$$f_{R_{90}}(x) = R_{90} x R_{90}^{-1}$$

x	$f_{R_{90}}(x) = R_{90} x R_{90}^{-1}$
R_0	$R_{90} R_0 R_{90}^{-1} = R_0$
R_{90}	$R_{90} R_{90} R_{90}^{-1} = R_{90}$
R_{180}	$R_{90} R_{180} R_{90}^{-1} = R_{180}$
R_{270}	$R_{90} R_{270} R_{90}^{-1} = R_{270}$
H	$R_{90} H R_{90}^{-1} = V$
V	$R_{90} V R_{90}^{-1} = H$
D	$R_{90} D R_{90}^{-1} = D'$
D'	$R_{90} D' R_{90}^{-1} = D$

Note 1.1. The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

Theorem 1.2 (Cayley's Theorem (1854)). Every group is isomorphic to a group of permutations.

PROOF. Let G be any group. We prove that there exists a group $\mathcal{G}$ of permutations that is isomorphic to G . For any $g \in G$, we define a function $\Phi_g : G \rightarrow G$ by

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

Equivalently, Φ_g is a multiplication map by g on the left. Then Φ_g is a permutation on the set of elements of G .

Now let $\mathcal{G} = \{\Phi_g \mid g \in G\}$. Next, we prove that $\mathcal{G}$ is a group under the operation of function composition. Let $g, h \in G$, then we have

$$\Phi_g \circ \Phi_h(x) = \Phi_g(\Phi_h(x)) = \Phi_g(hx) = g(hx) = (gh)x = \Phi_{gh}(x),$$

which implies that $\Phi_g \circ \Phi_h = \Phi_{gh} \in \mathcal{G}$ as $gh \in G$. It is clear that, Φ_e is the identity map, and $\Phi_g^{-1} = \Phi_{g^{-1}}$. Thus, $\mathcal{G}$ is a group since function composition is associative.

Finally, we prove the map $f : G \rightarrow \mathcal{G}$ defined by

$$f(g) = \Phi_g \quad \text{for all } g \in G$$

is an isomorphism. If $\Phi_g = \Phi_h$, then

$$\Phi_g(e) = \Phi_h(e) \Rightarrow ge = he \Rightarrow g = h.$$

Therefore, f is one-to-one. It is clear that f is onto because of the construction of $\mathcal{G}$. Note that

$$f(ab) = \Phi_{ab} = \Phi_a \circ \Phi_b = f(a)f(b).$$

Hence, f is a group homomorphism. Thus, f is an isomorphism, and $G \cong \mathcal{G} \subseteq \text{Sym}(G)$. $\square$

Problem 1.4. The group $\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z} \right\}$ is isomorphic to what familiar group? What if $\mathbb{Z}$ is replaced by $\mathbb{R}$?

PROOF. Let

$$G = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z} \right\}$$

and consider the operation matrix multiplication. We now define a map $\varphi : \mathbb{Z} \rightarrow G$ by

$$\varphi(a) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}.$$

We prove that φ is a group isomorphism from $(\mathbb{Z}, +)$ to G .

Clearly, φ is a well-defined map. Let $\varphi(a) = \varphi(b)$. Then

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

This implies that $a = b$. Therefore, φ is injective. Next, we prove φ is surjective. Let

$$A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in G.$$

Then choose $a \in \mathbb{Z}$, and φ satisfies $\varphi(a) = A$.

Next, let $a, b \in \mathbb{Z}$. Then

$$\varphi(a + b) = \begin{bmatrix} 1 & a + b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \varphi(a)\varphi(b).$$

This shows that φ is a homomorphism. Therefore, φ is an isomorphism, and we conclude that

$$G \cong (\mathbb{Z}, +).$$

The similar argument works if we replace $\mathbb{R}$ by $\mathbb{Z}$. Thus,

$$\left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R} \right\} \cong (\mathbb{R}, +).$$

□

Problem 1.5. Prove that there are infinitely many subgroups $\mathbb{Z}$ isomorphic $\mathbb{Z}$.

PROOF. As we know that for each positive integer $n \in \mathbb{N}$, the subset

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$. Next, we define a map $\phi : \mathbb{Z} \rightarrow n\mathbb{Z}$ by $\phi(k) = nk$. Then ϕ is an isomorphism. Thus, $n\mathbb{Z} \cong \mathbb{Z}$. Since there are infinitely many positive integers n such that $n\mathbb{Z} \neq m\mathbb{Z}$ for all $n \neq m$, we conclude that there are infinitely many subgroups $\mathbb{Z}$ isomorphic $\mathbb{Z}$. □

Problem 1.6. If a group G is isomorphic to a group H , prove that $\text{Aut}(G)$ is isomorphic to $\text{Aut}(H)$.

PROOF. Let $\varphi : G \rightarrow H$ be an isomorphism. We define a map

$$\Phi : \text{Aut}(G) \rightarrow \text{Aut}(H)$$

by $\Phi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$ for all $\sigma \in \text{Aut}(G)$. It is clear that $\Phi(\sigma) \in \text{Aut}(H)$ as σ and φ are isomorphisms. Next, we prove that Φ is a homomorphism. Consider

$$\Phi(\sigma_1 \circ \sigma_2) = \varphi \circ (\sigma_1 \circ \sigma_2) \circ \varphi^{-1} = (\varphi \circ \sigma_1 \circ \varphi^{-1}) \circ (\varphi \circ \sigma_2 \circ \varphi^{-1}) = \Phi(\sigma_1) \circ \Phi(\sigma_2).$$

Therefore, Φ is a homomorphism. Next, we prove that Φ is bijective. Define a map $\Psi : \text{Aut}(H) \rightarrow \text{Aut}(G)$ by

$$\Psi(\beta) = \varphi^{-1} \circ \beta \circ \varphi.$$

Then

$$\Psi(\Phi(\sigma)) = \varphi^{-1} \circ (\varphi \circ \sigma \circ \varphi^{-1}) \circ \varphi = \sigma$$

for all $\sigma \in \text{Aut}(G)$. Also for all $\beta \in \text{Aut}(H)$, we have

$$\Phi(\Psi(\beta)) = \varphi \circ (\varphi^{-1} \circ \beta \circ \varphi) \circ \varphi^{-1} = \beta.$$

Thus, Φ and Ψ are inverse isomorphisms and conclude that Φ is a group isomorphism. Hence,

$$\text{Aut}(G) \cong \text{Aut}(H).$$

□

Problem 1.7. Let G be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g \in G$ is an automorphism if and only if G is Abelian.

PROOF. Assume that α is an automorphism. Then we have

$$\alpha(gh) = \alpha(g)\alpha(h)$$

for all $g, h \in G$. We now consider

$$\alpha(gh) = (gh)^{-1} = h^{-1}g^{-1}, \quad \text{and} \quad \alpha(g)\alpha(h) = g^{-1}h^{-1}.$$

This implies that

$$h^{-1}g^{-1} = g^{-1}h^{-1}.$$

Multiplying both sides on the right by h and on the left by g , we get $gh^{-1}g^{-1}h = 1$. Thus, $gh = hg$, and we conclude that G is Abelian.

Conversely, assume that G is Abelian. Then for all $g, h \in G$, we have

$$\alpha(gh) = (gh)^{-1} = g^{-1}h^{-1} = h^{-1}g^{-1} = \alpha(g)\alpha(h),$$

since $g^{-1}h^{-1} = h^{-1}g^{-1}$. This shows that α is a homomorphism. Clearly, the map α is a bijective with the inverse map $\alpha^{-1}(g) = g^{-1}$. Thus, α is an automorphism. □

Problem 1.8. Prove that the mapping $a \mapsto \log_{10} a$ is an isomorphism from $(\mathbb{R}^+, \cdot)$ to $(\mathbb{R}, +)$.

PROOF. We first show that φ is a group Homomorphism. Let $a, b \in \mathbb{R}^+$. Then

$$\varphi(ab) = \log_{10}(ab) = \log_{10} a + \log_{10} b = \varphi(a) + \varphi(b).$$

Therefore, φ is a homomorphism. Next, we prove φ is an injective map. Let $\varphi(a) = \varphi(b)$. Then $\log_{10} a = \log_{10} b$ and so $a = b$. Hence, φ is injective. For proving surjectivity, let $r \in \mathbb{R}$. Then choose $10^r \in \mathbb{R}^+$. Since

$$\varphi(10^r) = \log_{10}(10^r) = r,$$

it follows that φ is surjective. Thus, φ is a group isomorphism. □

Problem 1.9. Let

$$G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

and

$$H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}.$$

Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does this isomorphism preserve multiplication as well as addition?

PROOF. Define a map $\varphi : G \rightarrow H$ by

$$\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \quad \text{for all } a, b \in \mathbb{Q}.$$

We first prove that φ is an additive group isomorphism. Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ be elements of G . Then

$$\varphi(x + y) = \varphi((a + c) + (b + d)\sqrt{2}) = \begin{pmatrix} a + c & 2(b + d) \\ b + d & a + c \end{pmatrix}.$$

On the other hand

$$\varphi(x) + \varphi(y) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \begin{pmatrix} a + c & 2(b + d) \\ b + d & a + c \end{pmatrix}.$$

Thus, $\varphi(x + y) = \varphi(x) + \varphi(y)$. Next, if $\varphi(a + b\sqrt{2}) = \varphi(c + d\sqrt{2})$, then

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = \begin{pmatrix} c & 2d \\ d & c \end{pmatrix}.$$

This implies that $a = c$ and $b = d$, and so $a + b\sqrt{2} = c + d\sqrt{2}$. Thus, φ is injective. Let

$$M = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \in H.$$

Then choose $a + b\sqrt{2} \in G$ and we get $\varphi(a + b\sqrt{2}) = M$. This proves that φ is surjective. Thus, φ is an isomorphism of abelian groups.

Next, we prove that G and H are closed under multiplication. Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ in G . Then

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in G.$$

Let

$$A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}, \quad B = \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} \in H.$$

Then

$$AB = \begin{pmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{pmatrix} \in H.$$

Thus, G and H are closed under multiplication.

Note that

$$\varphi(xy) = \varphi(ac + 2bd + (ad + bc)\sqrt{2}) = \begin{pmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{pmatrix}$$

and

$$\varphi(x)\varphi(y) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + 2bd & 2(ad + bc) \\ ad + bc & ac + 2bd \end{pmatrix}.$$

Thus, $\varphi(xy) = \varphi(x)\varphi(y)$. □

2. Normal Subgroups

Let G be a group and H be a subgroup of G . Generally, it is not true that $aH = Ha$ for all $a \in G$. However, there are specific cases where this equality holds, and such cases play a fundamental role in the study of group theory. About 180 years ago, the first to recognize the importance of these special subgroups and highlight their importance in the broader structure of groups was Évariste Galois.

Definition 2.1 (Normal Subgroup). Let G be a group and H be a subgroup of G . Then H is called a *normal subgroup* of G if $aH = Ha$ for all $a \in G$ and denote by $H \triangleleft G$.

Example 2.1. Every subgroup of an Abelian group is normal.

Theorem 2.1 (Normal Subgroup Test). A subgroup H of a group G is *normal* in G if and only if

$$xHx^{-1} \subseteq H \quad \text{for every } x \in G.$$

PROOF. Assume H is normal in G , i.e. $xH = Hx$ for all $x \in G$. Let $x \in G$ and $h \in H$. Since $xH = Hx$, there exists $h' \in H$ such that $xh = h'x$. This implies that $xhx^{-1} = h' \in H$ and $xHx^{-1} \subseteq H$.

Conversely, suppose that $xHx^{-1} \subseteq H$ for every $x \in G$. Take $x = a$. Then we obtain $aHa^{-1} \subseteq H$, which implies $aH \subseteq Ha$. We now take $x = a^{-1}$. This implies that $a^{-1}Ha \subseteq H$ or equivalently $Ha \subseteq aH$. Thus, $aH = Ha$ for all $a \in G$, and hence H is normal in G . □

Example 2.2. The center $Z(G)$ of a group is always normal.

Proposition 2.1. Let $H \triangleleft G$ and $K \leq G$. Then

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

is a subgroup of G .

PROOF. Note that $e = ee \in HK$. Let $a = h_1k_1 \in HK$ and $b = h_2k_2 \in HK$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$ab^{-1} = h_1k_1(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}.$$

Since $H \triangleleft G$ and $(k_1k_2^{-1})h_2^{-1}(k_1k_2^{-1})^{-1} \in H$, we have

$$h_1(k_1k_2^{-1})h_2^{-1} = (h_1h')(k_1k_2^{-1}) \in HK$$

for some $h' \in H$. Thus, $ab^{-1} \in HK$ and HK is a subgroup of G . $\square$

Example 2.3. Suppose a group G has a unique subgroup H of finite order. Then H is a normal subgroup of G . Note that for any $g \in G$, gHg^{-1} is a subgroup of G and $|gHg^{-1}| = |H|$. Thus, gHg^{-1} must be H .

Example 2.4. The group $SL(2, \mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$. Let $A \in GL_2(\mathbb{R}) = G$, $B \in SL(2, \mathbb{R}) = H$. Then

$$\det(ABA^{-1}) = (\det A)(\det B)(\det A)^{-1} = (\det A)(\det A)^{-1} = 1.$$

Thus, $ABA^{-1} \in H$ and $AHA^{-1} \subseteq H$ by normal subgroup test.

Problem 2.1. Let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid a, b, d \in \mathbb{R}, ad \neq 0 \right\}.$$

Is H a normal subgroup of $GL_2(\mathbb{R})$?

Solution 2.1. We first prove that H is a subgroup of $GL_2(\mathbb{R})$. Let $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in H$. Since

$$A^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix}$$

is an element of H , we conclude that A is invertible. Thus, H is closed under inverses.

Clearly, H is closed under multiplication since

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \in H.$$

Next, we prove H is not normal in $GL_2(\mathbb{R})$. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H, \quad P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R}).$$

Then

$$PAP^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Hence, H is not a normal subgroup.

Problem 2.2. Let $G = GL_2(\mathbb{R})$ and $K \leq \mathbb{R}^*$. Show that

$$H = \{A \in G \mid \det A \in K\}$$

is a normal subgroup of G .

Solution 2.2. First we prove that H is a subgroup of $G = GL_2(\mathbb{R})$. Let $A, B \in H$. Then

$$\det(AB) = \det A \cdot \det B \in K,$$

since K is a subgroup of $\mathbb{R}^*$. Thus, $AB \in H$.

Next, if $A \in H$, then $\det A \in K$ implies

$$\det A^{-1} = (\det A)^{-1} \in K,$$

since K is a subgroup. Therefore, $A^{-1} \in H$. Thus, H is a subgroup of G .

Next, we prove that H is normal in G . Let $A \in H$ and $P \in G$. Then we obtain

$$\det(PAP^{-1}) = \det(P) \cdot \det(A) \cdot \det(P^{-1}) = \det(A),$$

since $\det(P^{-1}) = \frac{1}{\det(P)}$. Therefore,

$$\det(PAP^{-1}) = \det(A) \in K,$$

and hence $PAP^{-1} \in H$. Thus, H is a normal subgroup of $\text{GL}_2(\mathbb{R})$.

Problem 2.3. Prove that a factor group (quotient group) of a cyclic group is cyclic.

Solution 2.3. Let G be a cyclic group and N be a normal subgroup of G . We now prove that the factor group G/N is cyclic. As G is cyclic, there exists an element $g \in G$ such that $G = \langle g \rangle$.

We now consider the coset $gN \in G/N$. We prove that

$$G/N = \langle gN \rangle.$$

Let $xN \in G/N$. Since $G = \langle g \rangle$, we have $x = g^k$ for some integer k . Therefore,

$$xN = g^k N = (gN)^k.$$

Thus, every element of G/N is a power of gN . This shows that

$$G/N = \langle gN \rangle.$$

Hence, G/N is generated by gN and it is a cyclic group.

Problem 2.4. Prove that a factor group of an abelian group is abelian.

Solution 2.4. Let G be an abelian group and N be a normal subgroup of G . We prove that the factor group G/N is abelian.

Let $aN, bN \in G/N$ be any two cosets. Then consider

$$(aN)(bN) = abN \quad \text{and} \quad (bN)(aN) = baN.$$

Since G is abelian, we have $ab = ba$ and so

$$abN = baN.$$

Therefore,

$$(aN)(bN) = (bN)(aN).$$

Thus, G/N is an abelian group.

Problem 2.5. Let H be a normal subgroup of a group G . Then prove that the centralizer $C(H)$ of H in G is a normal subgroup of G .

Solution 2.5. Recall that the centralizer of H in G is defined by

$$C(H) = \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\}.$$

We prove that $C(H)$ is a normal subgroup of G . Let $g \in C(H)$ and $x \in G$. For $h \in H$, we have $xhx^{-1} \in H$, since H is a normal subgroup of G . Note that

$$(xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1} = xghg^{-1}x^{-1}$$

as $(xgx^{-1})^{-1} = xg^{-1}x^{-1}$. Since $g \in C(H)$, it follows that $ghg^{-1} = h$. Thus,

$$xghg^{-1}x^{-1} = xhx^{-1}.$$

Thus,

$$(xgx^{-1})(xhx^{-1})(xgx^{-1})^{-1} = xhx^{-1}$$

and we conclude that $xgx^{-1} \in C(H)$. Hence, $C(H)$ is a normal subgroup of G .

Problem 2.6. If $f : G \rightarrow G'$ be a group isomorphism, then prove that if $H \trianglelefteq G$, then $f(H) \trianglelefteq G'$.

Solution 2.6. Let $f : G \rightarrow G'$ be an isomorphism and $H \trianglelefteq G$.

Let $g' \in G'$ and $h' \in f(H)$. Then $g' = f(g)$ for some $g \in G$, and $h' = f(h)$ for some $h \in H$. This implies that

$$g'h'g'^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1}).$$

Since H is normal in G , we have $ghg^{-1} \in H$, and hence

$$f(ghg^{-1}) \in f(H).$$

Therefore, $g'h'g'^{-1} \in f(H)$ and we conclude that $f(H)$ is a normal subgroup of G' .

3. Cosets and Lagrange's Theorem

"The reader will find no figures in this work. The methods which I set forth do not require either constructions or geometrical or mechanical reasonings: but only algebraic operations, subject to a regular and uniform rule of procedure."

— Joseph-Louis Lagrange

Let G be a group and let H be a non-empty subset of G . Recall that for any $a \in G$, the set aH is defined by $\{ah \mid h \in H\}$. Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

Definition 3.1 (Cosets). Let H be a subgroup of a group G . Then the set aH is called the left coset of H in G containing a , whereas Ha is called the right coset of H in G containing a . The element a is called the coset representative of aH or Ha .

Example 3.1. Let $H = \{0, 3, 6\}$ be a subset of $\mathbb{Z}_9$ under addition. In this case, we use the notation $a + H$ instead of aH . Then the cosets of H in $\mathbb{Z}_9$ are

$$\begin{aligned} 0 + H &= \{0, 3, 6\} = 3 + H = 6 + H, \\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H, \\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H. \end{aligned}$$

Example 3.2. Let $A = \{R_0, R_{180}\}$ be a subset of D_4 , the dihedral group of order 8. Then

$$\begin{aligned} R_0A &= A, \\ R_{90}A &= \{R_{90}, R_{270}\} = R_{270}A, \\ R_{180}A &= \{R_{180}, R_0\} = A, \\ VA &= \{V, H\} = HA, \\ DA &= \{D, D'\} = D'A. \end{aligned}$$

Example 3.3. Let $G = S_3$ and $H = \{(1), (13)\}$. Then the left cosets of H in G are

$$\begin{aligned} (1)H &= H, \\ (12)H &= \{(12), (12)(13)\} = \{(12), (132)\} = (132)H, \\ (13)H &= \{(13), (1)\} = H, \\ (23)H &= \{(23), (23)(13)\} = \{(23), (123)\} = (123)H. \end{aligned}$$

Remark 3.1. From Example 3.3, we have

$$(12)H = \{(12), (132)\} \quad \text{but} \quad H(12) = \{(12), (123)\}.$$

Thus, it is not always true that $aH = Ha$.

Proposition 3.1 (Properties of Cosets). Let H be a subgroup of a group G and let $a, b \in G$. Then

- (1) $a \in aH$.
- (2) $aH = H$ if and only if $a \in H$.
- (3) $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
- (4) $aH = bH$ if and only if $a \in bH$.
- (5) $aH = bH$ or $aH \cap bH = \emptyset$.

- (6) $aH = bH$ if and only if $a^{-1}b \in H$.
- (7) $|aH| = |bH|$.
- (8) $aH = Ha$ if and only if $H = aHa^{-1}$.
- (9) aH is a subgroup of G if and only if $a \in H$.

PROOF. (1) It is clear that, $a = ae \in aH$.

- (2) Assume that $aH = H$. Then $a = ae \in aH = H$.

Conversely, assume that $a \in H$. To show that $aH \subseteq H$ and $H \subseteq aH$. Clearly, $aH \subseteq H$. Let $h \in H$. Since $a \in H$ and $h \in H$, we have $a^{-1}h \in H$. Therefore,

$$h = eh = (aa^{-1})h = a(a^{-1}h) \in aH.$$

Thus, $H \subseteq aH$ and $aH = H$.

- (3) For all $h \in H$, we have $(ab)h = a(bh)$ and $h(ab) = (ha)b$. Thus, $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
- (4) Assume that $aH = bH$. Then $a = ae \in aH = bH$. Conversely, if $a \in bH$, then $a = bh$ for some $h \in H$. Therefore,

$$aH = (bh)H = b(hH) = bH.$$

- (5) If $aH \cap bH = \emptyset$, then we are done. Otherwise, there exists an element c in $aH \cap bH$. From Property (4), we have

$$cH = aH \quad \text{and} \quad cH = bH.$$

Thus, $aH = bH$.

- (6) This result follows from Property (2), since $aH = bH$ if and only if $H = a^{-1}bH$.
- (7) We define a map f from aH to bH by $ah \mapsto bh$. Then f is onto, and f is one-to-one from the cancellation property. Thus, f is a bijective and $|aH| = |bH|$.
- (8) Note that $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H$ if and only if $aHa^{-1} = H$.
- (9) Assume that aH is a subgroup of G . Then $e \in G$, the identity element. This implies that $aH \cap eH \neq \emptyset$. From Property (5), we have $aH = eH = H$. Thus, $a \in H$ by Property (2). Conversely, assume that $a \in H$. Again by Property (2), we conclude that $aH = H$.

□

Theorem 3.1 (Lagrange's Theorem). Let G be a finite group and let H be a subgroup of G . Then $|H|$ divides $|G|$. Moreover, the number of distinct left (or right) cosets of H in G is $\frac{|G|}{|H|}$.

PROOF. Let $a_1H, a_2H, \dots, a_rH$ be the distinct left cosets of H in G . Then for every $a \in G$, $aH = a_iH$ for some i .

By Property (1) of Proposition 3.1, we have $a \in aH$. Therefore, every $g \in G$ belongs to a_iH for some a_i . Thus,

$$G = a_1H \cup a_2H \cup \dots \cup a_rH.$$

By Property (5) of Proposition 3.1, the above union is disjoint. That is,

$$|G| = |a_1H| + |a_2H| + \dots + |a_rH|.$$

As $|a_iH| = |H|$ for all i , it follows that $|G| = r|H|$. This completes the proof. □

Definition 3.2. Let G be a group and H be a subgroup of G . Then the number of left cosets of H in G is called the *index* of H in G and it is denoted by $[G : H]$.

Remark 3.2. It is clear that the index of H in G is $[G : H] = \frac{|G|}{|H|}$ if G and H are finite groups. If G is an infinite group, then the quotient $\frac{|G|}{|H|}$ does not make any sense. It is interesting to note that there are infinite groups that have finite or infinite index subgroups. For example, $\{0\}$ is of infinite index in $\mathbb{Z}$, but $\langle n \rangle$ is of index n in $\mathbb{Z}$ for all $n \in \mathbb{N}$.

Corollary 3.1. Let G be a finite group and let H be a subgroup of G . Then

$$[G : H] = \frac{|G|}{|H|}.$$

Corollary 3.2. Let G be a finite group and $g \in G$. Then $|g|$ divides $|G|$.

PROOF. We know that $|g|$ is equal to the order of the subgroup generated by g . By applying Lagrange's Theorem, we get that the order of g divides the order of G . $\square$

Corollary 3.3. A group of prime order is cyclic.

PROOF. Let G be a group with prime order. Let $e \neq a \in G$. Then $|\langle a \rangle|$ divides $|G|$ and $|\langle a \rangle| \neq 1$. Thus, $|\langle a \rangle| = |G|$. $\square$

Corollary 3.4. Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.

PROOF. By Corollary 3.2, the order of a divides the order of G . Therefore, $|G| = |a|k$ for some positive integer k . Thus,

$$a^{|G|} = a^{|a|k} = (a^{|a|})^k = e^k = e.$$

$\square$

Corollary 3.5 (Fermat's Little Theorem). For every integer a and every prime p , $a^p \equiv a \pmod{p}$.

PROOF. Let a be an integer and p be a prime. By the division algorithm, there exist q and r such that

$$a = pq + r, \quad \text{where } 0 \leq r < p.$$

Thus, $a \pmod{p} = r$ and it is enough to prove that $r^p \pmod{p} \equiv r$. If $r = 0$, the result is trivial. Assume that $r \neq 0$. Then $r \in U(p)$ (recall that $U(p) = \{1, 2, \dots, p-1\}$ is a group under multiplication modulo p).

From Corollary 3.4, we have

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

Thus,

$$a^p \equiv r^p \pmod{p} \equiv r \pmod{p} \equiv a \pmod{p}.$$

This completes the proof. $\square$

Proposition 3.2. Prove that the converse of Lagrange's theorem is false.

PROOF. Note that $|A_4| = 12$ and 6 divides 12. We now prove that A_4 has no subgroups of order 6. It is easy to see that there are 8 elements in A_4 has order 3. Assume that there exists a subgroup H of A_4 of order 6.

Let $a \in A_4$ with $|a| = 3$. If $a \notin H$, then $A_4 = H \cup aH$ as H is of index 2 in A_4 . But a^2 must be in either H or aH .

Case I: Suppose $a^2 \in H$. Then $(a^2)^2 = a^4 = a \in H$, which is a contradicts to $a \notin H$.

Case II: Suppose $a^2 \in aH$. Then $a^2 = ah$ for some $h \in H$. Therefore, $a = a^2h^{-1} \in H$, again a contradiction.

This shows that if there is a subgroup H of A_4 of order 6, then H contains all eight elements of order 3 in A_4 , which is impossible. Thus, A_4 has no subgroup of order 6. $\square$

Theorem 3.2. Let H and K be two finite subgroups of a group G . Then

$$|HK| = \frac{|H||K|}{|H \cap K|},$$

where $HK = \{hk \mid h \in H, k \in K\}$.

PROOF. Note that $|HK|$ may not be equal to $|H||K|$. That is,

$$hk = h_1k_1$$

for some $h \neq h_1$ and $k \neq k_1$. Suppose $hk = h_1k_1$. Then $h^{-1}h_1 = kk^{-1} \in H \cap K$. This implies that $h' = ht$ and $k_1 = t^{-1}k$ for some $t \in H \cap K$.

Thus, each pair (h, k) and $(ht, t^{-1}k)$ gives the same product hk for every $t \in H \cap K$. This shows that each element in HK is represented exactly $|H \cap K|$ times among the $|H||K|$ total products. Therefore,

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

□

Proposition 3.3. Let H and K be subgroups of a group G . Then HK is a subgroup of G if and only if $HK = KH$.

PROOF. Assume that HK is a subgroup of G . Since $K \leq HK$ and $H \leq HK$, and HK is closed under multiplication, it follows that

$$KH \subseteq HK.$$

Let $hk \in HK$. As HK is a subgroup, there exists $a \in HK$ such that

$$hk = a^{-1}.$$

Write $a = h_1k_1$. Then

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH.$$

This implies that $HK \subseteq KH$. Thus, $HK = KH$.

Conversely, assume that $HK = KH$. We have to prove HK is a subgroup of G . Let $a, b \in HK$ and

$$a = h_1k_1, \quad b = h_2k_2,$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$b^{-1} = (h_2k_2)^{-1} = k_2^{-1}h_2^{-1},$$

which implies

$$ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}.$$

Let $k_3 = k_1k_2^{-1} \in K$ and $h_3 = h_2^{-1} \in H$. Thus,

$$ab^{-1} = h_1k_3h_3.$$

Since $HK = KH$, there exist $h_4 \in H$, $k_4 \in K$ such that

$$k_3h_3 = h_4k_4.$$

Hence,

$$ab^{-1} = h_1h_4k_4.$$

As $h_1h_4 \in H$ and $k_4 \in K$, we have $ab^{-1} \in HK$. Thus, HK is a subgroup of G by the subgroup test. □

Remark 3.3. The equality $HK = KH$ does not imply that every element of H commute with elements of K . For example, consider the following groups $G = D_{2n}$, $H = \langle r \rangle$ and $K = \langle s \rangle$: Note that $HK = KH = G$ such that HK is a subgroup and $rs = sr^{-1}$.

Corollary 3.6. Let H and K are subgroups of G and K be a normal subgroup of G . Then HK is a subgroup of G .

PROOF. It is enough to prove $HK = KH$. Let $h \in H$, $k \in K$. By assumption, we have $hkh^{-1} \in K$. This implies that $hk = (hkh^{-1})h \in KH$. Thus, $HK \subseteq KH$. Note that

$$kh = h(h^{-1}kh) \in HK.$$

Thus, $KH \subseteq HK$, and HK is a subgroup of G by Proposition 3.2. □

Problem 3.1. Let H be a subgroup of $\mathbb{R}^*$, the group of non-zero real numbers under multiplication. If $\mathbb{R}^+ \subseteq H \subseteq \mathbb{R}^*$, prove that $H = \mathbb{R}^+$ or $H = \mathbb{R}^*$.

Solution 3.1. Note that $\mathbb{R}^* = \mathbb{R}^+ \cup (-\mathbb{R}^+)$. Suppose H is a subgroup such that $\mathbb{R}^+ \subseteq H \subseteq \mathbb{R}^*$. If H contains any real number $r < 0$, then $-1 = r/|r| \in H$ since both r and $|r|$ are in H .

Note that for all $x \in \mathbb{R}^+$, $-x = (-1)x \in H$. Therefore, $\mathbb{R}^* \subseteq H$. Hence, $H = \mathbb{R}^*$. Otherwise, H contains only positive reals, that is, $H = \mathbb{R}^+$. Thus, $H = \mathbb{R}^+$ or $H = \mathbb{R}^*$.

Problem 3.2. Prove that any group G of order $n > 2$, cannot have a subgroup H of order $n - 1$.

Solution 3.2. Assume that there exists a subgroup $H \leq G$ with $|H| = n - 1$, where $|G| = n > 2$. Then the index of H in G is

$$[G : H] = \frac{|G|}{|H|} = \frac{n}{n-1}.$$

Since the index of a subgroup H in G must be an integer, it follows that $\frac{n}{n-1}$ is an integer, which is a contradiction to $n > 2$. Thus, there is no subgroup $H \leq G$ with $|H| = n - 1$, where $|G| = n > 2$.

Problem 3.3. Prove that $(\mathbb{Q}, +)$ has no proper subgroup of finite index.

Solution 3.3. Assume that there exists a proper subgroup H of $\mathbb{Q}$ has the finite index, that is, $[\mathbb{Q} : H] = n$. Then we have

$$\mathbb{Q}/H = \{q_1 + H, q_2 + H, \dots, q_n + H\}.$$

We now consider the subset of rational numbers

$$S = \left\{0, \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\right\} \subset \mathbb{Q}.$$

Note that S has $n + 1$ elements, but there are only n cosets of H . From the pigeonhole principle, there exist distinct elements i, j with $0 \leq i < j \leq n$ such that

$$\frac{i}{n} + H = \frac{j}{n} + H.$$

This implies that $\frac{j-i}{n} \in H$. Hence, H contains a rational number of the form $\frac{1}{m}$ for some positive integer m .

Next, if $\frac{1}{m} \in H$ for some positive integer m , then for any integer $a \in \mathbb{Z}$, we have

$$\frac{a}{m} = a \cdot \frac{1}{m} \in H$$

as H is a subgroup. Therefore, H contains all rational numbers with a denominator dividing m .

Let $\frac{r}{s}$ be an arbitrary element of $\mathbb{Q}$. Since H has an element $\frac{1}{m}$ for some m and s divides ms , we can write

$$\frac{r}{s} = \frac{rm}{sm} = rm \cdot \frac{1}{sm}.$$

This implies that $\frac{1}{sm} \in H$ and hence $\frac{r}{s} \in H$. Thus, $H = \mathbb{Q}$, a contradiction. Therefore, $\mathbb{Q}$ has no proper subgroup of finite index.

Problem 3.4. Prove that if a subgroup H has index 2 in a group G , then H is a normal subgroup of G .

Solution 3.4. Assume that H is a subgroup of G and the index of H in G is 2, that is, $[G : H] = 2$. Then there exist exactly two left cosets of H in G , say H and gH . Then

$$G = H \cup gH$$

for some $g \in G \setminus H$, here the union is disjoint.

We now prove that $gHg^{-1} \subseteq H$ for all $g \in G$. Let $x \in G$. Then, either $x \in H$ or $x \notin H$. Suppose $x \in H$. Then for all $h \in H$, we have

$since H is a subgroup.$

Suppose $x \notin H$. Then $x \in G \setminus H$ and consider xhx^{-1} , where $h \in H$. Suppose $xhx^{-1} \notin H$. Then $xhx^{-1} \in xH$. This implies that

$$xhx^{-1} = xh' \quad \text{for some } h' \in H.$$

Then multiplying both sides on the left by x^{-1} , we obtain

$$hx^{-1} = h' \Rightarrow h = h'x \in Hx.$$

This is not possible as $H \cap Hx = \emptyset$. Hence, $xhx^{-1} \in H$.

Therefore, for all $x \in G$ we have $xHx^{-1} \subseteq H$. Thus, H is a normal subgroup of G .

Problem 3.5. Let $\phi(n)$ be Euler's totient function. Prove that if a is relatively prime to n , then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Solution 3.5. Let U_n be the multiplicative group of integers modulo n , i.e.,

$$U_n = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}.$$

Then U_n is a group under multiplication modulo n and the order of U_n is $\phi(n)$. As $\gcd(a, n) = 1$, it follows that the residue class of a modulo n lies in U_n and hence has a multiplicative inverse in this group.

From Lagrange's Theorem, the order of any element in a finite group divides the order of the group. Thus,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Problem 3.6. Let $H = \{a + bi \in \mathbb{C}^* \mid a^2 + b^2 = 1\}$. Give a geometric description of the coset $(3 + 4i)H$ and, more generally, $(c + di)H$.

Solution 3.6. The set H is the unit circle in the complex plane, that is H contains all complex numbers of modulus 1. Thus, $H = \{z \in \mathbb{C}^* \mid |z| = 1\}$. We now consider the coset $(3 + 4i)H = \{(3 + 4i)z \mid |z| = 1\}$ is the circle of radius 5 centered at the origin.

Thus, the geometric description of the coset $(3 + 4i)H$ is the circle of radius 5, centred at the origin (see Figure 1).

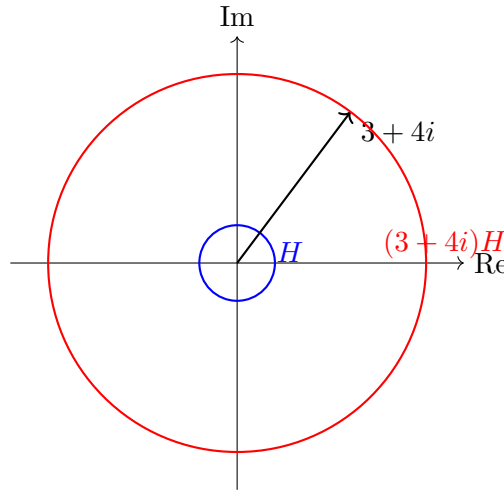


FIGURE 1. The coset $(3 + 4i)H$ as a scaled image of the unit circle H .

Problem 3.7. Let G be a group of order pq where p and q are primes. Prove that every proper subgroup of G is cyclic.

Solution 3.7. Let G be a group of order pq with $p < q$ both primes. By Lagrange's theorem, any proper subgroup has order 1, p , or q . Thus, every subgroup of order p or q is cyclic as a group of prime order is cyclic. Note that the trivial subgroup is cyclic as well. Therefore, every proper subgroup of G is cyclic.

Problem 3.8. Let G be a finite group of order n and $(m, n) = 1$. If $g \in G$ and $g^m = e$, then $g = e$.

Solution 3.8. Let $|G|=n$ and $g^m=e$. Let d be the order of g . Then $d \mid m$ and $d \mid n$. Since $\gcd(m,n)=1$, the only common divisor is 1 and hence $d=1$. Thus, $g=e$.

Problem 3.9. Prove that the finite subgroups of $\mathbb{C}^*$ are precisely the cyclic groups of complex n th roots of unity

$$\mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\} \quad \text{for } n \in \mathbb{Z}_{>0}.$$

Solution 3.9. Let $G \leq \mathbb{C}^*$ be a finite subgroup. Then every $z \in G$ satisfies $z^k = 1$ for some k . This implies that $|z|^k = 1$ and so $|z|=1$. Therefore, G is a finite subgroup of the unit circle $S^1 = \{z \in \mathbb{C} \mid |z|=1\}$. It is known that the finite subgroups of S^1 are exactly the groups of n th roots of unity

$$\mu_n = \{e^{2\pi i k/n} \mid 0 \leq k < n\}.$$

These are cyclic of order n , generated by $e^{2\pi i/n}$. Thus, the only finite subgroups of $\mathbb{C}^*$ are the cyclic groups μ_n for $n \geq 1$.

Problem 3.10. Show that in a group G of odd order, the equation $x^2 = a$ has a unique solution for all $a \in G$.

Solution 3.10. Let G be a group of odd order. Suppose $x^2 = a$ and $y^2 = a$ for some $x, y \in G$. Then

$$x^2 = y^2 \implies x^{-2}y^2 = e.$$

We can rewrite this as

$$(x^{-1}y)^2 = e.$$

Thus, $x^{-1}y$ is an element whose square is the identity, so its order divides 2. Since G has odd order, it has no non-identity element of order 2. Hence

$$x^{-1}y = e \implies x = y.$$

This shows that the solution to $x^2 = a$ is unique.

It remains to show that a solution exists for every $a \in G$. Since G has odd order, every element has a unique inverse power $x^{(n+1)/2}$ satisfying

$$\left(x^{(n+1)/2}\right)^2 = x,$$

where $n = |G|$. Applying this to a , we obtain an element x such that $x^2 = a$.

Therefore, for every $a \in G$, the equation $x^2 = a$ has a unique solution.

Problem 3.11. Let G be a group with $|G|=pqr$, where p, q , and r are distinct primes. If H and K are subgroups of G with $|H|=pq$ and $|K|=qr$, then $|H \cap K|=q$.

Solution 3.11. Let $|G|=pqr$, where $p < q < r$ are distinct primes. Let $|H|=pq$ and $|K|=qr$. We know that

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

Since $HK \leq G$, we have $|HK| \leq |G| = pqr$. Therefore, we have

$$\frac{pq \cdot qr}{|H \cap K|} \leq pqr.$$

This implies that

$$\frac{pq \cdot qr}{pqr} \leq |H \cap K| \quad \text{and so} \quad q \leq |H \cap K|.$$

Since $|H \cap K| \leq |H| = pq$ and $|K| = qr$, we have $|H \cap K|$ divides both pq and qr . The only common divisor of pq and qr is q . Thus, $|H \cap K| = q$.

4. Quotient Groups

Let G be a group, and let H be a subgroup of G . Recall that the set $gH = \{gh \mid h \in H\}$ is a *left coset* of H and $Hg = \{hg \mid h \in H\}$ is a *right coset* of H . It is natural to ask the following question. Does the set of all distinct cosets (left or right cosets) of G form a group? The answer is no! In this section, we prove that the set of all distinct cosets (left or right cosets) of a subgroup H of G forms a group if H is a normal subgroup of G .

Theorem 4.1 (O. Hölder, 1889). Let G be a group and let H be a normal subgroup of G . The set

$$G/H = \{aH \mid a \in G\}$$

is a group under the operation $(aH)(bH) = abH$.¹

PROOF. First, we prove that the operation is well-defined. Let $a, a', b, b' \in G$ and $aH = a'H$ and $bH = b'H$. We now prove that $aHbH = a'Hb'H$. That is, $abH = a'b'H$. (This shows that the definition of multiplication depends only on the cosets and not on the coset representatives.) From $aH = a'H$ and $bH = b'H$, we have $a' = ah_1$ and $b' = bh_2$ for some $h_1, h_2 \in H$. Therefore,

$$a'b'H = (ah_1)(bh_2)H = a(h_1b)H = a(h_1Hb) = aHb = abH.$$

Thus, the above operation is well-defined. Note that $eH = H$ is the identity and $a^{-1}H$ is the inverse of aH . Since

$$(aHbH)cH = (ab)HcH = (ab)cH = a(bc)H = aH(bc)H = aH(bHcH),$$

we conclude that G/H is a group. □

Remark 4.1. The converse of the above theorem holds true. That is, H is normal in G if $aHbH = abH$ is a group operation on the set of left cosets of H in G .

Example 4.1. Let $5\mathbb{Z} = \{0, \pm 5, \pm 10, \pm 15, \dots\}$. We determine the set of all left cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ to construct $\mathbb{Z}/5\mathbb{Z}$. Note that there are five cosets of $5\mathbb{Z}$ in $\mathbb{Z}$ as follows

$$\begin{aligned} 0 + 5\mathbb{Z} &= \{0, \pm 5, \pm 10, \dots\}, \\ 1 + 5\mathbb{Z} &= \{1, 6, 11, \dots; -4, -9, -14, \dots\}, \\ 2 + 5\mathbb{Z} &= \{2, 7, 12, \dots; -3, -8, -13, \dots\}, \\ 3 + 5\mathbb{Z} &= \{3, 8, 13, \dots; -2, -7, -12, \dots\}, \\ 4 + 5\mathbb{Z} &= \{4, 9, 14, \dots; -1, -6, -11, \dots\}. \end{aligned}$$

We now have the Cayley table below:

+	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$
$0 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$
$1 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$
$2 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$
$3 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$
$4 + 5\mathbb{Z}$	$4 + 5\mathbb{Z}$	$0 + 5\mathbb{Z}$	$1 + 5\mathbb{Z}$	$2 + 5\mathbb{Z}$	$3 + 5\mathbb{Z}$

Thus, $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$. In general, we can easily prove the following theorem.

Theorem 4.2. Let $n > 0$ be an integer and let

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}.$$

Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

¹The notation G/H was first used by C. Jordan.

Example 4.2. Let $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$ and $H = \{1, 17\}$. Then G/H is an Abelian group of order 8. Note that we have eight distinct left cosets, which are

$$\begin{aligned} 1H &= \{1, 17\}, \\ 3H &= \{3, 19\}, \\ 5H &= \{5, 21\}, \\ 7H &= \{7, 23\}, \\ 9H &= \{9, 25\}, \\ 11H &= \{11, 27\}, \\ 13H &= \{13, 29\}, \\ 15H &= \{15, 31\}. \end{aligned}$$

Thus, we have the quotient group G/H . Note that $(3H)^2 = 9H \neq H$. This implies that $3H$ has order at least 4. Thus, $G/H \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. It is easy to prove that $7H$ and $9H$ have order 2. Therefore, $G/H \neq \mathbb{Z}_8$ as a cyclic group of even order has unique element of order 2. Therefore, $U(32)/H \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \cong U(16)$.

Proposition 4.1. Let G be a group and let $Z(G)$ be the center of G . If $G/Z(G)$ is cyclic, then G is Abelian.

PROOF. It is sufficient to prove that $Z(G) = G$. Let $G/Z(G) = \langle gZ(G) \rangle$ and $a \in G$. Then there exists an integer i such that

$$aZ(G) = (gZ(G))^i = g^iZ(G).$$

This implies that $a = g^i z$ for some $z \in Z(G)$. Note that $a \in C(g)$ as $g^i, z \in C(g)$. Thus, $g \in Z(G)$ and so $gZ(G) = Z(G)$. Hence, $G/Z(G)$ is trivial. That is, $G = Z(G)$ and so G is abelian. $\square$

Proposition 4.2. For any group G , $G/Z(G) \cong \text{Inn}(G)$.

PROOF. Consider the map $T : G/Z(G) \rightarrow \text{Inn}(G)$ defined by $T(gZ(G)) = f_g$, where $f_g(x) = gxg^{-1}$ for all $x \in G$. We now prove that T is well defined (that is, the image of a coset of $Z(G)$ depends only on the coset itself and not on the element representing the coset). Let $gZ(G) = hZ(G)$. Then $h^{-1}g \in Z(G)$. This implies that

$$h^{-1}gx = xh^{-1}g \quad \text{for all } x \in G.$$

Therefore, $gxg^{-1} = h x h^{-1}$ for all $x \in G$. Thus, $f_g = f_h$. It is clear that T is one-to-one and T is onto. We now prove T is an operation-preserving map. It follows directly from the fact that

$$f_g \circ f_h = f_{gh} \quad \text{for all } g, h \in G.$$

Thus, $G/Z(G) \cong \text{Inn}(G)$. $\square$

Theorem 4.3 (Cauchy's Theorem for Abelian Groups). Let G be a finite abelian group and p be a prime that divides $|G|$. Then G has an element of order p .

PROOF. Let $|G| = n$. We prove this theorem by induction on n . It is clear that the statement is true for $|G| = 2$. We assume that the statement is true for all abelian groups of order less than n . Let g be any non-identity element of G . Then $|g|$ is a positive integer. By the Fundamental theorem of arithmetic, $|g|$ is divisible by some prime q . Then $|g| = qt$ for some $t \in \mathbb{N}$. Moreover, if $h = g^t$, then $|h| = q$.

If $q = p$, then we are done. If $q \neq p$, then consider the cyclic subgroup $N = \langle g \rangle$ generated by g . Since G is abelian, we have N is normal and $|N| = q$. By Lagrange's theorem, we obtain

$$|G/N| = \frac{|G|}{|N|} = \frac{n}{q}.$$

Note that $\frac{n}{q} < n$. From the induction hypothesis, the theorem is true for G/N . So, we have $|G/N| = |N||G/N| = q|G/N|$. Since $q \neq p$, we have p divides $|G/N|$. Therefore, G/N contains an element of order p , say aN . Note that

$$(aN)^p = a^p N = eN,$$

where e denotes the identity of G . Thus, $a^p \in N$. Consider

$$a^{pq} = (a^p)^q = e.$$

This implies that a must have order dividing pq .

Note that a cannot have order 1 (otherwise aN would have order 1 instead of p). Also a cannot have order q (otherwise $(aN)^q = N \Rightarrow p \mid q$), contradicting the fact that q is a prime different from p .

Thus, $|a| = p$ or $|a| = pq$. If $|a| = p$, then take $g = a$. If $|a| = pq$, then take $g = a^q$. Thus, the statement holds for abelian groups of order n . $\square$

Problem 4.1. Let $N \trianglelefteq G$, and $H \leq G$ with $N \leq H$. Prove that $H/N \trianglelefteq G/N$ if and only if $H \trianglelefteq G$.

Solution 4.1. Assume that $H/N \trianglelefteq G/N$. Let $g \in G$. Then

$$gN \cdot H/N \cdot g^{-1}N = (gHg^{-1})N \subseteq HN = H,$$

since $N \leq H$. This implies that $HN = H$. Therefore,

$$gHg^{-1} \subseteq H.$$

Thus, H is a normal subgroup of G as $g \in G$ is arbitrary.

Conversely, assume that $H \trianglelefteq G$. Then

$$gHg^{-1} \subseteq H.$$

for every $g \in G$. This implies that

$$(gN)(H/N)(g^{-1}N) = (gHg^{-1})N = HN = H$$

for all $g \in G$. Thus,

$$gN(H/N)(gN)^{-1} \subseteq H/N,$$

and we conclude that H/N is a normal subgroup of G/N .

Problem 4.2. Let G be a group, and let p be a prime number. If

$$H = \{g^p \mid g \in G\}$$

is a subgroup of G , then prove that

- (1) $H \trianglelefteq G$,
- (2) every non-identity element of G/H has order p .

Solution 4.2. (1) We have prove that $H \trianglelefteq G$. It is enough to show that $gHg^{-1} \subseteq H$ for all $g \in G$. Let $x \in H$. Then $x = a^p$ for some $a \in G$. This implies that

$$gxg^{-1} = ga^p g^{-1} = (gag^{-1})^p \in H$$

for all $g \in G$. Thus, $gHg^{-1} \subseteq H$, and hence H is normal subgroup of G .

(2) Let $g \in G$ be such that $g \notin H$, that is, $gH \neq H$. Then we consider the coset $gH \in G/H$. Note that

$$(gH)^p = g^p H.$$

Since $g^p \in H$, we have $g^p H = H$. Therefore, $(gH)^p = H$. Therefore, the order of the coset gH divides p . If $gH \neq H$, then the order must be exactly p . Thus, every non-identity element of G/H has order p .

Problem 4.3. Let G be a non-abelian group. Prove that $\text{Aut}(G)$ is not cyclic.

Solution 4.3. Assume that $\text{Aut}(G)$ is cyclic. Then every subgroup of $\text{Aut}(G)$ is cyclic and abelian. We consider the group of inner automorphisms of G defined by

$$\text{Inn}(G) = \{\varphi_g : x \mapsto gxg^{-1} \mid g \in G\}.$$

Note that $\text{Inn}(G)$ is is a normal subgroup of $\text{Aut}(G)$ and

$$\text{Inn}(G) \cong G/Z(G),$$

where $Z(G)$ is the center of G . As G is non-abelian, we have $Z(G) \subsetneq G$. This implies that $G/Z(G)$ is non-trivial. Also $G/Z(G)$ is also non-abelian as G is non-abelian. Therefore, $\text{Inn}(G) \cong G/Z(G)$ is non-abelian.

Thus, $\text{Aut}(G)$ contains a non-abelian subgroup $\text{Inn}(G)$, which is a contradiction to the assumption that $\text{Aut}(G)$ is cyclic.

Problem 4.4. Prove that the center $Z(G)$ is not a maximal subgroup of G (recall that a proper subgroup H of a group G is called *maximal* if there is no subgroup K such that $H \subsetneq K \subsetneq G$).

Solution 4.4. Assume that $Z(G)$ is a maximal subgroup of G . Then G is non-abelian since $Z(G) \leq G$. Thus, $Z(G) \subsetneq G$. Let $g \in G \setminus Z(G)$. Then G does not commute with some element $x \in G$. We now consider the centralizer of G

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

Note that $Z(G) \subseteq C_G(g)$ as all elements of the center commute with every element. Also since $g \notin Z(G)$ and $g \in C_G(g)$, we have $C_G(g)$ properly contains $Z(G)$. Note that $C_G(g) \neq G$ as G does not commute with all elements of G . Thus, we obtain

$$Z(G) \subsetneq C_G(g) \subsetneq G.$$

This contradicts the assumption that $Z(G)$ is a maximal subgroup. Hence, $Z(G)$ of a group is not a maximal subgroup of G .

5. The Isomorphism Theorems

In this section, we discuss some relations between quotient groups and homomorphisms, and straightforward consequences.

Theorem 5.1 (First Isomorphism Theorem (Jordan, 1870)). Let $f : G \rightarrow G'$ be a group homomorphism. Then the quotient group $G/\ker f$ is isomorphic to the image of f . That is,

$$G/\ker f \cong \text{Im}(f).$$

PROOF. We define a map $\varphi : G/\ker f \rightarrow \text{Im}(f)$ by

$$\varphi(g \ker f) = f(g).$$

Well-definiteness: Let $g \ker f = g' \ker f$. Then $g^{-1}g' \in \ker f$ and $f(g^{-1}g') = e$. This implies that

$$f(g)^{-1}f(g') = e \quad \text{and hence} \quad f(g) = f(g').$$

Thus, $\varphi(g \ker f) = \varphi(g' \ker f)$ and φ is well-defined.

Homomorphism: Let $g_1, g_2 \in G$. Then

$$\varphi((g_1 \ker f)(g_2 \ker f)) = \varphi(g_1 g_2 \ker f) = f(g_1 g_2) = f(g_1)f(g_2) = \varphi(g_1 \ker f) \cdot \varphi(g_2 \ker f).$$

Thus, φ is a homomorphism.

Surjectivity: Recall that $\text{Im}(f) = \{f(g) \mid g \in G\}$. Then for any $y \in \text{Im}(f)$ there exists $g \in G$ such that $f(g) = y$. Therefore, $y = \varphi(g \ker f)$ and so φ is surjective.

Injectivity: Assume that $\varphi(g \ker f) = e$. That is, $f(g) = e$. Then $g \in \ker f$, and $g \ker f = \ker f$, the identity in $G/\ker f$. Therefore, φ is injective. Thus,

$$G/\ker f \cong \text{Im}(f).$$

□

Corollary 5.1. Let f be a homomorphism from a finite group G to a finite group G' . Then $|f(G)|$ divides $|G|$ and $|G'|$.

Corollary 5.2. Let $\varphi : G \rightarrow H$ be a homomorphism of groups.

- (1) φ is injective if and only if $\ker \varphi = \{1\}$.
- (2) $[G : \ker \varphi] = |\varphi(G)|$.

Example 5.1. $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$.

Example 5.2. Let G be a group G and H be a subgroup of G . Recall that the *normalizer* of H in G is

$$N(H) = \{x \in G \mid xHx^{-1} = H\}$$

and the *centralizer* of H in G is

$$C(H) = \{x \in G \mid xhx^{-1} = h \text{ for all } h \in H\}.$$

Then consider the map $\phi : N(H) \rightarrow \text{Aut}(H)$ defined by $\phi(g) = \varphi_g$, where $\varphi_g(h) = ghg^{-1}$ for all $h \in H$, the inner automorphism of H induced by G . Then ϕ is a homomorphism with kernel $C(H)$. From Theorem 5.1, we have

$$N(H)/C(H) \cong \text{a subgroup of } \text{Aut}(H).$$

Theorem 5.2. Every normal subgroup of a group G is the kernel of a homomorphism of G . In particular, a normal subgroup N is the kernel of the mapping $g \mapsto gN$ from G to G/N .

PROOF. Let N be a normal subgroup of G . We define a map $\varphi : G \rightarrow G/N$ by $\varphi(g) = gN$. Then

$$\varphi(xy) = (xy)N = xNyN = \varphi(x)\varphi(y).$$

It is clear that, $g \in \ker \varphi$ if and only if $gN = \varphi(g) = N$ if and only if $g \in N$. Thus, N is the kernel of φ . $\square$

Definition 5.1. The map defined by $\varphi : G \rightarrow G/N$ by $\varphi(g) = gN$ is called the *natural homomorphism* from G to G/N .

Theorem 5.3 (The Second Isomorphism Theorem). Let K be a subgroup of a group G and $N \trianglelefteq G$ be a normal subgroup of G . Then

$$\frac{K}{K \cap N} \cong \frac{KN}{N}.$$

PROOF. First, we define a map $\varphi : K \rightarrow \frac{KN}{N}$ by

$$\varphi(k) = kN.$$

It is clear that φ is well-defined. Next, we prove φ is a bijective homomorphism. Let $k_1, k_2 \in K$. Then

$$\varphi(k_1k_2) = (k_1k_2)N = k_1N \cdot k_2N = \varphi(k_1)\varphi(k_2).$$

Therefore, φ is a homomorphism. Note that

$$\ker(\varphi) = \{k \in K : kN = N\} = \{k \in K : k \in N\} = K \cap N.$$

Since the image of φ is

$$\varphi(K) = \{kN : k \in K\} \subseteq KN/N$$

and for any element $kn \in KN$ (with $k \in K, n \in N$), we have $knN = kN$. Therefore, φ is a onto map. From the First Isomorphism Theorem, we obtain that

$$\frac{K}{K \cap N} \cong \frac{KN}{N}.$$

$\square$

Theorem 5.4 (Third Isomorphism Theorem). Let G be a group and $N \trianglelefteq G, M \trianglelefteq G$ such that $N \leq M$. Then

$$\frac{G/N}{M/N} \cong G/M.$$

PROOF. Consider the natural projection map $\pi : G \rightarrow G/N$ defined by $\pi(g) = gN$. Then M/N is a normal subgroup of G/N as $M \trianglelefteq G$. We now define a map $\varphi : G/N \rightarrow G/M$ by

$$\varphi(gN) = gM.$$

Assume that $gN = g'N$. Then $g^{-1}g' \in N \subseteq M$ and so $gM = g'M$. Hence, φ is well-defined. For $g_1, g_2 \in G$, we have

$$\varphi(g_1N \cdot g_2N) = \varphi(g_1g_2N) = g_1g_2M = g_1M \cdot g_2M = \varphi(g_1N)\varphi(g_2N).$$

Thus, φ is a homomorphism. Next, we consider

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

Note that for any $gM \in G/M$, we have $\varphi(gN) = gM$. So, the image of φ is G/M . From the First Isomorphism Theorem, we have

$$\frac{G/N}{M/N} \cong G/M.$$

□

Problem 5.1. Let $\mathbb{R}^*$ be the group of non-zero real numbers under multiplication, and let R be a positive integer. Define a map

$$\varphi : \mathbb{R}^* \rightarrow \mathbb{R}^*, \quad \varphi(x) = x^r.$$

- (1) Show that φ is a group homomorphism.
- (2) Determine the kernel of φ .
- (3) For which values of R is φ an isomorphism?

Solution 5.1. (1) We prove that φ is a homomorphism. Let $x, y \in \mathbb{R}^*$. Then

$$\varphi(xy) = (xy)^r = x^r y^r = \varphi(x) \cdot \varphi(y).$$

Thus, φ is a homomorphism.

(2) We need to find Kernel of φ . Note that the kernel is the set of elements mapped to the identity, that is,

$$\ker \varphi = \{x \in \mathbb{R}^* \mid x^r = 1\}.$$

Case (i): If R is odd, then the only real solution to $x^r = 1$ is $x = 1$. Thus,

$$\ker \varphi = \{1\}.$$

Case (ii): If R is even, then both $x = 1$ and $x = -1$ satisfy $x^r = 1$. Thus

$$\ker \varphi = \{1, -1\}.$$

(3) Note that φ is an isomorphism if φ is injective and surjective. As we know,

$$\ker \varphi = \{1\} \iff r \text{ is odd.}$$

Also,

- (i) if R is odd, then every $y \in \mathbb{R}^*$ has a real R th root.
- (ii) If R is even, then every negative number does not have real R th roots. In this case, φ is not surjective.

Thus, φ is an isomorphism if and only if R is odd.

Problem 5.2. Let A and B be groups. Show that the set

$$H = \{(a, 1) \mid a \in A\}$$

is a normal subgroup of $A \times B$, and that the quotient group $(A \times B)/H$ is isomorphic to B .

Solution 5.2. First we prove that $H \leq A \times B$. Let $a_1, a_2 \in A$. Then

$$(a_1, 1)(a_2, 1) = (a_1 a_2, 1) \in H,$$

and

$$(a_1, 1)^{-1} = (a_1^{-1}, 1) \in H.$$

Thus, H is a subgroup by the subgroup test.

Next, we prove that $H \trianglelefteq A \times B$. Let $(a, b) \in A \times B$, and $(x, 1) \in H$. Then

$$(a, b)(x, 1)(a, b)^{-1} = (ax, b)(a^{-1}, b^{-1}) = (axa^{-1}, 1) \in H$$

since $axa^{-1} \in A$. Thus, H is normal in $A \times B$.

Finally, we prove that $(A \times B)/H \cong B$. We define a map

$$\varphi : A \times B \rightarrow B, \quad \varphi(a, b) = b.$$

Then it is clear that φ is a surjective homomorphism since

$$\varphi((a_1, b_1)(a_2, b_2)) = \varphi(a_1a_2, b_1b_2) = b_1b_2 = \varphi(a_1, b_1) \cdot \varphi(a_2, b_2).$$

The kernel of φ is

$$\ker \varphi = \{(a, 1) \mid a \in A\} = H.$$

From the First Isomorphism Theorem, we conclude that

$$(A \times B)/H \cong B.$$

Problem 5.3. Let $f : G \rightarrow H$ and $g : H \rightarrow K$ be group homomorphisms. Define the composition $g \circ f : G \rightarrow K$ by $(g \circ f)(x) = g(f(x))$.

- (1) Show that $g \circ f$ is a group homomorphism.
- (2) How are $\ker f$ and $\ker(g \circ f)$ related?
- (3) If f and g are surjective and G is finite, describe the index $[\ker(g \circ f) : \ker(f)]$ in terms of $|H|$ and $|K|$.

Solution 5.3. (1) First, we prove that $g \circ f$ is a homomorphism. Let $x_1, x_2 \in G$. Then

$$(g \circ f)(x_1x_2) = g(f(x_1x_2)) = g(f(x_1)f(x_2)) = g(f(x_1))g(f(x_2)) = (g \circ f)(x_1)(g \circ f)(x_2).$$

Therefore, $g \circ f$ is a group homomorphism.

(2) We find a relation between $\ker f$ and $\ker(g \circ f)$. Note that

$$\ker(g \circ f) = \{x \in G \mid g(f(x)) = 1_K\}.$$

This implies that

$$\ker(g \circ f) = f^{-1}(\ker g).$$

Since

$$\ker f = \{x \in G \mid f(x) = 1_H\},$$

it is clear that

$$\ker f \subseteq \ker(g \circ f),$$

Thus,

$$\ker(g \circ f) = f^{-1}(\ker g) \quad \text{and} \quad \ker f \subseteq \ker(g \circ f).$$

(3) Let f and G be surjective and G is finite. We know that

$$|G/\ker f| = |H| \quad \text{and} \quad |G/\ker(g \circ f)| = |K|.$$

Therefore, we obtain that

$$[\ker(g \circ f) : \ker(f)] = \frac{|\ker(g \circ f)|}{|\ker(f)|} = \frac{|G/\ker(f)|}{|G/\ker(g \circ f)|} = \frac{|H|}{|K|}.$$

Problem 5.4. Let $G \leq S_n$, the symmetric group. For each $\sigma \in G$, define

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even,} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

- (1) Show that $\text{sgn} : G \rightarrow \{1, -1\}$ is a group homomorphism under multiplication.
- (2) Determine $\ker(\text{sgn})$.
- (3) Use this to show that A_n is a normal subgroup of S_n of index 2.

Solution 5.4. (1) Let $\sigma, \tau \in G$. Then the parity of $\sigma\tau$ is the sum of the parities (mod 2). Therefore,

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau).$$

Thus, sgn is a homomorphism from G to the multiplicative group $\{1, -1\}$.

(2) We now find the kernel of sgn . Note that

$$\ker(\text{sgn}) = \{\sigma \in G \mid \text{sgn}(\sigma) = 1\},$$

This shows that $\ker(\text{sgn})$ is the set of even permutations in G . In particular, if $G = S_n$, then

$$\ker(\text{sgn}) = A_n.$$

(3) Note that $\text{sgn} : S_n \rightarrow \{1, -1\}$ is a surjective homomorphism with kernel A_n . From the First Isomorphism Theorem, we have

$$S_n/A_n \cong \{1, -1\}.$$

Hence, A_n is a normal subgroup of S_n with $[S_n : A_n] = 2$. Thus, A_n is a normal subgroup of S_n of index 2.

Problem 5.5. Let G and H be groups. Define a map $\pi : G \times H \rightarrow G$ by

$$\pi(g, h) = g.$$

(1) Show that π is a group homomorphism.

(2) Determine $\ker(\pi)$.

This map is called the **projection** of $G \times H$ onto G .

Solution 5.5. (1) Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Then

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

On the other hand, we have

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

Thus,

$$\pi((g_1, h_1)(g_2, h_2)) = \pi(g_1, h_1) \cdot \pi(g_2, h_2),$$

and so π is a group homomorphism.

(2) Note that

$$\ker(\pi) = \{(g, h) \in G \times H \mid \pi(g, h) = 1_G\} = \{(1_G, h) \mid h \in H\}.$$

This shows that

$$\ker(\pi) = \{(1, h) \mid h \in H\} \cong H.$$

Problem 5.6. Let G be a subgroup of some dihedral group. For each $x \in G$, define

$$f(x) = \begin{cases} +1, & \text{if } x \text{ is a rotation,} \\ -1, & \text{if } x \text{ is a reflection.} \end{cases}$$

(1) Show that $f : G \rightarrow \{\pm 1\}$ is a group homomorphism.

(2) What is $\ker(f)$?

(3) Why does this prove that the set of all rotations in a dihedral group is a normal subgroup of index 2?

Solution 5.6. (1) Recall that D_{2n} contains rotations or reflections. Note that the product of two rotations is a rotation, and the product of two reflections is a rotation. Also the product of a rotation and a reflection (in either order) is a reflection. Hence, the map f satisfies

$$f(xy) = f(x)f(y).$$

Thus, f is a homomorphism from G to $\{\pm 1\}$.

(2) The kernel of f is

$$\ker(f) = \{x \in G \mid f(x) = +1\} \text{ (The set of all rotations in } G\text{).}$$

(3) As f is a homomorphism and $\{\pm 1\}$ has order 2, the kernel (rotations) is a normal subgroup of index 2. Thus, the set of all rotations forms a normal subgroup of the dihedral group.

Problem 5.7. Prove that $(\mathbb{Z} \times \mathbb{Z})/(\langle(a, 0)\rangle + \langle(0, b)\rangle) \cong \mathbb{Z}_a \times \mathbb{Z}_b$.

Solution 5.7. Let $G = \mathbb{Z} \times \mathbb{Z}$ and $N = \langle(a, 0)\rangle + \langle(0, b)\rangle$. Define a homomorphism

$$\varphi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b, \quad \text{by} \quad \varphi(m, n) = (m \bmod a, n \bmod b).$$

Clearly, the map φ is surjective with

$$\ker(\varphi) = \{(m, n) \in \mathbb{Z}^2 \mid a \mid m, b \mid n\} = \langle(a, 0)\rangle + \langle(0, b)\rangle = N.$$

From the First Isomorphism Theorem, we obtain that

$$(\mathbb{Z} \times \mathbb{Z})/N \cong \mathbb{Z}_a \times \mathbb{Z}_b.$$

Problem 5.8. Prove that the alternating group A_n is a normal subgroup of the symmetric group S_n , i.e., $A_n \trianglelefteq S_n$.

Solution 5.8. As we know, the alternating group A_n is a subgroup of all even permutations in S_n . We now recall the *sign homomorphism*

$$\text{sgn} : S_n \rightarrow \{1, -1\}$$

defined by

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

for all $\sigma \in S_n$. Then the map sgn is a group homomorphism since

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma) \cdot \text{sgn}(\tau).$$

for all $\sigma, \tau \in S_n$. Note that the kernel of sgn is the set of all elements $\sigma \in S_n$ such that $\text{sgn}(\sigma) = 1$. Therefore,

$$A_n = \ker(\text{sgn}).$$

Thus, the result follows from the fact that the kernel of a group homomorphism is a normal subgroup of S_n .

Problem 5.9. Suppose that $k \mid n$. Prove that $\mathbb{Z}_n/\langle k \rangle \cong \mathbb{Z}_{n/k}$.

Solution 5.9. Let $G = \mathbb{Z}_n$ and $k \mid n$. Let $H = \langle k \rangle \leq \mathbb{Z}_n$. Then the order of H is

$$|H| = \frac{n}{\gcd(k, n)} = \frac{n}{k}.$$

Therefore, the index of $\langle k \rangle$ in $\mathbb{Z}_n$ is given by

$$[G : H] = \frac{n}{n/k} = k.$$

We now define a map

$$\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{n/k} \quad \text{by} \quad \varphi([x]_n) = [x]_{n/k}.$$

Clearly, the map φ is well-defined since $x \equiv y \pmod{n/k}$ for all $x \equiv y \pmod{n}$. Also the kernel of this map φ is given by

$$\ker(\varphi) = \{x \in \mathbb{Z}_n \mid x \equiv 0 \pmod{n/k}\} = \langle k \rangle.$$

By the First Isomorphism Theorem, we conclude that

$$\mathbb{Z}_n/\langle k \rangle \cong \mathbb{Z}_{n/k}.$$

Problem 5.10. Determine all group homomorphisms $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, where $\mathbb{Z}_n$ is the cyclic group of order n under addition.

Solution 5.10. Assume that the map $\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is a group homomorphism. We know that $\mathbb{Z}_n$ is a cyclic group generated by $[1]$. Therefore, every homomorphism is determined by the image of $[1]$. Let

$$\varphi([1]) = [k] \in \mathbb{Z}_n.$$

Then

$$\varphi([m]) = \varphi([1 + 1 + \cdots + 1]) = m \cdot \varphi([1]) = [km].$$

for any $[m] \in \mathbb{Z}_n$. This implies that

$$\varphi([m]) = [km]_n.$$

Therefore, the function

$$\varphi_k([m]) = [km] \pmod{n}$$

is a homomorphism for each $k \in \mathbb{Z}_n$. Thus, the set of all homomorphisms $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ given by

$$\text{Hom}(\mathbb{Z}_n, \mathbb{Z}_n) = \{\varphi_k \mid k \in \mathbb{Z}_n\}, \quad \text{where } \varphi_k([m]) = [km]_n.$$

Remark 5.1. The map φ_k is injective if and only if $\ker \varphi_k = \{0\}$, that is, $\varphi_k([m]) = [0]$. This shows that φ_k is injective if and only if $m \equiv 0 \pmod{n}$ if and only if $\gcd(k, n) = 1$. Thus, φ_k is an isomorphism if and only if $k \in \mathbb{Z}_n^*$, the unit group modulo n . Hence,

$$\varphi_k \text{ is an automorphism} \iff \gcd(k, n) = 1.$$

Thus, we have $\phi(n)$ automorphisms, where ϕ is Euler's totient function.

Problem 5.11. Let $H = \{z \in \mathbb{C}^* : |z| = 1\}$. Prove that $\mathbb{C}^*/H \cong \mathbb{R}^+$, the group of positive real numbers under multiplication.

Solution 5.11. We define a map

$$\varphi : \mathbb{C}^* \rightarrow \mathbb{R}^+ \quad \text{by} \quad \varphi(z) = |z|.$$

Then φ is a homomorphism since

$$\varphi(z_1 z_2) = |z_1 z_2| = |z_1| |z_2| = \varphi(z_1) \varphi(z_2).$$

The kernel of φ is

$$\ker \varphi = \{z \in \mathbb{C}^* : |z| = 1\} = H.$$

Note that every positive real number r is the modulus of $r \in \mathbb{C}^*$. Therefore, the map φ is surjective. From the First Isomorphism Theorem, we conclude that

$$\mathbb{C}^*/H \cong \mathbb{R}^+.$$

Problem 5.12. Define $\varphi : \mathbb{R} \rightarrow \text{GL}(2, \mathbb{R})$ by:

$$\varphi(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}.$$

Show that φ is a group homomorphism (under addition), and determine its kernel.

Solution 5.12. First, we prove that φ is a homomorphism. Let $x, y \in \mathbb{R}$. Recall that

$$\cos(x + y) = \cos x \cos y - \sin x \sin y, \quad \sin(x + y) = \sin x \cos y + \cos x \sin y.$$

Let

$$\varphi(x) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix}, \quad \varphi(y) = \begin{bmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{bmatrix}.$$

Then we compute

$$\varphi(x)\varphi(y) = \begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} \begin{bmatrix} \cos y & \sin y \\ -\sin y & \cos y \end{bmatrix} = \begin{bmatrix} \cos(x + y) & \sin(x + y) \\ -\sin(x + y) & \cos(x + y) \end{bmatrix} = \varphi(x + y).$$

Thus, φ is a homomorphism.

The kernel of φ is given by

$$\ker(\varphi) = \{x \in \mathbb{R} \mid \varphi(x) = I\}.$$

Consider

$$\begin{bmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This implies that $\cos x = 1$ and $\sin x = 0$. Thus,

$$\ker(\varphi) = \{x \in \mathbb{R} \mid x = 2\pi n, n \in \mathbb{Z}\} = 2\pi\mathbb{Z}.$$

Problem 5.13. Show that the determinant function

$$\det : \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$$

is a surjective group homomorphism and find the kernel of the map $\det$.

PROOF. Let $A, B \in \mathrm{GL}_n(\mathbb{R})$. Then the determinant satisfies the multiplicative property

$$\det(AB) = \det(A) \cdot \det(B).$$

Thus, $\det$ is a group homomorphism.

Let $r \in \mathbb{R}^\times$. Then consider the diagonal matrix

$$D = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{R}).$$

Clearly, $\det(D) = r$. Thus, $\det$ is a surjective map. Next, we find the kernel of $\det$. Note that

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

Thus, $\det : \mathrm{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times$ is a surjective group homomorphism with kernel $\mathrm{SL}_n(\mathbb{R})$. $\square$

6. Simple Groups and Composition Series

Definition 6.1 (Simple Group). A group G (finite or infinite) is called simple if $|G| > 1$ and $\{e\}$ and G are the only normal subgroups of G .

Remark 6.1. Suppose that $|G|$ is a prime. Then by Lagrange's Theorem, $\{e\}$ and G are the only subgroups of G . Therefore, G is simple. Also for every abelian simple group is isomorphic to $\mathbb{Z}_p$, where p is a prime.

As we know, simple groups cannot be broken down into smaller normal subgroups such as n and the quotient group G/N . As a consequence, they play an important role similar to that of prime numbers in the arithmetic of the integers $\mathbb{Z}$.

Definition 6.2. Let G be a group, and let

$$(1) \quad 1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

be a sequence of subgroups. For $0 \leq i \leq k-1$, $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, then the sequence (1) is called a **composition series**.

The quotient groups N_{i+1}/N_i are called the **composition factors** of G if the above sequence (1) is a composition series.

Definition 6.3. A group G is **solvable** if there exists a chain of subgroups

$$1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_s = G$$

such that the quotient G_{i+1}/G_i is abelian for $i = 0, 1, \dots, s-1$.

Problem 6.1. Suppose G is a finite simple group and contains subgroups H and K such that $[G : H]$ and $[G : K]$ are primes. Show that $|H| = |K|$.

Solution 6.1. Assume G is a finite simple group with subgroups H and K with $[G : H] = p$ and $[G : K] = q$, where p and q are primes.

Consider the action of G on the left cosets G/H by left multiplication. We know that this action is a homomorphism

$$\varphi : G \rightarrow S_p,$$

where S_p is the symmetric group on p elements. Since G is simple and $\ker(\varphi)$ is a normal subgroup of G , it follows that either $\ker(\varphi) = G$ or $\ker(\varphi) = \{e\}$.

(i) If $\ker(\varphi) = G$, then G acts trivially on G/H , which is a contradiction.

(ii) If $\ker(\varphi) = \{e\}$, then φ is injective.

Thus, G embeds into S_p , and so $|G|$ divides $p!$. Since $[G : H] = p$ and $[G : K] = q$, we have $|G| = p \cdot |H|$ and $|G| = q \cdot |K|$. Therefore,

$$p \cdot |H| = q \cdot |K|.$$

Suppose $p = q$, then $|H| = |K|$ it is clear that $|H| = |K|$. Without loss of generality, assume that $p > q$. As $|G| = p \cdot |H|$ divides $p!$ and p is prime, it follows that $|H|$ divides $(p-1)!$. Since $p > q$, we have q does not divide $(p-1)!$. Thus, q divides $|H|$. Similarly, p divides $|K|$.

Note that $p \cdot |H| = q \cdot |K|$. This implies that p divides $|K|$. Since $p > q$ and $|K|$ divides $(q-1)!$, which is a contradiction to p cannot divide $(q-1)!$. Thus, $p = q$.

7. Transpositions and the Alternating Group

As we know, every element of the symmetric group S_n can be written as a product of disjoint cycles. Also every element in S_n can be written in different ways as a product of (not necessarily disjoint) cycles. For example, let us consider the group S_3 and the element $\alpha = (1\ 2\ 3) \in S_3$. Note that α can be written in the following ways:

$$\alpha = (1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(1\ 3)(1\ 2)(1\ 3) = (1\ 2)(2\ 3).$$

In this section, we study a special class of subgroups of S_n that consists of all permutations of length 2.

Definition 7.1 (Transposition). A 2-cycle is called a transposition.

Theorem 7.1. Every permutation is a product of transpositions.

PROOF. We know that any permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. Let

$$\sigma = \gamma_1 \gamma_2 \cdots \gamma_k,$$

where each γ_i is a disjoint cycle of length ≥ 2 . Let $\gamma = (a_1\ a_2\ \dots\ a_r)$ be a cycle of length $r \geq 2$. Then we can write

$$\gamma = (a_1\ a_r)(a_1\ a_{r-1}) \cdots (a_1\ a_2),$$

which is a product of $r-1$ transpositions. Thus, σ is a product of transpositions. $\square$

Example 7.1. Let $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$. Then we write each cycle as a product of transpositions as follows.

$$(1\ 12\ 8\ 10\ 4) = (1\ 4)(1\ 10)(1\ 8)(1\ 12),$$

$$(2\ 13) = (2\ 13),$$

$$(5\ 11\ 7) = (5\ 7)(5\ 11),$$

$$(6\ 9) = (6\ 9).$$

Thus, $\sigma = (1\ 4)(1\ 10)(1\ 8)(1\ 12)(2\ 13)(5\ 7)(5\ 11)(6\ 9)$.

Example 7.2. We can write the permutation $(1\ 2\ 3\ 4\ 5)$ as a product of translations in different ways as

$$(1\ 2\ 3\ 4\ 5) = (5\ 4)(5\ 3)(5\ 2)(5\ 1)$$

and

$$(1\ 2\ 3\ 4\ 5) = (5\ 4)(5\ 2)(2\ 1)(2\ 5)(2\ 3)(1\ 3).$$

Definition 7.2 (Even and Odd Permutations). A permutation is called an even permutation if it can be expressed as a product of an even number of 2-cycles. A permutation is called an odd permutation if it can be expressed as a product of an odd number of 2-cycles.

Example 7.3. The permutation

$$\sigma = (1\ 2\ 3) = (1\ 3)(1\ 2)$$

is an even permutation and

$$\sigma' = (1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$$

is an odd permutation.

Theorem 7.2. The set of even permutations in S_n forms a subgroup of S_n .

PROOF. Note that the identity permutation in S_n is even since it can be expressed as a product of zero transpositions. Also the product of two even permutations is even, and the inverse of an even permutation is even. Thus, by the subgroup test, the set of all even permutations in S_n forms a subgroup of S_n . $\square$

Definition 7.3 (Alternating Group of Degree n). The group of even permutations of n symbols is denoted by A_n and is called the alternating group of degree n .

Theorem 7.3. For $n > 1$, the alternating group of degree n has order $\frac{n!}{2}$.

PROOF. Note that for each odd permutation σ , the permutation $(12)\sigma$ is even. By the cancellation property of groups, we have $(12)\sigma \neq (12)\tau$ if $\sigma \neq \tau$. Thus, there are at least as many even permutations as there are odd ones. Similarly, for each even permutation σ , the permutation $(12)\sigma$ is odd and $(12)\sigma \neq (12)\tau$ if $\sigma \neq \tau$. Thus, there are at least as many odd permutations as there are even ones. Therefore, we conclude that the number of even and odd permutations is equal. As $|S_n| = n!$, it follows that $|A_n| = \frac{n!}{2}$. $\square$

Note 7.1.

- (i) The names of the symmetric group S_n and the alternating group A_n originate from the theory of polynomials in n variables. A symmetric polynomial in variables $x_1, x_2, \dots, x_n$ remains unchanged under any transposition of two variables, while an alternating polynomial changes sign under such transpositions.
- (ii) The polynomial $x_1x_2x_3$ is symmetric and the polynomial $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ is alternating. As we know that every element of S_n is a product of transpositions, symmetric polynomials are invariant under all of S_n . Alternating polynomials are invariant under A_n since they consist of even permutations.
- (iii) The permutation groups and alternating groups are fundamental in group theory. Notably, A_5 has significant historical importance.

Problem 7.1. Suppose that H is a subgroup of S_n of odd order. Prove that $H \subseteq A_n$.

Solution 7.1. We consider the restriction of the sign homomorphism $\text{sgn} : S_n \rightarrow \{\pm 1\}$ to the subgroup H of S_n defined by

$$\text{sgn}|_H : H \rightarrow \{\pm 1\}$$

Then the kernel of $\text{sgn}|_H$ is $H \cap A_n$ and the image of $\text{sgn}|_H$ is a subgroup of $\{\pm 1\}$. Since $|H|$ is odd, by Lagrange's Theorem, we have $H/(H \cap A_n) \cong \{\pm 1\}$ if $\text{sgn}|_H$ is surjective. This implies that 2 divides $|H|$, which is a contradiction. Therefore, $\text{sgn}|_H$ must be trivial, that is,

$$\text{sgn}(h) = 1 \quad \text{for all } h \in H$$

Thus, $H \subseteq A_n$.

Problem 7.2. Show that every element in A_n for $n \geq 3$ can be expressed as a 3-cycle or a product of 3-cycles.

Solution 7.2. Let $\sigma \in A_n$, the group of even permutations. Then σ can be written as a product of an even number of transpositions, say

$$\sigma = \tau_1\tau_2 \cdots \tau_{2k},$$

where each τ_i is a transposition.

Suppose $\tau_1 = (ab)$, $\tau_2 = (cd)$ are disjoint permutations. Then

$$(ab)(cd) = (acb)(bdc).$$

This is a product of two 3-cycles.

Next, let $\tau_1 = (ab)$, $\tau_2 = (bc)$ be two permutations. Then

$$(ab)(bc) = (abc),$$

which is a 3-cycle. Note that every element in A_n is a product of an even number of transpositions, and each such pair of such transpositions can be expressed as a product of 3-cycles. Thus, $\sigma \in A_n$ can be written as a product of 3-cycles.

Problem 7.3. Determine all integers n for which $H = \{\alpha \in A_n \mid \alpha^2 = e\}$ is a subgroup of A_n .

Solution 7.3. Note that the set $H = \{\alpha \in A_n \mid \alpha^2 = e\}$ contains every element of order 1 or 2 in A_n , and the identity element belongs to H . From the direct calculations, we find that if $n = 1, 2$, then $H = \{e\}$ is trivial. Moreover, for $n = 3$, we have $H = \{e\}$. But for $n = 4$, we take $\alpha = (12)(34)$ and $\beta = (13)(24)$ in A_4 . Note that α and β both are of order 2, but the product $\alpha\beta$ is a 4-cycle of order 4, which is not in H . Thus, the only integers n for which $H \leq A_n$ are $n = 1, 2, 3$.

CHAPTER 4

Group Actions

"As far as the laws of mathematics refer to reality, they are not certain, and as far as they are certain, they do not refer to reality. "

— Albert Einstein

In this section, we discuss the concept of a group acting on a set and explore several examples of such actions. The concept of "action" serves as a central theme in this text, allowing us to examine algebraic objects by investigating how they can be applied within different structures.

1. Group Actions and Permutation Representations

Definition 1.1 (Group Action). Let G be a group. An action of G on a set A is a map

$$G \times A \rightarrow A, \quad (g, a) \mapsto g \cdot a$$

satisfying the following properties

- (1) $1 \cdot a = a$ for all $a \in A$, where 1 is the identity element of G ,
- (2) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$.

We denote ga for $g \cdot a$. Let G act on A . For each $g \in G$, we define the map

$$\sigma_g : A \rightarrow A, \quad \sigma_g(a) = g \cdot a.$$

Then we prove the following.

- (i) For each $g \in G$, σ_g is a permutation of A .
 - (ii) The map $\varphi : G \rightarrow S_A$ defined by $\varphi(g) = \sigma_g$ is a group homomorphism.
- (i) We prove that σ_g is a permutation. Consider

$$(\sigma_{g^{-1}} \circ \sigma_g)(a) = \sigma_{g^{-1}}(g \cdot a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a.$$

Similarly, we can prove that

$$(\sigma_g \circ \sigma_{g^{-1}})(a) = a.$$

Thus, $\sigma_{g^{-1}}$ is the inverse of σ_g , and σ_g is a permutation.

- (ii) We prove that φ is a homomorphism. Let $\varphi(g) = \sigma_g$. Then we have

$$\varphi(g_1 g_2)(a) = \sigma_{g_1 g_2}(a) = (g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = (\varphi(g_1) \circ \varphi(g_2))(a)$$

for all $g_1, g_2 \in G$ and $a \in A$. Thus, $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$ and φ is a homomorphism.

From the above argument, we see that a group action means each $g \in G$ acts as a permutation on A compatible with the group operation. The map $\varphi : G \rightarrow S_A$ is called the *permutation representation* associated with the given action.

Conversely, if $\varphi : G \rightarrow S_A$ is any homomorphism, then the map

$$g \cdot a := \varphi(g)(a)$$

defines a group action of G on A . Thus, the set of all group actions G on a set A and the set of all homomorphisms from G into S_A are in one-to-one correspondence. Thus, we have the following result.

Proposition 1.1. Let G be a group and A be a non-empty set. Then there exists a bijection between the actions of G on A and the homomorphisms of G into S_A .

Note 1.1. Here, the group elements appear on the left, so it is a *left action*. Similarly, we can define a *right action*.

Example 1.1. Let G be a group and A a non-empty set. Let $ga = a$ for all $g \in G, a \in A$. Then it is a group action of G on A , and it is called the *trivial action* and we say G acts *trivially* on A .

Example 1.2. Let A be any non-empty set. Then the symmetric group S_A acts on A by $\sigma \cdot a = \sigma(a)$ for all $\sigma \in S_A, a \in A$. The identity map from S_A to itself is the associated permutation representation.

Example 1.3. Let us name the vertices of an n -gon. Then for all element α of D_{2n} gives a permutation σ_α of $\{1, 2, \dots, n\}$. The map from $D_{2n} \times \{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$ defined by

$$(\alpha, i) \mapsto \sigma_\alpha(i)$$

is a group action of D_{2n} on $\{1, 2, \dots, n\}$.

Example 1.4. Let G be a group and $A = G$. Then we define a map from $G \times A$ to A by $g \cdot a = ga$ for all $g \in G$ and $a \in A$. This defines a group action of G on G by left multiplication

$$g : a \mapsto ga \quad \text{for all } a \in G.$$

This action is called the *left regular action* of G on G itself. Suppose G is an additive group. Then $a \mapsto g+a$, and we call this by *left translation*.

Definition 1.2 (Kernel of the action). The *kernel* of a group action is the set of elements in G that act trivially on every element of A .

Definition 1.3 (Stabilizer of an element). For each $a \in A$, the *stabilizer* of a in G is the set G_a of elements of G that fix the element a .

Definition 1.4 (Faithful action). An action of G on A is said to be *faithful* if its kernel is the trivial subgroup, that is, consists only of the identity element of G .

Proposition 1.2. Assume that a group G is acting on the non-empty set A . Then the relation on A defined by

$$a \sim b \iff a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For every $a \in A$, the number of elements in the equivalence class which contains a is $[G : G_a]$.

PROOF. First, we prove that $\sim$ is an equivalence relation.

Reflexivity: Since $a = 1 \cdot a$ for all $a \in A$ (by axiom (2) of a group action), we have $a \sim a$.

Symmetry: Assume that $a \sim b$. Then $a = g \cdot b$ for some $g \in G$. This implies that

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = 1 \cdot b = b$$

Thus, $b \sim a$.

Transitivity: Assume that $a \sim b$ and $b \sim c$. Then $a = g \cdot b$ and $b = h \cdot c$ for some $g, h \in G$. Then

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c.$$

Thus, $a \sim c$ and the relation $\sim$ is an equivalence relation.

Next, we prove that the number of elements in the equivalence class containing a is $[G : G_a]$. Let C_a be the equivalence class of a , that is,

$$C_a = \{g \cdot a \mid g \in G\}.$$

Suppose $b = g \cdot a \in C_a$. Then gG_a is a left coset of G_a in G . We define a map

$$\phi : C_a \rightarrow G/G_a, \quad \text{by } g \cdot a \mapsto gG_a.$$

Clearly, this map is well-defined and surjective because for any $g \in G, g \cdot a \in C_a$. Next, we prove this is an injective map. If $g \cdot a = h \cdot a$, then

$$g^{-1}h \cdot a = a \Rightarrow g^{-1}h \in G_a \Rightarrow gG_a = hG_a.$$

This implies that ϕ is an injective map. Thus, ϕ is a bijection and hence

$$|C_a| = [G : G_a].$$

□

Remark 1.1. From Proposition 1.2, the group G action on the non-empty set A , partitions the set A into disjoint equivalence classes.

Definition 1.5. Let G be a group acting on a non-empty set A .

- (1) For $a \in A$, the set $\{g \cdot a \mid g \in G\}$ is called the *orbit* of a under the action of G .
- (2) The action of G on A is said to be *transitive* if there is only one orbit, that is, for any $a, b \in A$, there exists $g \in G$ such that $g \cdot a = b$.

Example 1.5. Let G be a group acting on a set A .

- (1) Suppose G acts trivially on A , i.e., $g \cdot a = a$ for all $g \in G$ and $a \in A$. Then the stabilizer of any element $a \in A$ is $G_a = G$, and the orbit of each element is the singleton set $\{a\}$. This action is transitive if and only if $|A| = 1$.
- (2) Let $G = S_n$, the symmetric group on n elements, and let $A = \{1, 2, \dots, n\}$. Then G acts transitively on A via the natural permutation action. The stabilizer of any element $i \in A$ is the subgroup $G_i \cong S_{n-1}$, and its index in G is $[G : G_i] = n = |A|$.

Problem 1.1. Let $X = \mathbb{C} \cup \{\infty\}$ and let $G = \text{GL}(2, \mathbb{C})$. Define an action of G on X by linear fractional transformations as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}, \quad z \in X,$$

where the image of ∞ is $\frac{a}{c}$ and the image of $-\frac{d}{c}$ is ∞ . Prove that this defines a group action of G on X .

Solution 1.1. First, we prove that the identity acts trivially. Note that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot z = \frac{1 \cdot z + 0}{0 \cdot z + 1} = \frac{z}{1} = z.$$

For $z = \infty$, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \infty = \frac{1}{0} = \infty,$$

by convention, since ∞ maps to a/c and here $c = 0$, so the image is ∞ . Therefore, for the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$, we have

$$I \cdot z = z \quad \text{for all } z \in X.$$

Next, we prove that compatibility. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

Then we have

$$AB = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}.$$

Next, we compute

$$(AB) \cdot z = \frac{(ae + bg)z + (af + bh)}{(ce + dg)z + (cf + dh)}.$$

On the other hand, we compute

$$B \cdot z = \frac{ez + f}{gz + h}.$$

Next, we compute

$$A \cdot \left(\frac{ez + f}{gz + h} \right) = \frac{a \cdot \frac{ez + f}{gz + h} + b}{c \cdot \frac{ez + f}{gz + h} + d} = \frac{a(ez + f) + b(gz + h)}{c(ez + f) + d(gz + h)}.$$

Simplifying the numerator and denominator, we obtain

$$A \cdot (B \cdot z) = \frac{(ae + bg)z + (af + bh)}{(ce + dg)z + (cf + dh)} = (AB) \cdot z.$$

Thus, for every $A, B \in G$ and $z \in X$, we have

$$(AB) \cdot z = A \cdot (B \cdot z).$$

Therefore, the given map defines a group action of $GL(2, \mathbb{C})$ on X by linear fractional transformations.

Problem 1.2. Prove that the orbits of an action partition the set.

Solution 1.2. Let G be a group acting on a set X . Recall that the *orbit* of x , for any $x \in X$, under the action of G is

$$\mathcal{O}_x = \{g \cdot x \mid g \in G\}.$$

We now prove that the set of all orbits forms a partition of X . That is,

- (i) every element $x \in X$ lies in some orbit,
 - (ii) if two orbits $\mathcal{O}_x$ and $\mathcal{O}_y$ have a non-empty intersection, then they are equal.
- (i) For any $x \in X$, clearly $x = e \cdot x \in \mathcal{O}_x$, since $e \in G$ is the identity element. Hence, each element of X belongs to some orbit.
- (ii) Suppose $\mathcal{O}_x \cap \mathcal{O}_y \neq \emptyset$. Then there exists some $z \in X$ such that $z \in \mathcal{O}_x$ and $z \in \mathcal{O}_y$. So there exist $g, h \in G$ such that

$$z = g \cdot x = h \cdot y.$$

Let $u \in \mathcal{O}_x$. Then $u = g' \cdot x$ for some $g' \in G$. Since $x = g^{-1} \cdot z = g^{-1} \cdot (h \cdot y)$, we can write

$$u = g' \cdot x = g' \cdot (g^{-1} \cdot (h \cdot y)) = (g'g^{-1}h) \cdot y,$$

which implies $u \in \mathcal{O}_y$. So $\mathcal{O}_x \subseteq \mathcal{O}_y$. Similarly, we obtain $\mathcal{O}_y \subseteq \mathcal{O}_x$. Thus,

$$\mathcal{O}_x = \mathcal{O}_y.$$

Problem 1.3. Let G be a group. Suppose p is the smallest prime dividing $|G|$. Show that any subgroup of index p in G is normal in G .

Solution 1.3. Let G be a group acting on the set of left cosets G/H by left multiplication

$$g \cdot xH = gxH \quad \text{for all } g, x \in G.$$

Note that this is a well-defined group action. Also this action gives a group homomorphism

$$\varphi : G \rightarrow S_p$$

defined by $\varphi(g)(xH) = gxH$. Note that the kernel of φ is given by

$$\ker(\varphi) = \bigcap_{g \in G} gHg^{-1},$$

which is the largest normal subgroup of G contained in H .

Using the First Isomorphism Theorem, we obtain that

$$G/\ker(\varphi) \cong \varphi(G).$$

Thus,

$$|G : \ker(\varphi)| = |\varphi(G)| \leq |S_p| = p!.$$

Since $\ker(\varphi) \leq H$ and $[G : H] = p$, it follows that

$$[G : \ker(\varphi)] = [G : H] \cdot [H : \ker(\varphi)] = p \cdot [H : \ker(\varphi)].$$

Hence, $|G : \ker(\varphi)|$ is divisible by p . Let

$$|\varphi(G)| = |G : \ker(\varphi)| = p \cdot m$$

for some integer $m = [H : \ker(\varphi)]$. Since p is the smallest prime dividing $|G|$ and $|\varphi(G)| \leq p!$, we have p is the smallest prime dividing $|\varphi(G)|$. Suppose $|\varphi(G)| = p \cdot m$. Then $m \geq 1$. Next, if $m > 1$, then m must

be divisible by some prime R with $r < p$, contradicting the minimality of p . Thus, $m = 1$ and $|\varphi(G)| = p$. Hence, $\ker(\varphi) = H$. Thus, $\ker(\varphi) = \bigcap_{g \in G} gHg^{-1} = H$ is a normal subgroup of G .

Problem 1.4. Let $G = \text{GL}(n, \mathbb{R})$ and $X = M_{n \times n}(\mathbb{R})$. Define an action of G on X by conjugation as follows

$$A \cdot M = AMA^{-1}, \quad \text{for all } A \in \text{GL}(n, \mathbb{R}), M \in M_{n \times n}(\mathbb{R}).$$

Prove that this defines a group action of $\text{GL}(n, \mathbb{R})$ on $M_{n \times n}(\mathbb{R})$.

Solution 1.4. We define an action of the group $G = \text{GL}(n, \mathbb{R})$ on the set $X = M_{n \times n}(\mathbb{R})$ by

$$A \cdot M = AMA^{-1}, \quad A \in \text{GL}(n, \mathbb{R}), M \in M_{n \times n}(\mathbb{R}).$$

We now prove that this is a group action.

Let I be the $n \times n$ identity matrix. Then for every $M \in M_{n \times n}(\mathbb{R})$,

$$I \cdot M = IMI^{-1} = M.$$

Thus, the identity element of the group acts as the identity transformation on X .

Next, we prove Compatibility with the group operation. Let $A, B \in \text{GL}(n, \mathbb{R})$ and let $M \in M_{n \times n}(\mathbb{R})$. Then

$$A \cdot (B \cdot M) = A(BMB^{-1})A^{-1} = (AB)M(AB)^{-1} = (AB) \cdot M.$$

Hence

$$A \cdot (B \cdot M) = (AB) \cdot M,$$

which implies that the action respects the group multiplication in $\text{GL}(n, \mathbb{R})$.

2. Cayley's Theorem

"As for everything else, so for a mathematical theory: beauty can be perceived but not explained."

— Arthur Cayley

Let G be a group and H be a subgroup of G . Denote by A the set of all left cosets of H in G . Then we define an action of G on A by

$$g \cdot aH = gaH \quad \text{for all } g \in G, aH \in A,$$

where gaH is the left coset with representative of ga . Then G acts on A by left multiplication. Suppose that $H = \{1\}$. Then $aH = \{a\}$.

Theorem 2.1. Let G be a group and let H be a subgroup of G . Let G act by left multiplication on the set A of left cosets of H in G . Let π_H be the associated permutation representation of this action. Then the following statements are true.

- (1) The action of G is transitive on A .
- (2) The stabilizer of $1H \in A$ in G is the subgroup H .
- (3) The kernel of π_H is given by

$$\ker(\pi_H) = \bigcap_{x \in G} xHx^{-1},$$

and $\ker(\pi_H)$ is the largest normal subgroup of G contained in H .

PROOF. (1) First we prove that G acts transitively on A . Let aH and bH be any two elements of A and let $g = ba^{-1}$. Then

$$g \cdot aH = (ba^{-1})aH = bH.$$

Thus, any two elements of A lie in the same orbit, that is, G acts transitively on A .

(2) Note that the stabilizer of the point $1H$ is given by

$$\{g \in G \mid g \cdot 1H = 1H\} = \{g \in G \mid gH = H\} = H.$$

Thus, the stabilizer of $1H \in A$ in G is H and H is a subgroup of H itself.

(3) Recall that the kernel is

$$\begin{aligned}\ker(\pi_H) &= \{g \in G \mid gxH = xH \text{ for all } x \in G\} \\ &= \{g \in G \mid x^{-1}gx \in H \text{ for all } x \in G\} \\ &= \{g \in G \mid g \in xHx^{-1} \text{ for all } x \in G\} \\ &= \bigcap_{x \in G} xHx^{-1}.\end{aligned}$$

Next, we assume that N is a normal subgroup of G such that $N \subseteq H$. Then for all $x \in G$, we have $xNx^{-1} = N \subseteq xHx^{-1}$. This implies that

$$N \subseteq \bigcap_{x \in G} xHx^{-1} = \ker(\pi_H).$$

Thus, $\ker(\pi_H)$ is the largest normal subgroup of G contained in H . □

Corollary 2.1 (Cayley's Theorem). Let G be a group. Then G is isomorphic to a subgroup of some symmetric group. Further, if G has a finite order n , then G is isomorphic to a subgroup of S_n .

PROOF. Let $H = \{1\}$. Then applying the above theorem, we get a homomorphism from G to S_G . Note that the kernel of this homomorphism is a subset of $H = \{1\}$. Therefore, G is isomorphic to its image in S_G . In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n . □

Corollary 2.2. Let G be a finite group of order n . Assume that p is the smallest prime dividing $|G|$. Then every subgroup of G with index p is normal.

PROOF. Assume that H is a subgroup of G with index of H in G is p . Let π_H be the permutation representation and $K = \ker(\pi_H)$. Suppose $[H : K] = k$. Then

$$[G : H][H : K] = [G : K] = pk.$$

As H has p left cosets, by the First Isomorphism Theorem, G/K is isomorphic to a subgroup of S_p . Moreover, by Lagrange's Theorem, we have $pk = |G/K|$ divides $p!$. Thus,

$$k \mid \frac{p!}{p} = (p-1)!.$$

Note that for each prime divisor of $(p-1)!$ are $< p$. From the minimality of p implies that for each prime divisor of k is $\geq p$. Thus, $k = 1$ and so $H = K$ is a normal subgroup of G . □

Remark 2.1. Note that the group A_4 has no subgroup of index 2. Therefore, a group of order n need not have a subgroup of index p .

Problem 2.1. Let p be a prime number. Prove that any group G of order $2p$ has a subgroup of order p , and that this subgroup is normal in G .

Solution 2.1. Let G be a group of order $2p$, where p is a prime. Since p divides $|G|$, G contains an element of order p by Cauchy's Theorem. Let H be the subgroup generated by such an element. Then H is a subgroup of G with $|H| = p$.

We now show that H is normal in G . The index of H in G is

$$[G : H] = \frac{|G|}{|H|} = \frac{2p}{p} = 2.$$

Any subgroup of index 2 is normal, because there are exactly two left cosets of H in G , namely H and $G \setminus H$, and any right coset of H must also be either H or $G \setminus H$. Thus, the left cosets and right cosets coincide, and hence

$$gH = Hg \quad \text{for all } g \in G.$$

This shows that H is normal in G . Therefore, G contains a subgroup of order p , and this subgroup is normal.

Problem 2.2. Let $|G| = pq$, where p and q are distinct primes. If G has a normal subgroup of order p and a normal subgroup of order q , prove that G is cyclic.

Solution 2.2. Let G be a finite group with $|G| = pq$, where p and q are distinct primes. Suppose $P \trianglelefteq G$ with $|P| = p$, and $Q \trianglelefteq G$ with $|Q| = q$. We prove that $G \cong C_{pq}$, a cyclic group of order pq .

Since $|P| = p$ and $|Q| = q$, and p and q are distinct primes, we have $\gcd(p, q) = 1$. Therefore, $PQ = \{pq \mid p \in P, q \in Q\} \subseteq G$ is a subgroup of G since P and Q are both normal in G . In particular, every element of PQ can be uniquely written as a product pq with $p \in P$, $q \in Q$. Note that $pq = qp$. Hence, $PQ \cong P \times Q$.

Therefore, $|PQ| = |P||Q| = pq = |G|$ and so $PQ = G$. Thus,

$$G \cong P \times Q \cong C_p \times C_q.$$

Since the direct product of two cyclic groups of co-prime order is cyclic, it follows that G is a cyclic group.

3. The Class Equation

Let G be a group which is acting on itself by **conjugation** as follows:

$$g \cdot a = gag^{-1} \quad \text{for all } g \in G, a \in G.$$

Note that

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot (g_2 a g_2^{-1}) = g_1 (g_2 a g_2^{-1}) g_1^{-1} \\ &= (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a, \\ 1 \cdot a &= 1 \cdot a \cdot 1^{-1} = a \end{aligned}$$

for all $a, g_1, g_2 \in G$. Therefore, this is a group action.

Definition 3.1. Two elements a and b in a group G are said to be **conjugate** in G if there exists $g \in G$ such that

$$b = gag^{-1}.$$

This implies that a and b are conjugates if and only if a and b are in the same orbit of the action of G on itself by conjugation.

The orbits of G acting on G itself by conjugation are called the **conjugacy classes** of G .

Example 3.1. (1) An action of an abelian group G on G itself by conjugation

$$g \cdot a = gag^{-1} = a \quad \text{for all } g, a \in G.$$

is the trivial action. Thus, for all $a \in G$ the conjugacy class of a is $\{a\}$.

(2) Suppose that $|G| > 1$. Then G does *not* act transitively on itself (unlike the action by left multiplication) by conjugation, since $\{1\}$ is always a conjugacy class as

$$g \cdot 1 = g1g^{-1} = 1 \quad \text{for all } g \in G.$$

More generally, the singleton set $\{a\}$ is a conjugacy class if and only if

$$gag^{-1} = a \quad \text{for every } g \in G,$$

which holds if and only if a commutes with every element of G , that is, $a \in Z(G)$, the center of G .

Group Action on the Power Set of a Group: If S is any subset of a group G , define

$$gSg^{-1} = \{gs g^{-1} \mid s \in S\}.$$

Then G acts on the set $\mathcal{P}(G)$ of all subsets of itself by defining

$$g \cdot S = gSg^{-1} \quad \text{for any } g \in G, S \in \mathcal{P}(G).$$

This definition satisfies the axioms of a group action as follows.

- **Identity:** For all $S \subseteq G$, we have

$$1 \cdot S = 1S1^{-1} = \{1s1^{-1} \mid s \in S\} = S.$$

- **Compatibility:** For all $g, h \in G$ and $S \subseteq G$, we have

$$g \cdot (h \cdot S) = g \cdot (hSh^{-1}) = g(hSh^{-1})g^{-1} = (gh)S(gh)^{-1} = (gh) \cdot S.$$

Definition 3.2. Two subsets S and T of a group G are said to be **conjugate** in G if there exists $g \in G$ such that

$$T = gSg^{-1}.$$

Therefore, S and T are conjugate if and only if S and T are in the same orbit of G acting on its subsets by conjugation.

Suppose S is a subset of G . Then by Proposition 1.2, the number of conjugates of S is equal to the index $[G : G_S]$. For the action by conjugation,

$$G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S),$$

which is the **normalizer** of S in G . Also note that $N_G(\{s\}) = C_G(s)$. We have the following proposition.

Proposition 3.1. The number of conjugates of a subset S in a group G is $[G : N_G(S)]$, the index of the normalizer of S .

$$\#\{\text{conjugates of } S\} = [G : N_G(S)].$$

In particular, the number of conjugates of an element $s \in G$ is $[G : C_G(s)]$, the index of the **centralizer** of s .

$$\#\{\text{conjugates of } s\} = [G : C_G(s)].$$

Remark 3.1. The action of G on itself by conjugation partitions G into the **conjugacy classes** of G , whose sizes can be computed using Proposition 3.1.

Theorem 3.1 (The Class Equation). Let G be a finite group and let $g_1, g_2, \dots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G . Then

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)].$$

PROOF. As we know that the singleton set $\{x\}$ is a conjugacy class of size one if and only if $x \in Z(G)$ (since $gxg^{-1} = x$ for all $g \in G$). Let $Z(G) = \{z_1 = 1, z_2, \dots, z_m\}$, and let $K_1, K_2, \dots, K_r$ be the conjugacy classes of G not in the center and g_i be a representative of K_i . Then the set of all conjugacy classes of G are

$$\{1\}, \{z_2\}, \dots, \{z_m\}, K_1, K_2, \dots, K_r.$$

Since the above sets are the partition of G , we conclude that

$$|G| = |Z(G)| + \sum_{i=1}^r |K_i| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)],$$

by Proposition 3.1. This completes the proof. $\square$

Theorem 3.2. Let p be a prime and let G be a group of order p^a for some $a \geq 1$. Then the center $Z(G)$ is non-trivial, i.e., $Z(G) \neq \{1\}$.

PROOF. From the class equation, we have

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)],$$

where $g_1, \dots, g_r$ are the distinct conjugacy class representatives not contained in the center. Note that $C_G(g_i) \neq G$ for all $i = 1, 2, \dots, r$. Therefore, the index $[G : C_G(g_i)]$ is divisible by p . As each term in the sum is divisible by p and $|G| = p^a$, we conclude that p divides $|Z(G)|$ and $Z(G) \neq \{1\}$. $\square$

Corollary 3.1. If $|G| = p^2$ for some prime p , then G is abelian. Also prove that any normal subgroup of order p lies in the center $Z(G)$ of G .

PROOF. Let G be a group of order p^2 , where p is prime. By the class equation, we know that $Z(G) \neq \{e\}$ and so $|Z(G)|$ is either p or p^2 .

Case 1: If $|Z(G)| = p^2$, then $Z(G) = G$, and hence G is abelian.

Case 2: Suppose $|Z(G)| = p$. Then $|G/Z(G)| = p$, and hence $G/Z(G)$ is cyclic. Choose $a \in G$ such that $G/Z(G) = \langle aZ(G) \rangle$. Then for any $g, h \in G$, there exist integers m, n and $x, y \in Z(G)$ such that

$$g = a^m x, \quad h = a^n y.$$

Since $x, y \in Z(G)$, they commute with a and with each other. Thus

$$gh = a^m x a^n y = a^{m+n} xy = a^n y a^m x = hg.$$

Therefore, G is abelian.

Since G is abelian, every subgroup is normal, and every element commutes with all others. Therefore, any normal subgroup of order p lies in the center $Z(G)$ of G . $\square$

Problem 3.1. Find the class equation of the group D_8 .

Solution 3.1. Recall that the group D_8 has elements

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

with defining relations $r^4 = e$, $s^2 = e$, and $srs = r^{-1}$.

We now find the conjugacy classes. Since e and r^2 commute with every element of D_8 , we have

$$\{e\}, \quad \{r^2\}.$$

Also, $srs = r^{-1} = r^3$, so r and r^3 form a conjugacy class:

$$\{r, r^3\}.$$

The reflections split into two conjugacy classes:

$$\{s, r^2s\}, \quad \{rs, r^3s\}.$$

Hence, the class equation of D_8 is

$$|D_8| = 1 + 1 + 2 + 2 + 2 = 8.$$

Problem 3.2. Let n be an odd integer of the form $2k + 1$. Show that the conjugacy classes in D_{2n} are given by

$$\{1\}, \quad \{r^{\pm 1}\}, \quad \{r^{\pm 2}\}, \quad \dots, \quad \{r^{\pm k}\}, \quad \{sr^b \mid b = 0, 1, \dots, n-1\}.$$

Find the class equation for D_{2n} .

Solution 3.2. We know that the dihedral group D_{2n} is generated by a rotation r of order n and a reflection s , with relations $r^n = 1$, $s^2 = 1$, and $srs = r^{-1}$. Here $n = 2k + 1$ is odd.

First, we find the conjugacy classes of rotations. For any integer a , we have

$$sr^a s = r^{-a}.$$

Since n is odd, $r^a \neq r^{-a}$ for every $a = 1, 2, \dots, k$. Conjugation by r does not change powers of r , so the conjugacy classes of nontrivial rotations are

$$\{r^a, r^{-a}\} \quad \text{for } a = 1, 2, \dots, k.$$

Next, we find the conjugacy classes of reflections. Every reflection has the form sr^b . Conjugating a reflection by rotations, we obtain

$$r(sr^b)r^{-1} = sr^{b+2},$$

and since n is odd, the map $b \mapsto b + 2$ permutes all exponents modulo n .

Note that the identity 1 forms its own class.

Thus, all reflections are conjugate to each other. Hence, the reflections form one class,

$$\{sr^b \mid b = 0, 1, \dots, n-1\}.$$

Collecting all conjugacy classes, we have

$$\{1\}, \quad \{r^{\pm 1}\}, \quad \{r^{\pm 2}\}, \quad \dots, \quad \{r^{\pm k}\}, \quad \{sr^b : b = 0, 1, \dots, n-1\}.$$

The sizes of these classes are

$$1, \quad 2, 2, \dots, 2 \text{ (} k \text{ times)}, \quad n.$$

Thus, the class equation of D_{2n} is

$$|D_{2n}| = 1 + 2k + n = 2n.$$

4. Automorphisms

Definition 4.1. An isomorphism from a group G onto itself is called an *automorphism* of G . Denote by $\text{Aut}(G)$ the set of all automorphisms of G .

Remark 4.1. It is easy to prove that $\text{Aut}(G)$ forms a group under composition. Note that automorphisms of a group G are permutations of G , and hence $\text{Aut}(G)$ is a subgroup of the symmetric group S_G .

Proposition 4.1. Let G be a group and H be a normal subgroup of G . Then G acts on H by conjugation defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \quad \text{for each } h \in H.$$

For every $g \in G$, conjugation by G is an automorphism of H . The permutation representation of this action is a homomorphism of G into $\text{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

PROOF. Let φ_g be conjugation by G , that is, $\varphi_g(h) = ghg^{-1}$. Since H is a normal subgroup of G , φ_g maps H to itself. As the conjugation defines a group action, it follows that

$$\varphi_e = \text{id}_H, \quad \text{and} \quad \varphi_a \circ \varphi_b = \varphi_{ab} \quad \text{for all } a, b \in G.$$

This implies that for every map φ_g is a bijection from H to itself and $\varphi_{g^{-1}}$ is the inverse of φ_g . Note that for all $h, k \in H$, we have

$$\varphi_g(hk) = g(hk)g^{-1} = (ghg^{-1})(gkg^{-1}) = \varphi_g(h)\varphi_g(k).$$

Therefore, φ_g is a homomorphism from H to H , and conclude that φ_g is an automorphism.

Note that the permutation representation $\psi : G \rightarrow S_H$ defined by $\psi(g) = \varphi_g$ is a homomorphism and the image of ψ contained in $\text{Aut}(H) \subseteq S_H$. Consider

$$\ker(\psi) = \{g \in G \mid \varphi_g = \text{id}_H\} = \{g \in G \mid ghg^{-1} = h \text{ for all } h \in H\} = C_G(H).$$

By the First Isomorphism Theorem, we conclude that

$$G/C_G(H) \cong \psi(G) \leq \text{Aut}(H).$$

□

Corollary 4.1. Let K be a subgroup of the group G and $g \in G$. Then gKg^{-1} is also a subgroup of G of the same order.

PROOF. Let $\varphi_g : G \rightarrow G$ be the map defined by $\varphi_g(x) = gxg^{-1}$. From Proposition 4.1, we have φ_g is an automorphism of G . As we know that automorphisms preserve subgroup structure and order, it follows that $\varphi_g(K) = gKg^{-1}$ is a subgroup of G and

$$|gKg^{-1}| = |K|.$$

In particular, if $x, y \in G$ are conjugate, then $y = gxg^{-1}$ for some $g \in G$, and so $|y| = |x|$ as isomorphisms preserve the order of elements. □

Corollary 4.2. Let H be a subgroup of a group G . Then the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

PROOF. Let H be a normal subgroup of $N_G(H)$. Then by Proposition 4.1 (for $G = N_G(H)$), we conclude that the conjugation map

$$\varphi : N_G(H) \rightarrow \text{Aut}(H), \quad g \mapsto (h \mapsto ghg^{-1})$$

is a group homomorphism with kernel $C_G(H)$. From the First Isomorphism Theorem, we have

$$N_G(H)/C_G(H) \cong \varphi(N_G(H)) \leq \text{Aut}(H).$$

Next, for $H = G$, we have $N_G(G) = G$ and $C_G(G) = Z(G)$. Thus,

$$G/Z(G) \cong \text{Inn}(G) \leq \text{Aut}(G).$$

□

Definition 4.2 (Inner Automorphism). Let G be a group and $g \in G$. Then the conjugation by G is called an *inner automorphism* of G . The set of all inner automorphisms is denoted by $\text{Inn}(G)$. Note that $\text{Inn}(G) \leq \text{Aut}(G)$.

Example 4.1. Let G be a group. Then G is an abelian group if and only if every inner automorphism is trivial.

Definition 4.3. A subgroup H of a group G is called *characteristic* in G if every automorphism of G maps H to itself, that is,

$$\varphi(H) = H \quad \text{for all } \varphi \in \text{Aut}(G).$$

Proposition 4.2. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\varphi(n)$, where φ is Euler's totient function.

PROOF. Let $\mathbb{Z}_n = \langle x \rangle$ for some generator $x \in \mathbb{Z}_n$. Suppose $\psi \in \text{Aut}(\mathbb{Z}_n)$. Then $\psi(x) = x^a$ for some $a \in \mathbb{Z}$ uniquely determined by ψ . Denote ψ by ψ_a . As ψ_a is an automorphism, x and x^a have the same order. Therefore, $\gcd(a, n) = 1$. Moreover, for all a coprime to n , the map $x \mapsto x^a$ is an automorphism of $\mathbb{Z}_n$. Thus, the map

$$\Psi : \text{Aut}(\mathbb{Z}_n) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \psi_a \mapsto a \pmod{n}$$

is surjective. Clearly, Ψ is injective. Since

$$\psi_a \circ \psi_b(x) = \psi_a(x^b) = (x^b)^a = x^{ab} = \psi_{ab}(x)$$

for all $\psi_a, \psi_b \in \text{Aut}(\mathbb{Z}_n)$, we have

$$\Psi(\psi_a \circ \psi_b) = \Psi(\psi_{ab}) = ab \pmod{n} = \Psi(\psi_a)\Psi(\psi_b).$$

Hence, Ψ is a homomorphism. Thus, Ψ is an isomorphism. □

Problem 4.1. Let G be a group of order pq , where p and q are primes with $p \leq q$. If $p \nmid (q-1)$, then G is abelian.

Solution 4.1. Suppose $Z(G) \neq 1$. Then by Lagrange's Theorem $G/Z(G)$ is a cyclic group and hence G is abelian.

Next, we assume $Z(G) = 1$. Note that if every non-identity element of G has order p , then the centralizer of every non-identity element has index q . From the class equation for G , we obtain

$$pq = 1 + kq.$$

But this is impossible as q does not divide 1. Thus, G has an element x of order q . Now let $H = \langle x \rangle$. Since H has index p , the smallest prime p dividing $|G|$, we conclude that the subgroup H is normal in G . As $Z(G) = 1$, it follows that $C_G(H) = H$. Therefore, $G/H = N_G(H)/C_G(H)$ is a group of order p isomorphic to a subgroup of $\text{Aut}(H)$ by Corollary 4.1. From Proposition 4.2, $\text{Aut}(H)$ has order $\varphi(q) = q-1$, which is a contradiction to $p \nmid (q-1)$. Thus, G is an abelian group.

Problem 4.2. Find the automorphisms of the group Q_8 , the quaternion group.

Solution 4.2. Note that the element -1 is the only element of order 2 in Q_8 . Hence, every automorphism of Q_8 must fix -1 .

We now consider the elements i, j, k which have order 4. Therefore, an automorphism must send i, j, k to elements of order 4, that is, to $\pm i, \pm j$, or $\pm k$.

The group Q_8 is generated by i and j , and $k = ij$. Therefore, an automorphism is completely determined by the images of i and j . Choose $\varphi(i)$ to be any element of $\{\pm i, \pm j, \pm k\}$ (6 choices). Once $\varphi(i)$ is chosen, $\varphi(j)$ can be any element of order 4 different from $\pm\varphi(i)$ (4 choices). Then $\varphi(k) = \varphi(i)\varphi(j)$ is automatically determined.

Hence,

$$|\text{Aut}(Q_8)| = 6 \times 4 = 24.$$

Thus, the automorphisms of Q_8 are obtained by permuting the elements $\pm i, \pm j, \pm k$ in a way that preserves the relation $ij = k$, and

$$\text{Aut}(Q_8) \cong S_4.$$

Problem 4.3. Find the inner automorphisms of the group D_8 , the Dihedral group of order 8.

Solution 4.3. Recall the center of D_8 is

$$Z(D_8) = \{e, r^2\}.$$

Hence, the inner automorphism induced by r^2 is trivial. An inner automorphism of D_8 is of the form

$$\varphi_g(x) = gxg^{-1}, \quad g \in D_8.$$

Thus, two elements of D_8 induce the same inner automorphism if and only if they differ by an element of the center. Therefore, the group of inner automorphisms is

$$\text{Inn}(D_8) \cong D_8/Z(D_8).$$

Since $|D_8| = 8$ and $|Z(D_8)| = 2$, we obtain

$$|\text{Inn}(D_8)| = \frac{8}{2} = 4.$$

Hence, there are exactly four inner automorphisms of D_8 . In particular,

$$\text{Inn}(D_8) \cong D_8/Z(D_8) \cong V_4,$$

the Klein four group.

Problem 4.4. Let G be a group of order 45 with a normal subgroup P of order 32. Then prove that G is abelian.

Solution 4.4. Since

$$|G| = 45 = 3^2 \cdot 5 \quad \text{and} \quad |P| = 9,$$

the subgroup P is a Sylow 3-subgroup of G . By hypothesis, P is normal in G .

The quotient group G/P has order

$$|G/P| = \frac{45}{9} = 5.$$

Hence, G/P is cyclic.

Let $g \in G$. Since G/P is cyclic, every element of G/P is of the form $(gP)^n$ for some integer n . Therefore, for any $x, y \in G$, their cosets commute in G/P , that is,

$$(xP)(yP) = (yP)(xP).$$

This implies

$$xyP = yxP,$$

and hence

$$xyx^{-1}y^{-1} \in P.$$

Since P has order 9, it is abelian. Moreover, P is normal in G , so every commutator lies in P and commutes with all elements of P . Hence, all commutators in G are trivial.

Therefore,

$$xy = yx \quad \text{for all } x, y \in G.$$

Thus, G is abelian.

5. Sylow's Theorem

In this section, we discuss the converse of Lagrange's Theorem. As a consequence, we prove some results.

Definition. Let G be a finite group and let p be a prime number.

- (1) If the order of G is p^a for some $a \geq 1$, then G is called a **p -group**. A subgroup H of G is called a **p -subgroup** if H is a p -group.
- (2) If G is a group of order $p^a m$, where $p \nmid m$, then a subgroup of order p^a is called a **Sylow p -subgroup** of G .
- (3) The set of all Sylow p -subgroups of G is denoted by $\text{Syl}_p(G)$. Also we denote $n_p(G)$ or n_p as the number of such subgroups.

Historical note: The term *Sylow p -subgroup* is named after the Norwegian mathematician **Ludvig Sylow** (1832–1918). In his 1872 paper, Sylow established fundamental results on the existence, congruence, and number of maximal p -subgroups of a finite group, which are now collectively known as *Sylow's theorems*. These theorems have formed the basis of much of modern finite group theory.

Lemma 5.1. Let $P \in \text{Syl}_p(G)$. If Q is any p -subgroup of G , then

$$Q \cap N_G(P) = Q \cap P.$$

PROOF. Let $H = Q \cap N_G(P)$. As $P \leq N_G(P)$, it follows that $P \cap Q \leq H$.

We now prove the other inclusion $H \leq P \cap Q$. From the hypothesis $H \leq Q$, so it is enough to prove that $H \leq P$. Note that PH is a subgroup of G since $H \leq N_G(P)$. Also we have

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

This shows that PH is a p -group. As $P \leq PH$, the order of PH is divisible by $|P| = p^a$, the largest power of p dividing $|G|$. Therefore, $|PH| = p^a = |P|$. Thus, $PH = P$ and so $H \leq P$. $\square$

Theorem 5.1 (Sylow's Theorem). Let G be a finite group of order $|G| = p^a m$, where p is a prime and $p \nmid m$. Then

- (1) Sylow p -subgroups of G exist, that is, $\text{Syl}_p(G) \neq \emptyset$.
- (2) If P is a Sylow p -subgroup of G and Q is any p -subgroup of G , then there exists $g \in G$ such that $Q \leq gPg^{-1}$. In particular, all Sylow p -subgroups of G are conjugate in G .
- (3) The number of Sylow p -subgroups of G satisfies

$$n_p \equiv 1 \pmod{p}.$$

In particular, n_p divides m as n_p is the index in G of the normalizer $N_G(P)$ ($n_p = [G : N_G(P)]$) for any Sylow p -subgroup P .

PROOF. (1) We Prove this by induction on $|G|$. Clearly, if $|G| = 1$, then the result is trivial. Assume that statement (1) is true for all groups of smaller order than $|G|$.

Assume that $p \mid |Z(G)|$. Then $Z(G)$ contains a subgroup N of order p by Cauchy's theorem for abelian groups. Let $\bar{G} = G/N$. Then $|\bar{G}| = p^{a-1}m$. By induction, we have $\bar{G}$ has a subgroup $\bar{P}$ of order p^{a-1} . Let $P \leq G$ be a subgroup such that $P/N = \bar{P}$. Then $|P| = |P/N| \cdot |N| = p^a$. Thus, P is a Sylow p -subgroup of G .

Next, we assume that $p \nmid |Z(G)|$. Then consider the class equation

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)],$$

where $g_1, \dots, g_r$ are representatives of the distinct non-central conjugacy classes. Note that if $p \mid [G : C_G(g_i)]$ for all i , then $p \mid |Z(G)|$, a contradiction. Therefore, there exists i such that $p \nmid [G : C_G(g_i)]$. Let $H = C_G(g_i)$. Then $|H| < |G|$ (as $g_i \notin Z(G)$) and $|H| = p^a k$, where $p \nmid k$. Again, by induction, H has a Sylow p -subgroup P . As $|P| = p^a$, it follows that P is a Sylow p -subgroup of G .

(2) Let P be a Sylow p -subgroup of G (by (1)). Denote $S = \{gPg^{-1} \mid g \in G\}$ by possible set of all its conjugates with $|S| = n_p = r$. Let Q be any p -subgroup of G . The group Q acts on S by conjugation. Write $S = \bigsqcup_{i=1}^s \mathcal{O}_i$ as the disjoint union of Q -orbits. Choose a representatives $P_i \in \mathcal{O}_i$ for $i = 1, 2, \dots, s$. Then

$$|\mathcal{O}_i| = [Q : N_Q(P_i)] = [Q : Q \cap P_i]$$

since $N_Q(P_i) = N_G(P_i) \cap Q$ (by Lemma 5.1). Let $Q = P_1$. Then $|\mathcal{O}_1| = 1$. Also for all $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$ and hence $|\mathcal{O}_i| > 1$ for all $i > 1$ (since P_1 is a p -group). Thus,

$$r = \sum_{i=1}^s |\mathcal{O}_i| \equiv 1 \pmod{p}.$$

Now assume that Q is not contained in any conjugate of P . Then $Q \cap P_i < Q$ for all i . Therefore, $|\mathcal{O}_i| > 1$ and $p \mid |\mathcal{O}_i|$, which is a contradiction to $r \equiv 1 \pmod{p}$ (here, r does not depend on the choice of Q). Thus, $Q \leq gPg^{-1}$ for some $g \in G$.

(3) From (2), for all Sylow p -subgroups are conjugate. Therefore, the set $\text{Syl}_p(G) = S$ and $n_p = r \equiv 1 \pmod{p}$. Thus,

$$n_p = [G : N_G(P)]$$

and hence n_p divides $|G| = p^a m$. Finally, we conclude that $n_p \mid m$ as $p \nmid n_p$. This completes the proof. $\square$

Corollary 5.1. Let P be a Sylow p -subgroup of G . Then the following are equivalent

- (1) P is the unique Sylow p -subgroup of G , that is, $n_p = 1$.
- (2) P is a normal subgroup of G .
- (3) P is characteristic in G .
- (4) Every subgroups generated by elements of p -power order are p -groups. That is, if $X \subseteq G$ such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p -group.

PROOF. (1) $\Rightarrow$ (2) Assume that P is the unique Sylow p -subgroup of G . Then $gPg^{-1} = P$ for all $g \in G$ as $gPg^{-1} \in \text{Syl}_p(G)$. Thus, P is normal in G .

(2) $\Rightarrow$ (1) Suppose P normal in G and $Q \in \text{Syl}_p(G)$. Then there exists $g \in G$ such that $Q = gPg^{-1} = P$ by Sylow's Theorem. Thus, $\text{Syl}_p(G) = \{P\}$.

(3) $\Rightarrow$ (2) It is clear that characteristic subgroups are normal.

(2) $\Rightarrow$ (3) Assume that P is normal in G . Then P is the unique subgroup of G of order p^a . Thus, P is characteristic in G .

(1) $\Rightarrow$ (4) Assume that the statement (1) holds. Let $X \subseteq G$ such that $|x| = p^k$ (for some integer k) for all $x \in X$. Then for all $x \in X$ there exists $g \in G$ such that $x \in gPg^{-1} = P$ from the conjugacy part of Sylow's theorem (Theorem 5.1 (2)). Thus, $X \subseteq P$ and so $\langle X \rangle \subseteq P$, which is a p -group. Thus, $\langle X \rangle$ is a p -group.

(4) $\Rightarrow$ (1) We now assume that (4) holds. Let X be the union of all Sylow p -subgroups of G . Note that if $P \in \text{Syl}_p(G)$, then $P \subseteq \langle X \rangle$, which is a p -group. As P is a p -subgroup of maximal order, we have $P = \langle X \rangle$. Hence, there is only one Sylow p -subgroup. $\square$

Remark 5.1. Let G be a finite group and p be a prime.

- (1) Suppose $p \nmid |G|$. Then the Sylow p -subgroup of G is the trivial group.
- (2) If $|G| = p^a$, then G itself is the unique Sylow p -subgroup of G .

Example 5.1. (a) The symmetric group S_3 has three Sylow 2-subgroups which are $H_1 = \langle (1\ 2) \rangle$, $H_2 = \langle (2\ 3) \rangle$ and $H_3 = \langle (1\ 3) \rangle$. Also S_3 has a unique Sylow 3-subgroup $A_3 = \langle (1\ 2\ 3), (1\ 3\ 2), e \rangle$ and hence A_3 is normal in S_3 . Note that $3 \equiv 1 \pmod{2}$.

(b) The alternating group A_4 has a unique Sylow 2-subgroup

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4.$$

Also A_4 has four Sylow 3-subgroups which are $\{(123), (132)\}$, $\{(124), (142)\}$, $\{(134), (143)\}$, and $\{(234), (243)\}$. Note that $4 \equiv 1 \pmod{3}$.

(c) The symmetric group S_4 has $n_2 = 3$ and $n_3 = 4$. As S_4 contains a subgroup isomorphic to D_8 (the dihedral group of order 8), it follows that every Sylow 2-subgroup of S_4 is isomorphic to D_8 .

Problem 5.1. Find all the Sylow 3-subgroups of the symmetric group S_4 .

Solution 5.1. We know that $|S_4| = 24$ and a Sylow 3-subgroup has order equal to the largest power of 3 dividing 24, which is $3^1 = 3$. By Sylow's theorems, the number of Sylow 3-subgroups is given by

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 24.$$

Thus, $n_3 \in \{1, 4\}$. Next, we find all the elements of S_4 with order 3. Note that elements of order 3 in S_4 are precisely the following 3-cycles

$$(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3).$$

Note that every cyclic subgroup of order 3 contains exactly two non-identity elements, as the group is cyclic of order 3. Therefore, the number of distinct subgroups of order 3 is

$$\frac{8}{2} = 4.$$

Thus, $n_3 = 4$, and we have the following Sylow 3-subgroups of S_4

$$\begin{aligned} P_1 &= \langle (1\ 2\ 3) \rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ P_2 &= \langle (1\ 2\ 4) \rangle = \{e, (1\ 2\ 4), (1\ 4\ 2)\}, \\ P_3 &= \langle (1\ 3\ 4) \rangle = \{e, (1\ 3\ 4), (1\ 4\ 3)\}, \\ P_4 &= \langle (2\ 3\ 4) \rangle = \{e, (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned}$$

Problem 5.2. Prove that G is a finite group of order $p^n m$, where p is a prime and $p \nmid m$. Show that the number of Sylow p -subgroups of G divides m .

Solution 5.2. Let n_p denote the number of Sylow p -subgroups of G . By Sylow's theorems, we have

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid |G| = p^n m.$$

But all Sylow p -subgroups have order p^n , and the number n_p divides the index $m = |G|/p^n$. Thus, $n_p \mid m$.

Problem 5.3. Find the class equation for non-abelian groups of order 39.

Solution 5.3. Let G be a non-abelian group of order $39 = 3 \cdot 13$, where $3 < 13$ are primes. By Sylow's theorems, we analyze the structure of G as follows:

(i) The number n_{13} of Sylow 13-subgroups satisfies:

$$n_{13} \equiv 1 \pmod{13} \quad \text{and} \quad n_{13} \mid 3.$$

Thus, $n_{13} = 1$, and the Sylow 13-subgroup is unique and hence normal in G .

(ii) The number n_3 of Sylow 3-subgroups satisfies:

$$n_3 \equiv 1 \pmod{3} \quad \text{and} \quad n_3 \mid 13.$$

Therefore, $n_3 = 13$, so there are 13 distinct Sylow 3-subgroups, none of which are normal.

Since G is non-abelian, its center $Z(G)$ must be proper. Moreover, if $Z(G) \neq \{e\}$, then the quotient $G/Z(G)$ would be of smaller order and possibly cyclic, which would imply G is abelian, a contradiction. Thus, $|Z(G)| = 1$.

The class equation takes the form

$$|G| = |Z(G)| + \sum [G : C_G(g_i)] = 1,$$

where each class size divides 39 and is greater than 1 for non-central elements. Hence, possible sizes are 3, 13, or 39. Thus, we have the following class equation of the form

$$39 = 1 + 3a + 13b,$$

where a is the number of classes of size 3 and b is the number of classes of size 13.

By solving the following

$$3a + 13b = 38,$$

we get the unique solution $a = 4$ and $b = 2$.

Thus, the class equation is

$$39 = 1 + 4 \cdot 3 + 2 \cdot 13 = 1 + 12 + 26.$$

Problem 5.4. Let G be a finite group of order $p^n m$, where $p \nmid m$, and suppose that $p > m$. Prove that a Sylow p -subgroup of G is normal in G .

Solution 5.4. Let n_p be the number of Sylow p -subgroups of G . Then by Sylow's Theorem, we have

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid m.$$

Since $p > m$, the only integer $\leq m$ which is $\equiv 1 \pmod{p}$ is 1. Thus, $n_p = 1$ and so the Sylow p -subgroup is unique and therefore normal.

Problem 5.5. Suppose that G is a group of order 168. If G has more than one Sylow 7-subgroup, exactly how many does it have?

Solution 5.5. Since $|G| = 168 = 2^3 \cdot 3 \cdot 7$, the number n_7 of Sylow 7-subgroups satisfies

$$n_7 \equiv 1 \pmod{7} \quad \text{and} \quad n_7 \mid \frac{168}{7} = 24.$$

Note that divisors of 24 which satisfy $\equiv 1 \pmod{7}$ are 1, 8. If G has more than one Sylow 7-subgroup, then $n_7 \neq 1$, and hence $n_7 = 8$. Therefore, G has exactly 8 Sylow 7-subgroups.

CHAPTER 5

Direct and Semidirect Products, and Abelian Groups

"It appears to me that if one wishes to make progress in mathematics, one should study the masters and not the pupils. "

— Niels Henrik Abel

1. Direct Products

Definition 1.1 (Direct Product). Let $G_1, G_2, \dots, G_n$ be groups with respective operations $*_1, *_2, \dots, *_n$. The **direct product** of G_i 's is the set

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_i \in G_i \text{ for } i = 1, 2, \dots, n\},$$

with the operation defined component-wise as follows

$$(2) \quad (g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n).$$

In the case of infinitely many groups G_i , the direct product is defined by

$$\prod_{i \in \mathbb{N}} G_i = \{(g_1, g_2, \dots) \mid g_i \in G_i \text{ for each } i \in \mathbb{N}\},$$

with operation

$$(g_1, g_2, \dots) * (h_1, h_2, \dots) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots).$$

Remark 1.1. As usual we write Equation (2) simply by removing $*_i$ as follow

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n).$$

Example 1.1. Let $G_i = \mathbb{R}$, where $i = 1, 2, \dots, n$, with the operation of addition. Then the direct product $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R} = \mathbb{R}^n$ is the Euclidean n -space and the operation is defined by

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n).$$

Example 1.2. Let $G_1 = \mathbb{Z}$, $G_2 = S_3$ and $G_3 = \text{GL}_2(\mathbb{R})$, where the group operations are addition, function composition, and matrix multiplication, respectively. Then the operation in $G_1 \times G_2 \times G_3$ is defined as follows

$$(n, a, A)(m, r, B) = (n + m, a \circ r, A \cdot B).$$

Proposition 1.1. If $G_1, G_2, \dots, G_n$ are groups, then the direct product

$$G = G_1 \times G_2 \times \cdots \times G_n$$

is a group. Moreover, the order of G is the product of the order of G_i if each G_i is finite. That is,

$$|G| = |G_1| \cdot |G_2| \cdots |G_n|.$$

If any G_i is infinite, then the order of G is infinite.

PROOF. Let $G = G_1 \times G_2 \times \cdots \times G_n$. The operation on G is defined component-wise as follows

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n).$$

Clearly, the operation is satisfies the closure property.

We now prove the associativity. Let $(a_1, \dots, a_n), (b_1, \dots, b_n), (c_1, \dots, c_n) \in G$. Then

$$\begin{aligned} (a_1, \dots, a_n) [(b_1, \dots, b_n)(c_1, \dots, c_n)] &= (a_1, \dots, a_n)(b_1 c_1, \dots, b_n c_n) \\ &= (a_1(b_1 c_1), \dots, a_n(b_n c_n)) \\ &= ((a_1 b_1) c_1, \dots, (a_n b_n) c_n) \quad (\text{since } G_i \text{ is a group for all } i) \\ &= [(a_1 b_1, \dots, a_n b_n)(c_1, \dots, c_n)]. \end{aligned}$$

Let e_i be the identity of G_i . Then the identity element of G is $(e_1, e_2, \dots, e_n)$ since

$$(g_1, \dots, g_n)(e_1, \dots, e_n) = (g_1 e_1, \dots, g_n e_n) = (g_1, \dots, g_n).$$

Let g_i^{-1} be the inverse of g_i in G_i . Then the inverse of $(g_1, \dots, g_n)$ is $(g_1^{-1}, \dots, g_n^{-1})$ since

$$(g_1, \dots, g_n)(g_1^{-1}, \dots, g_n^{-1}) = (e_1, \dots, e_n).$$

It is clear that

$$|G| = |G_1| \cdot |G_2| \cdots |G_n|.$$

if G_i is finite for all $i = 1, 2, \dots, n$. Also the order of G is infinite if G_i is infinite for some i . $\square$

Proposition 1.2. Let $G = G_1 \times G_2 \times \cdots \times G_n$ be the direct product of the groups $G_1, G_2, \dots, G_n$.

- (1) For each fixed i , the set of elements of G having the identity of G_j in the j -th position for all $j \neq i$, and arbitrary elements of G_i in position i , forms a subgroup of G isomorphic to G_i , that is,

$$G_i \cong \{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\},$$

where g_i appears in the i -th position. If we identify G_i with this subgroup, then

$$G_i \leq G \quad \text{and} \quad G/G_i \cong \left(\prod_{\substack{j=1 \\ j \neq i}}^n G_j \right).$$

- (2) For each fixed i , define the projection map

$$\pi_i : G \rightarrow G_i, \quad \pi_i((g_1, g_2, \dots, g_n)) = g_i.$$

Then π_i is a surjective homomorphism with kernel

$$\ker \pi_i = \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) \mid g_j \in G_j \text{ for all } j \neq i\} \cong \prod_{\substack{j=1 \\ j \neq i}}^n G_j.$$

- (3) If $x \in G_i$ and $y \in G_j$ for $i \neq j$, then $xy = yx$.

PROOF. (1) Let $H_i = \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$. It is clear that, H_i is a subgroup of G . Also the map

$$\varphi : G_i \rightarrow H_i, \quad \varphi(g_i) = (1, \dots, 1, g_i, 1, \dots, 1)$$

is clearly an isomorphism. Thus, $G_i \cong H_i \leq G$.

Next, consider the map

$$\psi : G \rightarrow G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$

defined by

$$\psi((g_1, g_2, \dots, g_n)) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n).$$

Then ψ is a surjective homomorphism, and its kernel is

$$\ker \psi = \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\} = H_i.$$

By the First Isomorphism Theorem, we have $H_i \trianglelefteq G$ and

$$G/H_i \cong \prod_{\substack{j=1 \\ j \neq i}}^n G_j.$$

(2) Clearly, the projection map

$$\pi_i : G \rightarrow G_i, \quad \pi_i((g_1, g_2, \dots, g_n)) = g_i.$$

is a surjective homomorphism with the kernel

$$\ker \pi_i = \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) : g_i \in G_i\}.$$

A similar argument in (1), we conclude that

$$\ker \pi_i \cong \prod_{\substack{j=1 \\ j \neq i}}^n G_j.$$

(3) Let $x = (1, \dots, 1, g_i, 1, \dots, 1)$ and $y = (1, \dots, 1, g_j, 1, \dots, 1)$, where $g_i \in G_i$, $g_j \in G_j$, and $i \neq j$. Then

$$xy = (1, \dots, g_i, \dots, g_j, \dots, 1) = yx,$$

since the group operation acts independently in each coordinate. $\square$

Theorem 1.1. Let G and H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

PROOF. Let $|G| = m$ and $|H| = n$. Then it is clear that $|G \times H| = mn$.

Assume that $G \times H$ is cyclic. Let (g, h) be a generator of $G \times H$. Then $|(g, h)| = mn$. Since the order of (g, h) is the least common multiple of the orders of $g \in G$ and $h \in H$, we have

$$|(g, h)| = \text{lcm}(|g|, |h|) = \text{lcm}(m, n).$$

But $|(g, h)| = mn$, so $\text{lcm}(m, n) = mn$, which holds if and only if $\gcd(m, n) = 1$. Hence, m and n are relatively prime.

Conversely, assume that $\gcd(m, n) = 1$. Let $G = \langle g \rangle$ and $H = \langle h \rangle$. Then

$$|(g, h)| = \text{lcm}(|g|, |h|) = \text{lcm}(m, n).$$

Since $\gcd(m, n) = 1$, we have $\text{lcm}(m, n) = mn = |G \times H|$. Therefore, (g, h) has order mn and hence generates $G \times H$. Thus, $G \times H$ is cyclic. $\square$

Corollary 1.1. Let $G_1, G_2, \dots, G_n$ be finite cyclic groups. Then the external direct product

$$G_1 \times G_2 \times \dots \times G_n$$

is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.

Corollary 1.2. Let $m = n_1 n_2 \dots n_k$. Then

$$\mathbb{Z}_m \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$$

if and only if $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Example 1.3. Let p be a prime and $n \in \mathbb{Z}^+$. Then

$$E_{p^n} = \underbrace{(\mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z})}_{n \text{ factors}}.$$

is an abelian group of order p^n with the property that $x^p = 1$ for all $x \in E_{p^n}$. This group is called the *elementary abelian group* of order p^n .

Problem 1.1. Let p be a prime. Then the elementary abelian group $E = E_{p^2}$, which has order p^2 , contains exactly $p + 1$ subgroups of order p .

Solution 1.1. Since E is an elementary abelian group of order p^2 , we have $E \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Every non-identity element of E has order p , and hence generates a cyclic subgroup of order p .

Note that any two distinct subgroups of order p intersect trivially. Therefore, the $p^2 - 1$ non-identity elements of E are partitioned into disjoint subsets of size $p - 1$, where each subset consists of the $p - 1$ non-identity elements of a cyclic subgroup of order p .

Thus, the number of such subgroups is

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

In particular, when $p = 2$, the group $E \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the Klein four-group, which indeed has exactly three subgroups of order 2.

Problem 1.2. The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element.

Solution 1.2. Let $G_1, G_2, \dots, G_n$ be finite groups and let

$$G = G_1 \times G_2 \times \cdots \times G_n.$$

Let

$$g = (g_1, g_2, \dots, g_n) \in G,$$

where $g_i \in G_i$ for each i .

Let $|g_i| = m_i$ be the order of g_i in G_i , and let

$$m = \text{lcm}(m_1, m_2, \dots, m_n).$$

Then

$$g^m = (g_1^m, g_2^m, \dots, g_n^m) = (e_1, e_2, \dots, e_n),$$

since $m_i \mid m$ for each i . Hence, $g^m = e$, and so $|g| \mid m$.

Conversely, suppose $g^k = e$ for some positive integer k . Then

$$(g_1^k, g_2^k, \dots, g_n^k) = (e_1, e_2, \dots, e_n),$$

which implies $g_i^k = e_i$ for each i . Thus, $m_i \mid k$ for all i .

Therefore, $m = \text{lcm}(m_1, m_2, \dots, m_n) \mid k$. In particular, m is the smallest positive integer such that $g^m = e$.

Hence, the order of g is

$$|g| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|).$$

Problem 1.3. Let $G = G_1 \times G_2 \times \cdots \times G_n$ be the direct product of groups. Show that the center of G is the direct product of the centers of the G_i :

$$Z(G) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n).$$

Deduce that G is abelian if and only if each G_i is abelian.

Solution 1.3. Let $G = G_1 \times G_2 \times \cdots \times G_n$ and $z \in G$. Then $z = (z_1, z_2, \dots, z_n)$ for some $z_i \in G_i$. To find $Z(G)$, we have find all $z \in G$ such that $zg = gz$ for all $g \in G$. Let $g = (g_1, g_2, \dots, g_n) \in G$. Then

$$zg = (z_1g_1, z_2g_2, \dots, z_ng_n), \quad gz = (g_1z_1, g_2z_2, \dots, g_nz_n).$$

This shows that $zg = gz$ if and only if $z_ig_i = g_iz_i$ for each i , that is, $z_i \in Z(G_i)$. Thus,

$$Z(G) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n).$$

Next, we know that G_i is abelian if and only if $Z(G_i) = G_i$. Hence, G is abelian if and only if each G_i is abelian.

2. The Fundamental Theorem of Finitely Generated Abelian Groups

Definition 2.1. (1) A group G is *finitely generated* if there is a finite subset S of G such that $G = \langle S \rangle$.
 (2) For each $r \in \mathbb{Z}_{\geq 0}$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$, where $\mathbb{Z}^0 = \{0\}$. The group $\mathbb{Z}^r$ is called the *free abelian group of rank r* .

We now state the fundamental classification theorem for finitely generated abelian groups.

Theorem 2.1 (Fundamental Theorem of Finitely Generated Abelian Groups). Let G be a finitely generated abelian group. Then

- (1) There exist integers $r \geq 0$ and $n_1, n_2, \dots, n_s \geq 2$ such that $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$, and

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}.$$

- (2) This decomposition is unique up to isomorphism: if

$$G \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_u}$$

where $t \geq 0$, $m_j \geq 2$, and $m_{j+1} \mid m_j$ for all $1 \leq j \leq u-1$, then $t = r$, $u = s$, and $m_j = n_j$ for all j .

(Proof is omitted).

Corollary 2.1. Let n be a positive integer that is the product of distinct primes. Then up to isomorphism, the only abelian group of order n is the cyclic group $\mathbb{Z}_n$.

Example 2.1. Let $n = 180 = 2^2 \cdot 3^2 \cdot 5$. Then we find all abelian groups of order 180 up to isomorphism using invariant factors. For this, we must choose n_1 such that $n_1 \mid n$ and is divisible by $2 \cdot 3 \cdot 5 = 30$. The possible values for n_1 are

$$n_1 = 180, \quad 90, \quad 60, \quad 30.$$

For each choice of n_1 , we determine suitable values of $n_2, n_3, \dots$ such that

$$n_1 n_2 \cdots n_t = 180, \quad \text{and } n_i \mid n_{i+1} \text{ for all } i.$$

For example: If $n_1 = 90$, then $n_2 = 2$ gives $n_1 n_2 = 180$ and $2 \mid 90$. The corresponding group is $\mathbb{Z}_{90} \times \mathbb{Z}_2$. If $n_1 = 30$, then the only valid n_2 is 6, since $30 \cdot 6 = 180$ and $6 \mid 30$. This gives the group $\mathbb{Z}_{30} \times \mathbb{Z}_6$.

Similarly, we obtain all possible combinations as below:

Invariant Factors	Abelian Group
180	$\mathbb{Z}_{180}$
90, 2	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
60, 3	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
30, 6	$\mathbb{Z}_{30} \times \mathbb{Z}_6$

This process illustrates how the classification of abelian groups of a given finite order depends on the prime factorization of the order.

Theorem 2.2. Let G be a finite abelian group of order $n > 1$, and let

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

be the prime factorization of n . Then

- (1) G is isomorphic to a direct product

$$G \cong A_1 \times A_2 \times \cdots \times A_k,$$

where each A_i is an abelian group of order $p_i^{a_i}$.

- (2) For each i , the group A_i is isomorphic to a direct product of cyclic groups. That is,

$$A_i \cong \mathbb{Z}_{p_i^{\beta_{i1}}} \times \mathbb{Z}_{p_i^{\beta_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{ir}}},$$

where the exponents satisfy $\beta_{i1} \geq \beta_{i2} \geq \cdots \geq \beta_{ir} \geq 1$ and $\beta_{i1} + \beta_{i2} + \cdots + \beta_{ir} = a_i$.

- (3) This decomposition is unique up to isomorphism. That is, if

$$G \cong B_1 \times B_2 \times \cdots \times B_k,$$

where each B_i is an abelian group of order $p_i^{a_i}$, then $B_i \cong A_i$, and they have the same invariant factors.

3. Commutator Subgroups

Definition 3.1. Let G be a group and $A, B \subseteq G$ be non-empty subsets. Let $x, y \in G$.

- (1) The commutator of x and y is defined as

$$[x, y] = x^{-1}y^{-1}xy.$$

- (2) The commutator of subsets A and B is defined as

$$[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle,$$

the subgroup generated by all commutators of elements from A and B .

- (3) The commutator subgroup of G , denoted G' or $[G, G]$, is defined by

$$G' = \langle [x, y] \mid x, y \in G \rangle,$$

the subgroup of G generated by all commutators of elements of G .

Proposition 3.1. Let G be a group and $x, y \in G$. If $H \leq G$, then we have the following.

- (1) $xy = yx[x, y]$. In particular, $xy = yx$ if and only if $[x, y] = 1$.
- (2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.
- (3) For any automorphism $\alpha \in \text{Aut}(G)$, we have $\alpha([x, y]) = [\alpha(x), \alpha(y)]$. In particular, G' is characteristic in G , and the quotient group G/G' is abelian.

PROOF. (1) We have

$$[x, y] = x^{-1}y^{-1}xy.$$

Multiply both sides on the left by x and then y on the left side again, we obtain

$$xy = yx[x, y].$$

This implies that

$$xy = yx[x, y] \quad \text{or} \quad [x, y] = x^{-1}y^{-1}xy.$$

Thus, $xy = yx$ if and only if $[x, y] = 1$, the identity.

- (2) Suppose $H \trianglelefteq G$. Then for all $h \in H$, $g \in G$, we have $ghg^{-1} \in H$. Note that

$$[h, g] = h^{-1}g^{-1}hg = h^{-1}(g^{-1}hg) \in H$$

since both $h \in H$ and $g^{-1}hg \in H$, and H is a subgroup. Therefore, $[h, g] \in H$, and hence $[H, G] \leq H$.

Conversely, suppose that $[H, G] \leq H$. We now prove that $H \trianglelefteq G$. Let $h \in H$ and $g \in G$. Since

$$[h, g] = h^{-1}g^{-1}hg,$$

we have the identity

$$g^{-1}hg = h[h, g].$$

Since $h \in H$ and $[h, g] \in [H, G] \leq H$, and H is a subgroup, it follows that $g^{-1}hg \in H$. Therefore, H is closed under conjugation by elements of G . Thus,

$$H \trianglelefteq G.$$

- (3) Let $\alpha \in \text{Aut}(G)$. Then

$$\alpha([x, y]) = \alpha(x^{-1}y^{-1}xy) = \alpha(x)^{-1}\alpha(y)^{-1}\alpha(x)\alpha(y) = [\alpha(x), \alpha(y)].$$

Hence, automorphisms preserve commutators and so the image of any commutator under α is again a commutator. Therefore, the commutator subgroup

$$G' = \langle [x, y] \mid x, y \in G \rangle$$

is fixed under every automorphism, i.e., G' is a characteristic subgroup of G .

Let xG' and yG' be arbitrary elements of G/G' . By definition of the group operation in G/G' ,

$$(xG')(yG') = (xy)G'.$$

Since $[x, y] = x^{-1}y^{-1}xy \in G'$, we can write

$$xy = yx[x, y].$$

Therefore,

$$(xy)G' = (yx[x, y])G' = (yx)G',$$

because $[x, y] \in G'$. Thus,

$$(xG')(yG') = (yx)G' = (yG')(xG').$$

This shows that xG' and yG' commute in G/G' . Thus, the group G/G' is abelian. $\square$

Theorem 3.1. Let G be a group, and let $H, K \leq G$ be subgroups such that

- (1) $H \trianglelefteq G$ and $K \trianglelefteq G$, and
- (2) $H \cap K = \{1\}$.

Then the product $HK \leq G$ is isomorphic to the external direct product $H \times K$.

PROOF. First, we note that the product HK is a subgroup of G as $H \trianglelefteq G$ and $K \trianglelefteq G$. Let $h \in H$ and $k \in K$. Since $H \trianglelefteq G$, it follows that the conjugate $k^{-1}hk \in H$ and so

$$h^{-1}(k^{-1}hk) \in H.$$

But also, since $K \trianglelefteq G$, $h^{-1}k^{-1}h \in K$, we have

$$(h^{-1}k^{-1}h)k \in K.$$

We now consider

$$h^{-1}k^{-1}hk \in H \cap K = \{1\}.$$

This implies that

$$h^{-1}k^{-1}hk = 1 \quad \text{and hence} \quad hk = kh.$$

Thus, every element of H commutes with every element of K .

We now define a map $\varphi : HK \rightarrow H \times K$ by

$$\varphi(hk) = (h, k).$$

Clearly, the map φ is well-defined since the representation hk is unique. We now prove that φ is a homomorphism. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Since elements of H and K commute, we have

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1h_2k_1k_2.$$

This shows that

$$\varphi((h_1k_1)(h_2k_2)) = \varphi(h_1h_2k_1k_2) = (h_1h_2, k_1k_2),$$

and also

$$\varphi(h_1k_1) \cdot \varphi(h_2k_2) = (h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2).$$

Therefore, φ is a homomorphism.

Since each $hk \in HK$ maps uniquely to $(h, k) \in H \times K$, the map φ is bijective. Hence, φ is an isomorphism, and we conclude that

$$HK \cong H \times K. \quad \square$$

Definition 3.2. Let G be a group, and let $H, K \trianglelefteq G$ be normal subgroups such that $H \cap K = \{1\}$. Then the subgroup $HK \leq G$ is called the *internal direct product* of H and K . On the other hand, the group $H \times K$, formed from H and K as abstract groups, is referred to as the *external direct product* of H and K .

Problem 3.1. Find the commutator subgroups of S_4 and A_4 .

Solution 3.1. First, we consider the group S_4 . The alternating group A_4 is a normal subgroup of S_4 of index 2. Hence, the quotient group S_4/A_4 has order 2 and is abelian.

Since the commutator subgroup is the smallest normal subgroup with abelian quotient, we obtain

$$[S_4, S_4] \leq A_4.$$

Every 3-cycle is an element of A_4 , and A_4 is generated by 3-cycles. Moreover, each 3-cycle can be expressed as a commutator in S_4 . Hence,

$$A_4 \leq [S_4, S_4].$$

Therefore,

$$[S_4, S_4] = A_4.$$

Now consider the group A_4 . Let

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\},$$

the Klein four subgroup of A_4 . This subgroup is normal in A_4 .

The quotient group A_4/V_4 has order 3 and is cyclic, and hence abelian. Therefore,

$$[A_4, A_4] \leq V_4.$$

Each non-identity element of V_4 is a commutator of elements of A_4 . Hence,

$$V_4 \leq [A_4, A_4].$$

Thus,

$$[A_4, A_4] = V_4.$$

Hence, the commutator subgroups are

$$[S_4, S_4] = A_4 \quad \text{and} \quad [A_4, A_4] = V_4.$$

Problem 3.2. Let n be a positive odd integer. Then the dihedral group D_{4n} is isomorphic to the direct product $D_{2n} \times \mathbb{Z}_2$.

Solution 3.2. Consider the group

$$D_{4n} = \langle r, s \mid r^{2n} = s^2 = 1, srs = r^{-1} \rangle.$$

Let $H = \langle r^2, s \rangle$. Since $(r^2)^n = r^{2n} = 1$ and $s^2 = 1$, and

$$sr^2s = (srs)^2 = r^{-2},$$

we see that $H \cong D_{2n}$, the dihedral group of order $2n$.

Next, let $K = \langle r^n \rangle$. Since $(r^n)^2 = r^{2n} = 1$, we have $K \cong \mathbb{Z}_2$. Also r^n commutes with both R and S since

$$sr^ns = (srs)^n = r^{-n} = r^n,$$

as n is odd. This implies that $r^n \in Z(D_{4n})$. Thus, $K \leq Z(D_{4n})$ and it is normal in D_{4n} .

Note that H is generated by even powers of R and S , while K contains the odd power r^n . This shows that $H \cap K = \{1\}$ since $r^n \notin H$.

Now observe that every element of D_{4n} can be written as either r^k or $r^k s$, where $0 \leq k < 2n$. Any such element can also be uniquely written as hk for some $h \in H$, $k \in K$, since $|H| = 2n$, $|K| = 2$, and $|H||K| = 4n = |D_{4n}|$. Moreover, since H and K commute element-wise, the map

$$\varphi : H \times K \rightarrow D_{4n}, \quad \varphi(h, k) = hk$$

is a homomorphism. Clearly, φ is bijective. Hence, $D_{4n} \cong D_{2n} \times \mathbb{Z}_2$.

Problem 3.3. Let $x, y \in G$. Then the commutator $[y, x] = [x, y]^{-1}$. Deduce that for any subsets $A, B \subseteq G$, we have $[A, B] = [B, A]$.

Solution 3.3. Let $x, y \in G$. By definition of the commutator,

$$[x, y] = x^{-1}y^{-1}xy.$$

Then

$$[y, x] = y^{-1}x^{-1}yx.$$

We compute

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx.$$

Hence,

$$[y, x] = [x, y]^{-1}.$$

Now let $A, B \subseteq G$. Recall that $[A, B]$ is the subgroup of G generated by all commutators $[a, b]$ with $a \in A$ and $b \in B$.

From the first part, we have

$$[b, a] = [a, b]^{-1} \quad \text{for all } a \in A, b \in B.$$

Hence, every generator of $[B, A]$ is the inverse of a generator of $[A, B]$.

Therefore,

$$[B, A] \leq [A, B].$$

By symmetry, the same argument gives

$$[A, B] \leq [B, A].$$

Thus,

$$[A, B] = [B, A].$$

Problem 3.4. A subgroup $H \leq G$ is normal if and only if $[G, H] \subseteq H$.

Solution 3.4. Let $H \leq G$. First, we assume that H is normal in G . Let $g \in G$ and $h \in H$. Since H is normal, we have

$$ghg^{-1} \in H.$$

Since $h^{-1} \in H$ and H is a subgroup, it follows that

$$[g, h] = g^{-1}h^{-1}gh = h^{-1}(ghg^{-1}) \in H.$$

Hence, every commutator $[g, h]$ lies in H , and therefore,

$$[G, H] \subseteq H.$$

Conversely, assume that $[G, H] \subseteq H$. Let $g \in G$ and $h \in H$. Then

$$[g, h] = g^{-1}h^{-1}gh \in H.$$

Since $h \in H$ and H is a subgroup, we obtain

$$ghg^{-1} = h[g, h] \in H.$$

Thus, $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. Therefore, H is normal in G .

Hence, a subgroup $H \leq G$ is normal if and only if $[G, H] \subseteq H$.

CHAPTER 6

Ring and Module Theory

“As for methods I have sought to give them all the rigour that one requires in geometry, so as never to have recourse to the reasons drawn from the generality of algebra.”

— Augustin-Louis Cauchy

In this chapter, we introduce the basic ideas of ring and module theory. These ideas help us understand important algebraic structures in abstract algebra. They form the foundation for studying rings and modules and are useful in various fields, including number theory, cryptography, coding theory, and computer science. This chapter draws on standard results and illustrative examples from [5].

1. Rings and Examples

Let us consider the structure of the integers modulo n , where n is a positive integer. It is well known that this construction leads us to the group $(\mathbb{Z}/n\mathbb{Z}, +_n)$. Recall that $\mathbb{Z}/n\mathbb{Z}$ consists of equivalence classes of integers under congruence modulo n . Denote by $[a]$ the equivalence class of an integer a modulo n , that is,

$$[a] = \{ a + kn \mid k \in \mathbb{Z} \}.$$

The operation addition in $\mathbb{Z}/n\mathbb{Z}$ is defined by

$$[a] + [b] := [a + b].$$

It is easy to see that the above operation is well-defined and gives the structure of an abelian group.

We now discuss the multiplicative structure that $\mathbb{Z}/n\mathbb{Z}$ inherits from the integers. The multiplication is defined by

$$[a][b] := [ab].$$

We now prove that the operation is well-defined. Let $[a] = [a']$ and $[b] = [b']$. That is, $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then n divides both $a - a'$ and $b - b'$, and it follows that n divides

$$ab - a'b' = (a - a')b + a'(b - b'),$$

so that $[ab] = [a'b']$. Therefore, multiplication is well defined on the set $\mathbb{Z}/n\mathbb{Z}$. Also the multiplication in $\mathbb{Z}$ is associative, commutative, and distributes over addition, it follows that these properties hold in $\mathbb{Z}/n\mathbb{Z}$. Note that $\mathbb{Z}/n\mathbb{Z}$ contains the multiplicative identity 1. We call the structure $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ a *commutative ring with identity*. More generally, we have the following definition.

Definition 1.1 (Ring). A *ring* is a set R together with two binary operations, usually called addition and multiplication, defined by $(a, b) \mapsto a + b$ and $(a, b) \mapsto ab$, respectively, satisfying the following properties:

- (i) The set R , with the addition operation, forms an abelian group.
- (ii) Multiplication is associative: for all $a, b, c \in R$, we have

$$a(bc) = (ab)c.$$

- (iii) Multiplication distributes over addition from both sides: for all $a, b, c \in R$,

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc.$$

The element $0 \in R$ denotes the additive identity, and for each $a \in R$, the additive inverse is written as $-a$.

Definition 1.2. A ring R is said to be *commutative* if multiplication is commutative, that is

$$ab = ba \quad \text{for all } a, b \in R.$$

Definition 1.3. A ring R is called a *ring with identity* if there exists an element $1 \in R$ such that

$$1a = a1 = a \quad \text{for all } a \in R.$$

Theorem 1.1 (Properties of a ring). Let a, b, c be elements of a ring R . Then the following properties hold:

- (1) $a \cdot 0 = 0 \cdot a = 0$.
- (2) $a(-b) = (-a)b = -(ab)$.
- (3) $(-a)(-b) = ab$.
- (4) $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore, if R has a multiplicative identity element 1 , then

- (5) $(-1)a = -a$.
- (6) $(-1)(-1) = 1$.

PROOF. (1) Since $0 + 0 = 0$, we have

$$a \cdot 0 = a(0 + 0) = a \cdot 0 + a \cdot 0.$$

Subtracting $a \cdot 0$ from both sides gives $a \cdot 0 = 0$. Similarly, $0 \cdot a = 0$.

(2) By distributivity, we have

$$a(-b) + ab = a(-b + b) = a \cdot 0 = 0 \Rightarrow a(-b) = -(ab).$$

Similarly, $(-a)b = -(ab)$.

(3) Using part (2), we obtain

$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab.$$

(4) Using distributivity, we get that

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac,$$

and similarly, $(b - c)a = ba - ca$.

(5) Since $(-1)a + a = (-1 + 1)a = 0a = 0$, we get $(-1)a = -a$.

(6) By part (5), $(-1)(-1) = -(-1) = 1$.

□

Proposition 1.1.

- (1) If a ring R has a multiplicative identity 1 , then it is unique.
- (2) If an element in a ring R has a multiplicative inverse, then it is unique.

PROOF. (1) Suppose a ring R has two multiplicative identities, say 1 and $1'$. Then

$$1 = 1 \cdot 1' = 1'.$$

Therefore, the identity element is unique.

(2) Suppose $a \in R$ has two multiplicative inverses b and c , i.e.,

$$ab = ba = 1 \quad \text{and} \quad ac = ca = 1.$$

Then

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

Thus, the inverse of a is unique.

□

Note 1.1. It is often convenient not to assume that the multiplicative identity 1 must be distinct from the additive identity 0 . However, if $1 = 0$ in a ring R , then for any $a \in R$, we have

$$a = 1a = 0a = 0.$$

Thus, every element of R is zero, and R consists of a single element. Such a ring is called the *zero ring*.

Note that a non-zero element of a commutative ring with unity need not have a multiplicative inverse. When it does, the element is called a *unit* of the ring. Thus, an element a is a unit if its multiplicative inverse a^{-1} exists in the ring, that is, if there exists an element b such that $ab = ba = 1$.

Example 1.1. The ring of integers $\mathbb{Z}$, equipped with standard addition and multiplication, is a commutative ring with unity, where the multiplicative identity is 1. The only elements of $\mathbb{Z}$ that have multiplicative inverses within $\mathbb{Z}$ are 1 and -1 , and hence these are the only *units* in $\mathbb{Z}$.

Example 1.2. For any integer $n > 0$, the set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, under addition and multiplication modulo n , forms a commutative ring with unity, where 1 is the multiplicative identity. An element $a \in \mathbb{Z}_n$ is a unit if there exists $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \pmod{n}$. The set of all such units is denoted by $U(n)$ and consists precisely of those elements a for which $\gcd(a, n) = 1$.

Example 1.3. The set $\mathbb{Z}[x]$ of all polynomials in the variable x with integer coefficients, under the usual polynomial addition and multiplication, forms a commutative ring with unity. The multiplicative identity in this ring is the constant polynomial $f(x) = 1$.

Example 1.4. Let $M_2(\mathbb{Z})$ denote the set of all 2×2 matrices with integer entries. Then $M_2(\mathbb{Z})$ is a ring under matrix addition and multiplication. The ring $M_2(\mathbb{Z})$ is *non-commutative* since, in general, matrix multiplication does not commute. However, it has the multiplicative identity, namely the 2×2 identity matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Example 1.5. The set $2\mathbb{Z}$ of even integers, with usual addition and multiplication, forms a commutative ring. However, it does *not* contain a multiplicative identity, as the element 1 is not in $2\mathbb{Z}$. Hence, $2\mathbb{Z}$ is a commutative ring *without unity*.

Example 1.6. Let $R_1, R_2, \dots, R_n$ be rings. We now construct a new ring from them by taking the Cartesian product of these rings and defining operations component-wise as follows. Define

$$R_1 \oplus R_2 \oplus \dots \oplus R_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in R_i \text{ for } i = 1, 2, \dots, n\}.$$

We define addition and multiplication in this set component-wise as follows.

$$\begin{aligned} (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n), \\ (a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) &= (a_1 b_1, a_2 b_2, \dots, a_n b_n). \end{aligned}$$

With these operations, the set $R_1 \oplus R_2 \oplus \dots \oplus R_n$ forms a ring, which is called the *direct sum* of the rings $R_1, R_2, \dots, R_n$.

Example 1.7. Let R be a non-zero commutative ring with identity. Define the set $R[X_1, X_2, \dots, X_n]$ to be the collection of all polynomials in the indeterminate $X_1, X_2, \dots, X_n$ with coefficients in R , where each polynomial is a finite linear combination of monomials of the form

$$a_\alpha X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n} \quad \text{with } a_\alpha \in R \text{ and } \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n.$$

Then $R[X_1, X_2, \dots, X_n]$, under the usual operations of polynomial addition and multiplication, forms a commutative ring with identity.

Definition 1.4 (Subring). A subset S of a ring R is called a *subring* if S is itself a ring under the addition and multiplication operations inherited from R .

Theorem 1.2 (Subring Test). Let R be a ring. A non-empty subset $S \subseteq R$ is a subring if $a - b \in S$ and $ab \in S$ for all $a, b \in S$.

PROOF. Since S is non-empty and closed under subtraction, $0 = a - a \in S$, and additive inverses exist. Closure under subtraction and multiplication ensures that S is closed under addition (as $a + b = a - (-b)$) and multiplication. Hence, S is a ring under the operations of R , and thus it is a subring. $\square$

Example 1.8. The set $\{0\}$, consisting only of the additive identity, is a subring of any ring R . It is called the *trivial subring*. Similarly, the entire ring R is a subring of itself.

Example 1.9. For any positive integer n , the set

$$n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$$

is a subring of the ring of integers $\mathbb{Z}$. It is closed under subtraction and multiplication and contains the additive identity.

Example 1.10. The set of *Gaussian integers*, defined by

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

forms a subring of the complex numbers $\mathbb{C}$. It is closed under complex addition and multiplication.

Example 1.11. Let R be the ring of all real-valued functions of a real variable, with operations defined pointwise. The set of all functions $f \in R$ such that $f(0) = 0$ forms a subring of R . These are exactly the functions whose graphs pass through the origin.

Example 1.12. Consider the ring of all 2×2 matrices over $\mathbb{Z}$. The set of all diagonal matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{where } a, b \in \mathbb{Z},$$

is a subring of this matrix ring. It is closed under matrix addition and multiplication.

Definition 1.5 (Zero-divisor). A non-zero element a in a commutative ring R is called a *zero-divisor* if there exists $b \neq 0$ in R such that $ab = 0$.

Definition 1.6 (Integral domain). An *integral domain* is a commutative ring with unity that contains no zero-divisors.

Theorem 1.3 (Cancellation Law). Let a, b, c be elements of an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

PROOF. Let $ab = ac$. Then

$$ab - ac = 0 \Rightarrow a(b - c) = 0.$$

Since $a \neq 0$ and the ring is an integral domain, it follows that $b - c = 0$, and hence $b = c$. $\square$

Problem 1.1. Let R be a ring. Show that $M_n(R)$, the set of all $n \times n$ matrices with entries in R , is a ring under usual matrix addition and matrix multiplication. Furthermore, if R is commutative with $|R| > 1$, then $M_n(R)$ is commutative if and only if $n = 1$.

Solution 1.1. Let $A = (a_{ij}), B = (b_{ij}) \in M_n(R)$. Define

$$(A + B)_{ij} = a_{ij} + b_{ij}, \quad (AB)_{ij} = \sum_{k=1}^n a_{ik}b_{kj}.$$

Then $(M_n(R), +)$ is an abelian group since addition is associative and commutative, the zero matrix is the additive identity, and the inverse of $A \in M_n(R)$ is $-A$.

Next, matrix multiplication is associative since R is associative and

$$((AB)C)_{ij} = \sum_{k=1}^n (AB)_{ik}c_{kj} = \sum_{k=1}^n \left(\sum_{\ell=1}^n a_{i\ell}b_{\ell k} \right) c_{kj} = \sum_{\ell=1}^n a_{i\ell} \left(\sum_{k=1}^n b_{\ell k}c_{kj} \right) = (A(BC))_{ij},$$

for $A, B, C \in M_n(R)$. Distributivity of multiplication over addition also carries over from R . Thus, $M_n(R)$ is a ring. If R has 1_R , then the identity matrix I_n (with 1_R on the diagonal and 0 elsewhere) serves as the multiplicative identity in $M_n(R)$.

Assume R is commutative with $|R| > 1$. It is clear that if $n = 1$, then $M_1(R) \cong R$ is commutative by hypothesis.

Conversely, suppose $n \geq 2$. Then we prove that $M_n(R)$ is not commutative. Let E_{ij} denote the $n \times n$ matrix whose (i, j) -entry is 1_R and all other entries are 0. These are called the *matrix units*. They satisfy

$$E_{ij}E_{kl} = \delta_{jk}E_{il}, \quad \text{where } \delta_{jk} = \begin{cases} 1 & \text{if } j = k, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, for $n \geq 2$, consider $A = E_{12}$ and $B = E_{21}$. Then

$$AB = E_{12}E_{21} = E_{11}, \quad BA = E_{21}E_{12} = E_{22}.$$

Since $n \geq 2$, we have $E_{11} \neq E_{22}$. It shows that $AB \neq BA$. Therefore, $M_n(R)$ is not commutative when $n \geq 2$.

Thus, $M_n(R)$ is commutative if and only if $n = 1$.

Problem 1.2. Let R and S be rings.

- (1) Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication.
- (2) Show that $R \times S$ is commutative if and only if both R and S are commutative.
- (3) Prove that $R \times S$ has an identity if and only if both R and S have identities.

Solution 1.2. Define addition and multiplication on $R \times S$ by

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2).$$

(1) It is clear that $(R \times S, +)$ is an abelian group since addition is defined component-wise and both $(R, +)$ and $(S, +)$ are abelian groups. The zero element is $(0_R, 0_S)$ and the inverse of (r, s) is $(-r, -s)$.

Next, we prove multiplication is associative. For this $(r_i, s_i) \in R \times S$, where $i = 1, 2, 3$, we have

$$((r_1, s_1)(r_2, s_2))(r_3, s_3) = ((r_1r_2)r_3, (s_1s_2)s_3),$$

and

$$(r_1, s_1)((r_2, s_2)(r_3, s_3)) = (r_1(r_2r_3), s_1(s_2s_3)).$$

These are equal by associativity in R and S . Also distributivity also holds component-wise. Hence, $R \times S$ is a ring.

(2) Suppose both R and S are commutative. Then

$$(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2) = (r_2r_1, s_2s_1) = (r_2, s_2)(r_1, s_1)$$

for all $(r_1, s_1), (r_2, s_2) \in R \times S$. Hence, $R \times S$ is commutative.

Conversely, if $R \times S$ is commutative, then

$$(r, 0_S)(r', 0_S) = (rr', 0) = (r'r, 0) = (r', 0_S)(r, 0_S).$$

Therefore, $rr' = r'r$. Hence, R is commutative. Similarly, it is easy to prove S is commutative.

(3) If R and S have identities 1_R and 1_S , then

$$(1_R, 1_S)(r, s) = (r, s) = (r, s)(1_R, 1_S).$$

Thus, $(1_R, 1_S)$ is an identity in $R \times S$.

Conversely, suppose $R \times S$ has an identity (e_R, e_S) . Then

$$(r, 0_S)(e_R, e_S) = (re_R, 0) = (r, 0_S)$$

for all $r \in R$. Hence, $re_R = r$ for all r . Therefore, e_R is an identity in R . Similarly e_S is an identity in S .

Problem 1.3. Let R be a ring and $a \in R$. Define

$$C(a) = \{r \in R \mid ra = ar\}.$$

Then prove that $C(a)$ is a subring of R containing a and the center of R , $Z(R) = \{z \in R \mid zx = xz \text{ for all } x \in R\}$, is the intersection of the subrings $C(a)$ as a ranges over R .

Solution 1.3. Since $0a = a0 = 0$ and $aa = aa$, we have $0, a \in C(a)$. So $C(a)$ non-empty. If $r, s \in C(a)$, then

$$(r - s)a = ra - sa = ar - as = a(r - s).$$

This shows that $r - s \in C(a)$. Similarly,

$$(rs)a = r(sa) = r(as) = (ra)s = (ar)s = a(rs),$$

so $rs \in C(a)$. Thus, $C(a)$ is closed under subtraction and multiplication. Since $C(a)$ is non-empty and satisfies the subring test, it is a subring of R containing a .

Now let us determine the center. By definition,

$$Z(R) = \{z \in R \mid zx = xz \text{ for all } x \in R\}.$$

For a fixed $a \in R$, an element z belongs to $Z(R)$ only if $za = az$, that is, $z \in C(a)$. Conversely, if $z \in C(a)$ for every $a \in R$, then z commutes with every element of R . Hence, $z \in Z(R)$.

Therefore,

$$Z(R) = \bigcap_{a \in R} C(a),$$

as required.

2. Ideals and Factor Rings

Recall that normal subgroups play a fundamental role in constructing factor groups in group theory. Analogously, in ring theory, *ideals* are crucial for defining *factor rings* (also called *quotient rings*).

Definition 2.1 (Ideal). Let R be a ring. A subring $I \subseteq R$ is called a (*two-sided*) *ideal* of R if for every $r \in R$ and every $a \in I$, both $ra \in I$ and $ar \in I$. In other words, I is closed under multiplication by elements of R from both sides.

Note 2.1. An ideal I is said to be a *proper ideal* if $I \subsetneq R$. It is easy to see that from the definition, ideals "absorb" multiplication from the ring. That is,

$$rI = \{ra \mid a \in I\} \subseteq I \quad \text{and} \quad Ir = \{ar \mid a \in I\} \subseteq I \quad \text{for all } r \in R.$$

Theorem 2.1 (Ideal Test). Let R be a ring. A non-empty subset $I \subseteq R$ is an ideal of R if

- (1) $a - b \in I$ whenever $a, b \in I$,
- (2) $ra \in I$ and $ar \in I$ for all $a \in I$ and $r \in R$.

PROOF. Proof follows from the definition of an ideal and the subring test. □

Example 2.1. (1) The sets $\{0\}$ and R are always ideals of a ring R . The ideal $\{0\}$ is called the *trivial ideal*.

- (2) For any positive integer n , the set $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.
- (3) If R is a commutative ring with unity and $a \in R$, then the set $(a) = \{ra \mid r \in R\}$ is an ideal called the *principal ideal* generated by a .
- (4) Let $R[x]$ be the ring of real polynomials, and let $I \subseteq R[x]$ be the set of all polynomials with zero constant term. Then I is an ideal of $R[x]$, and in fact $I = (x)$.
- (5) If $a_1, a_2, \dots, a_n \in R$, the set

$$(a_1, a_2, \dots, a_n) = \{r_1a_1 + r_2a_2 + \dots + r_na_n \mid r_i \in R\}$$

is an ideal of R , known as the *ideal generated by* $a_1, \dots, a_n$.

- (6) In $\mathbb{Z}[x]$, the set of polynomials with even constant terms forms an ideal. This ideal is generated by x and 2, i.e., $(x, 2)$.
- (7) Let R be the ring of all real-valued functions on $\mathbb{R}$. The set of all differentiable functions is a subring, but not an ideal of R .

2.1. Factor Rings. Let R be a ring and A be an ideal of R . Since A is a normal subgroup under addition, we can form the factor group

$$R/A = \{r + A \mid r \in R\}.$$

To define multiplication on cosets, we define

$$(r + A)(s + A) = rs + A.$$

Theorem 2.2. Let R be a ring and $A \subseteq R$. Then R/A is a ring under coset addition and multiplication if and only if A is an ideal of R .

PROOF. Assume that A is an ideal of R . Suppose $s + A = s' + A$ and $t + A = t' + A$. Then $s = s' + a$ and $t = t' + b$ for some $a, b \in A$. Consider

$$st = (s' + a)(t' + b) = s't' + s'b + at' + ab.$$

Since A is an ideal, we have $s'b, at', ab \in A$. This shows that

$$st + A = s't' + A,$$

and hence multiplication is well-defined.

Conversely, assume that R/A is a ring under coset addition and multiplication. Suppose A is not an ideal (but it is a subring). Then for some $a \in A$, $r \in R$, either $ra \notin A$ or $ar \notin A$. In this case, $(a + A)(r + A) = ar + A$ differs from $0 + A$, which contradicts the operation multiplication is well-defined. $\square$

Example 2.2. (1) $2\mathbb{Z}/6\mathbb{Z} = \{0 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$ is a factor ring under mod 6 operations.

(2) Let $R = \left\{ \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in \mathbb{Z} \right\}$, and let $I \subset R$ be the subset with all entries even. Then R/I has 16 elements, each represented by a matrix with entries 0 or 1.

(3) $\mathbb{Z}[i]/\langle 2 - i \rangle$. Here, $\langle 2 - i \rangle$ denotes the ideal generated by $2 - i$ in the Gaussian integers. Elements are of the form $a + bi + \langle 2 - i \rangle$, and the ring turns out to be isomorphic to $\mathbb{Z}_5$.

Definition 2.2 (Prime and Maximal ideal). A *prime ideal* P of a commutative ring R is a proper ideal such that whenever $a, b \in R$ and $ab \in P$, then $a \in P$ or $b \in P$.

A *maximal ideal* of a commutative ring R is a proper ideal M such that if I is an ideal of R with $M \subseteq I \subseteq R$, then either $I = M$ or $I = R$.

Thus, the only ideal that properly contains a maximal ideal is the entire ring.

Example 2.3. Let $n > 1$ be an integer. Then in the ring of integers $\mathbb{Z}$, the ideal $n\mathbb{Z}$ is prime if and only if n is prime.

Example 2.4. The ideal $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$. Assume that A is an ideal of $\mathbb{R}[x]$ that properly contains $\langle x^2 + 1 \rangle$. Let $f(x) \in A$ and $f(x) \notin \langle x^2 + 1 \rangle$. Then by the Division Algorithm,

$$f(x) = q(x)(x^2 + 1) + r(x),$$

where $\deg r(x) < 2$, so $r(x) = ax + b$ with a and b not both zero. Since $r(x) = f(x) - q(x)(x^2 + 1) \in A$, we have $ax + b \in A$. We now consider

$$(ax + b)(ax - b) = a^2x^2 - b^2 \in A,$$

and

$$a^2(x^2 + 1) = a^2x^2 + a^2 \in A.$$

This implies that

$$(a^2x^2 + a^2) - (a^2x^2 - b^2) = a^2 + b^2 \in A.$$

Therefore, A contains a non-zero constant $a^2 + b^2$, and hence $1 \in A$, which implies $A = \mathbb{R}[x]$. Thus, $\langle x^2 + 1 \rangle$ is maximal.

Example 2.5. The ideal $\langle x^2 + 1 \rangle$ is not prime in $\mathbb{Z}_2[x]$, since it contains $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1$ (here $2x = 0$ in $\mathbb{Z}_2$), but it does not contain $x + 1$.

Theorem 2.3. Let R be a commutative ring with unity, and let A be an ideal of R . Then R/A is an integral domain if and only if A is a prime ideal.

PROOF. Suppose that R/A is an integral domain and $ab \in A$. Then

$$(a + A)(b + A) = ab + A = A,$$

which is the zero element in R/A . Since R/A has no zero divisors, it follows that either $a + A = A$ or $b + A = A$, that is, $a \in A$ or $b \in A$. Hence, A is a prime ideal.

Conversely, assume that A is a prime ideal. Then R/A is a commutative ring with unity. Suppose

$$(a + A)(b + A) = ab + A = A.$$

This implies $ab \in A$. Since A is prime, we must have $a \in A$ or $b \in A$. Therefore, $a + A = A$ or $b + A = A$, which means that one of the factors is zero in R/A . Hence, R/A has no zero divisors and is an integral domain. $\square$

Definition 2.3. Let R be a ring with identity $1 \neq 0$, and let A be a subset of R .

- (1) The *ideal generated by A* , denoted by $\langle A \rangle$, is the intersection of all ideals of R that contain A , that is,

$$\langle A \rangle = \bigcap \{ I \subseteq R \mid I \text{ is an ideal of } R \text{ and } A \subseteq I \}.$$

Equivalently, $\langle A \rangle$ is the smallest ideal of R containing A .

- (2) We define

$$RA = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R, a_i \in A, n \in \mathbb{Z}_{>0} \right\},$$

with the convention that $RA = 0$ if $A = \emptyset$.

Similarly,

$$AR = \left\{ \sum_{i=1}^n a_i r_i \mid r_i \in R, a_i \in A, n \in \mathbb{Z}_{>0} \right\},$$

and

$$RAR = \left\{ \sum_{i=1}^n r_i a_i r'_i \mid r_i, r'_i \in R, a_i \in A, n \in \mathbb{Z}_{>0} \right\}.$$

- (3) If $A = \{a\}$ consists of a single element, then the ideal $\langle A \rangle$ is written as $\langle a \rangle$ and is called a *principal ideal*.
 (4) If $A = \{a_1, a_2, \dots, a_n\}$ is a finite subset of R , then the ideal $\langle A \rangle$ is written as

$$\langle a_1, a_2, \dots, a_n \rangle = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n \mid r_1, r_2, \dots, r_n \in R\}$$

and is called a *finitely generated ideal*.

Problem 2.1. Let R be a ring (assume two-sided ideals, in particular the statement holds if R is commutative). If A and B are ideals of R , define their sum and intersection by

$$A + B := \{a + b \mid a \in A, b \in B\}, \quad A \cap B := \{x \in R \mid x \in A \text{ and } x \in B\}.$$

Define the *product ideal* AB by

$$AB := \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{Z}_{>0}, a_i \in A, b_i \in B \right\},$$

that is, AB consists exactly of all *finite sums* of elements of the form $a_i b_i$ with $a_i \in A, b_i \in B$. Prove that $A + B, A \cap B$ and AB are ideals of R , and that

$$AB \subseteq A \cap B \subseteq A + B.$$

Solution 2.1. First, we prove that $A + B$ is an ideal of R . Let $x = a_1 + b_1$ and $y = a_2 + b_2$ and $r \in R$. Then $x + y = (a_1 + a_2) + (b_1 + b_2) \in A + B$, $rx = ra_1 + rb_1 \in A + B$ and $xr = a_1 r + b_1 r \in A + B$ since A and B are ideals.

Next, we prove that $A \cap B$ is an ideal. For this, if $x, y \in A \cap B$, then $x + y \in A$ and $x + y \in B$. Therefore, $x + y \in A \cap B$. Similarly, $-x \in A \cap B$ and $rx, xr \in A \cap B$ for all $r \in R$.

Finally, we prove that AB is an ideal of R . By definition, every element of AB is a finite sum $\sum_{i=1}^n a_i b_i$ with $a_i \in A, b_i \in B$. Since sums of such finite sums are again finite sums of products, it follows that AB is closed under addition. For $r \in R$,

$$r \left(\sum_{i=1}^n a_i b_i \right) = \sum_{i=1}^n (ra_i) b_i, \quad \left(\sum_{i=1}^n a_i b_i \right) r = \sum_{i=1}^n a_i (b_i r),$$

and since $ra_i \in A$ and $b_i r \in B$, both products lie in AB . Thus, AB is an ideal.

Note that for all i , $a_i b_i$ of AB lies in A (because A is an ideal and $a_i b_i \in A$). Similarly, $a_i b_i \in B$. Therefore, $a_i b_i \in A \cap B$. Hence, every finite sum of such generators lies in $A \cap B$, and $AB \subseteq A \cap B$. Finally, if $x \in A \cap B$ then $x = x + 0$ with $x \in A$ and $0 \in B$. Hence, $x \in A + B$ and so $A \cap B \subseteq A + B$. Thus,

$$AB \subseteq A \cap B \subseteq A + B.$$

Problem 2.2. Show that the ideal $(2, x)$ in $\mathbb{Z}[x]$ is not principal.

Solution 2.2. By definition, we have

$$(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}.$$

This implies that $(2, x)$ consists exactly of those polynomials in $\mathbb{Z}[x]$ whose constant term is even. In particular, $(2, x)$ is a proper ideal.

Suppose, for a contradiction, that $(2, x) = (a(x))$ for some $a(x) \in \mathbb{Z}[x]$. Since $2 \in (a(x))$, there exists $p(x) \in \mathbb{Z}[x]$ with

$$2 = p(x)a(x).$$

This implies that both $p(x)$ and $a(x)$ to be constant polynomials. Hence, $a(x), p(x) \in \{\pm 1, \pm 2\}$.

- If $a(x) = \pm 1$, then $(a(x)) = \mathbb{Z}[x]$, which is not proper, a contradiction.
- If $a(x) = \pm 2$, then $(a(x)) = (2)$. But $x \in (2, x)$ would imply $x \in (2)$, i.e. $x = 2q(x)$ for some $q(x) \in \mathbb{Z}[x]$, which is impossible.

Thus, no such $a(x)$ exists, and we conclude that $(2, x)$ is not a principal ideal.

Problem 2.3. Show that every ideal of $\mathbb{Z}$ is principal. In particular, prove that for integers $n, m \neq 0$ we have

$$\langle n, m \rangle = \langle d \rangle,$$

where $d = \gcd(n, m)$, and deduce that n and m are relatively prime if and only if $\langle n, m \rangle = \langle 1 \rangle$.

Solution 2.3. Note that $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ for all $n \in \mathbb{Z}$. Thus, every ideal of $\mathbb{Z}$ is generated by a single integer, i.e. every ideal of $\mathbb{Z}$ is principal.

Now let $n, m \neq 0$ and let $d = \gcd(n, m)$. By Bézout's identity, there exist $r, s \in \mathbb{Z}$ such that

$$d = rn + sm.$$

Hence, $d \in \langle n, m \rangle$, which implies $\langle d \rangle \subseteq \langle n, m \rangle$.

Conversely, since $d \mid n$ and $d \mid m$, both n and m lie in $\langle d \rangle$, which implies $\langle n, m \rangle \subseteq \langle d \rangle$. Therefore,

$$\langle n, m \rangle = \langle d \rangle.$$

Finally, n and m are relatively prime if and only if $\gcd(n, m) = 1$ if and only if

$$\langle n, m \rangle = \langle 1 \rangle.$$

Problem 2.4. Show that the ideal $\langle x \rangle$ is a prime ideal in $\mathbb{Z}[x]$, but it is not a maximal ideal in $\mathbb{Z}[x]$.

Solution 2.4. First, we prove that $\langle x \rangle$ is a prime ideal in $\mathbb{Z}[x]$. Define a ring homomorphism

$$\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}$$

by $\varphi(f(x)) = f(0)$. This map is surjective.

Clearly,

$$\ker(\varphi) = \langle x \rangle.$$

By the First Isomorphism Theorem, we have

$$\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}.$$

Since $\mathbb{Z}$ is an integral domain, it follows that $\mathbb{Z}[x]/\langle x \rangle$ is an integral domain. Hence, $\langle x \rangle$ is a prime ideal of $\mathbb{Z}[x]$.

Next we show that $\langle x \rangle$ is not a maximal ideal in $\mathbb{Z}[x]$. Consider the ideal

$$\langle 2, x \rangle \leq \mathbb{Z}[x].$$

Clearly,

$$\langle x \rangle \subsetneq \langle 2, x \rangle \subsetneq \mathbb{Z}[x].$$

Thus, $\langle x \rangle$ is properly contained in another proper ideal of $\mathbb{Z}[x]$. Therefore, $\langle x \rangle$ is not a maximal ideal.

Hence, the ideal $\langle x \rangle$ is a prime ideal but not a maximal ideal in $\mathbb{Z}[x]$.

Problem 2.5. Let R be a commutative ring. Let I and J be ideals of R , and let P be a prime ideal with

$$IJ \subseteq P.$$

Prove that $I \subseteq P$ or $J \subseteq P$.

Solution 2.5. Recall that IJ denotes the ideal generated by all finite sums of products xy with $x \in I$ and $y \in J$. If $I \subseteq P$ then we are done. Otherwise choose

$$a \in I \setminus P.$$

For every $b \in J$, we have $ab \in IJ \subseteq P$. Since P is prime and $a \notin P$, we have $b \in P$ as $ab \in P$. Hence, $J \subseteq P$.

Therefore, either $I \subseteq P$ or $J \subseteq P$, as required.

3. Modules over Rings and Examples

Definition 3.1 (Left R -Module). Let R be a ring. A *left R -module* M is an abelian group $(M, +)$ together with a scalar multiplication

$$R \times M \longrightarrow M, \quad (r, m) \mapsto rm,$$

such that for all $r, r' \in R$ and $m, m' \in M$ satisfies

- (1) $r(r'm) = (rr')m$,
- (2) $(r + r')m = rm + r'm$,
- (3) $r(m + m') = rm + rm'$.

If R has an identity element 1, the module M is called *unital* if

$$1m = m \quad \text{for all } m \in M.$$

Remark 3.1. One may also define *right R -modules*. In this case, the scalar multiplication is written mr with $m \in M$ and $r \in R$, and the analogues of (1)–(3) above hold. When R is commutative ring, the distinction between left and right disappears, and one simply speaks of an R -module.

Example 3.1. Every abelian group can be regarded as a unital $\mathbb{Z}$ -module. Indeed, if $(M, +)$ is an abelian group, then we define scalar multiplication by

$$n \cdot m = \begin{cases} m + m + \cdots + m & \text{if } n > 0 \text{ (} n \text{ terms),} \\ 0 & \text{if } n = 0, \\ -((-n) \cdot m) & \text{if } n < 0. \end{cases}$$

This definition uses only the group operation of M and makes M into a unital $\mathbb{Z}$ -module.

For example, if $M = \mathbb{Z}^2$ with component-wise addition, then

$$3 \cdot (2, 4) = (2, 4) + (2, 4) + (2, 4) = (6, 12),$$

and

$$(-2) \cdot (2, 4) = -(2 \cdot (2, 4)) = -(4, 8) = (-4, -8).$$

Thus, the above example shows that the action of $\mathbb{Z}$ corresponds exactly to repeated addition in the abelian group.

Example 3.2. If R is a ring, then R itself is naturally both a left R -module and a right R -module, with scalar multiplication given by the ring multiplication. Moreover, if I is a two-sided ideal of R , then the quotient ring R/I inherits both a left R -module and a right R -module structure by

$$r \cdot (x + I) = (rx) + I \quad \text{and} \quad (x + I) \cdot r = (xr) + I$$

for all $r, x \in R$. Note that these module structures are unital whenever R has an identity.

Example 3.3. The set of all complex numbers $\mathbb{C}$ is an $\mathbb{R}$ -module, where the addition $+$ is the usual addition of complex numbers and the scalar multiplication $\cdot : \mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C}$ is given by

$$r \cdot (a + bi) = (ra) + (rb)i, \quad r \in \mathbb{R}, \quad a, b \in \mathbb{R}.$$

Example 3.4. Let R be a unitary ring and let n be a positive integer. Consider the abelian group R^n consisting of all n -tuples of elements of R under component-wise addition

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n).$$

Define a scalar multiplication by

$$r \cdot (x_1, \dots, x_n) = (rx_1, \dots, rx_n), \quad r \in R.$$

Then R^n becomes a left R -module.

Example 3.5. Let R be a unitary ring and let $R^{\mathbb{N}}$ denote the set of all functions $f : \mathbb{N} \rightarrow R$ (equivalently, all sequences of elements of R). Define addition pointwise as

$$(f + g)(n) = f(n) + g(n), \quad \text{where } f, g \in R^{\mathbb{N}} \text{ and } n \in \mathbb{N}.$$

This makes $(R^{\mathbb{N}}, +)$ an abelian group.

We now define scalar multiplication as

$$(rf)(n) = r f(n), \quad r \in R, \quad n \in \mathbb{N}.$$

Then $R^{\mathbb{N}}$ becomes a left R -module.

Example 3.6. Let R be a ring. The set $M_{m \times n}(R)$ of all $m \times n$ matrices with entries in R forms an abelian group under matrix addition.

(1) **As a left R -module.** Let $r \in R$ and $A = (a_{ij}) \in M_{m \times n}(R)$, then we define scalar multiplication as follows.

$$r \cdot A = (ra_{ij}) \in M_{m \times n}(R).$$

This makes $M_{m \times n}(R)$ into a left R -module.

(2) **As a left $M_m(R)$ -module.** Let $S = M_m(R)$, the ring of $m \times m$ matrices over R . We now give $M_{m \times n}(R)$ the structure of a left S -module as follows. Let $S \in M_m(R)$ and $A \in M_{m \times n}(R)$. If $S = (s_{ij})$ and $A = (a_{jk})$, then the (i, k) -entry of SA is given by

$$(SA)_{ik} = \sum_{j=1}^m s_{ij} a_{jk}.$$

Thus, $M_{m \times n}(R)$ carries simultaneously the structure of a left R -module (by scalar action on entries) and a left $M_m(R)$ -module (by matrix multiplication).

Example 3.7. Let R be a ring and S be a non-empty index set. Let $\{M_s\}_{s \in S}$ be a family of left R -modules. Then the *direct product*

$$\prod_{s \in S} M_s$$

is defined as the Cartesian product of the underlying abelian groups of the M_s , equipped with coordinate-wise addition defined by

$$(x_s)_{s \in S} + (y_s)_{s \in S} = (x_s + y_s)_{s \in S},$$

and scalar multiplication by $r \in R$ is defined by coordinate-wise as

$$r \cdot (x_s)_{s \in S} = (rx_s)_{s \in S}.$$

Then it is easy to verify that $\prod_{s \in S} M_s$ is a left R -module with the operations defined above.

Remark 3.2. If S is finite, then the direct product coincides with the direct sum $\bigoplus_{s \in S} M_s$ (defined in the next example). Also, if S is infinite, then the direct sum is a R -submodule of the direct product consisting of those families $(x_s)_{s \in S}$ in which all but finitely many x_s are zero.

Example 3.8. Let R be a ring and S be a non-empty index set. Let $\{M_s\}_{s \in S}$ be a family of left R -modules. Then the *direct sum*

$$\bigoplus_{s \in S} M_s$$

is the subset of the direct product $\prod_{s \in S} M_s$ consisting of all families $(x_s)_{s \in S}$ such that

$$x_s = 0 \quad \text{for all but finitely many } s \in S.$$

Addition and scalar multiplication are defined coordinate-wise as follows.

$$(x_s)_{s \in S} + (y_s)_{s \in S} = (x_s + y_s)_{s \in S}, \quad r \cdot (x_s)_{s \in S} = (rx_s)_{s \in S}.$$

Then $\bigoplus_{s \in S} M_s$ is a left R -module with the above operations.

Remark 3.3. If S is finite, then

$$\bigoplus_{s \in S} M_s = \prod_{s \in S} M_s.$$

Also, if S is infinite, then the direct sum is a proper submodule of the direct product.

Example 3.9. Let R be a non-zero ring with identity and S be a non-empty set. We define the left R -module

$$F(S) = \bigoplus_{s \in S} R,$$

the direct sum of copies of R indexed by S . For each $s \in S$, let $i_s : R \rightarrow F(S)$ denote the natural embedding into the s -th component. Next, we define a map

$$\partial : S \longrightarrow F(S), \quad \partial(s) = i_s(1),$$

where 1 is the multiplicative identity of R . The module $F(S)$, together with the function ∂ , is called the *free left R -module on S* .

Definition 3.2 (R -Submodule). Let R be a ring and M a left R -module. An R -submodule of M is a subset $N \subseteq M$ such that

- (1) $(N, +)$ is an additive subgroup of $(M, +)$,
- (2) $rm \in N$ for all $r \in R$ and $m \in N$.

Equivalently, N is a submodule if it is closed under addition and under scalar multiplication by elements of R .

When the context is clear, we can omit the qualifier “left”.

Example 3.10. Let R be a ring with identity and M a unital left R -module. For $m \in M$, the R -submodule of M generated by m is

$$Rm = \{rm : r \in R\}.$$

Note that Rm is an abelian group since

$$(r \pm s)m = rm \pm sm,$$

and it is closed under scalar multiplication since

$$s(rm) = (sr)m.$$

Moreover, Rm contains m since $1m = m$.

Remark 3.4. If M is not unital, then the submodule generated by m may not equal Rm . This explains why the assumption of unitality was required in the construction of free R -modules.

More generally, if $\{m_1, \dots, m_n\} \subseteq M$ and M is unital, then the submodule generated by $m_1, \dots, m_n$ is

$$Rm_1 + Rm_2 + \dots + Rm_n.$$

Example 3.11 (Ideals as Submodules). Recall from Example 3.2 that R can be regarded as a left R -module. In this setting, the left R -submodules of R are precisely the *left ideals* of R . Recall that a subset $I \subseteq R$ is a left ideal if

- (1) I is an additive subgroup of R , and
- (2) $ra \in I$ for all $r \in R$ and $a \in I$.

If R has an identity, then R is a unital left R -module, and the left ideal of R generated by an element $a \in R$ is

$$Ra = \{ra : r \in R\}.$$

Similarly, the right ideals are exactly the right R -submodules of the right R -module R .

Recall that if R is commutative, then the notions of left ideals, right ideals, and two-sided ideals coincide.

Remark 3.5. Let R be a ring and M be a left R -module. If N is an R -submodule of M , then the quotient abelian group M/N becomes a left R -module by

$$r \cdot (m + N) = (rm) + N, \quad r \in R, \quad m \in M.$$

It is clear that the above operation is well defined and satisfies the module axioms. The resulting R -module M/N is called the *quotient module* of M by N .

Problem 3.1. Let R be a ring. Let M be a left R -module, and let $I \subseteq R$ be a *right* ideal. Define the annihilator of I in M by

$$\text{Ann}_M(I) = \{m \in M \mid a \cdot m = 0 \text{ for all } a \in I\}.$$

Prove that $\text{Ann}_M(I)$ is a submodule of M .

Solution 3.1. Clearly, $0 \in \text{Ann}_M(I)$ as $a \cdot 0 = 0$ for every $a \in I$. If $m, n \in \text{Ann}_M(I)$, then for every $a \in I$ we have

$$a \cdot (m + n) = a \cdot m + a \cdot n = 0 + 0 = 0.$$

This implies that $m + n \in \text{Ann}_M(I)$. On the other hand, we have

$$a \cdot (-m) = -(a \cdot m) = -0 = 0$$

Therefore, $-m \in \text{Ann}_M(I)$ and hence $\text{Ann}_M(I)$ is an additive subgroup of M .

Next, let $r \in R$ and $m \in \text{Ann}_M(I)$. For every $a \in I$, we have

$$a \cdot (r \cdot m) = (ar) \cdot m.$$

Note that $ar \in I$, since I is a right ideal. Since m is annihilated by every element of I , we have $(ar) \cdot m = 0$. Therefore, $a \cdot (r \cdot m) = 0$ for all $a \in I$ and hence $r \cdot m \in \text{Ann}_M(I)$.

Thus, $\text{Ann}_M(I)$ is closed under addition, additive inverses, and scalar multiplication, hence it is an R -submodule of M .

Problem 3.2. Let M be an abelian group and let $\text{End } M$ be the set of all endomorphisms on M , i.e. the set of all group homomorphisms $f : M \rightarrow M$.

- (1) Show that $\text{End } M$ is an abelian group under the law $(f, g) \mapsto f + g$ defined by

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in M.$$

- (2) Prove that the following

- (a) $(\text{End } M, +, \circ)$ is a unitary ring.
- (b) M is an $\text{End } M$ -module under the action

$$\text{End } M \times M \rightarrow M, \quad (f, m) \mapsto f \cdot m = f(m).$$

- (c) If R is a unitary ring and $\mu : R \rightarrow \text{End } M$ is a ring morphism such that $\mu(1_R) = \text{id}_M$, then M is an R -module under the action

$$R \times M \rightarrow M, \quad (\lambda, m) \mapsto \lambda m := [\mu(\lambda)](m).$$

Solution 3.2. (1) First, we verify that $(\text{End } M, +)$ is an abelian group.

• **Associativity:** Let $f, g, h \in \text{End } M$ and $x \in M$. Then

$$((f + g) + h)(x) = (f + g)(x) + h(x) = (f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x)) = (f + (g + h))(x).$$

• **Commutativity:** $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$.

• **Identity:** The zero map $0 : M \rightarrow M$, $0(x) = 0$, satisfies $(f + 0)(x) = f(x)$.

• **Inverse:** Define $(-f)(x) = -f(x)$, then $(f + (-f))(x) = 0$.

Hence, $(\text{End } M, +)$ is an abelian group.

- (2) (a) Composition of elements in $\text{End } M$ satisfies associative, and $\text{End } M$ has identity id_M , and $\circ$ distributes over $+$ as follows.

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

Hence, $(\text{End } M, +, \circ)$ is a unitary ring.

- (b) Define the action $(f, m) \mapsto f(m)$. For $f, g \in \text{End } M$ and $m \in M$,

$$(f + g) \cdot m = (f + g)(m) = f(m) + g(m) = f \cdot m + g \cdot m,$$

$$(f \circ g) \cdot m = (f \circ g)(m) = f(g(m)) = f \cdot (g \cdot m),$$

and $\text{id}_M \cdot m = m$. Hence, M is a left $\text{End } M$ -module.

- (c) Let $\mu : R \rightarrow \text{End } M$ be a ring homomorphism with $\mu(1_R) = \text{id}_M$. Define $\lambda m := [\mu(\lambda)](m)$.

Then for $\lambda, \rho \in R$ and $m, n \in M$, we have

$$(\lambda + \rho)m = [\mu(\lambda + \rho)](m) = (\mu(\lambda) + \mu(\rho))(m) = \mu(\lambda)(m) + \mu(\rho)(m) = \lambda m + \rho m,$$

$$(\lambda \rho)m = [\mu(\lambda \rho)](m) = (\mu(\lambda) \circ \mu(\rho))(m) = \mu(\lambda)(\mu(\rho)(m)) = \lambda(\rho m),$$

$$1_R m = [\mu(1_R)](m) = \text{id}_M(m) = m.$$

Hence, M is a left R -module.

Problem 3.3. Let S be a non-empty set and R a unitary ring. Define F as the set of all functions $f : S \rightarrow R$ such that $f(s) = 0$ for all but finitely many $s \in S$.

Define addition and scalar multiplication on F by

$$(f + g)(s) = f(s) + g(s), \quad (\lambda f)(s) = \lambda f(s), \quad f, g \in F, \lambda \in R.$$

Show that F is a left R -module under these operations.

Solution 3.3. (1) Abelian group under addition:

- (a) **Closure:** Let $f, g \in F$. Since $f(s) = 0$ and $g(s) = 0$ for all but finitely many $s \in S$, $(f + g)(s) = f(s) + g(s) = 0$ for all but finitely many $s \in S$. Hence, $f + g \in F$.

- (b) **Associativity:** It is clear.

- (c) **Identity:** The zero function $0(s) = 0$ satisfies $(f + 0)(s) = f(s)$.

- (d) **Inverses:** For $f \in F$, define $(-f)(s) = -f(s)$. Then $(f + (-f))(s) = 0$.

- (e) **Commutativity:** $(f + g)(s) = f(s) + g(s) = g(s) + f(s) = (g + f)(s)$.

- (2) Compatibility with scalar multiplication:

- (a) **Distributivity over function addition:** For $\lambda \in R$,

$$\lambda \cdot (f + g)(s) = \lambda(f(s) + g(s)) = \lambda f(s) + \lambda g(s) = (\lambda f + \lambda g)(s).$$

- (b) **Distributivity over ring addition:** For $\lambda, \mu \in R$,

$$(\lambda + \mu) \cdot f(s) = (\lambda + \mu)f(s) = \lambda f(s) + \mu f(s) = (\lambda f + \mu f)(s).$$

- (c) **Compatibility with ring multiplication:** For $\lambda, \mu \in R$,

$$(\lambda \mu) \cdot f(s) = (\lambda \mu)f(s) = \lambda(\mu f(s)) = \lambda \cdot (\mu f)(s).$$

- (d) **Identity element:** $1_R \cdot f(s) = 1_R f(s) = f(s)$.

Since all module axioms are satisfied, F is a left R -module.

Problem 3.4. Let M be an R -module and let $r, s \in R$.

- (1) Show that if $r - s \in \text{Ann}_R M$, then $rx = sx$ for all $x \in M$.
(2) Deduce that M can be regarded as an $R/\text{Ann}_R M$ -module.

(3) Show that the annihilator of M in $R/\text{Ann}_R M$ is zero.

Solution 3.4. (1) Suppose $r - s \in \text{Ann}_R M$. By definition,

$$(r - s)x = 0 \quad \text{for all } x \in M.$$

Expanding the left-hand side gives

$$rx - sx = 0 \implies rx = sx, \quad \forall x \in M.$$

(2) Consider the quotient ring $R/\text{Ann}_R M$ and define an action on M by

$$(r + \text{Ann}_R M) \cdot x := rx, \quad r \in R, x \in M.$$

This is well-defined because if $r + \text{Ann}_R M = s + \text{Ann}_R M$, then $r - s \in \text{Ann}_R M$, and by Part (1), $rx = sx$ for all $x \in M$.

The module axioms follow immediately from the fact that M as an R -module. Hence, M is an $R/\text{Ann}_R M$ -module.

(3) Let $\bar{r} = r + \text{Ann}_R M \in R/\text{Ann}_R M$, and assume

$$\bar{r} \cdot x = 0 \quad \text{for all } x \in M.$$

By the definition of the action, we obtain $rx = 0$ for all $x \in M$. Hence, $r \in \text{Ann}_R M$. Consequently,

$$\bar{r} = r + \text{Ann}_R M = 0 \quad \text{in } R/\text{Ann}_R M.$$

Therefore, the annihilator of M in $R/\text{Ann}_R M$ is zero.

Problem 3.5. Let M be an R -module. The module M is called *simple* if its only submodules are $\{0\}$ and M . Prove that M is simple if and only if every non-zero element of M generates M , that is,

$$\forall x \in M, x \neq 0 \implies Rx = M.$$

Solution 3.5. First, we assume that M is simple. Let $x \in M$ with $x \neq 0$. The set

$$Rx = \{rx : r \in R\}$$

is a submodule of M . Since $x \neq 0$, we have $Rx \neq \{0\}$. Note that the only possible non-zero submodule is M itself, since M simple. Hence, $Rx = M$. Thus, every non-zero element of M generates M .

Conversely, suppose that every non-zero $x \in M$ satisfies $Rx = M$. Let N be any submodule of M . If $N = \{0\}$, we are done. Otherwise, pick a non-zero $x \in N$. Then $Rx = M$, but since $x \in N$ and N is closed under scalar multiplication, we must have $Rx \subseteq N$. Hence, $M \subseteq N$, which implies $N = M$. Therefore, the only submodules of M are $\{0\}$ and M . Thus, we conclude that M is simple.

Problem 3.6. Let R be a commutative ring with unity and let M be an R -module. For each $r \in R$ define

$$rM = \{rx : x \in M\}, \quad M_r = \{x \in M : rx = 0\}.$$

(1) Prove that both rM and M_r are R -submodules of M .

(2) Suppose $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, where $n = rs$ with $\gcd(r, s) = 1$. Show that $rM = M_s$.

Solution 3.6. (1) Clearly, $0 = r \cdot 0 \in rM$. If $x, y \in M$, then

$$(rx) + (ry) = r(x + y) \in rM.$$

Hence, rM is closed under addition. For any $a \in R$ and $x \in M$,

$$a(rx) = (ar)x = r(ax) \in rM.$$

This implies that rM is closed under scalar multiplication. Thus, rM is a R -submodule.

Next, since $r \cdot 0 = 0$, we have $0 \in M_r$. If $x, y \in M_r$ then $rx = ry = 0$, and hence

$$r(x + y) = rx + ry = 0.$$

This implies that $x + y \in M_r$. For any $a \in R$ and $x \in M_r$,

$$r(ax) = a(rx) = a \cdot 0 = 0.$$

Therefore, $ax \in M_r$. Thus, M_r is also a R -submodule.

- (2) Let $R = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$ with $n = rs$, $\gcd(r, s) = 1$. Then we have

$$rM = \{ r[k] : k \in \mathbb{Z} \} = \{ [rk] : k \in \mathbb{Z} \},$$

and

$$M_s = \{ [k] \in \mathbb{Z}/n\mathbb{Z} : s[k] = [sk] = [0] \}.$$

If $[y] = [rk] \in rM$, then

$$s[y] = s[rk] = [srk] = [nk] = [0],$$

hence $[y] \in M_s$.

Let $[k] \in M_s$. Then $[sk] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$ and so $n \mid sk$. Since $n = rs$, we get $rs \mid sk$. This implies that there exists $t \in \mathbb{Z}$ such that

$$sk = trs.$$

by cancelling s (since $\gcd(r, s) = 1$), we obtain $k = tr$. Hence,

$$[k] = [tr] = r[t] \in rM.$$

Thus, we conclude that

$$rM = M_s.$$

4. Ring and Module Homomorphisms

Definition 4.1 (Ring Homomorphism). Let R and S be rings. A map

$$\varphi : R \longrightarrow S$$

is called a *ring homomorphism* if

- (1) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$.
- (2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a, b \in R$.
- (3) If R and S have unity 1_R and 1_S , respectively, then $\varphi(1_R) = 1_S$.

Remark 4.1. A ring homomorphism preserves additive inverses since $\varphi(-a) = -\varphi(a)$. The kernel of φ , defined by

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

is an ideal of R , and the image of φ is a subring of S .

Example 4.1. (1) Consider the map

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \quad \varphi(k) = [k]_n,$$

where $\mathbb{Z}_n$ is the ring of integers modulo n . Then φ is a ring homomorphism because

$$\varphi(a + b) = [a + b]_n = [a]_n + [b]_n = \varphi(a) + \varphi(b),$$

$$\varphi(a \cdot b) = [a \cdot b]_n = [a]_n \cdot [b]_n = \varphi(a) \cdot \varphi(b),$$

and $\varphi(1) = [1]_n$.

- (2) Let R be a commutative ring and $I \subseteq R$ an ideal. Define the natural projection

$$\pi : R \longrightarrow R/I, \quad \pi(r) = r + I.$$

Then π is a surjective ring homomorphism with kernel I .

- (3) Consider $R = \mathbb{C}$ and $S = \mathbb{C}$. Define

$$\varphi : \mathbb{C} \longrightarrow \mathbb{C}, \quad \varphi(z) = \bar{z}.$$

This is a ring homomorphism.

- (4) Let $R = \mathbb{Z}$ and $S = \mathbb{Q}$. The inclusion map

$$\iota : \mathbb{Z} \longrightarrow \mathbb{Q}, \quad \iota(n) = n,$$

is a ring homomorphism. This is injective, but not surjective.

- (5) Let R be a ring, $R[X]$ the polynomial ring over R , and let $a \in R$. Define

$$\varphi_a : R[X] \longrightarrow R, \quad \varphi_a(f(X)) = f(a).$$

Then φ_a is a ring homomorphism. This is the standard *evaluation homomorphism*.

- (6) Let $R = M_n(R)$ be the ring of $n \times n$ matrices over a ring R , and let $S = R$. Define

$$\varphi : M_n(R) \longrightarrow R, \quad \varphi(A) = \text{tr}(A),$$

the trace of A . Then $\varphi(A+B) = \varphi(A) + \varphi(B)$ and $\varphi(cA) = c\varphi(A)$ for $c \in R$. Therefore, it is an additive group homomorphism. Note that it is not multiplicative, hence not a ring homomorphism. But the additive and multiplicative properties both hold.

- (7) Let R be a ring and $f(X) \in R[X]$ a fixed polynomial. Define

$$\varphi : R[X] \longrightarrow R[X]/(f(X)), \quad \varphi(g(X)) = g(X) + (f(X)).$$

This is the natural quotient homomorphism and it is surjective with kernel $(f(X))$.

Definition 4.2 (R -Module Homomorphism). Let R be a ring, and let M and N be left R -modules. A map $\varphi : M \rightarrow N$ is called an *R -module homomorphism* if

- (1) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$, and
- (2) $\varphi(rx) = r\varphi(x)$ for all $r \in R, x \in M$.

Definition 4.3 (Isomorphism of R -Modules). An R -module homomorphism $\varphi : M \rightarrow N$ is an *isomorphism* if φ is both injective and surjective. In this case, M and N are said to be *isomorphic* and denoted by

$$M \cong N.$$

Definition 4.4. Let $\varphi : M \rightarrow N$ be an R -module homomorphism. The *kernel* of φ is

$$\ker(\varphi) = \{ m \in M \mid \varphi(m) = 0 \},$$

and the *image* of φ is

$$\text{im}(\varphi) = \{ \varphi(m) \in N \mid m \in M \}.$$

Remark 4.2. For R -modules M and N , the set of all R -module homomorphisms from M to N is denoted $\text{Hom}_R(M, N)$.

Remark 4.3. Every R -module homomorphism is a homomorphism of the underlying additive groups. However, not every group homomorphism between the additive groups of R -modules is an R -module homomorphism, since it may fail to respect scalar multiplication.

Example 4.2. (i) Let R be a ring and $M = R^n$ for some $n \in \mathbb{Z}^+$. For each $i \in \{1, \dots, n\}$, the projection map

$$\pi_i : R^n \rightarrow R, \quad \pi_i(x_1, \dots, x_n) = x_i,$$

is a surjective R -module homomorphism. Its kernel is the R -submodule of all n -tuples with a zero in the i -th coordinate.

- (ii) For the ring $R = \mathbb{Z}$, any $\mathbb{Z}$ -module homomorphism is the same as a group homomorphism of the underlying abelian groups.
- (iii) Let R be a ring, I a two-sided ideal of R , and suppose M and N are R -modules annihilated by I , that is,

$$am = 0, \quad an = 0 \quad \text{for all } a \in I, m \in M, n \in N.$$

Then any R -module homomorphism $N \rightarrow M$ is an (R/I) -module homomorphism. In particular, if A is an abelian group such that $pa = 0$ for all $a \in A$ and for some prime p , then any group homomorphism $A \rightarrow A$ is a $\mathbb{Z}/p\mathbb{Z}$ -module homomorphism.

Proposition 4.1. Let M, N , and L be R -modules.

- (1) A map $\varphi : M \rightarrow N$ is an R -module homomorphism if and only if

$$\varphi(rx + y) = r\varphi(x) + \varphi(y) \quad \text{for all } x, y \in M, r \in R.$$

(2) Let $\varphi, \psi \in \text{Hom}_R(M, N)$. Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m), \quad \text{for all } m \in M.$$

Then $\varphi + \psi \in \text{Hom}_R(M, N)$, and with the above operation $\text{Hom}_R(M, N)$ is an abelian group. If R is commutative, define for $r \in R$

$$(r\varphi)(m) = r \cdot \varphi(m), \quad m \in M.$$

Then $r\varphi \in \text{Hom}_R(M, N)$, and with this scalar multiplication $\text{Hom}_R(M, N)$ is an R -module.

(3) If $\varphi \in \text{Hom}_R(L, M)$ and $\psi \in \text{Hom}_R(M, N)$, then $\psi \circ \varphi \in \text{Hom}_R(L, N)$.

(4) With addition as in (2) and multiplication given by function composition, $\text{Hom}_R(M, M)$ is a ring with multiplicative identity the identity map id_M .

PROOF. (1) If φ is an R -module homomorphism, then

$$\varphi(rx + y) = \varphi(rx) + \varphi(y) = r\varphi(x) + \varphi(y).$$

Conversely, assume $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $r \in R, x, y \in M$. Choosing $r = 1$, we obtain

$$\varphi(x + y) = \varphi(x) + \varphi(y).$$

This shows that φ is additive. Choosing $y = 0$, we obtain

$$\varphi(rx) = r\varphi(x),$$

and hence φ is a scalar multiplication. Thus, φ is an R -module homomorphism.

(2) For $\varphi, \psi \in \text{Hom}_R(M, N)$, the map $\varphi + \psi$ is additive since

$$\begin{aligned} (\varphi + \psi)(x + y) &= \varphi(x + y) + \psi(x + y) \\ &= \varphi(x) + \varphi(y) + \psi(x) + \psi(y) \\ &= (\varphi + \psi)(x) + (\varphi + \psi)(y). \end{aligned}$$

Similarly, we obtain

$$(\varphi + \psi)(rx) = \varphi(rx) + \psi(rx) = r\varphi(x) + r\psi(x) = r(\varphi + \psi)(x).$$

Thus, $\varphi + \psi \in \text{Hom}_R(M, N)$. It is straightforward to verify that $\text{Hom}_R(M, N)$ with this operation forms an abelian group.

If R is commutative, then define $(r\varphi)(m) = r\varphi(m)$, and we compute

$$(r\varphi)(x + y) = r(\varphi(x) + \varphi(y)) = r\varphi(x) + r\varphi(y),$$

and

$$(r\varphi)(sx) = r\varphi(sx) = r(s\varphi(x)) = (rs)\varphi(x) = s(r\varphi)(x).$$

Thus, $r\varphi \in \text{Hom}_R(M, N)$. Hence, $\text{Hom}_R(M, N)$ is an R -module.

(3) Let $\varphi \in \text{Hom}_R(L, M)$ and $\psi \in \text{Hom}_R(M, N)$. For $x, y \in L, r \in R$, we compute

$$\begin{aligned} (\psi \circ \varphi)(rx + y) &= \psi(\varphi(rx + y)) \\ &= \psi(r\varphi(x) + \varphi(y)) \\ &= r\psi(\varphi(x)) + \psi(\varphi(y)) \\ &= r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y). \end{aligned}$$

Thus, $\psi \circ \varphi$ is an R -module homomorphism.

(4) Since the domain and co-domain of elements of $\text{Hom}_R(M, M)$ are both M , composition is well-defined. By (3), composition is closed in $\text{Hom}_R(M, M)$. It is associative by definition of function composition. The additive structure is abelian by (2). The multiplicative identity is the identity map $\text{id}_M : M \rightarrow M$. Thus, $\text{Hom}_R(M, M)$ is a ring. $\square$

Problem 4.1. Let R be a ring, and let $\varphi : M \rightarrow N$ be an R -module homomorphism. Then

(i) $\ker(\varphi)$ is an R -submodule of M , and

(ii) $\text{im}(\varphi)$ is an R -submodule of N .

Solution 4.1. (i) Let $x, y \in \ker(\varphi)$ and $r \in R$. Then

$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0.$$

This implies that $x + y \in \ker(\varphi)$. Moreover,

$$\varphi(rx) = r\varphi(x) = r \cdot 0 = 0,$$

and hence $rx \in \ker(\varphi)$. Thus, $\ker(\varphi)$ is a R -submodule of M .

(ii) Let $u, v \in \text{im}(\varphi)$ and $r \in R$. Then $u = \varphi(x)$ and $v = \varphi(y)$ for some $x, y \in M$, and we compute

$$u + v = \varphi(x) + \varphi(y) = \varphi(x + y) \in \text{im}(\varphi),$$

and

$$ru = r\varphi(x) = \varphi(rx) \in \text{im}(\varphi).$$

Hence, $\text{im}(\varphi)$ is a submodule of N .

Problem 4.2. Let M and N be R -modules and let $f : M \rightarrow N$ be an R -module homomorphism. Show that for every submodule $X \subseteq M$, the image

$$f(X) = \{f(x) : x \in X\}$$

is a submodule of N , and for every submodule $Y \subseteq N$, the preimage

$$f^{-1}(Y) = \{m \in M : f(m) \in Y\}$$

is a submodule of M .

Solution 4.2. First, we prove that the image $f(X)$ is a submodule of N . Since $0_M \in X$, we have $f(0_M) = 0_N \in f(X)$ and so the image contains the zero element. If $y_1 = f(x_1)$ and $y_2 = f(x_2)$ are elements of $f(X)$ with $x_1, x_2 \in X$, then

$$y_1 - y_2 = f(x_1) - f(x_2) = f(x_1 - x_2).$$

Since X is a submodule of M , we have $x_1 - x_2 \in X$, and hence $y_1 - y_2 \in f(X)$. Moreover, for any $\lambda \in R$,

$$\lambda y_1 = \lambda f(x_1) = f(\lambda x_1) \in f(X),$$

as $\lambda x_1 \in X$. Thus, $f(X)$ is closed under subtraction and scalar multiplication, which shows that $f(X)$ is a submodule of N .

We now consider the preimage $f^{-1}(Y)$. Since $f(0_M) = 0_N \in Y$, it follows that $0_M \in f^{-1}(Y)$. If $a, b \in f^{-1}(Y)$, then $f(a), f(b) \in Y$. As Y is a submodule of N , we have

$$f(a - b) = f(a) - f(b) \in Y,$$

and hence $a - b \in f^{-1}(Y)$. Furthermore, for any $\lambda \in R$,

$$f(\lambda a) = \lambda f(a) \in Y,$$

which implies $\lambda a \in f^{-1}(Y)$. Hence, $f^{-1}(Y)$ is closed under subtraction and scalar multiplication, proving that it is a submodule of M .

5. Universal Property

Theorem 5.1 (Universal Property of the Quotient Ring). Let A be a ring and I be an ideal of A . Then the quotient ring A/I satisfies the following universal property: for any ring homomorphism $f : A \rightarrow B$ such that $f(I) = \{0\}$, there exists a unique ring homomorphism

$$\tilde{f} : A/I \longrightarrow B$$

such that

$$f = \tilde{f} \circ \pi,$$

where $\pi : A \rightarrow A/I$ is the canonical projection.

Equivalently, the following diagram commutes (see Figure 1).

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \exists! g & \\ A/I & & \end{array}$$

FIGURE 1. Universal mapping property of the quotient ring A/I .

This property defines the quotient ring A/I up to unique isomorphism.

PROOF. Define $g: A/I \rightarrow B$ by

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

First, we prove g is a well-defined map. Suppose $a_1 + I = a_2 + I$. Then $a_1 - a_2 \in I$, and since $f(I) = 0$,

$$f(a_1) - f(a_2) = f(a_1 - a_2) = 0.$$

Thus, $f(a_1) = f(a_2)$ and hence g is well-defined.

Next, we prove g is a homomorphism. For $a_1, a_2 \in A$, we have

$$g((a_1 + I) + (a_2 + I)) = g(a_1 + a_2 + I) = f(a_1 + a_2) = f(a_1) + f(a_2) = g(a_1 + I) + g(a_2 + I).$$

Similarly,

$$g((a_1 + I)(a_2 + I)) = g(a_1 a_2 + I) = f(a_1 a_2) = f(a_1)f(a_2) = g(a_1 + I)g(a_2 + I).$$

Finally, we prove the uniqueness. If $h: A/I \rightarrow B$ is another ring homomorphism with $f = h \circ \pi$, then for all $a \in A$, we have

$$h(a + I) = h(\pi(a)) = f(a) = g(a + I).$$

Therefore, $h = g$. Thus, g exists and is unique, proving the universal property. $\square$

Example 5.1. Let G be a group. We can make the free abelian group

$$\mathbb{Z}G = \left\{ \sum_{i=1}^n m_i g_i \mid n \geq 0, m_i \in \mathbb{Z}, g_i \in G \right\}$$

on the elements of G into a ring by defining multiplication of

$$x = \sum_{i=1}^n m_i g_i, \quad y = \sum_{j=1}^k n_j h_j \quad (m_i, n_j \in \mathbb{Z}, g_i, h_j \in G),$$

by

$$x \cdot y = \sum_{i=1}^n \sum_{j=1}^k m_i n_j (g_i h_j),$$

where $g_i h_j$ denotes the product in G .

It is clear that $\mathbb{Z}G$ is a ring with identity 1_G , and that G is embedded as a subgroup of the unit group $(\mathbb{Z}G)^\times$ by identifying each $g \in G$ with $1 \cdot g$.

The ring $\mathbb{Z}G$ is called the *integral group ring* of G .

Universal Property. Let $\iota: G \rightarrow \mathbb{Z}G$ be the canonical embedding $g \mapsto 1 \cdot g$. If $\varphi: G \rightarrow R^\times$ is a group homomorphism from G to the unit group of a ring R , then there exists a unique ring homomorphism

$$\psi: \mathbb{Z}G \longrightarrow R$$

such that $\psi \circ \iota = \varphi$.

The map ψ exists as a homomorphism of additive groups by the universal property of free abelian groups, and it can be easily verified that ψ also preserves multiplication.

Equivalently, the following diagram commutes (see Figure 2).

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & R^\times \\ \downarrow \iota & \nearrow \exists! \psi & \\ \mathbb{Z}G & & \end{array}$$

FIGURE 2. Universal mapping property of the integral group ring of G .

Example 5.2. Let R be a non-zero ring with identity, and let S be a non-empty set. Recall from Example 3.9, the direct sum

$$F(S) = \bigoplus_{s \in S} R$$

is called the *free left R -module* on S . Let $\iota_s: R \rightarrow F(S)$ denote the usual embedding map of each summand. Define the map

$$\partial: S \rightarrow F(S), \quad \partial(s) = \iota_s(1).$$

Then the left R -module $F(S)$ satisfies a universal mapping property similar to that of free abelian groups. This is illustrated in Figure 3 and can be stated as follows.

Whenever M is a unital left R -module and $\varphi: S \rightarrow M$ is a function, there exists a unique R -module homomorphism

$$\psi: F(S) \rightarrow M$$

such that $\psi \circ \partial = \varphi$.

The existence of ψ as an R -module homomorphism follows from the universal mapping property of direct sums, once the property is established for the case when S is a singleton set. Indeed, if A is any left R -module and $a \in A$, then the map $r \mapsto ra$ is the unique R -module homomorphism from R to A sending $1 \in R$ to a . Equivalently, the following diagram commutes.

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & M \\ \downarrow \partial & \nearrow \exists! \psi & \\ F(S) & & \end{array}$$

FIGURE 3. Universal mapping property of a free left R -module.

Proposition 5.1. Let R be a ring, and let $\varphi: M_1 \rightarrow M_2$ be an R -module homomorphism between left R -modules. Set $N_0 = \ker \varphi$, and let N be an R -submodule of M_1 with $N \subseteq N_0$. Define the quotient map

$$q: M_1 \rightarrow M_1/N.$$

Then there exists an R -module homomorphism

$$\bar{\varphi}: M_1/N \rightarrow M_2$$

such that $\varphi = \bar{\varphi} \circ q$, that is, $\bar{\varphi}(m_1 + N) = \varphi(m_1)$ for all $m_1 \in M_1$. Moreover, $\bar{\varphi}$ has the same image as φ , and its kernel is

$$\ker \bar{\varphi} = \{h_0 N \mid h \in N_0\}.$$

Remark 5.1. Similar to the case for groups, the homomorphism φ is said to *factor through* the quotient module M_1/N , or equivalently, to *descend* to M_1/N . This means that φ can be expressed as the composition of the quotient map $q: M_1 \rightarrow M_1/N$ followed by a well-defined homomorphism $\bar{\varphi}: M_1/N \rightarrow M_2$. This factorization is illustrated in Figure 4.

$$\begin{array}{ccc}
 M_1 & \xrightarrow{\varphi} & M_2 \\
 q \downarrow & \nearrow \bar{\varphi} & \\
 M_1/N & &
 \end{array}$$

FIGURE 4. Factorization of an R -module homomorphism through a quotient module.

Corollary 5.1. Let R be a ring, and let $\varphi: M_1 \rightarrow M_2$ be an R -module homomorphism between left R -modules. Suppose that φ is surjective and has kernel N . Then φ induces a canonical isomorphism of left R -modules

$$M_1/N \cong M_2.$$

Theorem 5.2 (First Isomorphism Theorem). Let R be a ring, and let $\varphi: M_1 \rightarrow M_2$ be a surjective homomorphism of left R -modules with kernel $K = \ker(\varphi)$. Then the map

$$N_1 \mapsto \varphi(N_1)$$

gives a one-to-one correspondence between

- (a) the R -submodules $N_1 \leq M_1$ containing K , and
- (b) the R -submodules of M_2 .

Moreover, under this correspondence, the map

$$m + N_1 \mapsto \varphi(m) + \varphi(N_1)$$

defines an isomorphism of left R -modules

$$M_1/N_1 \cong M_2/\varphi(N_1).$$

Remark 5.2. In the special case where φ is the canonical quotient map

$$q: M \rightarrow M/K,$$

for an R -submodule $K \leq M$, and N is any submodule containing K , the above theorem ensures that

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

Theorem 5.3 (Second Isomorphism Theorem). Let R be a ring, M a left R -module, and let $N_1, N_2 \leq M$ be R -submodules. Then

- (a) The intersection $N_1 \cap N_2$ is an R -submodule of N_1 .
- (b) The sum $N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$ is an R -submodule of M .
- (c) The map

$$n_1 + (N_1 \cap N_2) \mapsto n_1 + N_2$$

induces a well-defined isomorphism of left R -modules

$$\frac{N_1}{N_1 \cap N_2} \cong \frac{N_1 + N_2}{N_2}.$$

Problem 5.1. Let R be a ring, and let $\{M_s\}_{s \in S}$ be a family of left R -modules. For each $s \in S$, let N_s be a left R -submodule of M_s . Consider the direct sum

$$M = \bigoplus_{s \in S} M_s \quad \text{and} \quad N = \bigoplus_{s \in S} N_s.$$

Then the natural projection maps induce an R -module isomorphism

$$\frac{M}{N} \cong \bigoplus_{s \in S} \frac{M_s}{N_s}.$$

Solution 5.1. Define a map

$$\varphi : M = \bigoplus_{s \in S} M_s \longrightarrow \bigoplus_{s \in S} (M_s / N_s)$$

by sending an element $(m_s)_{s \in S} \in M$ to the tuple $(m_s + N_s)_{s \in S}$.

It is clear that φ is well-defined since each $m_s \in M_s$, and $N_s \leq M_s$, the coset $m_s + N_s$ is well-defined in M_s / N_s .

The map φ is an R -module homomorphism, since it acts coordinate-wise, and quotient maps are module homomorphisms. Therefore, φ is a homomorphism.

Next, we prove φ is bijective. For any $(m_s + N_s)_{s \in S}$ in $\bigoplus_{s \in S} (M_s / N_s)$, pick representatives $m_s \in M_s$. Then $\varphi((m_s)_{s \in S}) = (m_s + N_s)_{s \in S}$, showing φ is onto. Suppose $\varphi((m_s)) = (N_s)$, the zero element in $\bigoplus_{s \in S} (M_s / N_s)$. Then each $m_s \in N_s$, and hence $(m_s) \in \bigoplus_{s \in S} N_s = N$. Thus, $\ker(\varphi) = N$.

By the First Isomorphism Theorem for modules, we conclude that

$$M/N \cong \text{Im}(\varphi) = \bigoplus_{s \in S} (M_s / N_s).$$

Definition 5.1. Let R be a non-zero commutative ring with identity. An *associative R -algebra* is a ring A that is also a left R -module such that multiplication

$$A \times A \rightarrow A$$

is R -linear in each variable. In other words, for all $r \in R$ and $a, b \in A$,

$$(ra)b = r(ab) = a(rb).$$

If A has a multiplicative identity 1_A , then every scalar multiple $r \cdot 1_A$ lies in the center of A , commuting with all elements of A .

Example 5.3. Consider polynomial rings and matrix rings whose scalars lie in a commutative ring with identity. In particular, every ring R can be viewed as an associative $\mathbb{Z}$ -algebra by regarding the additive group of R as a $\mathbb{Z}$ -module via the standard integer action.

To verify the compatibility condition for $\mathbb{Z}$ -algebras, observe that for $n = 1$,

$$(1 \cdot a)b = 1 \cdot (ab) = a(1 \cdot b)$$

since the $\mathbb{Z}$ -module R is unital. Assuming the property holds for a positive integer n , that is,

$$(na)b = n(ab) = a(nb),$$

one can use distributivity to deduce it for $n + 1$

$$((n + 1)a)b = (n + 1)(ab) = a((n + 1)b).$$

By induction, this holds for all positive integers n , and extends to all integers n using additive inverses.

Example 5.4. Let G be a group and R be a commutative ring with identity. The *group algebra* RG is defined as the free R -module generated by the elements of G . Explicitly,

$$RG = \left\{ \sum_{g \in G} r_g g \mid r_g \in R, \text{ finitely many } r_g \neq 0 \right\}.$$

The operation multiplication in RG is determined by extending the group multiplication bilinearly over R . For elements

$$\sum_i r_i g_i \quad \text{and} \quad \sum_j s_j h_j$$

in RG (with $r_i, s_j \in R$ and $g_i, h_j \in G$), the product is given by

$$\left(\sum_i r_i g_i \right) \cdot \left(\sum_j s_j h_j \right) = \sum_{i,j} r_i s_j (g_i h_j).$$

This multiplication equips RG with the structure of an associative R -algebra with identity, where the identity element is given by $1_R \cdot e$, with e the identity element of the group G . The algebra RG is called the *group algebra of G over R* . For $R = \mathbb{Z}$, this is the integral group ring.

Note that the group G embeds into the unit group $(RG)^\times$ via

$$\partial : G \rightarrow RG, \quad g \mapsto 1 \cdot g.$$

Next, we discuss the universal property of the group algebra. For any group homomorphism $\varphi : G \rightarrow A^\times$, where A is an associative R -algebra with identity, there exists a unique R -algebra homomorphism $\Phi : RG \rightarrow A$ such that $\Phi \circ \partial = \varphi$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A^\times \\ \partial \downarrow & \nearrow \Phi & \\ RG & & \end{array}$$

FIGURE 5. Universal mapping property of the group algebra RG .

Problem 5.2. Let A , B , and C be R -modules, and let $f : A \rightarrow B$ and $g : A \rightarrow C$ be R -module homomorphisms with f surjective. Prove that the following statements are equivalent.

- (1) There exists a unique R -module homomorphism $h : B \rightarrow C$ such that $h \circ f = g$.
- (2) $\ker f \subseteq \ker g$.
- (3) Show that h is injective if and only if $\ker f = \ker g$.

Solution 5.2. (1) $\implies$ (2) Assume that there exists a homomorphism $h : B \rightarrow C$ such that $h \circ f = g$. If $x \in \ker f$, then

$$g(x) = h(f(x)) = h(0_B) = 0_C.$$

This implies that $x \in \ker g$. Therefore, $\ker f \subseteq \ker g$.

(2) $\implies$ (1) Assume $\ker f \subseteq \ker g$. To define $h : B \rightarrow C$, consider any $b \in B$. Since f is surjective, there exists $x \in A$ with $f(x) = b$. We define

$$h(b) := g(x).$$

First, we prove h is well-defined. For this, if $x, y \in A$ satisfy $f(x) = f(y) = b$, then

$$f(x - y) = f(x) - f(y) = 0_B \implies x - y \in \ker f \subseteq \ker g \implies g(x) = g(y).$$

Uniqueness follows from the surjectivity of f since for any $b \in B$, $b = f(x)$ for some x and hence $h(b) = h(f(x)) = g(x)$.

Next, we prove that h is an R -module homomorphism. Let $x, y \in A$ and $\lambda \in R$. Then

$$h(f(x) + f(y)) = h(f(x + y)) = g(x + y) = g(x) + g(y) = h(f(x)) + h(f(y)),$$

$$h(\lambda f(x)) = h(f(\lambda x)) = g(\lambda x) = \lambda g(x) = \lambda h(f(x)).$$

Since f is surjective, this shows h is an R -module homomorphism.

(3) Suppose h is injective. If $x \in \ker g$, then

$$0_C = g(x) = h(f(x)) \implies f(x) \in \ker h = \{0_B\} \implies x \in \ker f.$$

Hence, $\ker g \subseteq \ker f$, and together with $\ker f \subseteq \ker g$, we get $\ker f = \ker g$.

Conversely, if $\ker f = \ker g$, let $b \in \ker h$. Then $b = f(y)$ for some $y \in A$ (since f is surjective), and

$$0_C = h(b) = h(f(y)) = g(y) \implies y \in \ker g = \ker f \implies b = f(y) = 0_B.$$

Thus, h is injective.

6. Integral Domains

Definition 6.1 (Skew Ring). A *skew ring*, also called a *division ring*, is a ring R with unity such that every non-zero element of R has a multiplicative inverse, that is, for each $a \in R \setminus \{0\}$, there exists $b \in R$ with

$$ab = ba = 1.$$

The multiplication in a skew ring need not be commutative.

Example 6.1. In the ring $\mathbb{Z}$, there are no zero divisors. The only units are ± 1 . Every non-zero integer has an inverse in the larger ring $\mathbb{Q}$, but not in $\mathbb{Z}$ itself.

Example 6.2. In the ring $\mathbb{Z}/n\mathbb{Z}$, the units are the residue classes $\bar{u}$ such that $\gcd(u, n) = 1$. If $\gcd(a, n) > 1$, then $\bar{a}$ is a zero divisor. Thus, every non-zero element is either a unit or a zero divisor. In particular, $\mathbb{Z}/n\mathbb{Z}$ is a division ring precisely when n is prime.

Example 6.3. Let R be the ring of all functions $f : [0, 1] \rightarrow \mathbb{R}$. A function is a unit if it is nowhere zero. If f vanishes at some point, then it is a zero divisor (since one can define a non-zero function g with $fg = 0$).

Example 6.4. Let D be a rational number that is not a perfect square, and define

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

This is a subring of $\mathbb{C}$ (or of $\mathbb{R}$ if $D > 0$). Hence, it is an integral domain.

Definition 6.2 (Zero-Divisors). Let R be a commutative ring. A non-zero element $a \in R$ is called a *zero-divisor* if there exists a non-zero element $b \in R$ such that

$$ab = 0.$$

Definition 6.3 (Integral Domain). An *integral domain* is a commutative ring with unity in which there are no zero-divisors, that is, for all $a, b \in R$,

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

Example 6.5. The ring of integers $\mathbb{Z}$ is an integral domain. Indeed, $\mathbb{Z}$ is a commutative ring with unity, and if $ab = 0$ for $a, b \in \mathbb{Z}$, then either $a = 0$ or $b = 0$.

Example 6.6. The ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is an integral domain.

Example 6.7. The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain. If $f(x), g(x) \in \mathbb{Z}[x]$ and $f(x)g(x) = 0$, then one of $f(x)$ or $g(x)$ must be the zero polynomial, because $\deg(fg) = \deg(f) + \deg(g)$.

Example 6.8. The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

Example 6.9. For a prime p , the ring $\mathbb{Z}_p$ of integers modulo p is an integral domain.

Example 6.10. If n is not prime, then the ring $\mathbb{Z}_n$ of integers modulo n is not an integral domain. For instance, if $n = ab$ with $1 < a, b < n$, then $\bar{a}, \bar{b} \neq 0$ in $\mathbb{Z}_n$ but $\bar{a}\bar{b} = \bar{0}$, showing the existence of zero-divisors.

Example 6.11. The ring $M_2(\mathbb{Z})$ of 2×2 matrices over the integers is not an integral domain. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

although neither factor is the zero matrix.

Example 6.12. The direct product ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain. Indeed, $(1, 0) \neq (0, 0)$ and $(0, 1) \neq (0, 0)$, but $(1, 0)(0, 1) = (0, 0)$. Hence, zero-divisors exist in $\mathbb{Z} \times \mathbb{Z}$.

Problem 6.1. Let R be a ring with $1 \neq 0$ (not commutative). Prove that R is a division ring if and only if its only left ideals are $\langle 0 \rangle$ and R .

Solution 6.1. Assume that R is a division ring. Then every non-zero $a \in R$ has inverse. If I is a non-zero left ideal and $0 \neq a \in I$ then $1 = a^{-1}a \in I$, and $I = R$. Hence, the only left ideals are $\langle 0 \rangle$ and R .

Conversely, assume the only left ideals of R are $\langle 0 \rangle$ and R . Let $0 \neq a \in R$. The left ideal $\langle a \rangle = Ra$ is non-zero, we have $Ra = R$. Thus, there exists $b \in R$ with $ba = 1$, and hence a has a left inverse. Next, we prove that a also has a right inverse. Consider the set

$$A = \{x \in R : xa = 0\}.$$

This set is a left ideal of R . If $A \neq \langle 0 \rangle$, then $A = R$ and so $1 \cdot a = 0$, contradicting $a \neq 0$. Hence, $A = \langle 0 \rangle$.

Let $e = ab$. The left ideal $L = R(1 - e)$ satisfies

$$La = R(1 - e)a = R(a - ea) = R(a - (ab)a) = R(a - a(ba)) = R(a - a \cdot 1) = R(0) = \{0\}.$$

Thus, $L \subseteq A = \{0\}$, which forces $1 - e = 0$, i.e. $ab = 1$. Hence, R is a division ring.

Theorem 6.1. Let R be a commutative ring, and let I be an ideal of R . Then I is prime if and only if the quotient ring R/I is an integral domain.

PROOF. Assume that I is prime. Then $I \neq R$ and so $R/I \neq 0$. If $(a + I)(b + I) = 0 + I$ in R/I , then $ab \in I$. Since I is prime, either $a \in I$ or $b \in I$, which means $a + I = 0 + I$ or $b + I = 0 + I$. Thus, R/I has no zero divisors, and hence R/I is an integral domain.

Conversely, suppose R/I is an integral domain. Then $R/I \neq 0$ and so $I \neq R$. If $ab \in I$ for some $a, b \in R$, then in R/I we have

$$(a + I)(b + I) = ab + I = 0 + I.$$

Since R/I is an integral domain, this implies $a + I = 0 + I$ or $b + I = 0 + I$, i.e. $a \in I$ or $b \in I$. Therefore, I is prime. $\square$

Proposition 6.1 (Existence of maximal ideals). Let R be a commutative ring with identity. Then every proper ideal of R is contained in a maximal ideal.

PROOF. Let I be a proper ideal of R . Consider the collection

$$\mathcal{S} = \{J \subseteq R \mid J \text{ is an ideal of } R, I \subseteq J, \text{ and } J \neq R\}.$$

Clearly, $\mathcal{S}$ is non-empty (since $I \in \mathcal{S}$), and it is partially ordered by inclusion.

Now let $\mathcal{C} \subseteq \mathcal{S}$ be a chain under inclusion. Define

$$J^* = \bigcup_{J \in \mathcal{C}} J.$$

Since $\mathcal{C}$ is totally ordered, J^* is an ideal of R containing every $J \in \mathcal{C}$. Moreover, $J^* \neq R$, and if $1 \in J^*$, then $1 \in J$ for some $J \in \mathcal{C}$, contradicting $J \neq R$. Thus, $J^* \in \mathcal{S}$ and serves as an upper bound of $\mathcal{C}$.

By Zorn's Lemma, $\mathcal{S}$ has a maximal element, say M . By construction, M is an ideal containing I , $M \neq R$, and M is maximal with respect to inclusion. Hence, M is a maximal ideal of R containing I . $\square$

Problem 6.2. Let R be an integral domain. Prove that $\langle a \rangle = \langle b \rangle$ for some $a, b \in R$ if and only if $a = ub$ for some unit $u \in R$.

Solution 6.2. Assume $\langle a \rangle = \langle b \rangle$. If $a = 0$ then $\langle a \rangle = \{0\}$. This implies that $\langle b \rangle = \{0\}$ and $b = 0$. Therefore, $a = ub$ holds for every unit u (since $0 = u \cdot 0$).

Now suppose $a \neq 0$. Since $\langle a \rangle = \langle b \rangle$, we have $a \in \langle b \rangle$ and $b \in \langle a \rangle$. Hence, there exist $s, t \in R$ with

$$a = sb, \quad b = ta.$$

Substituting the second into the first gives

$$a = s(ta) = (st)a.$$

This shows that $(1 - st)a = 0$. Since R is an integral domain and $a \neq 0$, we conclude $1 - st = 0$, i.e. $st = 1$. Thus, s has a right inverse t . Similarly, substituting $a = sb$ into $b = ta$ shows $ts = 1$. Therefore, s is a unit (with inverse t), and $a = sb$ expresses a as a unit times b .

Conversely, if $a = ub$ for some unit $u \in R$, then

$$\langle a \rangle = \langle ub \rangle \subseteq \langle b \rangle.$$

Multiplying both sides of $a = ub$ by u^{-1} gives $b = u^{-1}a$, and hence $\langle b \rangle \subseteq \langle a \rangle$. Thus, $\langle a \rangle = \langle b \rangle$.

Problem 6.3. Let R be a commutative ring with $1 \neq 0$. Suppose P is a prime ideal of R and P contains no zero divisors of R . Prove that R is an integral domain.

Solution 6.3. Recall an integral domain is a non-zero commutative ring with no zero divisors. Since P is a prime ideal, we have $P \neq R$ and so $R \neq \{0\}$.

Now suppose, for contradiction, that R has a zero divisor. Then there exist $x, y \in R$ with $x \neq 0$, $y \neq 0$ and $xy = 0$. But $0 \in P$, so the product $xy \in P$. Since P is prime, it follows that $x \in P$ or $y \in P$. Thus, P contains a non-zero element that annihilates a non-zero element of R , and hence P contains a non-zero zero divisor. This contradicts the hypothesis that P contains no zero divisors. Thus, R is an integral domain.

Problem 6.4. Let R be a commutative ring and let I, J be ideals of R . Suppose P is a prime ideal of R such that

$$IJ \subseteq P.$$

Prove that either $I \subseteq P$ or $J \subseteq P$.

PROOF. Assume, for contradiction, that neither I nor J is contained in P . Then there exist elements $a \in I \setminus P$ and $b \in J \setminus P$. Since $a \in I$ and $b \in J$, their product ab lies in IJ , hence $ab \in P$. Since P is prime, $ab \in P$ implies $a \in P$ or $b \in P$. This contradicts our choice of a and b . Therefore, either $I \subseteq P$ or $J \subseteq P$. $\square$

Problem 6.5. Let $\varphi : R \rightarrow S$ be a homomorphism of commutative rings. Prove that if P is a prime ideal of S then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P)$ is a prime ideal of R . Apply this to the special case when R is a subring of S and φ is the inclusion homomorphism to deduce that if P is a prime ideal of S then $P \cap R$ is either R or a prime ideal of R .

PROOF. Suppose P is a prime ideal of S . If $\varphi^{-1}(P) = R$ there is nothing to prove. Otherwise, let $a, b \in R$ with $ab \in \varphi^{-1}(P)$. Then $\varphi(ab) = \varphi(a)\varphi(b) \in P$. Since P is prime, $\varphi(a) \in P$ or $\varphi(b) \in P$. Hence, $a \in \varphi^{-1}(P)$ or $b \in \varphi^{-1}(P)$. Thus, $\varphi^{-1}(P)$ is a prime ideal of R .

For the inclusion homomorphism $\varphi : R \hookrightarrow S$, we have $\varphi^{-1}(P) = P \cap R$. So if P is prime in S , then $P \cap R$ is either R or a prime ideal of R . $\square$

Definition 6.4. Let R be a commutative ring. An element $x \in R$ is called *nilpotent* if there exists an integer $m > 0$ such that $x^m = 0$.

Problem 6.6. Let R be a commutative ring with $1 \neq 0$ and let $x \in R$ be nilpotent. Then prove the following.

- (a) x is either 0 or a zero divisor.
- (b) For every $r \in R$ the element rx is nilpotent.
- (c) $1 + x$ is a unit in R .
- (d) The sum of a nilpotent element and a unit is a unit.

Solution 6.4. (a) If $x = 0$ there is nothing to prove. Suppose $x \neq 0$ and let $n \geq 1$ be minimal with $x^n = 0$. Then $x^{n-1} \neq 0$, and

$$x \cdot x^{n-1} = x^n = 0.$$

This shows that x annihilates the non-zero element x^{n-1} , and hence x is a zero divisor.

(b) If $x^n = 0$, then for any $r \in R$ we have

$$(rx)^n = r^n x^n = r^n \cdot 0 = 0.$$

Thus, rx is nilpotent.

(c) Let $x^n = 0$. Consider the finite geometric sum

$$y := 1 - x + x^2 - \cdots + (-1)^{n-1} x^{n-1}.$$

Using $x^n = 0$ and commutativity of R , we obtain

$$(1+x)y = 1 + x - x - x^2 + x^2 + x^3 - \cdots + (-1)^{n-1}x^{n-1} + (-1)^{n-1}x^n = 1 - x^n = 1.$$

Similarly, we can show that $y(1+x) = 1$. Thus, y is the inverse of $1+x$, and $1+x$ is a unit.

(d) Let $u \in R$ be a unit and x nilpotent. Then $u^{-1}x$ is nilpotent by (b). By (c), $1 + u^{-1}x$ is a unit, and

$$u + x = u(1 + u^{-1}x)$$

is a product of units, hence a unit. This proves that the sum of a nilpotent element and a unit is a unit.

7. Unique Factorization

In the integers $\mathbb{Z}$ and in the polynomial ring $K[X]$, where $K = \mathbb{R}$ or $\mathbb{C}$, every non-zero, non-unit element factors into primes, and this factorization is unique (up to order and multiplication of factors by units). We now study this idea in greater generality. Since zero divisors complicate factorization, we restrict our attention to *integral domains*.

Let

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

Define the *norm*

$$N(a + b\sqrt{-5}) = a^2 + 5b^2,$$

which satisfies the multiplicative property

$$N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5}).$$

The units in $R = \mathbb{Z}[\sqrt{-5}]$ are exactly $\{\pm 1\}$. Indeed, if $u \in R$ is a unit, then $uv = 1$ for some $v \in R$, so

$$N(u)N(v) = N(uv) = N(1) = 1,$$

hence $N(u) = 1$. Conversely, if $N(u) = 1$, then $u \cdot \bar{u} = 1$, and so u has inverse $\bar{u}$ in R . The equation $a^2 + 5b^2 = 1$ has only integer solutions $a = \pm 1$, $b = 0$, and therefore

$$R^\times = \{\pm 1\}.$$

Thus, every element of R can be factored into irreducibles (non-units that cannot be written as a product of two non-units), but uniqueness of factorization may fail.

Failure of Unique Factorization. Consider $6 \in R$. We have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Now check the irreducibility as follows.

- $N(2) = 4$, $N(3) = 9$,
- $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$.

None of these norms can be written as a product of smaller norms, so 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible.

Thus, 6 has two distinct factorizations into irreducibles:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and these are not related by multiplication with units. Hence, $\mathbb{Z}[\sqrt{-5}]$ is an integral domain in which *unique factorization fails*.

7.1. Irreducibles and Primes. The failure of unique factorization in $\mathbb{Z}[\sqrt{-5}]$ shows that unique factorization is not universal for integral domains. This forces us to be more precise with terminology.

In $\mathbb{Z}$, the factors in a complete factorization were called “primes.” Their defining property was that they could not be factored further, and they also satisfied the property that a prime dividing a product must divide one of the factors. For general integral domains, these two notions are distinct.

Definition 7.1. Let R be an integral domain.

- (1) A non-zero element $a \in R$ is said to *divide* $b \in R$ if $b = ac$ for some $c \in R$. In this case, a is called a *factor* of b .
- (2) A non-zero, non-unit $r \in R$ is called *irreducible* if, whenever $r = r_1r_2$ in R , then either r_1 or r_2 is a unit. non-zero, non-units that are not irreducible are called *reducible*.
- (3) A non-zero, non-unit $p \in R$ is called *prime* if, whenever p divides ab , it follows that p divides a or p divides b .

Proposition 7.1. Every prime element is irreducible.

PROOF. Suppose p is prime and $p = r_1r_2$ with r_1, r_2 both non-units. Since p divides r_1r_2 , we have $p \mid r_1$ or $p \mid r_2$. Without loss of generality, assume $p \mid r_1$. Then $r_1 = pc$ for some $c \in R$, and so

$$p = r_1r_2 = pcr_2.$$

Since R is an integral domain, we have $1 = cr_2$, and hence r_2 is a unit, a contradiction. Thus, p is irreducible. $\square$

Problem 7.1. Prove that an irreducible element need not be prime.

Solution 7.1. Let

$$R = \mathbb{Z}[\sqrt{-5}]$$

and define the norm $N : R \rightarrow \mathbb{Z}_{\geq 0}$ by

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Consider the element $\alpha = 1 + \sqrt{-5}$. Then

$$N(\alpha) = 6.$$

Suppose $\alpha = xy$ for some $x, y \in R$. Taking norms gives

$$6 = N(x)N(y).$$

The equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ have no solutions in integers. Hence, there are no elements of R with norm 2 or 3. It follows that one of $N(x)$ or $N(y)$ must be 1 and hence one of x or y is a unit. Therefore, α is irreducible.

On the other hand,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and hence

$$1 + \sqrt{-5} \mid 2 \cdot 3.$$

If $1 + \sqrt{-5}$ divided 2, then there would exist $r \in R$ such that

$$2 = (1 + \sqrt{-5})r.$$

By taking norms on both sides, we obtain

$$4 = N(2) = N(1 + \sqrt{-5})N(r) = 6N(r),$$

which is impossible. A similar argument shows that $1 + \sqrt{-5}$ does not divide 3.

Thus, $1 + \sqrt{-5}$ divides a product without dividing either factor. Hence, $1 + \sqrt{-5}$ is not prime, even though it is irreducible.

Problem 7.2. In the ring $\mathbb{Z}[i]$ of Gaussian integers, show that 3 is irreducible, but 2 and 5 are not irreducible.

Solution 7.2. Recall that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain. Define the norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ by

$$N(a + bi) = a^2 + b^2.$$

We now check the irreducibility of 3. We have

$$N(3) = 9.$$

Suppose

$$3 = \alpha\beta$$

for some $\alpha, \beta \in \mathbb{Z}[i]$. Taking norms gives

$$9 = N(\alpha)N(\beta).$$

The possible positive divisors of 9 are 1, 3, and 9. The equation $a^2 + b^2 = 3$ has no integer solutions. Hence, there is no element of $\mathbb{Z}[i]$ with norm 3. It follows that one of $N(\alpha)$ or $N(\beta)$ must be 1, so one of α or β is a unit. Therefore, 3 is irreducible in $\mathbb{Z}[i]$.

Next, observe that

$$2 = (1 + i)(1 - i).$$

Since

$$N(1 + i) = N(1 - i) = 2,$$

and neither $1 + i$ nor $1 - i$ is a unit, this expresses 2 as a product of two non-units. Hence, 2 is not irreducible in $\mathbb{Z}[i]$.

Finally, we prove non-irreducibility of 5. We have

$$5 = (2 + i)(2 - i).$$

Moreover,

$$N(2 + i) = N(2 - i) = 5,$$

and neither factor is a unit. Thus, 5 is a product of two non-units, and hence is not irreducible in $\mathbb{Z}[i]$.

7.2. Unique Factorization Domains. The distinction between “irreducible” and “prime” lies at the heart of the question of unique factorization.

Definition 7.2. An integral domain R is called a *unique factorization domain (UFD)* if the following hold:

(UFD1) Every non-zero non-unit of R is a finite product of irreducible elements.

(UFD2) Such factorizations are unique up to order and multiplication of the factors by units.

Proposition 7.2. Let R be an integral domain satisfying (UFD1), every non-zero non-unit factors into irreducibles. Then the following are equivalent.

(UFD2) Factorizations into irreducibles are unique up to order and multiplication by units.

(UFD2') Every irreducible element is prime.

Remark 7.1. In $\mathbb{Z}$, proving that irreducible elements are prime was the key step in establishing unique factorization.

PROOF. **(UFD2) $\implies$ (UFD2'):** Suppose factorization is unique. Let p be irreducible and $p \mid ab$. Factor a and b into irreducibles

$$a = p_1 p_2 \cdots p_m, \quad b = q_1 q_2 \cdots q_n.$$

Since $p \mid ab$, by uniqueness, p must be associated to some p_i or q_j . Hence, $p \mid a$ or $p \mid b$, and we conclude that p is prime.

(UFD2') $\implies$ (UFD2): Assume every irreducible is prime. Let a non-zero non-unit r have two irreducible factorizations

$$r = p_1 p_2 \cdots p_m = \varepsilon_0 q_1 q_2 \cdots q_n,$$

where ε_0 is a unit and $m \leq n$.

We prove this by induction on m . Clearly, $m > 0$. For $m = 1$, the result is true since r is irreducible. Since $p_m \mid r = q_1 \cdots q_n$ and p_m is prime, it divides some q_k . As q_k is irreducible, $q_k = \varepsilon p_m$ for a unit ε . Canceling p_m and q_k , we get

$$p_1 \cdots p_{m-1} = (\varepsilon_0 \varepsilon) q_1 \cdots \widehat{q_k} \cdots q_n,$$

where $\widehat{q_k}$ means q_k is omitted. By induction hypothesis, the factorization of r is unique, proving (UFD2). $\square$

7.3. Principal Ideal Domains and Unique Factorization. In a commutative ring R with identity, we denote the ideal generated by a single element $a \in R$ as

$$\langle a \rangle = \{ra : r \in R\}.$$

An ideal of this type is called *principal*. More generally, for elements $a_1, \dots, a_n \in R$, we write

$$\langle a_1, \dots, a_n \rangle = Ra_1 + \cdots + Ra_n,$$

the ideal generated by all of them.

Example 7.1. In $\mathbb{Z}[X]$, the ideal $\langle 2, X \rangle$ consists of all polynomials whose constant term is divisible by 2. That is,

$$\langle 2, X \rangle = 2\mathbb{Z}[X] + X\mathbb{Z}[X].$$

Proposition 7.3. Let R be an integral domain. A non-zero element $p \in R$ is prime if and only if the principal ideal $\langle p \rangle$ is prime.

PROOF. Assume that p is prime and p is not a unit. Then $\langle p \rangle \neq R$. Suppose $ab \in \langle p \rangle$ for some $a, b \in R$. Then $ab = pr$ for some $r \in R$, which implies $p \mid ab$. By primality of p , $p \mid a$ or $p \mid b$, i.e., $a \in \langle p \rangle$ or $b \in \langle p \rangle$. Hence, $\langle p \rangle$ is a prime ideal.

Conversely, assume $\langle p \rangle$ is prime and $p \neq 0$. Then p is not a unit. If $p \mid ab$, write $ab = pc$ for some $c \in R$, so $ab \in \langle p \rangle$. Since $\langle p \rangle$ is prime, $a \in \langle p \rangle$ or $b \in \langle p \rangle$, i.e., $p \mid a$ or $p \mid b$. Therefore, p is prime as an element of R . $\square$

Definition 7.3. An integral domain R is called a *principal ideal domain (PID)* if every ideal of R is generated by a single element.

Problem 7.3. Show that every ideal of the ring of integers $\mathbb{Z}$ is principal.

Solution 7.3. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then clearly $I = \langle 0 \rangle$.

Otherwise, let n be the smallest positive integer in I . For any $m \in I$, by the division algorithm there exist integers q and r such that

$$m = qn + r, \quad 0 \leq r < n.$$

Since $r = m - qn \in I$ and n is the smallest positive element of I , it follows that $r = 0$. Hence, $m \in \langle n \rangle$, which implies $I \subseteq \langle n \rangle$. It is clear that $\langle n \rangle \subseteq I$. Thus, $I = \langle n \rangle$.

Therefore, every ideal of $\mathbb{Z}$ is principal.

Problem 7.4. Show that every ideal of the ring of Gaussian integers $\mathbb{Z}[i]$ is principal.

Solution 7.4. Let I be a non-zero ideal of $\mathbb{Z}[i]$. Choose an element $a + bi \in I$ such that its norm

$$N(a + bi) = a^2 + b^2$$

is minimal among all non-zero elements of I .

Let $x + yi \in I$. By the division algorithm in $\mathbb{Z}[i]$, there exist Gaussian integers $q + ri$ and $r_0 + r_1i$ such that

$$x + yi = (a + bi)(q + ri) + (r_0 + r_1i), \quad N(r_0 + r_1i) < N(a + bi).$$

Since both $x + yi$ and $(a + bi)(q + ri)$ lie in I , the remainder $r_0 + r_1i$ also belongs to I .

By the minimality of $N(a + bi)$, we must have $r_0 + r_1i = 0$. Thus, $x + yi \in \langle a + bi \rangle$.

It follows that $I \subseteq \langle a + bi \rangle$. The reverse inclusion is immediate, and hence $I = \langle a + bi \rangle$. Therefore, every ideal of $\mathbb{Z}[i]$ is principal.

Theorem 7.1. Every principal ideal domain R is a unique factorization domain.

Remark 7.2. By Proposition 7.2, to show that a PID is a UFD, it suffices to verify conditions (UFD1) and (UFD2').

PROOF. First we prove (UFD1). Let $a_1 \in R$ be a non-zero non-unit. The ideal $\langle a_1 \rangle$ is proper and non-zero. Since every ideal is contained in a maximal ideal, we can find a maximal ideal $\langle c_1 \rangle$ with $\langle a_1 \rangle \subseteq \langle c_1 \rangle$. Since maximal ideals in a PID are prime. By Proposition 7.1, it follows that $\langle c_1 \rangle$ irreducible. Hence, $c_1 \mid a_1$, and we can write $a_1 = c_1 a_2$ for some $a_2 \in R$.

Repeating this process, we obtain a sequence of factorizations:

$$a_1 = c_1 c_2 \cdots c_n a_{n+1}, \quad \text{with each } c_i \text{ irreducible.}$$

This process cannot continue indefinitely. Otherwise, we get a strictly increasing chain of ideals

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \cdots$$

which is impossible in a PID because every ascending chain of ideals stabilizes. Thus, the process terminates, giving a factorization of a_1 into finitely many irreducibles. This establishes (UFD1).

Next, we prove (UFD2'). Let $p \in R$ be irreducible. Since $\langle p \rangle$ is proper, it is contained in a maximal ideal. Since R is a PID, maximal ideals are principal, and hence $\langle p \rangle$ is maximal. Since maximal ideals are prime, and Proposition 7.3 implies that p is prime. Hence, every irreducible element is prime, proving (UFD2'). $\square$

Corollary 7.1. In a principal ideal domain R , every non-zero prime ideal is maximal.

PROOF. Let $\langle p \rangle$ be a non-zero prime ideal of R . Proposition 7.3 shows that p is a prime element. Since prime elements are irreducible, the argument above shows that $\langle p \rangle$ is contained in a maximal ideal and must itself be maximal. $\square$

7.4. Euclidean Domains. Principal ideal domains (PIDs) do not appear very frequently, and recognizing them is sometimes non-trivial. A useful generalization of the technique used for $\mathbb{Z}$ is the notion of a Euclidean domain.

Definition 7.4. An integral domain R is called a *Euclidean domain* if there exists a function

$$\delta : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$$

such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ satisfying

$$a = bq + r, \quad \delta(r) < \delta(b).$$

Example 7.2. The integers $\mathbb{Z}$ with $\delta(n) = |n|$.

Problem 7.5. Prove that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain.

Solution 7.5. Define the norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ by

$$N(a + bi) = a^2 + b^2.$$

Clearly, $N(\alpha) = 0$ if and only if $\alpha = 0$, and

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \text{for all } \alpha, \beta \in \mathbb{Z}[i].$$

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We now prove that there exist $\gamma, \delta \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \delta \quad \text{with } N(\delta) < N(\beta).$$

Consider the quotient $\alpha/\beta \in \mathbb{C}$. Choose $\gamma \in \mathbb{Z}[i]$ such that γ is the Gaussian integer nearest to α/β . Define

$$\delta = \alpha - \beta\gamma.$$

Then

$$\frac{\delta}{\beta} = \frac{\alpha}{\beta} - \gamma.$$

By the choice of γ , the real and imaginary parts of $\frac{\delta}{\beta}$ have absolute value at most $\frac{1}{2}$. Hence

$$N\left(\frac{\delta}{\beta}\right) = \left(\Re\left(\frac{\delta}{\beta}\right)\right)^2 + \left(\Im\left(\frac{\delta}{\beta}\right)\right)^2 \leq \frac{1}{2}.$$

Multiplying by $N(\beta)$, we obtain

$$N(\delta) < N(\beta).$$

This prove that the division algorithm in $\mathbb{Z}[i]$ with respect to the norm N .

Therefore, $\mathbb{Z}[i]$ is a Euclidean domain.

Remark 7.3. Some rings may seem superficially similar to Euclidean domains, such as $\mathbb{Z}[\sqrt{-5}]$, but they fail to have unique factorization. Consequently, they cannot be Euclidean domains.

Theorem 7.2. Every Euclidean domain is a principal ideal domain.

PROOF. Let $I \subseteq R$ be a non-zero ideal. Choose $b \in I$ with $\delta(b)$ minimal. Clearly, $\langle b \rangle \subseteq I$. For any $a \in I$, write

$$a = bq + r, \quad \delta(r) < \delta(b),$$

with $q, r \in R$. Since $r = a - bq \in I$ and b has minimal δ , we must have $r = 0$. Hence, $a \in \langle b \rangle$ and $I = \langle b \rangle$. Thus, I is principal, and R is a PID. $\square$

Problem 7.6. Let $R = \mathbb{Z}[\sqrt{-5}]$ and define the norm

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Consider the ideal

$$I = (2, 1 + \sqrt{-5}) \subset R.$$

Show that I is not a principal ideal. Deduce that R is not a Euclidean domain.

Solution 7.6. Suppose that I is a principal ideal. Then there exist integers $a, b \in \mathbb{Z}$ such that

$$I = (a + b\sqrt{-5}).$$

Since $2 \in I$, there exists $\alpha \in R$ such that

$$2 = \alpha(a + b\sqrt{-5}).$$

Taking norms on both sides, we get

$$4 = N(2) = N(\alpha) N(a + b\sqrt{-5}) = N(\alpha) (a^2 + 5b^2).$$

Thus, $a^2 + 5b^2$ is a positive integer dividing 4, and hence

$$a^2 + 5b^2 \in \{1, 2, 4\}.$$

Case 1: $a^2 + 5b^2 = 4$.

Then $N(\alpha) = 1$ and so $\alpha = \pm 1$. Hence

$$a + b\sqrt{-5} = \pm 2.$$

But $1 + \sqrt{-5} \in I$, and its coefficients are not divisible by 2. This is a contradiction.

Case 2: $a^2 + 5b^2 = 2$.

This equation has no integer solutions. Hence, this case is not possible.

Case 3: $a^2 + 5b^2 = 1$.

Then $a + b\sqrt{-5} = \pm 1$, and so

$$I = R.$$

This implies that $1 \in I$. Therefore, there exist $y, \delta \in R$ such that

$$2y + (1 + \sqrt{-5})\delta = 1.$$

Multiplying both sides by $1 - \sqrt{-5}$, we obtain

$$2y(1 - \sqrt{-5}) + (1 + \sqrt{-5})(1 - \sqrt{-5})\delta = 1 - \sqrt{-5}.$$

Since

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6,$$

the right-hand side shows that $1 - \sqrt{-5}$ is divisible by 2 in R , which is impossible.

All cases lead to contradictions. Hence, the ideal I is not principal. Therefore, $R = \mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. Moreover, it is not a Euclidean domain.

Problem 7.7. Let

$$R = \mathbb{Z}[\omega], \quad \text{where } \omega = \frac{-1 + \sqrt{-3}}{2}.$$

Prove that R is a Euclidean domain. Deduce that R is a principal ideal domain and unique factorization domain.

Solution 7.7. First, we prove that R is a Euclidean domain.

Define the norm $N : R \rightarrow \mathbb{Z}_{\geq 0}$ by

$$N(a + b\omega) = a^2 - ab + b^2, \quad a, b \in \mathbb{Z}.$$

Recall that the above norm satisfies

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \text{for all } \alpha, \beta \in R.$$

Let $\alpha, \beta \in R$ with $\beta \neq 0$. We show that there exist $\gamma, \delta \in R$ such that

$$\alpha = \beta\gamma + \delta \quad \text{with} \quad N(\delta) < N(\beta).$$

Consider the quotient $\alpha/\beta \in \mathbb{Q}(\sqrt{-3})$. Write

$$\frac{\alpha}{\beta} = x + y\omega, \quad x, y \in \mathbb{Q}.$$

Choose integers $m, n \in \mathbb{Z}$ such that

$$|x - m| \leq \frac{1}{2}, \quad |y - n| \leq \frac{1}{2}.$$

Set $\gamma = m + n\omega \in R$ and define

$$\delta = \alpha - \beta\gamma.$$

Then

$$\frac{\delta}{\beta} = (x - m) + (y - n)\omega.$$

Using the definition of the norm, we obtain

$$N\left(\frac{\delta}{\beta}\right) = (x - m)^2 - (x - m)(y - n) + (y - n)^2 \leq \frac{3}{4}.$$

Multiplying by $N(\beta)$ gives

$$N(\delta) < N(\beta).$$

This shows that R is a Euclidean domain with respect to the norm N . Since every Euclidean domain is a principal ideal domain, and every principal ideal domain is a unique factorization domain, it follows that R is a unique factorization domain.

8. Finitely Generated Modules

Recall the *Fundamental Theorem of Finitely Generated Abelian Groups*, which states that every finitely generated abelian group is a direct sum of cyclic groups. Since abelian groups are $\mathbb{Z}$ -modules, we may ask whether an analogous result holds for modules over an arbitrary ring. Indeed, this theorem extends naturally to the setting where $\mathbb{Z}$ is replaced by a *principal ideal domain* (PID).

Definition 8.1 (Finitely Generated R -Module). Let R be a principal ideal domain, and let M be an R -module. A subset S of M is called a *set of generators* (or a *generating set*) of M if M is the smallest R -submodule of M that contains all elements of S . Equivalently, if we write

$$S = \{m_s \mid s \in I\} \subseteq M,$$

where I is some index set and each $m_s \in M$, then the submodule of M generated by S is

$$\langle S \rangle = \left\{ \sum_{s \in I} r_s m_s : r_s \in R, \text{ and only finitely many } r_s \neq 0 \right\}.$$

If $\langle S \rangle = M$, then S is a generating set of M .

If M is a unital R -module, then for each $s_0 \in I$, choosing $r_{s_0} = 1$ and all other $r_s = 0$ shows that $m_{s_0} \in \langle S \rangle$. Hence, every element m_s of S indeed lies in the submodule generated by S . For this reason, we will assume that all R -modules considered are unital.

We say that M is a *finitely generated R -module* if there exists a finite generating set $S = \{m_1, m_2, \dots, m_n\}$ such that

$$M = \langle m_1, m_2, \dots, m_n \rangle = \{r_1 m_1 + r_2 m_2 + \dots + r_n m_n : r_i \in R\}.$$

Proposition 8.1. Let R be a commutative ring with identity, and let

$$\varphi : M \longrightarrow N$$

be a homomorphism of unital R -modules. If both $\ker \varphi$ and $\text{im } \varphi$ are finitely generated, then M is finitely generated.

PROOF. Let $\{x_1, x_2, \dots, x_m\}$ be a finite set of generators for $\ker \varphi$, and $\{y_1, y_2, \dots, y_n\}$ a finite set of generators for $\text{im } \varphi$.

For each $1 \leq i \leq n$, choose an element $x'_i \in M$ such that

$$\varphi(x'_i) = y_i.$$

We claim that the finite set

$$S := \{x_1, \dots, x_m, x'_1, \dots, x'_n\}$$

generates M as an R -module.

Let $x \in M$ be arbitrary. Since $\varphi(x) \in \text{im } \varphi$, there exist elements $r_1, \dots, r_n \in R$ such that

$$\varphi(x) = r_1 y_1 + r_2 y_2 + \dots + r_n y_n.$$

Define

$$x' := r_1 x'_1 + r_2 x'_2 + \dots + r_n x'_n \in M.$$

Then

$$\varphi(x') = r_1 \varphi(x'_1) + r_2 \varphi(x'_2) + \dots + r_n \varphi(x'_n) = r_1 y_1 + \dots + r_n y_n = \varphi(x).$$

Hence,

$$\varphi(x - x') = 0,$$

which implies that $x - x' \in \ker \varphi$. Since $\ker \varphi$ is generated by $\{x_1, \dots, x_m\}$, there exist elements $s_1, \dots, s_m \in R$ such that

$$x - x' = s_1 x_1 + s_2 x_2 + \dots + s_m x_m.$$

Therefore,

$$x = s_1 x_1 + s_2 x_2 + \dots + s_m x_m + r_1 x'_1 + r_2 x'_2 + \dots + r_n x'_n.$$

This shows that x is an R -linear combination of elements of S , and hence S generates M . Thus, M is finitely generated. $\square$

Definition 8.2 (Free and Cyclic R -Modules). Let R be a commutative ring with identity. A *free R -module* is a direct sum (finite or infinite) of copies of the R -module R , that is,

$$M \cong \bigoplus_{i \in I} R,$$

for some index set I . If I is finite, say $I = \{1, 2, \dots, n\}$, then M is said to have *finite rank n* , and we write

$$M \cong R^n.$$

A unital R -module M is said to be *cyclic* if it is generated by a single element, that is, there exists $m_0 \in M$ such that

$$M = Rm_0 = \{rm_0 : r \in R\}.$$

In this case, the map

$$\begin{aligned} \varphi : R &\longrightarrow M, \\ r &\longmapsto rm_0 \end{aligned}$$

is a surjective R -module homomorphism with kernel

$$\ker \varphi = \{r \in R : rm_0 = 0\}.$$

By the First Isomorphism Theorem, we then have the canonical R -module isomorphism

$$M \cong R/I, \quad \text{where } I = \ker \varphi = \{r \in R : rm_0 = 0\}.$$

8.1. The Fundamental Theorem of Finitely Generated Modules. In the study of modules over a principal ideal domain (PID), one encounters a remarkable generalization of the *Fundamental Theorem of Finitely Generated Abelian Groups*. That classical result describes the structure of finitely generated abelian groups as direct sums of cyclic groups. When we view abelian groups as $\mathbb{Z}$ -modules, it is natural to ask whether a similar structural decomposition holds for finitely generated modules over an arbitrary principal ideal domain R .

Theorem 8.1 (Fundamental Theorem of Finitely Generated Modules). Let R be a principal ideal domain (PID). Then

- (a) The number of R -summands in a free R -module of finite rank is independent of the direct-sum decomposition.
- (b) Every R -submodule of a free R -module of finite rank n is itself a free R -module of rank $\leq n$.
- (c) Every finitely generated unital R -module is a finite direct sum of cyclic R -modules.

8.2. Chinese Remainder Theorem for rings. The existence of a decomposition of finitely generated modules into cyclic modules of a special kind relies on a general version of the *Chinese Remainder Theorem*. Its classical form concerns congruences for integers, but the module-theoretic structure theorem requires a much more general statement that applies to ideals in an arbitrary commutative ring.

Before stating the theorem, we recall two standard operations on ideals in a commutative ring R with identity. If I and J are ideals of R , then

- The *sum* of I and J is the ideal

$$I + J = \{x + y : x \in I, y \in J\}.$$

- The *product* of I and J is the ideal

$$IJ = \left\{ \sum_{k=1}^t x_k y_k : x_k \in I, y_k \in J, t \in \mathbb{N} \right\}.$$

It is straightforward to verify that both $I + J$ and IJ are indeed ideals of R .

We now state the general version of the Chinese Remainder Theorem, which will later allow us to decompose modules into direct sums corresponding to products of ideals.

Theorem 8.2 (Chinese Remainder Theorem). Let R be a commutative ring with identity, and let $I_1, I_2, \dots, I_n$ be ideals of R such that

$$I_i + I_j = R \quad \text{whenever } i \neq j.$$

Then the following statements hold:

- (a) For any elements $x_1, x_2, \dots, x_n \in R$, there exists an element $x \in R$ such that

$$x \equiv x_j \pmod{I_j}, \quad \text{i.e. } x - x_j \in I_j \text{ for all } j.$$

The element x is unique if $I_1 \cap I_2 \cap \dots \cap I_n = (0)$.

- (b) The natural ring homomorphism

$$\begin{aligned} \varphi : R &\longrightarrow \prod_{j=1}^n R/I_j, \\ r &\longmapsto (r + I_1, r + I_2, \dots, r + I_n) \end{aligned}$$

has kernel $\ker \varphi = I_1 I_2 \dots I_n$ and induces an onto homomorphism

$$R/(I_1 I_2 \dots I_n) \cong R/I_1 \times R/I_2 \times \dots \times R/I_n.$$

- (c) The intersection $I_1 \cap \dots \cap I_n$ is equal to the product $I_1 I_2 \dots I_n$.

Corollary 8.1. Let R be a principal ideal domain, and let

$$a = \varepsilon p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

be a factorization of a non-zero, non-unit element $a \in R$ into the product of a unit ε and powers of pairwise non-associate primes $p_1, \dots, p_n$. Then there is a ring isomorphism

$$R/(a) \cong R/(p_1^{k_1}) \times R/(p_2^{k_2}) \times \dots \times R/(p_n^{k_n}).$$

8.3. Noetherian Rings. In this section, R denotes a commutative ring with identity, and all R -modules considered will be unital. We begin by examining three equivalent finiteness conditions that an R -module may satisfy, each expressed in terms of its submodule structure.

Proposition 8.2. Let R be a commutative ring with identity, and let M be a unital R -module. Then the following conditions on R -submodules of M are equivalent:

- (a) **(Ascending Chain Condition)** Every strictly ascending chain of R -submodules

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots$$

terminates after finitely many steps (that is, $M_n = M_{n+1} = M_{n+2} = \dots$ for some n).

- (b) **(Maximum Condition)** Every non-empty collection of R -submodules of M has a maximal element under inclusion.

- (c) **(Finite Basis Condition)** Every R -submodule of M is finitely generated.

PROOF. (a) $\Rightarrow$ (b). Let $\mathcal{C}$ be a non-empty collection of R -submodules of M . Choose $M_1 \in \mathcal{C}$. If M_1 is not maximal, select $M_2 \in \mathcal{C}$ properly containing M_1 . If M_2 is not maximal, choose $M_3 \in \mathcal{C}$ properly containing M_2 , and continue in this way. By condition (a), this process must terminate after finitely many steps, yielding a maximal R -submodule in $\mathcal{C}$.

(b) $\Rightarrow$ (c). Let N be an R -submodule of M , and let $\mathcal{C}$ denote the collection of all finitely generated R -submodules of N . This collection is non-empty since $0 \in \mathcal{C}$. By (b), $\mathcal{C}$ has a maximal element, say N_0 . If $x \in N$ but $x \notin N_0$, then $N_0 + Rx$ is a finitely generated R -submodule of N properly containing N_0 , which contradicts maximality. Hence, $N_0 = N$, and therefore N is finitely generated.

(c) $\Rightarrow$ (a). Let

$$M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \dots$$

be a strictly ascending chain of R -submodules of M . Put

$$N = \bigcup_{n=1}^{\infty} M_n.$$

By (c), N is finitely generated, say $N = \langle x_1, x_2, \dots, x_k \rangle$. Each generator x_i lies in some M_{n_i} , and letting $n_0 = \max\{n_1, \dots, n_k\}$, we have $N = M_{n_0}$. Thus, the chain stops at M_{n_0} , proving (a). $\square$

Corollary 8.2. Let R be a commutative ring with identity. Then the following conditions on R are equivalent:

(a) **(Ascending chain condition for ideals)** Every strictly ascending chain of ideals in R

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

terminates after finitely many steps (that is, $I_n = I_{n+1} = I_{n+2} = \dots$ for some n).

(b) **(Maximum condition for ideals)** Every non-empty collection of ideals in R has a maximal element under inclusion.

(c) **(Finite basis condition for ideals)** Every ideal in R is finitely generated.

PROOF. Apply Proposition 8.2 with $M = R$, viewed as a unital R -module. Since the R -submodules of R are precisely its ideals, the result follows immediately. $\square$

Definition 8.3. (Noetherian ring) A commutative ring with identity satisfying any (and hence all) of the equivalent conditions in Corollary 8.2 is called a *Noetherian ring*.

Example 8.1. Principal ideal domains, such as $\mathbb{Z}$ and $\mathbb{R}[X]$, satisfy the finite basis condition for ideals since every ideal is singly generated. Thus, by Corollary 8.2, every principal ideal domain is Noetherian.

We now state some important results concerning Noetherian rings, which we shall present without proof.

Theorem 8.3 (Hilbert Basis Theorem). If R is a non-zero Noetherian commutative ring, then the polynomial ring $R[X]$ is also Noetherian.

Proposition 8.3. Let R be a Noetherian integral domain. Then every non-zero non-unit element of R can be expressed as a finite product of irreducible elements.

PROOF. Let $a \in R$ be a non-zero non-unit. If a is irreducible, there is nothing to prove.

Assume that a is not irreducible. Then $a = bc$ for some non-units $b, c \in R$. In particular,

$$(a) \subsetneq (b) \quad \text{and} \quad (a) \subsetneq (c).$$

If both b and c are irreducible, then a is a product of irreducible elements. Otherwise, at least one of them, say b , is not irreducible. Then $b = b_1 b_2$ with b_1, b_2 non-units, and hence

$$(a) \subsetneq (b) \subsetneq (b_1).$$

Continuing this process, we obtain a strictly ascending chain of ideals

$$(a) \subsetneq (b) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \dots$$

Since R is Noetherian, every ascending chain of ideals must terminate. Therefore, this process must stop after finitely many steps. Consequently, the resulting factorization consists entirely of irreducible elements.

Hence, a can be written as a finite product of irreducible elements. $\square$

Proposition 8.4. If R is a Noetherian commutative ring, then every R -submodule of a finitely generated unital R -module is also finitely generated.

PROOF. Let M be a finitely generated unital R -module, and let N be a submodule of M . Since M is finitely generated, there exists a surjective R -module homomorphism

$$\varphi : R^n \longrightarrow M$$

for some $n \geq 1$.

Let

$$N' := \varphi^{-1}(N).$$

Then N' is a submodule of R^n and hence an R -submodule of a finitely generated free R -module.

Since R is Noetherian, the free module R is Noetherian as an R -module. A finite direct sum of Noetherian modules is Noetherian, so R^n is a Noetherian R -module. Therefore, every submodule of R^n is finitely generated, and in particular, N' is finitely generated.

Finally, since φ is surjective, the image

$$N = \varphi(N')$$

is finitely generated. Hence, N is a finitely generated R -module. $\square$

Problem 8.1. Let $R = \mathbb{Z}[x]$. Show that

$$R/(\langle x \rangle \cap \langle x-1 \rangle) \cong R/\langle x \rangle \oplus R/\langle x-1 \rangle.$$

Solution 8.1. Since

$$\langle x \rangle + \langle x-1 \rangle = \langle 1 \rangle = R,$$

the ideals are comaximal. By the Chinese Remainder Theorem for modules,

$$R/(\langle x \rangle \cap \langle x-1 \rangle) \cong R/\langle x \rangle \oplus R/\langle x-1 \rangle.$$

Moreover,

$$\langle x \rangle \cap \langle x-1 \rangle = \langle x(x-1) \rangle.$$

Hence,

$$R/\langle x(x-1) \rangle \cong \mathbb{Z} \oplus \mathbb{Z}.$$

Problem 8.2. Let $a + bi$ be a prime element in $\mathbb{Z}[i]$. Then prove the following.

- (a) $a - bi$ is also prime in $\mathbb{Z}[i]$.
- (b) $N(a + bi)$ is a power of some positive prime p in $\mathbb{Z}$.
- (c) $N(a + bi)$ equals p or p^2 , where p is as in (b).
- (d) If $N(a + bi) = p$, then $a + bi = p$ up to multiplication by a unit.

Solution 8.2. Recall that the norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ is defined by

$$N(x + yi) = x^2 + y^2,$$

and satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(a) Complex conjugation is a ring automorphism of $\mathbb{Z}[i]$. If $a - bi = \alpha\beta$, then conjugating gives

$$a + bi = \bar{\alpha}\bar{\beta}.$$

Since $a + bi$ is prime, one of $\bar{\alpha}$ or $\bar{\beta}$ must be a unit, and hence one of α or β is a unit. Thus, $a - bi$ is prime.

(b) Since $a + bi$ is prime, it is irreducible. Suppose

$$N(a + bi) = mn$$

with $m, n \in \mathbb{Z}$ and $1 < m, n < N(a + bi)$. Then

$$a^2 + b^2 = mn.$$

In $\mathbb{Z}[i]$ we have

$$(a + bi)(a - bi) = mn.$$

If m and n are non-units in $\mathbb{Z}$, then this expresses $a + bi$ as a product of non-units, contradicting irreducibility. Hence, $N(a + bi)$ must be a power of a positive prime p in $\mathbb{Z}$.

(c) We have

$$N(a + bi) = a^2 + b^2 = p^k$$

for some $k \geq 1$. Since

$$(a + bi)(a - bi) = p^k$$

and $a + bi$ is prime in $\mathbb{Z}[i]$, it must divide one of the factors p or p^{k-1} . This implies that $k \leq 2$. Therefore,

$$N(a + bi) = p \quad \text{or} \quad N(a + bi) = p^2.$$

(d) Suppose $N(a + bi) = p$. Then

$$(a + bi)(a - bi) = p.$$

Since p is prime in $\mathbb{Z}$ and $a + bi$ divides p in $\mathbb{Z}[i]$, there exists $\alpha \in \mathbb{Z}[i]$ such that

$$p = (a + bi)\alpha.$$

Taking norms gives

$$p^2 = N(p) = N(a + bi)N(\alpha) = pN(\alpha),$$

and hence $N(\alpha) = p$. This shows that α is a unit. Hence, $a + bi$ differs from p by multiplication by a unit.

Problem 8.3. Prove that no prime element $a + bi$ in $\mathbb{Z}[i]$ has

$$N(a + bi) = p$$

where p is a rational prime of the form $4n + 3$. Conclude that every positive prime integer of the form $4n + 3$ is prime in $\mathbb{Z}[i]$.

Solution 8.3. Recall that the norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}_{\geq 0}$ is given by

$$N(a + bi) = a^2 + b^2,$$

and satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

Suppose that $a + bi$ is a prime element in $\mathbb{Z}[i]$ and that

$$N(a + bi) = p,$$

where p is a rational prime with $p \equiv 3 \pmod{4}$. Then

$$a^2 + b^2 = p.$$

Reducing this congruence modulo 4, we obtain

$$a^2 + b^2 \equiv p \equiv 3 \pmod{4}.$$

However, for any integer k , we have $k^2 \equiv 0$ or $1 \pmod{4}$. Hence, the sum of two squares can be congruent only to 0, 1, or 2 modulo 4. This is a contradiction. Therefore, no prime element $a + bi$ in $\mathbb{Z}[i]$ can have norm equal to a prime p of the form $4n + 3$.

We now prove the conclusion. Let p be a positive prime in $\mathbb{Z}$ with $p \equiv 3 \pmod{4}$. Suppose that p is not prime in $\mathbb{Z}[i]$. Then there exist non-units $\alpha, \beta \in \mathbb{Z}[i]$ such that

$$p = \alpha\beta.$$

Taking norms gives

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Since p is prime in $\mathbb{Z}$, the only positive divisors of p^2 are 1, p , and p^2 . As α and β are non-units, we must have

$$N(\alpha) = N(\beta) = p.$$

This contradicts the first part of the proof, since no element of $\mathbb{Z}[i]$ with norm p exists when $p \equiv 3 \pmod{4}$.

Hence, p cannot factor nontrivially in $\mathbb{Z}[i]$. Therefore, every positive prime integer of the form $4n + 3$ is prime in $\mathbb{Z}[i]$.

Problem 8.4. Let R be a Noetherian ring and let I be an ideal of R . Prove that the quotient ring R/I is Noetherian.

Solution 8.4. Let R be a Noetherian ring and let I be an ideal of R . We prove that R/I is Noetherian by showing that every ideal of R/I is finitely generated.

Let K be an ideal of R/I . Then there exists an ideal J of R with $I \subseteq J$ such that

$$K = J/I.$$

Since R is Noetherian, the ideal J is finitely generated. Thus, there exist elements $a_1, \dots, a_n \in R$ such that

$$J = \langle a_1, \dots, a_n \rangle.$$

We show that K is generated by the cosets $a_1 + I, \dots, a_n + I$. Let $x + I \in J/I$. Then $x \in J$, and hence there exist elements $r_1, \dots, r_n \in R$ such that

$$x = r_1 a_1 + \dots + r_n a_n.$$

Therefore,

$$x + I = (r_1 a_1) + I + \dots + (r_n a_n) + I = (r_1 + I)(a_1 + I) + \dots + (r_n + I)(a_n + I).$$

This shows that every element of J/I can be written as a linear combination of $a_1 + I, \dots, a_n + I$ with coefficients in R/I .

Hence

$$J/I = \langle a_1 + I, \dots, a_n + I \rangle,$$

and J/I is finitely generated. Since K was arbitrary, every ideal of R/I is finitely generated. Therefore, R/I is Noetherian.

Problem 8.5. Let R be a Noetherian ring. Then every surjective ring homomorphism $\varphi : R \rightarrow R$ is injective, and hence an isomorphism.

Solution 8.5. Let $\varphi : R \rightarrow R$ be a surjective ring homomorphism. For each positive integer n , let

$$K_n = \ker(\varphi^n),$$

where φ^n denotes the n -fold composition of φ with itself. Each K_n is an ideal of R , and these ideals form an ascending chain

$$K_1 \subseteq K_2 \subseteq K_3 \subseteq \dots$$

Indeed, if $r \in K_n$, then $\varphi^n(r) = 0$, and hence

$$\varphi^{n+1}(r) = \varphi(\varphi^n(r)) = \varphi(0) = 0,$$

so $r \in K_{n+1}$.

Since R is Noetherian, this ascending chain stabilizes. Thus, there exists a positive integer n such that

$$K_n = K_{n+1}.$$

Now let $r \in \ker \varphi$. Then $\varphi(r) = 0$. Since φ is surjective, so is φ^n . Therefore, there exists $r_0 \in R$ such that

$$r = \varphi^n(r_0).$$

Applying φ gives

$$0 = \varphi(r) = \varphi(\varphi^n(r_0)) = \varphi^{n+1}(r_0).$$

Hence, $r_0 \in \ker(\varphi^{n+1}) = K_{n+1} = K_n$. It follows that

$$r = \varphi^n(r_0) = 0.$$

Thus, $\ker \varphi = \{0\}$, and hence φ is injective. Since φ is both injective and surjective, it is an isomorphism.

Problem 8.6. Let d be a non-square integer. The quadratic ring

$$\mathbb{Z}[\sqrt{d}]$$

is Noetherian.

Solution 8.6. Since $\mathbb{Z}$ is a Noetherian ring, the polynomial ring $\mathbb{Z}[X]$ is Noetherian by Hilbert's basis theorem. Define a ring homomorphism

$$\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{d}]$$

by evaluation at $\sqrt{d}$, that is,

$$\phi(X) = \sqrt{d}.$$

This homomorphism is surjective. Moreover, its kernel is the ideal

$$\ker \phi = (X^2 - d).$$

Therefore,

$$\mathbb{Z}[\sqrt{d}] \cong \mathbb{Z}[X]/(X^2 - d).$$

Since $\mathbb{Z}[X]$ is Noetherian and a quotient of a Noetherian ring is Noetherian, it follows that $\mathbb{Z}[\sqrt{d}]$ is Noetherian.

Problem 8.7. The rings

$$\mathbb{Z}[\sqrt{2}, \sqrt{3}] \quad \text{and} \quad \mathbb{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}]$$

are Noetherian.

Solution 8.7. Since $\mathbb{Z}$ is a Noetherian ring, the polynomial ring $\mathbb{Z}[X, Y]$ is Noetherian. Consider the ring homomorphism

$$\phi : \mathbb{Z}[X, Y] \longrightarrow \mathbb{Z}[\sqrt{2}, \sqrt{3}]$$

defined by

$$\phi(X) = \sqrt{2}, \quad \phi(Y) = \sqrt{3}.$$

This homomorphism is surjective. Its kernel contains the ideal $(X^2 - 2, Y^2 - 3)$, and in fact

$$\ker \phi = (X^2 - 2, Y^2 - 3).$$

Therefore,

$$\mathbb{Z}[\sqrt{2}, \sqrt{3}] \cong \mathbb{Z}[X, Y]/(X^2 - 2, Y^2 - 3).$$

As a quotient of a Noetherian ring, $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$ is Noetherian.

Similarly, since $\mathbb{Z}$ is Noetherian, the polynomial ring $\mathbb{Z}[X, Y, Z]$ is Noetherian. Define a ring homomorphism

$$\psi : \mathbb{Z}[X, Y, Z] \longrightarrow \mathbb{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}]$$

by

$$\psi(X) = i, \quad \psi(Y) = \sqrt[3]{2}, \quad \psi(Z) = \sqrt[7]{10}.$$

This map is surjective, and its kernel is

$$\ker \psi = (X^2 + 1, Y^3 - 2, Z^7 - 10).$$

Hence

$$\mathbb{Z}[i, \sqrt[3]{2}, \sqrt[7]{10}] \cong \mathbb{Z}[X, Y, Z]/(X^2 + 1, Y^3 - 2, Z^7 - 10).$$

Again, being a quotient of a Noetherian ring, this ring is Noetherian.

CHAPTER 7

Fields and Galois Theory

“The art of doing mathematics consists in finding that special case which contains all the germs of generality.”

— David Hilbert

1. Fields and Examples

Fields play a central role in algebra and number theory. They form the foundation for many important mathematical structures such as vector spaces, polynomial rings, and algebraic extensions. Fields also provide the framework for the study of solutions to equations, both linear and non-linear, and are crucial in areas ranging from cryptography and coding theory to algebraic geometry and Galois theory. Finite fields, in particular, have applications in computer science and information theory, while familiar infinite fields such as the rationals, reals, and complex numbers serve as the basic building blocks for analysis and algebra. Some of the examples and theorems in this chapter are adapted from [2].

Definition 1.1. A *field* is a commutative ring F with unity $1 \neq 0$ in which every non-zero element is a unit, i.e. for each $a \in F \setminus \{0\}$ there exists $b \in F$ such that $ab = 1$.

Example 1.1. Some well-known examples of fields are:

- (1) The field of rational numbers $\mathbb{Q}$ with the usual addition and multiplication.
- (2) The field of real numbers $\mathbb{R}$ which includes all limits of convergent sequences of rationals.
- (3) The field of complex numbers $\mathbb{C}$ consisting of numbers of the form $a + bi$ with $a, b \in \mathbb{R}$ and $i^2 = -1$.
- (4) The finite field $\mathbb{Z}/p\mathbb{Z}$, where p is a prime number, with addition and multiplication modulo p .

Theorem 1.1 (Field of Fractions and its Universal Property). Let R be an integral domain. Define

$$R \times R^\times := \{(a, b) \in R \times R \mid b \neq 0\} / \sim, \quad \text{where } (a, b) \sim (c, d) \iff ad = bc.$$

Write the $\sim$ equivalence class of (a, b) as $[(a, b)]$. Let

$$F := \{[(a, b)] \mid (a, b) \in R \times R^\times\}$$

and define

$$[(a, b)] + [(c, d)] := [(ad + bc, bd)], \quad [(a, b)] \cdot [(c, d)] := [(ac, bd)].$$

Then

- (1) These operations are well defined on F (i.e. are independent of representatives) and make F a field. The additive identity is $[(0, 1)]$, the multiplicative identity is $[(1, 1)]$, and for $a \neq 0$ the inverse of $[(a, b)]$ is $[(b, a)]$.
- (2) The map $\eta : R \rightarrow F$ given by $\eta(r) = [(r, 1)]$ is an injective ring homomorphism (the *canonical embedding*).
- (3) (Universal property) If $\varphi : R \rightarrow F'$ is an injective ring homomorphism into a field F' with $\varphi(1) = 1$, then there exists a unique field homomorphism

$$\tilde{\varphi} : F \longrightarrow F' \quad \text{such that} \quad \tilde{\varphi} \circ \eta = \varphi,$$

namely

$$\tilde{\varphi}([(a, b)]) = \varphi(a) \varphi(b)^{-1}.$$

Consequently, we may identify R with the subring $\eta(R) \subseteq F$, and call F the *field of fractions* of R .

PROOF. (1) First, we prove $\sim$ is an equivalence relation. Reflexive and symmetric are immediate. For transitivity, if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$. Since R is an integral domain and $d \neq 0$, multiplying gives $adf = bcf = bde$, hence $af = be$. Thus, $(a, b) \sim (e, f)$.

Next, we prove the operation addition is well-defined. Let $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Then $ab' = a'b$ and $cd' = c'd$, and we obtain

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'd'bd + b'c'd'bd = (a'd' + b'c')bd,$$

using $ab' = a'b$ and $cd' = c'd$. This shows that $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$, and hence addition is well defined. Similarly, we prove multiplication is well-defined.

It is easy to see that commutativity and associativity of $+$ and $\cdot$ reduce to the corresponding properties in R . The additive identity is $[(0, 1)]$, and $[(a, b)]$ has additive inverse $[(-a, b)]$. The multiplicative identity is $[(1, 1)]$. If $a \neq 0$, then

$$[(a, b)] \cdot [(b, a)] = [(ab, ab)] = [(1, 1)]$$

and so non-zero elements have inverses. Distributivity follows by a direct computation as follows:

$$[(a, b)] \cdot \left([(c, d)] + [(e, f)] \right) = [(a(cf + de), bdf)] = [(ac, bd)] + [(ae, bf)].$$

Thus, we conclude that F is a field.

(2) Clearly, η is a ring homomorphism by construction. We now prove that the map $\eta : R \rightarrow F$ given by $\eta(r) = [(r, 1)]$ is injective. If $\eta(r) = \eta(s)$, then $[(r, 1)] = [(s, 1)]$, hence $r \cdot 1 = s \cdot 1$ and so $r = s$. Thus, η is injective.

(3) We prove the universal property. Define $\tilde{\varphi}([(a, b)]) = \varphi(a)\varphi(b)^{-1} \in F'$. If $(a, b) \sim (a', b')$, then $ab' = a'b$, so applying φ (a ring homomorphism) gives $\varphi(a)\varphi(b') = \varphi(a')\varphi(b)$, hence $\varphi(a)\varphi(b)^{-1} = \varphi(a')\varphi(b')^{-1}$; Thus, $\tilde{\varphi}$ is well defined. It is a ring homomorphism, sends 1 to 1, and satisfies $\tilde{\varphi} \circ \eta = \varphi$ since

$$\tilde{\varphi}(\eta(r)) = \tilde{\varphi}([(r, 1)]) = \varphi(r)\varphi(1)^{-1} = \varphi(r).$$

For uniqueness, if $\psi : F \rightarrow F'$ is any field homomorphism with $\psi \circ \eta = \varphi$, then for (a, b) with $b \neq 0$,

$$\psi([(a, b)]) = \psi(\eta(a)\eta(b)^{-1}) = \psi(\eta(a))\psi(\eta(b))^{-1} = \varphi(a)\varphi(b)^{-1} = \tilde{\varphi}([(a, b)]),$$

so $\psi = \tilde{\varphi}$. This proves the universal property. $\square$

Example 1.2. If K is a field, then $K[X]$ is an integral domain and its field of fractions is the rational function field $K(X)$. More generally, the field of fractions of $K[X_1, \dots, X_n]$ is $K(X_1, \dots, X_n)$.

Lemma 1.1. Let R be a non-zero commutative ring with identity. Then R is a field if and only if the only proper ideal of R is $\{0\}$.

PROOF. Suppose R is a field and let I be a non-zero ideal of R . Choose $0 \neq a \in I$. Since a is invertible, $a^{-1} \in R$, and hence

$$1 = aa^{-1} \in I.$$

Thus, $I = R$ and the only proper ideal is $\{0\}$.

Conversely, assume that the only proper ideal of R is $\{0\}$. Let $0 \neq a \in R$. Consider the principal ideal $I = \langle a \rangle = aR$. Since $a \neq 0$, we have $I \neq 0$, hence $I = R$ by assumption. Thus, $1 \in I$, and there exists $b \in R$ with $1 = ba$. Hence, a has an inverse, and we conclude that R is a field. $\square$

Proposition 1.1. Let R be a commutative ring with identity, and let I be an ideal of R . Then I is maximal if and only if the quotient ring R/I is a field.

PROOF. Consider the quotient homomorphism $\pi : R \rightarrow R/I$. By the First Isomorphism Theorem for modules, there is a bijection between the set of ideals of R/I and the set of ideals of R that contain I , given by

$$J \subseteq R/I \iff \pi^{-1}(J).$$

In particular, the only proper ideals of R/I correspond to the proper ideals of R that properly contain I .

Assume that I is maximal. Then the only proper ideal of R/I is $\{0\}$. By Lemma 1.1, R/I is a field. Conversely, if R/I is a field, then $\{0\}$ is its only proper ideal, and hence I must be maximal in R . $\square$

Corollary 1.1. Every maximal ideal in a commutative ring with identity is prime.

PROOF. Let I be maximal. By Proposition 1.1, R/I is a field. Since every field is an integral domain, we have R/I is an integral domain. By Proposition 6.1, we conclude that I is prime. $\square$

Example 1.3. In the polynomial ring $R = \mathbb{Z}[X]$, the ideal

$$I = X\mathbb{Z}[X]$$

is prime, since $\mathbb{Z}[X]/I \cong \mathbb{Z}$, which is an integral domain. However, I is not maximal. Indeed, consider the larger ideal

$$J = X\mathbb{Z}[X] + 2\mathbb{Z}[X],$$

which properly contains I and is still a proper ideal of R . Hence, I is prime but not maximal.

Problem 1.1. Let $R = \mathbb{Z}$ or $R = K[X]$, where K is a field. Then every non-zero prime ideal of R is maximal.

Solution 1.1. In both $\mathbb{Z}$ and $K[X]$, every non-zero prime ideal is generated by an irreducible element

$$I = \langle p \rangle,$$

where p is a prime integer in $\mathbb{Z}$ or an irreducible polynomial in $K[X]$.

Now suppose J is an ideal of R with $I \subsetneq J \subsetneq R$. Choose $a \in J \setminus I$. Since $a \notin \langle p \rangle$, it follows that $p \nmid a$. Thus, p and a are relatively prime in R .

By the Bézout identity, there exist $x, y \in R$ such that

$$xp + ya = 1.$$

Since $p \in I \subseteq J$ and $a \in J$, the right-hand side shows $1 \in J$. Hence, $J = R$, contradicting the assumption that J is proper. Therefore, I is not properly contained in any proper ideal. Thus, I is maximal.

Problem 1.2. Let R be a non-zero finite commutative ring with unity. Assume R has no zero divisors. Prove that R is a field.

Solution 1.2. Let $a \in R$ be a non-zero element. Consider the map

$$\varphi_a : R \rightarrow R, \quad \varphi_a(x) = ax.$$

If $\varphi_a(x) = \varphi_a(y)$, then $a(x - y) = 0$. Since R has no zero divisors and $a \neq 0$, we must have $x - y = 0$, hence $x = y$. Thus, φ_a is injective. Since R is finite, any injective map $R \rightarrow R$ is also surjective. Therefore, there exists $x \in R$ with $\varphi_a(x) = 1$, i.e. $ax = 1$. This shows that every non-zero element $a \in R$ has a multiplicative inverse. Since R is commutative and every non-zero element is invertible, we conclude that R is a field.

Problem 1.3. For every prime p , the ring of integers modulo p , denoted $\mathbb{Z}/p\mathbb{Z}$, is a field.

Solution 1.3. The ring $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring with unity $\bar{1} \neq \bar{0}$. Suppose $\bar{a}\bar{b} = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$. Then $p \mid ab$. Since p is prime, it divides a or b , so $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$. Thus, $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors, i.e. it is an integral domain. Moreover, $\mathbb{Z}/p\mathbb{Z}$ has exactly p elements, hence it is finite. By the previous problem, we conclude that $\mathbb{Z}/p\mathbb{Z}$ is a field.

Problem 1.4. Let R be a commutative ring with $1 \neq 0$. Prove that R is a field if and only if the only ideals of R are $\langle 0 \rangle$ and R .

Solution 1.4. Assume that R is a field. Let I be an ideal of R . If $I \neq \langle 0 \rangle$, then there exists $0 \neq a \in I$. Since R is a field, a has a multiplicative inverse $a^{-1} \in R$, and hence

$$1 = a^{-1}a \in I.$$

Therefore, $I = R$. Thus, the only ideals of R are $\langle 0 \rangle$ and R .

Conversely, suppose that the only ideals of R are $\langle 0 \rangle$ and R . Let $0 \neq a \in R$. Then the ideal $\langle a \rangle$ is not equal to $\langle 0 \rangle$, and hence $\langle a \rangle = R$. Therefore, there exists $r \in R$ such that

$$ra = 1.$$

This shows that every nonzero element of R has a multiplicative inverse. Hence, R is a field.

Problem 1.5. Let R be a commutative ring with 1. In the polynomial ring $R[x]$ consider the principal ideal $\langle x \rangle$ generated by x . Then

- (1) $\langle x \rangle$ is a prime ideal of $R[x]$ if and only if R is an integral domain.
- (2) $\langle x \rangle$ is a maximal ideal of $R[x]$ if and only if R is a field.

Solution 1.5. Define the evaluation homomorphism at 0,

$$\varphi : R[x] \longrightarrow R, \quad f(x) \mapsto f(0).$$

Clearly, φ is a surjective ring homomorphism and $\ker \varphi = \langle x \rangle$ (the polynomials with zero constant term are exactly those divisible by x). By the First Isomorphism Theorem,

$$R[x]/\langle x \rangle \cong R.$$

(1) An ideal I is prime if and only if the quotient ring $R[x]/I$ is an integral domain. Applying this to $I = \langle x \rangle$ and using the isomorphism above, $\langle x \rangle$ is prime in $R[x]$ exactly when $R[x]/\langle x \rangle \cong R$ is an integral domain. Thus, $\langle x \rangle$ is prime if and only if R is an integral domain.

(2) An ideal I is maximal if and only if the quotient $R[x]/I$ is a field. Again using $R[x]/\langle x \rangle \cong R$, we see that $\langle x \rangle$ is maximal if and only if R is a field.

Definition 1.2 (Characteristic of a field). Let F be a field with identity 1_F . For $n \in \mathbb{Z}_{>0}$, define

$$n \cdot 1_F = \underbrace{1_F + \cdots + 1_F}_{n \text{ times}}.$$

The *characteristic* of F , denoted $\text{ch}(F)$ or $\text{char}(F)$, is the least integer $p > 0$ such that $p \cdot 1_F = 0$, if such p exists; otherwise $\text{ch}(F) = 0$.

Proposition 1.2. The characteristic of a field is either 0 or a prime number p . Moreover, if $n \cdot 1_F = 0$, then $p \mid n$.

PROOF. If $\text{ch}(F) = 0$, we are done. Suppose $\text{ch}(F) = n > 0$. If $n = ab$ with $1 < a, b < n$, then

$$0 = n \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F).$$

Since F has no zero divisors, one of $a \cdot 1_F$ or $b \cdot 1_F$ is 0, contradicting minimality of n . Thus, n is prime.

Now if $n \cdot 1_F = 0$, then we write $n = qp + r$ with $0 \leq r < p$. This implies that

$$0 = n \cdot 1_F = (qp + r) \cdot 1_F = r \cdot 1_F.$$

By minimality of p , $r = 0$, hence $p \mid n$. □

Example 1.4. (1) The fields $\mathbb{Q}$ and $\mathbb{R}$ both have characteristic 0.

$$\text{ch}(\mathbb{Q}) = \text{ch}(\mathbb{R}) = 0.$$

(2) For any prime p , the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p .

(3) The polynomial ring $\mathbb{F}_p[x]$ over the finite field $\mathbb{F}_p$ has characteristic p , as does its field of fractions $\mathbb{F}_p(x)$ (the field of rational functions in x over $\mathbb{F}_p$).

Proposition 1.3. Every field F contains a unique subfield isomorphic either to $\mathbb{Q}$ or to a finite field $\mathbb{F}_p$ for some prime p .

PROOF. Define a ring homomorphism

$$\varphi : \mathbb{Z} \longrightarrow F, \quad \varphi(n) = n \cdot 1_F.$$

The kernel of φ is an ideal of $\mathbb{Z}$, hence of the form $m\mathbb{Z}$ for some integer $m \geq 0$. Thus, φ factors through

$$\bar{\varphi} : \mathbb{Z}/m\mathbb{Z} \longrightarrow F.$$

If $m = p$ is prime, then $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ is a field, and the image of $\overline{\varphi}$ is a subfield of F isomorphic to $\mathbb{F}_p$.

Next, if $m = 0$, then φ is injective, embedding $\mathbb{Z}$ into F . This extends uniquely to a homomorphism

$$\psi : \mathbb{Q} \longrightarrow F, \quad \psi\left(\frac{k}{\ell}\right) = \varphi(k) \varphi(\ell)^{-1}, \quad \ell \neq 0,$$

which is well defined and injective. Hence, F contains a subfield isomorphic to $\mathbb{Q}$. $\square$

Definition 1.3. The subfield of F given by Proposition 1.3 is called the *prime subfield* of F . The *characteristic* of F is defined as

$$\text{ch}(F) = \begin{cases} 0, & \text{if the prime subfield of } F \text{ is isomorphic to } \mathbb{Q}, \\ p, & \text{if the prime subfield of } F \text{ is isomorphic to } \mathbb{F}_p \text{ for some prime } p. \end{cases}$$

Problem 1.6. Let F be a field and let $f(t) \in F[t]$. Then prove the following statements.

- (a) If $\text{char}(F) = 0$, then $f'(t) = 0$ if and only if $f(t)$ is a constant polynomial.
- (b) If $\text{char}(F) = p > 0$, then

$$f(t)^p = f^p(t^p),$$

and if $f'(t) = 0$, then there exists a polynomial $g(t) \in F[t]$ such that

$$f(t) = g(t^p).$$

Solution 1.6. (a) Write

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n, \quad a_i \in F.$$

Then

$$f'(t) = a_1 + 2a_2 t + \cdots + na_n t^{n-1}.$$

If $f(t)$ is constant, then clearly $f'(t) = 0$. Conversely, if $f'(t) = 0$ and $\text{char}(F) = 0$, then

$$a_1 = 2a_2 = \cdots = na_n = 0.$$

Since the characteristic is zero, each integer $1, 2, \dots, n$ is non-zero in F , and hence $a_1 = a_2 = \cdots = a_n = 0$. Thus, $f(t) = a_0$ is constant.

(b) Assume $\text{char}(F) = p > 0$. Let

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n.$$

Then

$$f(t)^p = (a_0 + a_1 t + \cdots + a_n t^n)^p = a_0^p + a_1^p t^p + \cdots + a_n^p t^{np},$$

since all intermediate binomial coefficients are divisible by p . Hence

$$f(t)^p = f^p(t^p),$$

where $f^p(t) = a_0^p + a_1^p t + \cdots + a_n^p t^n$.

Now suppose that $f'(t) = 0$. Then

$$a_1 = 2a_2 = \cdots = na_n = 0.$$

Since characteristic of F is p , this implies that $a_i = 0$ whenever $p \nmid i$. Therefore,

$$f(t) = a_0 + a_p t^p + a_{2p} t^{2p} + \cdots.$$

Define $g(t) = a_0 + a_p t + a_{2p} t^2 + \cdots \in F[t]$. Then, we conclude that $f(t) = g(t^p)$.

Problem 1.7. Prove that an integral domain with finitely many elements is a field.

Solution 1.7. Let R be a finite integral domain. To prove R is a field, it suffices to prove that every non-zero element of R has a multiplicative inverse.

Let $a \in R$ with $a \neq 0$. Consider the map

$$\varphi : R \rightarrow R, \quad \varphi(x) = ax.$$

Since R is an integral domain, multiplication by any nonzero element is injective. Hence, if $\varphi(x) = \varphi(y)$, then $ax = ay$, and by the cancellation law we obtain $x = y$.

Since R has a finite number of elements, every injective map from R to itself is also surjective. Hence, φ is surjective. In particular, there exists an element $b \in R$ such that

$$\varphi(b) = ab = 1.$$

Thus, a has a multiplicative inverse b in R . Since $a \neq 0$ was arbitrary, every non-zero element of R is a unit. Therefore, R is a field.

Problem 1.8. Let R be a commutative ring with $1 \neq 0$. An element $x \in R$ is *nilpotent* if there exists $m \in \mathbb{Z}_{>0}$ such that $x^m = 0$. Then prove the following statements.

- (a) Let $n = a^k b$ for some integers a, b and $k \geq 1$. Show that the class $\overline{ab} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent.
- (b) Let $a \in \mathbb{Z}$. Prove that the element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n also divides a . In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.
- (c) Let X be a non-empty set and F a field. Let R be the ring of functions $X \rightarrow F$ with point-wise addition and multiplication. Prove that R contains no non-zero nilpotent elements.

Solution 1.8. (a) Suppose $n = a^k b$. In $\mathbb{Z}/n\mathbb{Z}$ consider $\overline{ab}$. Then

$$(ab)^k = a^k b^k = (a^k b) b^{k-1} = n b^{k-1}.$$

Thus, $n \mid (ab)^k$ and so $(\overline{ab})^k = \overline{0}$. Hence, $\overline{ab}$ is nilpotent.

(b) Write $n = \prod_{i=1}^r p_i^{e_i}$ with distinct primes p_i . Assume that $\overline{a}$ is nilpotent. Then a^m is divisible by n for some m . Thus, $p_i^{e_i} \mid a^m$ for all i , which implies $p_i \mid a$. Hence, every prime divisor of n divides a .

Conversely, suppose every p_i dividing n also divides a . Let $v_{p_i}(a) = f_i \geq 1$, where $v_p(a)$ denotes the largest integer $f \geq 0$ such that $p^f \mid a$ (the p -adic valuation of a). Choose

$$m = \max_{1 \leq i \leq r} \left\lceil \frac{e_i}{f_i} \right\rceil.$$

Then $mf_i \geq e_i$ for all i , and hence $p_i^{e_i} \mid a^m$. Therefore, $n \mid a^m$, i.e. $\overline{a}^m = \overline{0}$. Thus, $\overline{a}$ is nilpotent.

For $n = 72 = 2^3 \cdot 3^2$, the criterion says $\overline{a}$ is nilpotent iff $6 \mid a$. So the nilpotent elements are exactly the classes

$$\{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \dots, \overline{66}\},$$

that is, all multiples of 6 modulo 72.

(c) Suppose $f : X \rightarrow F$ is nilpotent in R . Then $f^m = 0$ for some $m > 0$, and hence $(f(x))^m = 0$ in F for each $x \in X$. But in a field, the only nilpotent element is 0, which implies $f(x) = 0$ for all x . Thus, f is the zero function. Therefore, R contains no non-zero nilpotent elements.

2. Vector Spaces

Abstract algebra is built upon three fundamental structures: *groups*, *rings*, and *fields*. We have already studied groups and rings in detail, and introduced the concept of a field. To explore fields more thoroughly, we now turn to some basic notions of vector space theory, which will play an important role in our further study.

Definition 2.1 (Vector Space). Let F be a field. A *vector space over F* is a set V together with two operations: addition $+: V \times V \rightarrow V$ and scalar multiplication $\cdot: F \times V \rightarrow V$, denoted $(a, v) \mapsto av$, such that $(V, +)$ is an abelian group and the following axioms hold for all $a, b \in F$ and all $u, v \in V$.

- (1) $a(u + v) = au + av$ (distributivity over vector addition),
- (2) $(a + b)v = av + bv$ (distributivity over field addition),
- (3) $a(bv) = (ab)v$ (compatibility with field multiplication),
- (4) $1v = v$, where 1 is the multiplicative identity in F .

The elements of V are called *vectors*, and the elements of F are called *scalars*. The operation av is called *scalar multiplication*. By convention, vectors are typically denoted by letters such as u, v, w , while scalars are denoted by a, b, c .

Example 2.1. The set $\mathbb{R}^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$. Addition and scalar multiplication are defined componentwise as

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n), \quad c(a_1, \dots, a_n) = (ca_1, \dots, ca_n)$$

for all $c \in \mathbb{R}$ and $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{R}^n$.

Example 2.2. The set $M_2(\mathbb{Q})$ of 2×2 matrices with entries in $\mathbb{Q}$ is a vector space over $\mathbb{Q}$. For $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \in M_2(\mathbb{Q})$ and $c \in \mathbb{Q}$, define

$$A + B = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix}, \quad cA = \begin{pmatrix} ca_1 & ca_2 \\ ca_3 & ca_4 \end{pmatrix}.$$

Example 2.3. The set $\mathbb{Z}_p[x]$ of polynomials with coefficients in $\mathbb{Z}_p$, where p is prime, is a vector space over $\mathbb{Z}_p$ with the usual polynomial addition and scalar multiplication.

Example 2.4. The set of complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$. Addition and scalar multiplication are the usual operations of complex numbers.

Example 2.5. Let E be a field and F a subfield of E . Then E is a vector space over F with vector addition and scalar multiplication given by the operations of E . This generalizes the previous example and plays a central role in the theory of fields.

Definition 2.2 (Subspace). Let V be a vector space over a field F , and let $W \subseteq V$. We say that W is a *subspace* of V if W itself is a vector space over F under the addition and scalar multiplication inherited from V .

Definition 2.3 (Span and Linear combination). Let V be a vector space over a field F , and let $v_1, v_2, \dots, v_n$ be (not necessarily distinct) elements of V . The set

$$\langle v_1, v_2, \dots, v_n \rangle = \{a_1v_1 + a_2v_2 + \dots + a_nv_n \mid a_1, a_2, \dots, a_n \in F\}$$

is called the *subspace of V spanned by $v_1, v_2, \dots, v_n$* .

Any element of the form

$$a_1v_1 + a_2v_2 + \dots + a_nv_n, \quad a_i \in F$$

is called a *linear combination* of $v_1, v_2, \dots, v_n$.

Definition 2.4 (Linearly dependent and Independent sets). Let V be a vector space over a field F , and let $S \subseteq V$ be a set of vectors.

- (a) The set S is said to be *linearly dependent over F* if there exist distinct vectors $v_1, v_2, \dots, v_n \in S$ and scalars $a_1, a_2, \dots, a_n \in F$, not all zero, such that

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0.$$

- (b) The set S is said to be *linearly independent over F* if it is not linearly dependent, that is, if

$$a_1v_1 + a_2v_2 + \dots + a_nv_n = 0, \quad a_i \in F,$$

then $a_1 = a_2 = \dots = a_n = 0$.

Example 2.6. Consider the vector space $\mathbb{R}^3$, and the vectors

$$(1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1).$$

We now check whether the above vectors are linearly independent over $\mathbb{R}$. Suppose there exist scalars $a, b, c \in \mathbb{R}$ such that

$$a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) = (0, 0, 0).$$

Carrying out the addition gives

$$(a, b, c) = (0, 0, 0).$$

Thus, $a = 0$, $b = 0$, and $c = 0$. Therefore, the given vectors are linearly independent.

Example 2.7. In $\mathbb{R}^3$, the vectors

$$(1, 0, 0), \quad (1, 0, 1), \quad (1, 1, 1)$$

are linearly independent over $\mathbb{R}$. To verify this, suppose there exist scalars $a, b, c \in \mathbb{R}$ such that

$$a(1, 0, 0) + b(1, 0, 1) + c(1, 1, 1) = (0, 0, 0).$$

This implies that

$$(a + b + c, c, b + c) = (0, 0, 0).$$

Thus, we obtain the system

$$a + b + c = 0, \quad c = 0, \quad b + c = 0.$$

From $c = 0$ and $b + c = 0$, it follows that $b = 0$, and then $a = 0$. Hence

$$a = b = c = 0.$$

Therefore, the given vectors are linearly independent.

Definition 2.5 (Basis). Let V be a vector space over a field F . A subset $B \subseteq V$ is called a *basis* of V if

- (1) B is linearly independent over F , and
- (2) every vector in V can be expressed as a linear combination of finitely many elements of B .

Example 2.8. In $\mathbb{R}^3$, the set

$$B = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

is a basis. Indeed, B is linearly independent, since the only solution to

$$a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) = (0, 0, 0)$$

with $a, b, c \in \mathbb{R}$ is $a = b = c = 0$. Moreover, every vector $(x, y, z) \in \mathbb{R}^3$ can be written as

$$(x, y, z) = x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1).$$

Therefore, B spans $\mathbb{R}^3$. Hence, B is a basis of $\mathbb{R}^3$, called the *standard basis*.

Definition 2.6 (Dimension). Let V be a vector space over a field F . The *dimension* of V , denoted $\dim(V)$, is the number of elements in any basis of V .

Remark 2.1. The dimension of a vector space V is well-defined because all bases of V have the same cardinality. In particular, the zero vector space $\{0\}$ has no non-zero vectors, and by convention it is assigned the empty set as a basis. Hence,

$$\dim(\{0\}) = 0.$$

Problem 2.1. Let F be a field and let K be a field containing F as a subfield. Show that K is a vector space over F .

Solution 2.1. Since $F \subseteq K$ and both are fields, the addition and multiplication in F are the restrictions of the corresponding operations in K . Define scalar multiplication by

$$\lambda \cdot x := \lambda x \quad (\lambda \in F, x \in K).$$

The vector space axioms follow directly from the field axioms of K . Hence, K is a vector space over F .

Problem 2.2. Let F be a field, and let K be a field containing F . Assume that $\dim_F K = n < \infty$. Show that for any $\alpha \in K$, the set

$$\{1, \alpha, \alpha^2, \dots, \alpha^n\}$$

is linearly dependent over F .

Solution 2.2. The vector space K has dimension n over F . Any set of more than n vectors in a vector space of dimension n is linearly dependent.

Since the set $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ contains $n + 1$ elements, it is linearly dependent over F .

Problem 2.3. Find a basis for each of the following vector spaces over $\mathbb{Q}$.

- (a) $\mathbb{Q}(\sqrt{2})$
- (b) $\mathbb{Q}(\sqrt[3]{2})$
- (c) $\mathbb{Q}(i)$
- (d) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Solution 2.3. (a) Every element of $\mathbb{Q}(\sqrt{2})$ can be written uniquely in the form

$$a + b\sqrt{2}, \quad a, b \in \mathbb{Q}.$$

This shows that $\mathbb{Q}(\sqrt{2})$ is spanned by $\{1, \sqrt{2}\}$. If

$$a + b\sqrt{2} = 0,$$

then $b = 0$ implies $a = 0$, since $\sqrt{2} \notin \mathbb{Q}$. Hence, the set is linearly independent and therefore forms a basis.

(b) Let $\alpha = \sqrt[3]{2}$. Since $\alpha^3 = 2 \in \mathbb{Q}$, every power of α of degree at least 3 can be reduced to a $\mathbb{Q}$ -linear combination of $1, \alpha, \alpha^2$. Thus, every element of $\mathbb{Q}(\alpha)$ has the form

$$a + b\alpha + c\alpha^2, \quad a, b, c \in \mathbb{Q}.$$

The set $\{1, \alpha, \alpha^2\}$ spans the space and is linearly independent. Hence, it is a basis.

(c) Every element of $\mathbb{Q}(i)$ can be written as

$$a + bi, \quad a, b \in \mathbb{Q}.$$

Since $i \notin \mathbb{Q}$, the elements 1 and i are linearly independent. Thus, $\{1, i\}$ spans the space and forms a basis.

(d) Any element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be expressed as

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q}.$$

Since $\sqrt{6} = \sqrt{2}\sqrt{3}$, every product of $\sqrt{2}$ and $\sqrt{3}$ can be expressed as a $\mathbb{Q}$ -linear combination of these four elements. The set $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent and spans the space, and hence is a basis.

Problem 2.4. Find a basis for each of the following matrix vector spaces over $\mathbb{R}$.

- (a) $M_2(\mathbb{R})$.
- (b) The space of all symmetric 2×2 real matrices.
- (c) The space of all 2×2 real matrices with trace zero.

Solution 2.4. (a) Every matrix in $M_2(\mathbb{R})$ has the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{R}.$$

Thus, $M_2(\mathbb{R})$ is spanned by the four matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

These matrices are clearly linearly independent, and hence form a basis.

(b) A symmetric 2×2 real matrix has the form

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}, \quad a, b, c \in \mathbb{R}.$$

Thus, the space is spanned by

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

These matrices are linearly independent and hence form a basis.

(c) A 2×2 real matrix has trace zero if and only if it has the form

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}, \quad a, b, c \in \mathbb{R}.$$

Thus, the space is spanned by

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

These matrices are linearly independent and therefore form a basis.

3. Field Extensions

Definition 3.1 (Extension Field). Let F and E be fields. We say that E is an *extension field* of F , written $F \subseteq E$, if

- (1) F is a subfield of E , and
- (2) the field operations of F are precisely the restrictions of the operations of E to F .

Remark 3.1. An extension field E of F can be viewed as a larger field obtained by adjoining new elements to F . The following classical example was given by Cauchy in 1847, the quotient ring

$$\mathbb{R}[x]/\langle x^2 + 1 \rangle$$

is a field that contains a root of the polynomial $x^2 + 1$ which does not exist in $\mathbb{R}$. This construction foreshadowed the general theory of adjoining roots of polynomials to form extension fields.

Definition 3.2 (Degree of a Field Extension). Let K/F be a field extension. By restricting the multiplication in K to scalars from F , the set K becomes a vector space over F . The *degree* of the extension, denoted

$$[K : F],$$

is defined to be the dimension of K as a vector space over F , that is,

$$[K : F] = \dim_F K.$$

The extension K/F is called *finite* if $[K : F] < \infty$, and *infinite* otherwise.

Remark 3.2. Every field F can be regarded as a vector space over its prime subfield (either $\mathbb{Q}$ or $\mathbb{F}_p$). Thus, $[F : \mathbb{Q}]$ or $[F : \mathbb{F}_p]$ describes how large F is relative to its simplest building blocks. For example

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2, \quad [\mathbb{C} : \mathbb{R}] = 2, \quad [\mathbb{R} : \mathbb{Q}] = \infty.$$

Remark 3.3. An important class of field extensions arises from adjoining roots of polynomials. For instance, over the real numbers $\mathbb{R}$, the equation

$$x^2 + 1 = 0$$

has no solution. This motivates enlarging $\mathbb{R}$ to a larger field in which the equation is solvable. By adjoining a symbol i with $i^2 = -1$, Gauss introduced the complex numbers

$$\mathbb{C} = \mathbb{R} + \mathbb{R}i,$$

and verified that $\mathbb{C}$ is a field. Thus, $\mathbb{C}$ is an extension of $\mathbb{R}$ in which $x^2 + 1$ has a root.

More generally, let F be a field and let $p(x) \in F[x]$ be a polynomial. One may ask whether there exists an extension field K/F that contains a root of $p(x)$. Since any root of an irreducible factor of $p(x)$ is also a root of $p(x)$, we may assume that $p(x)$ itself is irreducible. In this case, the quotient ring

$$F[x]/\langle p(x) \rangle$$

is a field, and it provides an extension of F in which $p(x)$ has a root.

Proposition 3.1. Let $\varphi : F \rightarrow F'$ be a homomorphism of fields. Then φ is either the zero map (sending every element of F to 0) or it is injective. In particular, the image of φ is either $\{0\}$ or a subfield of F' isomorphic to F .

PROOF. The kernel of a field homomorphism φ is an ideal of F . Since F is a field, its only ideals are $\{0\}$ and F itself. If $\ker(\varphi) = F$, then φ is the zero map. Next, if $\ker(\varphi) = \{0\}$, then φ is injective. Thus, φ is either identically zero or injective. In the injective case, the image $\varphi(F)$ is a subfield of F' isomorphic to F . $\square$

Lemma 3.1. Let F be a field and let $p(x) \in F[x]$ be a non-constant polynomial. If $p(x)$ is irreducible in $F[x]$, then the ideal $\langle p(x) \rangle$ is maximal in $F[x]$. Consequently, the quotient ring $F[x]/\langle p(x) \rangle$ is a field.

PROOF. Recall that $F[x]$ is a Euclidean domain, hence a principal ideal domain. Let I be an ideal of $F[x]$ with $\langle p(x) \rangle \subseteq I \subseteq F[x]$. If $I = \langle p(x) \rangle$ we are done, so assume $I \neq \langle p(x) \rangle$. Choose $f(x) \in I \setminus \langle p(x) \rangle$. Since $p(x)$ is irreducible and does not divide $f(x)$, the greatest common divisor $\gcd(p, f) = 1$. By Bézout's identity in $F[x]$ there exist $a(x), b(x) \in F[x]$ with

$$a(x)p(x) + b(x)f(x) = 1.$$

Both terms on the left lie in I , hence $1 \in I$. Therefore, $I = F[x]$. This shows that no ideal lies strictly between $\langle p(x) \rangle$ and $F[x]$, so $\langle p(x) \rangle$ is maximal.

Finally, the quotient of a ring by a maximal ideal is a field, so $F[x]/\langle p(x) \rangle$ is a field. $\square$

Theorem 3.1. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial of degree n . Define

$$K = F[x]/\langle p(x) \rangle, \quad \theta := x + \langle p(x) \rangle \in K.$$

Then K is a field extension of F of degree n , and θ is a root of $p(x)$ in K , i.e.

$$p(\theta) = 0 \quad \text{in } K.$$

Moreover, the set

$$\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$$

forms a basis of K as a vector space over F . Consequently,

$$[K : F] = n,$$

and each element of K has a unique expression of the form

$$a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1}, \quad a_i \in F.$$

PROOF. Since $p(x)$ is irreducible, the ideal $\langle p(x) \rangle$ is maximal in $F[x]$, and hence $K = F[x]/\langle p(x) \rangle$ is a field by Lemma 3.1. Let $f(x) \in F[x]$. By the division algorithm, we can write

$$f(x) = q(x)p(x) + r(x),$$

where $q(x), r(x) \in F[x]$ and $\deg(r) < n$. Thus, in the quotient K ,

$$f(x) \equiv r(x).$$

Therefore, every element of K is represented by a polynomial of degree less than n . This shows that $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ spans K over F .

Next, we prove linear independence. Suppose

$$b_0 + b_1\theta + b_2\theta^2 + \dots + b_{n-1}\theta^{n-1} = 0$$

in K , with coefficients $b_i \in F$. Then

$$b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} \in \langle p(x) \rangle.$$

This implies that $p(x)$ divides a polynomial of degree strictly less than n , which is impossible because $p(x)$ is irreducible of degree n . Hence, all $b_i = 0$, proving linear independence.

Therefore, $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ is a basis of K over F , and we conclude that $\dim_F K = n$, i.e., $[K : F] = n$. $\square$

Problem 3.1. Let $F = \mathbb{R}$ and $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Show that the quotient ring

$$K = \mathbb{R}[x]/\langle x^2 + 1 \rangle$$

is a field extension of degree 2 of $\mathbb{R}$ in which $x^2 + 1$ has a root, and describe explicitly the addition and multiplication in K .

Solution 3.1. The polynomial $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}$. Hence, the quotient ring

$$K = \mathbb{R}[x]/\langle x^2 + 1 \rangle$$

is a field extension of $\mathbb{R}$ of degree 2. Let $\theta = x \bmod \langle x^2 + 1 \rangle \in K$. Every element of K can be written uniquely in the form

$$a + b\theta \quad (a, b \in \mathbb{R}).$$

For $a + b\theta, c + d\theta \in K$, define addition as

$$(3) \quad (a + b\theta) + (c + d\theta) = (a + c) + (b + d)\theta.$$

Using the relation $\theta^2 = -1$ (since $x^2 \equiv -1 \pmod{x^2 + 1}$), we define multiplication as

$$(4) \quad (a + b\theta)(c + d\theta) = ac + (ad + bc)\theta + bd\theta^2$$

$$(5) \quad = (ac - bd) + (ad + bc)\theta.$$

Equations (3) and (5) are exactly the familiar rules for addition and multiplication in $\mathbb{C}$, if we identify θ with i . Define the map

$$\varphi : \mathbb{R}[x]/\langle x^2 + 1 \rangle \longrightarrow \mathbb{C}, \quad a + b\theta \mapsto a + bi.$$

This is a ring homomorphism, and since it is bijective (as both sides are 2-dimensional vector spaces over $\mathbb{R}$), it is an isomorphism.

4. Algebraic Elements

Definition 4.1. Let K and K' be fields.

- (1) A *field map* is a ring homomorphism $\varphi : K \rightarrow K'$ such that $\varphi(1) = 1$. Since fields have no non-trivial ideals, every field map is automatically injective.
- (2) If K and K' are extensions of a field F and $\varphi|_F = \text{id}_F$, then φ is called an *F-field map*.

Remark 4.1. (1) If φ is surjective, then it is a *field isomorphism*.

- (2) If φ is surjective and also fixes F , then it is an *F-isomorphism*.
- (3) When $K = K'$, a surjective φ is an *automorphism* of K .
- (4) If φ fixes F , then it is called an *F-automorphism*.

Definition 4.2. Let K/F be a field extension and let $x_1, \dots, x_n \in K$.

- (1) The *subring of K generated by F and $x_1, \dots, x_n$* , denoted by

$$F[x_1, \dots, x_n],$$

is the set of all polynomials in $x_1, \dots, x_n$ with coefficients in F , i.e.,

$$F[x_1, \dots, x_n] = \left\{ \sum_{(i_1, \dots, i_n) \in I} c_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n} \mid c_{i_1, \dots, i_n} \in F, I \subseteq \mathbb{Z}_{\geq 0}^n \text{ finite} \right\}.$$

- (2) The *subfield of K generated by F and $x_1, \dots, x_n$* , denoted by

$$F(x_1, \dots, x_n),$$

consists of all quotients

$$\frac{p(x_1, \dots, x_n)}{q(x_1, \dots, x_n)},$$

where $p, q \in F[x_1, \dots, x_n]$ and $q(x_1, \dots, x_n) \neq 0$. This field is called the field obtained by adjoining $x_1, \dots, x_n$ to F and can be regarded as the field of fractions of $F[x_1, \dots, x_n]$.

Remark 4.2. The field $F(x_1, \dots, x_n)$ can be regarded as the field of fractions of $F[x_1, \dots, x_n]$. Indeed, by the universal property of fraction fields, the natural embedding $F[x_1, \dots, x_n] \hookrightarrow F(x_1, \dots, x_n)$ factors through the field of fractions of $F[x_1, \dots, x_n]$.

Definition 4.3. Let K/F be a field extension and let $x \in K$.

- (1) For the polynomial ring $F[X]$ in one indeterminate X , there exists a unique *substitution homomorphism*

$$\varphi_x : F[X] \longrightarrow F[x],$$

defined by $\varphi_x(f(X)) = f(x)$ for all $f(X) \in F[X]$.

- (2) The element x is called *algebraic over F* if φ_x is not injective, i.e., if x is a root of some non-zero polynomial in $F[X]$.
- (3) The element x is called *transcendental over F* if φ_x is injective.

Definition 4.4 (Minimal Polynomial). Let K/F be a field extension and let $x \in K$ be algebraic over F . Consider the substitution homomorphism

$$\varphi_x : F[X] \longrightarrow F[x], \quad \varphi_x(f(X)) = f(x).$$

Then

$$\ker \varphi_x = \{f(X) \in F[X] \mid f(x) = 0\}$$

is a non-zero ideal of $F[X]$. Since $F[X]$ is a principal ideal domain, $\ker \varphi_x$ is generated by a single polynomial. Among all non-zero polynomials in $\ker \varphi_x$, there exists a unique monic polynomial of least degree. This polynomial, denoted by $F_0(X)$, satisfies

$$\ker \varphi_x = (F_0(X)),$$

and is called the *minimal polynomial* of x over F .

Proposition 4.1. Let $x \in K$ be algebraic over F . Then the minimal polynomial of x over F is irreducible in $F[X]$.

PROOF. Let $F(X)$ denote the minimal polynomial of x over F . Suppose $F(X) = G(X)H(X)$ with $G, H \in F[X]$ of smaller degree. Then $0 = F(x) = G(x)H(x)$, hence $G(x) = 0$ or $H(x) = 0$. This contradicts the minimality of $\deg F$, and we conclude that F is irreducible. $\square$

Theorem 4.1. If $x \in K$ is algebraic over F with minimal polynomial $F(X)$ of degree n , then

$$F(x) = F[x] \cong F[X]/(F(X)).$$

Moreover, every element of $F(x)$ has a unique expression of the form

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1}, \quad c_i \in F.$$

PROOF. Consider the evaluation map

$$\varphi_x : F[X] \longrightarrow F[x], \quad G(X) \mapsto G(x).$$

Its kernel is the ideal generated by the minimal polynomial $m_x(X)$ of x over F . Hence

$$F[x] \cong F[X]/(m_x(X)).$$

Since $m_x(X)$ is irreducible, the ideal $(m_x(X)) \subseteq F[X]$ is maximal. Thus, the quotient $F[X]/(m_x(X))$ is a field, which implies that $F[x]$ is a field. Therefore,

$$F(x) = F[x].$$

For uniqueness of representation, suppose an element of $F(x)$ has two distinct expansions

$$c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \quad \text{and} \quad d_0 + d_1x + \cdots + d_{n-1}x^{n-1},$$

with $c_i, d_i \in F$. Subtracting these gives a non-zero polynomial $H(X)$ of degree less than n with $H(x) = 0$, contradicting the minimality of $\deg m_x(X)$. Thus, the expansion is unique. $\square$

Corollary 4.1. If $x \in K$ is algebraic over F with minimal polynomial of degree n , then

$$[F(x) : F] = n,$$

and $\{1, x, x^2, \dots, x^{n-1}\}$ is an F -basis of $F(x)$.

Definition 4.5. A field extension K/F is called *algebraic* if every element of K is algebraic over F , that is, for each $x \in K$, there exists a non-zero polynomial $f(X) \in F[X]$ with $f(x) = 0$.

Proposition 4.2. Let K/F be a field extension of finite dimension $n = [K : F]$. Then K is algebraic over F , and for any $x \in K$, there exists a non-zero polynomial in $F[X]$ of degree at most n that vanishes at x .

PROOF. For any $x \in K$, consider the set of $n+1$ vectors $\{1, x, x^2, \dots, x^n\}$ in the n -dimensional vector space K over F . As these vectors are linearly dependent, there exist $a_0, a_1, \dots, a_n \in F$, not all zero, such that

$$a_0 + a_1x + \dots + a_nx^n = 0.$$

Thus, x is a root of the non-zero polynomial $f(X) = a_0 + a_1X + \dots + a_nX^n$. Since x was arbitrary, all elements of K are algebraic over F . $\square$

Definition 4.6. The *degree* of a field extension K/F is defined as the dimension of K as a vector space over F , denoted by $[K : F]$. If $[K : F] < \infty$, the extension is called *finite*. By Proposition 4.2, every finite extension is automatically algebraic.

Corollary 4.2. For any $x \in K$, the element x is algebraic over F if and only if the extension $F(x)/F$ is finite. In this case, the degree of the minimal polynomial of x over F equals $[F(x) : F]$.

PROOF. If x is algebraic over F , then $F(x)$ is generated by $1, x, x^2, \dots, x^{n-1}$, where n is the degree of the minimal polynomial of x . Hence, $[F(x) : F] = n < \infty$.

Conversely, if $[F(x) : F] < \infty$, then Proposition 4.2 implies that x is algebraic over F . If x is transcendental over F , then the set $\{1, x, x^2, \dots\}$ is linearly independent over F , implying $[F(x) : F] = \infty$, which is impossible. $\square$

Theorem 4.2. Let $F \subseteq K \subseteq L$ be fields, and suppose that $[K : F] = n$ and $[L : K] = m$, finite or infinite. Let $\{\omega_1, \omega_2, \dots\}$ be a basis of K over F , and $\{\xi_1, \xi_2, \dots\}$ be a basis of L over K . Then the set of all products

$$\{\omega_i \xi_j \mid i, j\}$$

forms a basis of L over F .

PROOF. Let $x \in L$. Since $\{\xi_j\}$ is a basis of L over K , we can write

$$x = \sum_j b_j \xi_j, \quad b_j \in K, \text{ finitely many } b_j \neq 0.$$

Each $b_j \in K$ can be expanded in terms of the F -basis $\{\omega_i\}$ as

$$b_j = \sum_i a_{ij} \omega_i, \quad a_{ij} \in F.$$

Substituting this into the expression for x gives

$$x = \sum_j \left(\sum_i a_{ij} \omega_i \right) \xi_j = \sum_{i,j} a_{ij} (\omega_i \xi_j),$$

which shows that x is a linear combination of the products $\omega_i \xi_j$. Hence, the set $\{\omega_i \xi_j\}$ spans L over F .

Suppose there is a relation

$$\sum_{i,j} c_{ij} (\omega_i \xi_j) = 0, \quad c_{ij} \in F.$$

By grouping terms with the same ξ_j , we obtain

$$\sum_j \left(\sum_i c_{ij} \omega_i \right) \xi_j = 0.$$

Since $\{\xi_j\}$ is linearly independent over K , we have

$$\sum_i c_{ij} \omega_i = 0 \quad \text{for each } j.$$

Then linear independence of $\{\omega_i\}$ over F implies $c_{ij} = 0$ for all i, j . Thus, the set $\{\omega_i \xi_j\}$ is linearly independent over F , completing the proof. $\square$

Corollary 4.3. Let $F \subseteq K \subseteq L$ be fields. Then

$$[L : F] = [L : K] [K : F].$$

Theorem 4.3. Let K/F be a field extension, and let $x_1, \dots, x_n \in K$ be algebraic over F . Then the field extension

$$F(x_1, \dots, x_n)/F$$

is finite and algebraic.

PROOF. We prove this by induction on n . For $n = 1$, we have $F(x_1)/F$ is finite since x_1 is algebraic over F . Assume $F(x_1, \dots, x_{i-1})/F$ is finite. Since x_i is algebraic over F , it is also algebraic over $F(x_1, \dots, x_{i-1})$. Hence

$$[F(x_1, \dots, x_i) : F(x_1, \dots, x_{i-1})] < \infty.$$

Applying the tower law repeatedly, we conclude that

$$[F(x_1, \dots, x_n) : F] < \infty.$$

Thus, $F(x_1, \dots, x_n)$ is a finite algebraic extension of F . $\square$

Remark 4.3. A finite algebraic extension of F that can be expressed as $F(x)$ for some $x \in K$ is called a *simple algebraic extension*.

Corollary 4.4. Let K/F be a field extension. The set of all elements of K that are algebraic over F forms a subfield of K .

PROOF. Let $x, y \in K$ be algebraic over F . Then by Theorem 4.3, the field $F(x, y)$ is a finite algebraic extension of F . Finite algebraic extensions are closed under addition, subtraction, multiplication, and taking inverses of non-zero elements. Therefore, $x \pm y$, xy , and x^{-1} (if $x \neq 0$) are algebraic over F . Hence, the set of algebraic elements of K forms a subfield. $\square$

Remark 4.4. Consider the field extension $\mathbb{C}/\mathbb{Q}$. The set of all elements in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$ forms a subfield, commonly referred to as the *field of algebraic numbers*. Any finite algebraic extension of $\mathbb{Q}$ contained in $\mathbb{C}$ is known as a *number field* or *algebraic number field*.

Although one can also define a number field as a simple algebraic extension of $\mathbb{Q}$, these definitions are equivalent due to the *Primitive Element Theorem*, which ensures that every finite algebraic extension of $\mathbb{Q}$ can be generated by a single element.

Problem 4.1. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field, where $D < 0$, and let $\mathcal{O}_K$ be its quadratic integer ring with field norm N . Suppose that $D = -1, -2, -3, -7$, or -11 . Prove that $\mathcal{O}_K$ is a Euclidean domain with respect to the norm N .

Solution 4.1. Let $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$. We now prove that there exist $q, r \in \mathcal{O}_K$ such that

$$\alpha = \beta q + r \quad \text{with} \quad N(r) < N(\beta).$$

Since $\beta \neq 0$, the quotient α/β lies in the field $K = \mathbb{Q}(\sqrt{D})$. Write

$$\frac{\alpha}{\beta} = x + y\sqrt{D},$$

where $x, y \in \mathbb{R}$.

Case 1: $D = -1$ or $D = -2$.

In these cases we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Choose integers $m, n \in \mathbb{Z}$ such that

$$|x - m| \leq \frac{1}{2} \quad \text{and} \quad |y - n| \leq \frac{1}{2}.$$

Let

$$q = m + n\sqrt{D} \in \mathcal{O}_K \quad \text{and} \quad r = \alpha - \beta q.$$

Then

$$\frac{r}{\beta} = (x - m) + (y - n)\sqrt{D}.$$

Taking norms gives

$$N\left(\frac{r}{\beta}\right) = (x - m)^2 + |D|(y - n)^2 \leq \frac{1}{4} + \frac{|D|}{4}.$$

For $D = -1$ or -2 , this quantity is strictly less than 1. Hence

$$N(r) < N(\beta),$$

and $\mathcal{O}_K$ is Euclidean in these cases.

Case 2: $D = -3, -7$, or -11 .

In these cases the ring of integers is

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right].$$

It is known that every element of K differs from an element of $\mathcal{O}_K$ by an element γ satisfying

$$N(\gamma) < 1.$$

Therefore, there exists $q \in \mathcal{O}_K$ such that

$$N\left(\frac{\alpha}{\beta} - q\right) < 1.$$

Let

$$r = \alpha - \beta q.$$

Then

$$N\left(\frac{r}{\beta}\right) < 1,$$

and therefore

$$N(r) < N(\beta).$$

In all cases, given $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$, we can write $\alpha = \beta q + r$ with $N(r) < N(\beta)$. Hence, $\mathcal{O}_K$ is a Euclidean domain with respect to the norm N .

5. Splitting Fields and Algebraically Closed Fields

Let F be a field. If $f(x)$ is any polynomial in $F[x]$, then we know that there exists a field K containing F as a subfield such that $f(x)$ has a root a in K . Equivalently, this means that $f(x)$ has a linear factor $(x - a)$ in $K[x]$.

Definition 5.1. Let F be a field and $f(x) \in F[x]$. An extension field K of F is called a *splitting field* of $f(x)$ over F if

- (1) $f(x)$ factors completely into linear factors (splits completely) in $K[x]$, that is,

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

for some $c \in F$ and $a_1, a_2, \dots, a_n \in K$, and

- (2) $f(x)$ does not split completely over any proper subfield of K containing F .

Theorem 5.1. For any field F and any polynomial $f(x) \in F[x]$, there exists an extension field K of F which is a splitting field for $f(x)$.

PROOF. We first show, by induction on the degree n of $f(x)$, that there exists an extension field E of F over which $f(x)$ splits completely into linear factors.

If $n = 1$, we may take $E = F$. We now assume that $n > 1$, and suppose that all irreducible factors of $f(x)$ over F have degree 1. Then $f(x)$ already splits completely in $F[x]$, and we may again take $E = F$.

Otherwise, let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$ of degree at least 2. Then there exists an extension field E_1 of F containing a root a of $p(x)$. Over E_1 , the polynomial $f(x)$ has a linear factor $(x - a)$, therefore we can write

$$f(x) = (x - a)f_1(x)$$

with $f_1(x) \in E_1[x]$ of degree $n - 1$.

By the induction hypothesis, there exists an extension field E of E_1 that contains all the roots of $f_1(x)$. Since $a \in E_1 \subseteq E$, it follows that E contains all the roots of $f(x)$. Hence, $f(x)$ splits completely in $E[x]$.

Finally, let K be the intersection of all subfields of E that contain F and all the roots of $f(x)$. Then K is a field containing F , and $f(x)$ splits completely in $K[x]$. Moreover, no proper subfield of K containing F has this property. Thus, K is a splitting field for $f(x)$ over F . $\square$

Definition 5.2. Let F be a field. An *algebraic closure* of F is a field $\overline{F}$ such that

- (1) $\overline{F}$ is algebraic over F , and
- (2) every polynomial $f(x) \in F[x]$ splits completely into linear factors over $\overline{F}$.

Definition 5.3. A field K is *algebraically closed* if every non-constant polynomial in $K[x]$ has a root in K .

If K is algebraically closed, then every polynomial in $K[x]$ splits completely, since once a root $a \in K$ is found, the remaining factor is again a polynomial over K , which must also have a root, and so on. Conversely, if every polynomial in $K[x]$ splits completely, then each has a root in K . Hence, a field is algebraically closed if and only if it is its own algebraic closure.

Note 5.1. If $\overline{F}$ is an algebraic closure of F , then $\overline{\overline{F}} = \overline{F}$.

Proposition 5.1. Let $\overline{F}$ be an algebraic closure of a field F . Then $\overline{F}$ is algebraically closed.

PROOF. By definition, $\overline{F}$ is an algebraic extension of F and every polynomial in $F[x]$ splits into linear factors over $\overline{F}$. Let $f(x) \in \overline{F}[x]$ be a non-constant polynomial. Since $\overline{F}$ is algebraic over F , each coefficient of $f(x)$ is algebraic over F . Hence, there exists a finite extension E of F such that

$$f(x) \in E[x].$$

Every element of E is algebraic over F . Since $\overline{F}$ is an algebraic closure of F , it contains all elements algebraic over F , and therefore it contains an algebraic closure of E .

Thus, the polynomial $f(x) \in E[x]$ splits completely into linear factors over $\overline{F}$. In particular, $f(x)$ has a root in $\overline{F}$.

Hence, every non-constant polynomial in $\overline{F}[x]$ has a root in $\overline{F}$. Therefore, $\overline{F}$ is algebraically closed. $\square$

Proposition 5.2. Let $f(x) \in F[x]$ be a polynomial of degree n . Then any splitting field K of $f(x)$ over F satisfies

$$[K : F] \leq n!.$$

PROOF. Set $\deg f = n$. If $n \leq 1$, then f splits over F and $[K : F] = 1 \leq n!$.

Choose a root a_1 of f in an algebraic closure $\overline{F}$ of F and put $F_1 = F(a_1)$. Then

$$[F_1 : F] = \deg(\min_{\overline{F}}(a_1)) \leq n.$$

We can write $f(x) = (x - a_1)g_1(x)$ with $g_1 \in F_1[x]$ and $\deg g_1 = n - 1$.

If g_1 already splits over F_1 , then any splitting field K is contained in F_1 , and hence $[K : F] \leq [F_1 : F] \leq n \leq n!$. Otherwise, choose a root a_2 of g_1 and set $F_2 = F_1(a_2)$. Then

$$[F_2 : F_1] = \deg(\min_{F_1}(a_2)) \leq \deg g_1 = n - 1$$

and thus $[F_2 : F] \leq n(n - 1)$.

Continuing, at step i ($1 \leq i \leq n$) if $f(x) = (x - a_1) \cdots (x - a_{i-1})g_{i-1}(x)$ over F_{i-1} with $\deg g_{i-1} = n - (i - 1)$, choose a root a_i of g_{i-1} and set $F_i = F_{i-1}(a_i)$. Then

$$[F_i : F_{i-1}] \leq n - (i - 1).$$

After at most n steps we reach a field $E = F_m$ in which f splits completely.

By multiplicativity of degrees in a tower,

$$[K : F] \leq [E : F] = \prod_{i=1}^m [F_i : F_{i-1}] \leq n \cdot (n - 1) \cdots 2 \cdot 1 = n!.$$

This proves the claim. □

Example 5.1 (Splitting Field of $x^n - 1$ and Cyclotomic Fields). Consider the polynomial $x^n - 1$ over the field $\mathbb{Q}$. Its roots are called the n th roots of unity.

Every non-zero complex number $a + bi \in \mathbb{C}$ can be expressed uniquely in polar form as

$$a + bi = r(\cos \theta + i \sin \theta) = re^{i\theta}, \quad r > 0, 0 \leq \theta < 2\pi.$$

Using this representation, the equation $x^n = 1$ has exactly n distinct solutions in $\mathbb{C}$ given by

$$\zeta_n^k = e^{2\pi i k/n} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right), \quad k = 0, 1, \dots, n - 1.$$

These points are the vertices of a regular n -gon inscribed in the unit circle of the complex plane, equally spaced at angular distance $2\pi/n$. Each satisfies $(\zeta_n^k)^n = 1$, so they are precisely the n th roots of unity.

It follows that $\mathbb{C}$ contains a splitting field for $x^n - 1$. The smallest subfield of $\mathbb{C}$ containing all n th roots of unity is

$$\mathbb{Q}(\zeta_n),$$

where $\zeta_n = e^{2\pi i/n}$ is a primitive n th root of unity. Thus, $\mathbb{Q}(\zeta_n)$ is the *splitting field of $x^n - 1$ over $\mathbb{Q}$* , and is called the *n th cyclotomic field*.

In general, if $K/\mathbb{Q}$ is any splitting field for $x^n - 1$, then the set of n th roots of unity in K forms a group under multiplication. Since the product of two n th roots of unity is again an n th root of unity, this group is closed under multiplication and is cyclic of order n .

Definition 5.4. A generator of the cyclic group of all n th roots of unity is called a *primitive n th root of unity*.

Note 5.2. If ζ_n denotes one primitive n th root of unity, then the other primitive n th roots of unity are precisely the elements

$$\zeta_n^a, \quad \text{where } 1 \leq a < n \text{ and } \gcd(a, n) = 1.$$

These are exactly the other generators of the cyclic group of order n . Hence, there are precisely $\varphi(n)$ primitive n th roots of unity, where $\varphi(n)$ denotes Euler's totient function.

5.1. Existence of Algebraically Closed Extensions. Given a field F , we have already seen how to construct finite extensions of F that contain all the roots of a particular polynomial $f(x) \in F[x]$. Intuitively, an *algebraic closure* of F should be a field obtained by adjoining the roots of *all* polynomials over F . However, combining infinitely many such extensions raises a technical difficulty; these splitting fields are not initially subfields of a common field, so we cannot simply “take their union.” To overcome this, we use an elegant construction due to Artin, which simultaneously adjoins formal roots for every polynomial in a systematic way. The argument depends on Zorn’s Lemma.

We first show that every field can be embedded in an algebraically closed field.

Theorem 5.2. For any field F , there exists an algebraically closed field K containing F .

PROOF. For each non-constant monic polynomial $f(x) \in F[x]$, introduce an indeterminate X_f , and consider the polynomial ring

$$R = F[\{X_f \mid f(x) \in F[x], \deg f \geq 1\}],$$

that is, the ring generated over F by all variables X_f indexed by the non-constant monic polynomials in $F[x]$.

Let I be the ideal of R generated by the polynomials $f(X_f)$,

$$I = \langle f(X_f) \mid f(x) \in F[x], \deg f \geq 1 \rangle.$$

We prove that I is a proper ideal. If $1 \in I$, then there exist finitely many $f_1, \dots, f_n \in F[x]$ and $g_1, \dots, g_n \in R$ such that

$$g_1 f_1(X_{f_1}) + g_2 f_2(X_{f_2}) + \dots + g_n f_n(X_{f_n}) = 1.$$

Let $X_{f_1}, \dots, X_{f_n}$ be all the variables appearing in the g_i . Choose a finite extension F' of F that contains a root a_i of each $f_i(x)$ for $i = 1, \dots, n$. Substitute $X_{f_i} = a_i$ for these variables and set the remaining $X_{f_j} = 0$. The left-hand side then evaluates to 0, contradicting the equality $1 = 0$ in F' . Hence, I is proper.

By Zorn’s Lemma, I is contained in a maximal ideal M of R . The quotient

$$K_1 = R/M$$

is then a field containing an isomorphic copy of F . For each $f(x) \in F[x]$, the image of X_f in K_1 is a root of $f(x)$, since $f(X_f) \in I \subseteq M$. Thus, every polynomial over F has a root in K_1 .

Now repeat the construction with K_1 in place of F , obtaining a field K_2 containing K_1 such that every polynomial over K_1 has a root in K_2 . Continuing inductively, we obtain an ascending chain of fields

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots,$$

where each K_{j+1} contains a root of every polynomial with coefficients in K_j .

Let

$$K = \bigcup_{j \geq 0} K_j.$$

Then K is a field containing F . If $h(x) \in K[x]$, its coefficients lie in some K_N for sufficiently large N . By construction, $h(x)$ has a root in K_{N+1} , hence in K . Therefore, every polynomial over K has a root in K , and K is algebraically closed. $\square$

5.2. Construction of the Algebraic Closure. Starting from the existence of an algebraically closed field containing a given field F , we can now construct an algebraic closure of F .

Proposition 5.3. Let K be an algebraically closed field, and let F be a subfield of K . Then the set

$$\overline{F} = \{a \in K \mid a \text{ is algebraic over } F\}$$

is an algebraic closure of F . Moreover, the algebraic closure of a field is unique up to isomorphism.

PROOF. By definition, every element of $\overline{F}$ is algebraic over F and so $\overline{F}$ is an algebraic extension of F . Let $f(x) \in F[x]$. Since K is algebraically closed, $f(x)$ factors completely in $K[x]$ as

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n), \quad a_i \in K.$$

As each a_i is a root of $f(x)$ and hence algebraic over F , $a_i \in \overline{F}$. Thus, $f(x)$ splits completely in $\overline{F}[x]$, showing that $\overline{F}$ is algebraically closed and algebraic over F . Hence, $\overline{F}$ is an algebraic closure of F .

The uniqueness (up to F -isomorphism) of the algebraic closure follows from the uniqueness of splitting fields and can be proved using Zorn's Lemma. $\square$

The most familiar example of an algebraically closed field is the field of complex numbers. The statement that $\mathbb{C}$ is algebraically closed is one of the central results connecting algebra and analysis. It guarantees that every non-constant polynomial with complex coefficients has at least one complex root, and therefore factors completely into linear terms in $\mathbb{C}[x]$. This result is known as the *Fundamental Theorem of Algebra*.

Theorem 5.3 (Fundamental Theorem of Algebra). The field of complex numbers $\mathbb{C}$ is algebraically closed.

Corollary 5.1. The field $\mathbb{C}$ contains an algebraic closure of each of its subfields. In particular,

$$\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}\}$$

is an algebraic closure of $\mathbb{Q}$.

Problem 5.1. Let n be a positive integer and let p be a prime such that $p \nmid n$. If

$$p \mid \Phi_n(a)$$

for some integer a , then prove that

$$p \equiv 1 \pmod{n}.$$

Solution 5.1. Let $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ be the canonical epimorphism. Since $p \mid \Phi_n(a)$, we have

$$\Phi_n(a) \equiv 0 \pmod{p}.$$

Recall that

$$t^n - 1 = \prod_{d \mid n} \Phi_d(t)$$

is the factorization of $t^n - 1$ into cyclotomic polynomials in $\mathbb{Z}[t]$. Reducing modulo p and evaluating at $t = a$, we obtain

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

Let m be the order of a in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $m \mid n$.

Suppose that $m < n$. Then

$$t^n - 1 = (t^m - 1) \prod_{\substack{d \mid n \\ d \nmid m}} \Phi_d(t).$$

Since $a^m \equiv 1 \pmod{p}$ and $\Phi_n(a) \equiv 0 \pmod{p}$, it follows that a is a common root of $t^m - 1$ and $\Phi_n(t)$ in $\mathbb{Z}/p\mathbb{Z}$.

Thus, a is a multiple root of $t^n - 1$ in $\mathbb{Z}/p\mathbb{Z}$. Since $p \nmid n$, the derivative

$$(t^n - 1)' = nt^{n-1}$$

is not identically zero modulo p . This is a contradiction.

Hence, $m = n$, and therefore $n \mid (p - 1)$. It follows that $p \equiv 1 \pmod{n}$.

Problem 5.2. Let $n > 1$ be an integer. Show that there exist infinitely many prime numbers p such that

$$p \equiv 1 \pmod{n}.$$

Solution 5.2. Suppose, for contradiction, that there are only finitely many primes $p_1, \dots, p_r$ such that

$$p_i \equiv 1 \pmod{n}.$$

Since the n th cyclotomic polynomial $\Phi_n(t)$ is monic, there exists an integer $N > 1$ such that

$$\Phi_n(M) > 1$$

for all integers $M > N$.

Set

$$M = p_1 p_2 \cdots p_r n^N,$$

with the convention that $p_1 \cdots p_r = 1$ if $r = 0$. Then $M > N$, and hence $\Phi_n(M) > 1$. Let p be a prime divisor of $\Phi_n(M)$.

Since the constant term of each cyclotomic polynomial $\Phi_d(t)$ is ± 1 , we have

$$\Phi_n(M) \equiv \pm 1 \pmod{p_i} \quad \text{for } 1 \leq i \leq r.$$

Thus, $p \neq p_1, \dots, p_r$.

Moreover, $\gcd(M, n) = 1$ and so $p \nmid n$. By Problem 5.1, it follows that

$$p \equiv 1 \pmod{n}.$$

This contradicts the assumption that $p_1, \dots, p_r$ are all primes congruent to 1 modulo n . Therefore, there exist infinitely many primes p such that $p \equiv 1 \pmod{n}$.

6. Separable Extensions

When studying polynomials over the real numbers, one observes that a polynomial having a repeated (or multiple) root exhibits distinctive behaviour. Such a root is also a root of the polynomial's derivative, causing the graph to “touch” or “flatten” at that point rather than crossing the axis. For irreducible polynomials over fields of characteristic 0, multiple roots cannot occur; however, in fields of positive characteristic this phenomenon can arise even for irreducible polynomials.

In this section, we formalize these ideas and introduce precise definitions that will be useful in later results.

Definition 6.1. Let K/F be an extension of fields, and let $f(t) \in F[t]$ be a non-constant polynomial with a root $\alpha \in K$.

- (1) The element α is called a *multiple root* of f in K if there exists an integer $r \geq 2$ and a polynomial $g(t) \in K[t]$ such that

$$f(t) = (t - \alpha)^r g(t) \quad \text{and} \quad g(\alpha) \neq 0.$$

The integer r is called the *multiplicity* of α .

- (2) If α is a root of f but not a multiple root, then we say that α is a *simple root*.

Definition 6.2. If

$$f(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \in F[t],$$

then the *derivative* of f is defined as

$$f'(t) = a_1 + 2a_2 t + 3a_3 t^2 + \cdots + na_n t^{n-1} = \sum_{i=1}^n i a_i t^{i-1}.$$

The derivative allows us to detect multiple roots algebraically. If α is a multiple root of f , then both $f(\alpha) = 0$ and $f'(\alpha) = 0$. In characteristic zero, this is the only way multiple roots can occur. In a positive characteristic, additional subtleties arise, which we will explore later.

Next, we recall some basic properties of the derivative operator on polynomials.

Proposition 6.1. Let $f, g \in F[t]$ and $a \in F$. Then the following hold

- (a) $(f + g)' = f' + g'$,

- (b) $(af)' = af'$,
- (c) $(fg)' = f'g + fg'$.

As noted earlier, if a polynomial has a multiple root, that root is also a root of its derivative. The following lemma formalizes this observation and shows that the notion of a multiple root is independent of the choice of field extension.

Lemma 6.1. Let K/F be an extension of fields, and let $f(t) \in F[t]$ be a non-constant polynomial with a root $\alpha \in K$. Then α is a simple root of f if and only if α is not a root of f' .

PROOF. We may write

$$f(t) = (t - \alpha)^r g(t)$$

for some $g(t) \in K[t]$ with $g(\alpha) \neq 0$ and integer $r \geq 1$. Differentiating gives

$$f'(t) = r(t - \alpha)^{r-1}g(t) + (t - \alpha)^r g'(t) = (t - \alpha)^{r-1}(rg(t) + (t - \alpha)g'(t)).$$

Thus, $t - \alpha$ divides $f'(t)$ in $K[t]$ if and only if either $r \geq 2$ or $r = 0$ in K (that is, $\text{char } F \mid r$). If $r = 1$, then $t - \alpha \nmid f'(t)$ and so α is a simple root of f . Hence, α is a multiple root of f if and only if α is a root of f' , as claimed. $\square$

Corollary 6.1. Let $f(t) \in F[t]$ be a non-constant polynomial. Then f has a multiple root in some extension field of F if and only if the ideal (f, f') in $F[t]$ is not the unit ideal.

PROOF. Suppose f has a multiple root α in an extension field K of F . Then the minimal polynomial $m_F(\alpha)$ over F divides both f and f' in $F[t]$. Hence, $(f, f') \subset (m_F(x)) \subsetneq F[t]$ and so (f, f') is not the unit ideal.

Conversely, assume that (f, f') is not the unit ideal of $F[t]$. Since $F[t]$ is a principal ideal domain, we have $(f, f') = (g)$ for some non-constant $g \in F[t]$. Let K/F be an extension field in which g has a root α . This shows that $f(\alpha) = f'(\alpha) = 0$, and hence α is a multiple root of f in K . $\square$

Definition 6.3. Let F be a field.

- (a) An irreducible polynomial $f(t) \in F[t]$ is called *separable over F* if it has no multiple roots in any field extension of F . Equivalently, f is separable if $\gcd(f, f') = 1$ in $F[t]$.
- (b) A non-constant polynomial $f(t) \in F[t]$ is called *separable over F* if each of its irreducible factors in $F[t]$ is separable. If f is not separable over F , then it is called *inseparable*.
- (c) Let K/F be a field extension and let $\alpha \in K$. We say that α is *separable over F* if it is a root of a separable polynomial in $F[t]$.
- (d) The field extension K/F is called *separable* if every element of K is separable over F .

Remark 6.1. In many textbooks, a non-constant polynomial $f(t) \in F[t]$ is called *separable* if it has no multiple roots in any extension field of F . This is equivalent to the earlier definition, but our formulation stating that all irreducible factors of f are separable is often more convenient for theoretical developments that follow.

Remark 6.2. Let K/F be a field extension, and let $f, g \in F[t]$ be non-constant polynomials. The following statements summarize some important properties of separability.

- (1) Every element of F is separable over F .
- (2) An element $\alpha \in K$ is separable over F if and only if α is algebraic over F and its minimal polynomial $m_F(\alpha)$ is separable over F . In particular, if K/F is separable, then it is algebraic.
- (3) If $\text{char } F = 0$ and K/F is algebraic, then K/F is separable. A field F in which every element algebraic over F is separable is called a *perfect field*. Hence, all fields of characteristic 0 are perfect. Moreover, every finite field is perfect, though fields of positive characteristic that are not perfect also exist.
- (4) A polynomial $f(t) \in F[t]$ is separable over F if and only if every divisor of f in $F[t]$ is separable over F .
- (5) If $f, g \in F[t]$ are separable, then their product fg is separable over F .

(6) If $L/K/F$ are field extensions and L/F is separable, then both L/K and K/F are separable.

Theorem 6.1. Let $K/E/F$ be a tower of field extensions. Then K/F is separable if and only if both K/E and E/F are separable.

PROOF. Assume that K/F is separable. Let $\alpha \in K$. Then α is separable over F . Since E is an intermediate field, the minimal polynomial of α over E divides the minimal polynomial of α over F . Hence, the minimal polynomial of α over E has distinct roots. Therefore, α is separable over E , and K/E is separable.

Now let $\beta \in E$. Since $\beta \in K$ and K/F is separable, β is separable over F . Thus, E/F is separable.

Conversely, suppose that both K/E and E/F are separable. Let $\alpha \in K$. Then α is separable over E . Hence, its minimal polynomial over E has distinct roots.

Since E/F is separable, every element of E is separable over F . Therefore, the coefficients of the minimal polynomial of α over E are separable over F . It follows that α is separable over F .

Thus, every element of K is separable over F , and hence K/F is separable. $\square$

Problem 6.1. Let F be a field of positive characteristic p . Prove the following statements.

- (a) The map $F \rightarrow F$ defined by $x \mapsto x^p$ is a monomorphism. Denote its image by F^p .
- (b) If K/F is an algebraic extension and $\alpha \in K$ is separable over $F(\alpha^p)$, then $\alpha \in F(\alpha^p)$.

Solution 6.1. (a) Define $\varphi : F \rightarrow F$ by $\varphi(x) = x^p$. Since $\text{char}(F) = p$, the binomial theorem gives

$$(x + y)^p = x^p + y^p \quad \text{for all } x, y \in F,$$

and hence $(xy)^p = x^p y^p$. Thus, φ is a ring homomorphism.

If $\varphi(x) = 0$, then $x^p = 0$, which implies $x = 0$ as F is a field. Hence, φ is injective, and therefore a monomorphism. Its image is

$$F^p := \{x^p \mid x \in F\}.$$

(b) Since K/F is algebraic, the element α is algebraic over $F(\alpha^p)$. Consider the polynomial

$$f(t) = t^p - \alpha^p \in F(\alpha^p)[t].$$

Then $f(\alpha) = 0$.

As $\text{char}(F) = p$, it follows that the formal derivative of $f(t)$ is

$$f'(t) = pt^{p-1} = 0.$$

Hence, every root of $f(t)$ is inseparable. If α is separable over $F(\alpha^p)$, then its minimal polynomial over $F(\alpha^p)$ must have distinct roots. This is possible only if the minimal polynomial has degree 1. Therefore,

$$\alpha \in F(\alpha^p).$$

Problem 6.2. Let F be a finite field of characteristic p . Show that F is perfect, that is, every algebraic extension of F is separable.

Solution 6.2. As $\text{char}(F) = p$, the Frobenius map

$$\varphi : F \rightarrow F, \quad x \mapsto x^p$$

is injective by part (a). Since F is finite, it follows that φ is also surjective. Hence,

$$F = F^p.$$

Let $f(x) \in F[x]$ be an irreducible polynomial. We now prove that $f(x)$ is separable. Suppose, to the contrary, that $f(x)$ is inseparable. Then $\text{char}(F) = p$ and

$$f(x) = g(x^p)$$

for some polynomial $g(x) \in F[x]$.

Write

$$g(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_i \in F.$$

Since $F = F^p$, for each a_i there exists $b_i \in F$ such that $a_i = b_i^p$. Thus,

$$f(x) = \sum b_i^p x^{pi} = \left(\sum b_i x^i \right)^p.$$

Hence, $f(x)$ is a p -th power in $F[x]$, which contradicts the assumption that $f(x)$ is irreducible. Therefore, $f(x)$ must be separable.

Since every irreducible polynomial over F is separable, we conclude that every algebraic extension of F is separable. Thus, F is perfect.

Problem 6.3. Let K/F be a field extension. Then prove the following statements.

- (a) If $\alpha \in K$ is separable over F , then $F(\alpha)/F$ is separable.
- (b) If $\alpha_1, \dots, \alpha_n \in K$ are separable over F , then $F(\alpha_1, \dots, \alpha_n)/F$ is separable.
- (c) Let

$$F_{\text{sep}} = \{\alpha \in K \mid \alpha \text{ is separable over } F\}.$$

Show that F_{sep} is a field.

Solution 6.3. (a) Let $\alpha \in K$ be separable over F , and set $E = F(\alpha)$. Let L be an algebraic closure of F . Since α is separable over F , it has distinct conjugates

$$\alpha = \alpha_1, \alpha_2, \dots, \alpha_n \in L.$$

Each F -embedding $\sigma_i : E \hookrightarrow L$ is determined by

$$\sigma_i(\alpha) = \alpha_i.$$

Thus, E has exactly $[E : F]$ distinct F -embeddings into L .

Let $\beta \in E$. Then β has distinct images under these embeddings. Hence, the minimal polynomial of β over F has distinct roots. Therefore, β is separable over F . Thus, every element of $F(\alpha)$ is separable over F , and $F(\alpha)/F$ is separable.

(b) Suppose $\alpha_1, \dots, \alpha_n \in K$ are separable over F . We proceed by induction on n .

For $n = 1$, the result follows from part (a).

Assume the statement holds for $n - 1$ elements and set

$$E = F(\alpha_1, \dots, \alpha_{n-1}).$$

By the induction hypothesis, E/F is separable. Since α_n is separable over F , it is also separable over E . By part (a), the extension $E(\alpha_n)/E$ is separable. Hence, $F(\alpha_1, \dots, \alpha_n)/F$ is separable as a tower of separable extensions.

(c) Let $\alpha, \beta \in F_{\text{sep}}$. Then α and β are separable over F . By part (b), the field $F(\alpha, \beta)/F$ is separable.

Since $\alpha + \beta$, $\alpha\beta$, and α^{-1} (if $\alpha \neq 0$) belong to $F(\alpha, \beta)$, and every element of this field is separable over F , it follows that

$$\alpha + \beta, \alpha\beta, \alpha^{-1} \in F_{\text{sep}}.$$

Clearly $0, 1 \in F_{\text{sep}}$. Thus, F_{sep} is closed under addition, multiplication, and inversion. Therefore, F_{sep} is a field.

Problem 6.4. Let K/F be a field extension and let $\alpha \in K$. We say that α is *purely inseparable* over F if its minimal polynomial $m_F(\alpha)$ has only one root in a splitting field of α . The extension K/F is called purely inseparable if every element of K is purely inseparable over F . Show that $\alpha \in K$ is both purely inseparable and separable over F if and only if $\alpha \in F$.

Solution 6.4. Suppose first that $\alpha \in F$. Then $m_F(\alpha) = x - \alpha$, which has degree 1. Hence, $m_F(\alpha)$ has exactly one root and is separable. Therefore, α is both purely inseparable and separable over F .

Conversely, suppose that $\alpha \in K$ is both purely inseparable and separable over F . Let $m_F(\alpha)$ be the minimal polynomial of α over F . Since α is purely inseparable over F , the polynomial $m_F(\alpha)$ has exactly one root in a splitting field. Since α is separable over F , the polynomial $m_F(\alpha)$ has distinct roots.

These two conditions imply that $m_F(\alpha)$ has exactly one distinct root. Hence, $\deg m_F(\alpha) = 1$. Therefore, $m_F(\alpha) = x - \alpha$, which implies $\alpha \in F$.

Problem 6.5. Let K/F be a field extension with $\text{char}(F) = p > 0$. Show that if $\alpha \in K$ is algebraic over F , then there exists a nonnegative integer n such that α^{p^n} is separable over F .

Solution 6.5. Let $\alpha \in K$ be algebraic over F , and let $m_F(\alpha) \in F[x]$ be its minimal polynomial.

Since $\text{char}(F) = p > 0$, the polynomial $m_F(\alpha)$ can be written in the form

$$m_F(\alpha)(x) = f(x^{p^n})$$

for some nonnegative integer n and some polynomial $f(x) \in F[x]$ whose formal derivative $f'(x)$ is not identically zero.

Let $\beta = \alpha^{p^n}$. Then $f(\beta) = 0$ and hence β is algebraic over F . Moreover, since $f'(x) \neq 0$, the polynomial $f(x)$ is separable. Thus, the minimal polynomial of β over F is separable.

Therefore, there exists a nonnegative integer n such that α^{p^n} is separable over F .

7. Galois Theory

In the previous chapter, we developed the basic ideas of field theory, studying fields and their extensions. In this chapter, we connect field theory with group theory by examining the structure of field automorphisms. Our main objective is to establish a correspondence between the intermediate fields of a finite extension K/F , where K is the splitting field of a separable polynomial in $F[t]$, and the subgroups of the Galois group

$$\text{Gal}(K/F) = \text{Aut}_F(K).$$

This correspondence, known as the *Fundamental Theorem of Galois Theory*, reveals a deep relationship between algebraic extensions and group symmetries. Moreover, we derive several fundamental results that unify the study of polynomials, field extensions, and automorphism groups.

Definition 7.1. Let F be a field and let G be a (multiplicative) group. A group homomorphism

$$\sigma : G \longrightarrow F^\times$$

is called a (*linear*) *character* of G over F (recall that $F^\times = \text{GL}_1(F)$, the group of invertible elements of F).

A collection of distinct characters $\sigma_1, \dots, \sigma_n : G \rightarrow F^\times$ is said to be *dependent* if there exist scalars $a_1, \dots, a_n \in F$, not all zero, such that

$$\sum_{i=1}^n a_i \sigma_i(g) = 0 \quad \text{for all } g \in G.$$

Equivalently, the function $\sum_{i=1}^n a_i \sigma_i : G \rightarrow F$ is the zero map. If no such non-trivial relation exists, the characters are said to be *independent*.

Remark 7.1. (1) If $\sigma : E \rightarrow F$ is a field homomorphism, then its restriction to $E^\times$ defines a character

$$\sigma : E^\times \rightarrow F^\times,$$

since a ring homomorphism sends units to units.

(2) The set of all characters of G over F ,

$$\{\sigma \mid \sigma : G \rightarrow F^\times \text{ is a character}\},$$

is not a group under addition, but it forms a group under pointwise multiplication of functions, defined by

$$(\sigma\tau)(g) := \sigma(g)\tau(g), \quad \text{for all } g \in G,$$

with the identity element given by the trivial character

$$1 : G \rightarrow F^\times, \quad g \mapsto 1_F.$$

Lemma 7.1 (Dedekind's Lemma). Let $\sigma_1, \dots, \sigma_n : G \rightarrow F^\times$ be distinct characters. Then the characters $\sigma_1, \dots, \sigma_n$ are independent over F .

PROOF. We proceed by induction on n . For $n = 1$, let $a_1\sigma_1(g) = 0$ for all $g \in G$. Then $a_1 = 0$ since $\sigma_1(g) \neq 0$ for all g . Hence, $\{\sigma_1\}$ is independent.

Assume the result holds for all sets of fewer than n characters, and suppose

$$\sum_{i=1}^n a_i \sigma_i(g) = 0 \quad \text{for all } g \in G,$$

for some $a_1, \dots, a_n \in F$, not all zero. By the inductive hypothesis, any proper subset of $\{\sigma_1, \dots, \sigma_n\}$ is independent, so each $a_i \neq 0$. Multiplying through by a_n^{-1} , we may assume $a_n = 1$. Then

$$\sum_{i=1}^{n-1} a_i \sigma_i(g) + \sigma_n(g) = 0 \quad \text{for all } g \in G.$$

Since $\sigma_1 \neq \sigma_n$, there exists $x \in G$ such that $\sigma_1(x) \neq \sigma_n(x)$. For all $g \in G$, we have

$$0 = \sum_{i=1}^{n-1} a_i \sigma_i(xg) + \sigma_n(xg) = \sum_{i=1}^{n-1} a_i \sigma_i(x) \sigma_i(g) + \sigma_n(x) \sigma_n(g).$$

Dividing by $\sigma_n(x) \neq 0$, we obtain

$$0 = \sum_{i=1}^{n-1} (\sigma_n(x)^{-1} a_i \sigma_i(x)) \sigma_i(g) + \sigma_n(g).$$

Subtracting this from the previous equation gives

$$0 = \sum_{i=1}^{n-1} a_i (1 - \sigma_n(x)^{-1} \sigma_i(x)) \sigma_i(g) \quad \text{for all } g \in G.$$

By the inductive hypothesis, the coefficients must all vanish

$$a_i (1 - \sigma_n(x)^{-1} \sigma_i(x)) = 0 \quad \text{for all } i = 1, \dots, n-1.$$

Since $a_i \neq 0$, we have $\sigma_i(x) = \sigma_n(x)$ for all i , contradicting the choice of x . Hence, all $a_i = 0$, and the characters are independent. $\square$

Corollary 7.1. Let $\sigma_1, \dots, \sigma_n : F \rightarrow K$ be distinct field homomorphisms. Then the corresponding characters

$$\sigma_1, \dots, \sigma_n : F^\times \rightarrow K^\times$$

are linearly independent.

Definition 7.2. Let F and K be fields, and let

$$S \subseteq \{\sigma : F \rightarrow K \mid \sigma \text{ is a field homomorphism}\}$$

be a non-empty subset of the set of all field homomorphisms from F to K . An element $a \in F$ is called a *fixed point under S* if

$$\sigma(a) = \tau(a) \quad \text{for all } \sigma, \tau \in S.$$

Example 7.1. Let S be a non-empty set of field homomorphisms $\sigma : F \rightarrow K$. Assume that F and K share the same prime subfield Δ , that is,

$$\Delta = \begin{cases} \mathbb{Q}, & \text{if } \text{char } F = 0, \\ \mathbb{Z}/p\mathbb{Z}, & \text{if } \text{char } F = p > 0. \end{cases}$$

Since every field homomorphism satisfies $\sigma(1_F) = 1_K$ and $1_\Delta = 1_F = 1_K$, it follows that

$$\sigma(x) = x \quad \text{for all } x \in \Delta \text{ and all } \sigma \in S.$$

Hence, every element of the prime subfield Δ is fixed by all homomorphisms in S .

In particular, if S is a collection of field homomorphisms $\sigma : K \rightarrow K$ containing the identity map 1_K , then an element $x \in K$ is a fixed point under S whenever

$$\sigma(x) = x \quad \text{for all } \sigma \in S.$$

As one might expect, the set of fixed points of a collection of field homomorphisms has additional algebraic structure.

Lemma 7.2. Let S be a non-empty set of field homomorphisms $\sigma : F \rightarrow K$, and define

$$E = \{x \in F \mid \sigma(x) = \tau(x) \text{ for all } \sigma, \tau \in S\}.$$

Then E is a subfield of F .

PROOF. Let $x, y \in E$ and $\sigma, \tau \in S$. Then $\sigma(x) = \tau(x)$ and $\sigma(y) = \tau(y)$, so

$$\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = \tau(x) \pm \tau(y) = \tau(x \pm y),$$

and similarly,

$$\sigma(xy) = \sigma(x)\sigma(y) = \tau(x)\tau(y) = \tau(xy).$$

If $x \neq 0$, then

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

Hence, $x \pm y$, xy , and x^{-1} (when defined) are all in E , and clearly $0, 1 \in E$. Thus, E is a subfield of F . $\square$

Definition 7.3. Let S be a non-empty set of field homomorphisms $\sigma : F \rightarrow K$. We define

$$F^S = \{x \in F \mid \sigma(x) = \tau(x) \text{ for all } \sigma, \tau \in S\},$$

and call F^S the *fixed field* of S .

In what follows, we are particularly interested in the fixed field of a *finite* set of field homomorphisms. Following a classical idea of Artin, we use linear algebra to study such fixed fields and to establish a lower bound on the size of a finite set of field homomorphisms. This bound plays a central role in the subsequent development of Galois theory.

Lemma 7.3 (Artin's Lemma). Let S be a finite non-empty set of field homomorphisms $\sigma : F \rightarrow K$. Then

$$[F : F^S] \geq |S|.$$

PROOF. Let $S = \{\sigma_1, \dots, \sigma_n\}$ with $n = |S| \geq 1$. Suppose that $[F : F^S] = r < n$. Let $\{\omega_1, \dots, \omega_r\}$ be a basis of F over F^S .

Consider the following homogeneous system of r linear equations in the n unknowns $x_1, \dots, x_n$ with coefficients in K .

$$\begin{cases} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n = 0, \\ \vdots \\ \sigma_1(\omega_r)x_1 + \sigma_2(\omega_r)x_2 + \cdots + \sigma_n(\omega_r)x_n = 0. \end{cases} \quad (*)$$

Note that there are fewer equations than unknowns ($r < n$). This implies that there exists a non-trivial solution $(x_1, \dots, x_n) \in K^n$ with not all x_i equal to zero.

Let $a \in F$. Write $a = \sum_{i=1}^r a_i \omega_i$ with each $a_i \in F^S$. For each i , multiply the i -th equation in $(*)$ by $\sigma_j(a_i)$ and use the fact that $\sigma_j(a_i) = \sigma_k(a_i)$ for all j, k , since $a_i \in F^S$. We obtain the equivalent system,

$$\sum_{j=1}^n \sigma_j(a_i \omega_i) x_j = 0 \quad (i = 1, \dots, r).$$

By adding these r equations, we obtain

$$\sum_{j=1}^n \sigma_j \left(\sum_{i=1}^r a_i \omega_i \right) x_j = \sum_{j=1}^n \sigma_j(a) x_j = 0.$$

Thus, for every $a \in F$, we have

$$\sum_{j=1}^n x_j \sigma_j(a) = 0$$

with not all x_j equal to zero. This shows that the set of characters $\{\sigma_1, \dots, \sigma_n\}$ is linearly dependent over F , contradicting Dedekind's Lemma.

Hence, our assumption $[F : F^S] < |S|$ is false, and therefore

$$[F : F^S] \geq |S|.$$

□

Corollary 7.2. Let S be a non-empty finite set of field automorphisms of a field K . Then

$$[K : K^S] \geq |S|.$$

The natural question now is, *when does equality hold in Artin's Lemma?* In general, equality need not be true. Indeed, it is possible to find finite sets of field automorphisms S of a field K for which $[K : K^S]$ is infinite.

To ensure equality, we must impose additional algebraic structure on the set S . The most important situation arises when S consists of automorphisms fixing a given subfield.

Definition 7.4. Let K/F be an extension of fields. The *Galois group* of the extension K/F is defined as

$$G(K/F) = \text{Aut}_F(K) = \{ \sigma : K \rightarrow K \mid \sigma \text{ is a field automorphism and } \sigma|_F = 1_F \}.$$

Thus, $G(K/F)$ consists of all automorphisms of K that leave every element of F fixed.

Lemma 7.4. If K/F is a field extension, then $G(K/F)$ is a subgroup of $\text{Aut}(K)$, and the base field F is contained in the fixed field $K^{G(K/F)}$.

PROOF. Each element of $G(K/F)$ is, by definition, an automorphism of K , and the composition and inverse of such automorphisms again fix F pointwise. Hence, $G(K/F)$ is a subgroup of $\text{Aut}(K)$. Moreover, since every $\sigma \in G(K/F)$ satisfies $\sigma(a) = a$ for all $a \in F$, we have $F \subseteq K^{G(K/F)}$. □

Corollary 7.3. If K/F is a finite field extension, then the Galois group $G(K/F)$ is finite and satisfies

$$[K : F] \geq |G(K/F)|.$$

PROOF. Let S be any non-empty finite subset of $G(K/F)$. Since $F \subseteq K^S$, it follows that

$$[K : F] \geq [K : K^S].$$

By Artin's Lemma, we have $[K : K^S] \geq |S|$, hence

$$[K : F] \geq [K : K^S] \geq |S|.$$

Therefore, $[K : F]$ is a uniform upper bound for the size of any finite subset of $G(K/F)$, so the group $G(K/F)$ itself must be finite and satisfies $[K : F] \geq |G(K/F)|$. □

We now arrive at the key definition linking the structure of field extensions to their automorphism groups.

Definition 7.5. A finite field extension K/F is called *Galois* if the base field F coincides with the fixed field of its Galois group, that is,

$$F = K^{G(K/F)}.$$

Equivalently, K/F is a Galois extension if every F -automorphism of K fixes exactly the elements of F .

Throughout this text, we shall refer to such extensions as *finite Galois extensions*. More generally, an algebraic extension K/F is called *Galois* if $F = K^{G(K/F)}$, that is, if F is precisely the field of elements fixed by all F -automorphisms of K .

Remark 7.2. Let K/F be a field extension. Then the following hold.

- (1) If $F = K^{G(K/F)}$, then for every $x \in K \setminus F$ there exists $\sigma \in G(K/F)$ such that $\sigma(x) \neq x$.
- (2) If $K/E/F$ is a tower of fields, then $G(K/E) \subseteq G(K/F)$.
- (3) If $E = K^{G(K/F)}$, then $G(K/E) \supseteq G(K/F)$, hence

$$G(K/F) = G(K/K^{G(K/F)}).$$

- (4) If K/F is finite, any field homomorphism $\sigma : K \rightarrow K$ fixing F is an element of $G(K/F)$, since such a σ is automatically bijective.

Artin's Lemma becomes considerably stronger when the finite set of field automorphisms forms a group. This establishes the fundamental correspondence between algebraic field extensions and groups of automorphisms, which is central to Galois theory.

Theorem 7.1 (Artin's Theorem). Let K be a field and let G be a finite subgroup of the automorphism group $\text{Aut}(K)$. Then the following hold.

- (a) The fixed field K^G satisfies

$$[K : K^G] = |G|.$$

- (b) The group G coincides with the full Galois group of the extension K/K^G , that is,

$$G = G(K/K^G).$$

- (c) Consequently, the extension K/K^G is Galois.

Our next goal is to understand the precise relationship between Galois groups and field extensions. As an immediate consequence of Artin's Theorem, we obtain the following fundamental correspondence result.

Corollary 7.4. Let K be a field, and let G_1, G_2 be finite subgroups of $\text{Aut}(K)$, the group of all field automorphisms of K . For each $i = 1, 2$, let

$$F_i = K^{G_i}$$

denote the corresponding fixed field of G_i . Then

$$F_1 = F_2 \quad \text{iff} \quad G_1 = G_2.$$

Corollary 7.5. Let K/F be a finite field extension. Then the extension K/F is Galois if and only if

$$[K : F] = |\text{Gal}(K/F)|.$$

PROOF. Assume that K/F is Galois. Then by definition $F = K^{\text{Gal}(K/F)}$. Applying Artin's Theorem to the finite group $\text{Gal}(K/F)$, we obtain

$$[K : F] = [K : K^{\text{Gal}(K/F)}] = |\text{Gal}(K/F)|.$$

Conversely, suppose that $[K : F] = |\text{Gal}(K/F)|$. Let $E = K^{\text{Gal}(K/F)}$ denote the fixed field of the Galois group. Then, by definition,

$$\text{Gal}(K/E) = \text{Gal}(K/F).$$

Since K/E is Galois by Artin's Theorem, we have

$$[K : E] = |\text{Gal}(K/E)|.$$

Hence,

$$[K : F] = [K : E][E : F] = |\text{Gal}(K/F)|.$$

It follows that $[E : F] = 1$, and therefore $E = F$. Thus, K/F is Galois. $\square$

7.1. Galois Extensions. The central goal of Galois theory is to establish a correspondence between the intermediate fields of a finite field extension and the subgroups of its Galois group $\text{Gal}(K/F)$. Our earlier results suggest that such a correspondence arises naturally when K/F is the splitting field of a separable polynomial. We now develop this idea more systematically.

Definition 7.6. A finite field extension K/F is said to be *normal* if K is the splitting field over F of some non-constant polynomial $f(t) \in F[t]$.

The defining property of a normal extension does not depend on the specific polynomial involved, except for whether or not that polynomial is separable.

This notion extends naturally to infinite or algebraic extensions. Let $\{f_i\}_{i \in I}$ be a family of non-constant polynomials in $F[t]$. We call an algebraic extension K/F the *splitting field* of the set $\{f_i\}_{i \in I}$ if

- (a) every f_i splits completely in K , and
- (b) K is the smallest algebraic extension of F with this property.

Such a field exists and is unique up to an F -isomorphism.

For instance, the splitting field of all minimal polynomials over F is an algebraically closed field, known as the *algebraic closure* of F . An algebraic extension K/F is therefore called *normal* if it is the splitting field of some set of non-constant polynomials in $F[t]$.

If $\{f_i\}_{i \in I}$ is a finite collection of polynomials, then K is the splitting field of $\{f_i\}$ over F if and only if it is the splitting field of their product $\prod_{i \in I} f_i$.

Proposition 7.1. Let K/F be a finite field extension. Then K/F is normal if and only if every irreducible polynomial in $F[t]$ that has a root in K splits completely over K .

PROOF. Assume that K is the splitting field over F of some non-constant polynomial $g(t) \in F[t]$. Let $f(t) \in F[t]$ be an irreducible polynomial having a root $\alpha \in K$. Suppose β is any root of f in some extension field $L \supseteq K$. We now prove that $\beta \in K$.

As f is irreducible, there exists an F -isomorphism

$$\tau : F(\alpha) \longrightarrow F(\beta), \quad \tau(\alpha) = \beta.$$

Since $K(\alpha)$ and $K(\beta)$ are splitting fields of g over $F(\alpha)$ and $F(\beta)$ respectively, τ extends to an F -isomorphism

$$\sigma : K(\alpha) \longrightarrow K(\beta).$$

In particular,

$$[K(\alpha) : F] = [K(\beta) : F].$$

Since $\alpha \in K$, we have $K(\alpha) = K$. This implies that

$$[K : F] = [K(\beta) : F] = [K(\beta) : K][K : F].$$

Thus, $[K(\beta) : K] = 1$, which implies $\beta \in K$. Hence, every root of f lies in K , and f splits completely over K .

Conversely, suppose that every irreducible polynomial in $F[t]$ with a root in K splits over K . As K/F is finite, there exist elements $\alpha_1, \dots, \alpha_r \in K$ such that

$$K = F(\alpha_1, \dots, \alpha_r).$$

Let $m_F(\alpha_i)$ denote the minimal polynomial of α_i over F . Each $m_F(\alpha_i)$ has a root in K , and by assumption each splits completely in K . Therefore, K is the splitting field of the product

$$f(t) = \prod_{i=1}^r m_F(\alpha_i)$$

over F , and hence K/F is normal. $\square$

Problem 7.1. Show that the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Solution 7.1. Consider the polynomial

$$f(t) = t^3 - 2 \in \mathbb{Q}[t].$$

This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with prime 2.

The element $\sqrt[3]{2}$ is a root of $f(t)$, and hence

$$\mathbb{Q}(\sqrt[3]{2})$$

contains a root of $f(t)$. The other roots of $f(t)$ are

$$\sqrt[3]{2}\omega \quad \text{and} \quad \sqrt[3]{2}\omega^2,$$

where ω is a primitive cube root of unity. Since $\omega \notin \mathbb{Q}(\sqrt[3]{2})$, it follows that the polynomial $f(t)$ does not split over $\mathbb{Q}(\sqrt[3]{2})$.

Therefore, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension.

Problem 7.2. Let p be a prime and let $F = (\mathbb{Z}/p\mathbb{Z})(x)$, where x is transcendental over $\mathbb{Z}/p\mathbb{Z}$. Consider the polynomial

$$f(t) = t^p - x \in F[t].$$

Show that the splitting field E of $f(t)$ over F is a normal extension of F but not a Galois extension.

Solution 7.2. We first show that $f(t)$ is irreducible over F . As x is transcendental over $\mathbb{Z}/p\mathbb{Z}$, the polynomial $t^p - x$ has no root in F . Hence, $f(t)$ is irreducible in $F[t]$.

Let α be a root of $f(t)$ in some extension field of F . Then

$$\alpha^p = x.$$

Since $\text{char}(F) = p$, we have

$$t^p - x = (t - \alpha)^p \in F(\alpha)[t].$$

Thus, $f(t)$ splits completely over $E = F(\alpha)$. Therefore, E is the splitting field of $f(t)$ over F , and hence E/F is a normal extension. Every F -automorphism of E must fix $x = \alpha^p$. In characteristic p , this forces α to be fixed. Therefore, the only F -automorphism of E is the identity.

Hence

$$\text{Gal}(E/F) = \{1_E\},$$

and the extension E/F is not Galois.

Definition 7.7. Let K/F be a normal finite field extension, and let E_1, E_2 be intermediate fields such that

$$F \subseteq E_i \subseteq K, \quad i = 1, 2.$$

We say that E_1 and E_2 are *conjugate over F* if there exists an automorphism

$$\sigma \in \text{Gal}(K/F)$$

such that the restriction $\sigma|_{E_1}: E_1 \rightarrow E_2$ is an isomorphism of fields.

Equivalently, E_1 and E_2 are conjugate over F if and only if there exists an F -isomorphism $E_1 \rightarrow E_2$.

Corollary 7.6. Let K/F be a finite normal field extension, and let E be an intermediate field such that

$$F \subseteq E \subseteq K.$$

Then the extension K/E is normal. Moreover, the following statements are equivalent.

- (1) E/F is normal.
- (2) $\sigma(E) = E$ for every $\sigma \in \text{Gal}(K/F)$.
- (3) The restriction $\sigma|_E$ lies in $\text{Gal}(E/F)$ for every $\sigma \in \text{Gal}(K/F)$.
- (4) The map

$$\Phi: \text{Gal}(K/F) \longrightarrow \text{Gal}(E/F), \quad \Phi(\sigma) = \sigma|_E,$$

is well-defined and surjective.

(5) E is the only conjugate of itself over F .

Proposition 7.2. Let K/F be a finite field extension of degree n . Suppose L/F is a finite normal extension containing K , and let

$$\tau_1, \tau_2, \dots, \tau_m : K \longrightarrow L$$

be all the distinct F -homomorphisms from K into L . Then the following statements hold.

- (1) $m \leq n$.
- (2) $m = n$ if and only if K/F is separable.
- (3) The fields $\tau_1(K), \dots, \tau_m(K)$ are precisely the distinct conjugates of K over F in L (and this set is independent of the chosen normal extension L/F).
- (4) Let

$$E = F(\tau_1(K) \cup \tau_2(K) \cup \dots \cup \tau_m(K)).$$

Then E/F is the *normal closure* of K/F , that is, E is the smallest normal extension of F containing K .

Corollary 7.7. Let K/F be a field extension, and let $\alpha \in K$ be algebraic over F . Then α is separable over F if and only if the simple extension $F(\alpha)/F$ is separable.

PROOF. Let $L/F(\alpha)$ be a finite normal extension. Then the minimal polynomial $m_F(\alpha)$ of α over F splits completely in L . Let $\alpha_1, \dots, \alpha_m$ be the distinct roots of $m_F(\alpha)$ in L . For each $i = 1, \dots, m$, there exists an F -isomorphism

$$\varphi_i : F(\alpha) \longrightarrow F(\alpha_i), \quad \varphi_i(\alpha) = \alpha_i.$$

These φ_i are precisely the distinct F -homomorphisms from $F(\alpha)$ into L . Hence,

$$[F(\alpha) : F] = \deg m_F(\alpha) = m$$

if and only if all the roots of $m_F(\alpha)$ are distinct if and only if α is separable over F . Therefore, α is separable over F exactly when $F(\alpha)/F$ is separable. $\square$

Proposition 7.3. Let K be the splitting field of a separable polynomial $f(t) \in F[t]$. Then K/F is both separable and Galois.

PROOF. Assume K is the splitting field of a separable polynomial $f(t) \in F[t]$, and $F \subsetneq K$. Let $\alpha \in K \setminus F$ be a root of f . Since α is separable over F , the simple extension $F(\alpha)/F$ is separable by Corollary 7.7. Hence, there exist

$$m = [F(\alpha) : F]$$

distinct F -homomorphisms

$$\varphi_1, \dots, \varphi_m : F(\alpha) \longrightarrow K.$$

Since K/F is normal, each φ_i extends to an F -automorphism of K , i.e., $\varphi_i \in \text{Gal}(K/F)$.

By induction on $[K : F]$, we may assume that $K/F(\alpha)$ is separable. Let

$$[K : F(\alpha)] = r.$$

Then there exist exactly r distinct $F(\alpha)$ -homomorphisms

$$\psi_1, \dots, \psi_r : K \longrightarrow K.$$

The compositions

$$S = \{ \varphi_i \psi_j \mid 1 \leq i \leq m, 1 \leq j \leq r \}$$

form the set of all distinct F -homomorphisms $K \rightarrow K$. Thus,

$$|S| = [K : F(\alpha)][F(\alpha) : F] = [K : F],$$

showing that K/F is separable.

Since $S \subseteq \text{Gal}(K/F)$, by Artin's Lemma implies that

$$|\text{Gal}(K/F)| = [K : F].$$

Therefore, K/F is Galois. $\square$

Corollary 7.8. Let K/F be a finite separable field extension, and let L/K be a normal closure of K/F . Then L/F is both separable and Galois.

PROOF. Write $K = F(\alpha_1, \dots, \alpha_n)$. By definition, L is the splitting field of the separable polynomial

$$\prod_{i=1}^n m_F(\alpha_i)$$

over F , where $m_F(\alpha_i)$ denotes the minimal polynomial of α_i over F . Since this product is separable, L/F is separable and, being a splitting field, also Galois. $\square$

Corollary 7.9. Let $K = F(\alpha_1, \dots, \alpha_n)$, where each α_i is separable over F . Then K/F is separable.

PROOF. Let L/K be a normal closure of K/F . Then L is the splitting field of the separable polynomial

$$\prod_{i=1}^n m_F(\alpha_i)$$

over F . Hence, L/F is separable, and therefore the subextension K/F is also separable. $\square$

Corollary 7.10. Let $K/E/F$ be a tower of finite field extensions. Then K/F is separable if and only if both K/E and E/F are separable.

PROOF. Necessary condition follows immediately from the definition of separability for algebraic extensions.

Conversely, let L/K be a finite normal extension. Denote by

$$\varphi_1, \dots, \varphi_m : E \longrightarrow L \quad \text{and} \quad \psi_1, \dots, \psi_n : K \longrightarrow L$$

the distinct F - and E -homomorphisms, respectively. Each φ_i can be lifted to an automorphism $\tilde{\varphi}_i \in \text{Gal}(L/F)$. Then, as in the proof of Proposition 7.2, the set

$$S = \{\tilde{\varphi}_i \psi_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$$

consists of mn distinct F -homomorphisms $K \rightarrow L$. Since K/E and E/F are separable, we have

$$[K : F] = [K : E][E : F] = mn.$$

Hence, K/F is separable by Proposition 7.2. $\square$

We now prove the main result, which explains when a finite extension K/F is Galois.

Theorem 7.2. Let K/F be a finite field extension. Then K/F is Galois if and only if it is both normal and separable.

PROOF. If K/F is normal and separable, then K/F is Galois by Proposition 7.3.

Conversely, assume K/F is Galois. Let L/K be a normal closure of K/F . Since K/F is Galois, we have

$$|\text{Gal}(K/F)| = [K : F],$$

and therefore the number of distinct F -homomorphisms $K \rightarrow L$ is also $[K : F]$. By Proposition 7.2, it follows that K/F is separable. Moreover, because every F -automorphism of K extends to L and $L = \bigcup_{\sigma \in \text{Gal}(K/F)} \sigma(K)$, we must have $L = K$. Hence, K/F is normal. Therefore, K/F is both normal and separable. $\square$

Corollary 7.11. Let K/F be a finite Galois extension, and let E be an intermediate field with

$$F \subseteq E \subseteq K.$$

Then

- (1) The extension K/E is Galois.
- (2) The subextension E/F is Galois if and only if it is normal.

PROOF. As K/F is Galois, it is both normal and separable. Hence, K/E and E/F are separable, and K/E is also normal. Thus, K/E is Galois. Furthermore, E/F is Galois if and only if E/F is normal. $\square$

Example 7.2. In general, if K/F is Galois and E is an intermediate field, the extension E/F need not be Galois. For example, let

$$K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}), \quad E = \mathbb{Q}(\sqrt[3]{2}), \quad F = \mathbb{Q}.$$

Then K/F is Galois, but E/F is not.

Question 7.1. If both K/E and E/F are Galois, must K/F also be Galois?

Definition 7.8. A field F is called *perfect* if every algebraic extension K/F is separable.

Remark 7.3. Let F be a field.

- (1) If $\text{char } F = 0$, then F is perfect.
- (2) Every finite field is perfect.
- (3) If F is perfect and K/F is a finite extension, then K/F is Galois if and only if it is normal.
- (4) If $p > 0$ is prime and $F = (\mathbb{Z}/p\mathbb{Z})(x)$ with x transcendental, then F is not perfect since $t^p - x \in F[t]$ is not separable.

Problem 7.3. Show that any algebraic extension of a perfect field is perfect.

Solution 7.3. Let F be a perfect field, and let K/F be an algebraic field extension. We now prove that every element of K is separable over K , or equivalently, that every irreducible polynomial in $K[x]$ is separable.

Let $f(x) \in K[x]$ be an irreducible polynomial, and let α be a root of $f(x)$ in some algebraic closure of K . Since K is algebraic over F , the element α is algebraic over F . Let $g(x) \in F[x]$ be the minimal polynomial of α over F . As F is perfect, the polynomial $g(x)$ is separable, and hence has distinct roots.

Since $f(x)$ is the minimal polynomial of α over K , we have

$$f(x) \mid g(x)$$

in $K[x]$. A factor of a separable polynomial is separable. Therefore, $f(x)$ is separable. Since every irreducible polynomial in $K[x]$ is separable, it follows that K is a perfect field.

Problem 7.4. Let F be a field and set $K = F$. Show that K/F is a Galois extension and determine $\text{Gal}(K/F)$.

Solution 7.4. Since $K = F$, every field automorphism of K that fixes F is the identity map. Therefore,

$$\text{Gal}(K/F) = \{1_K\}.$$

Clearly $[K : F] = 1$, and hence

$$[K : F] = |\text{Gal}(K/F)|.$$

Moreover, for any $a \in F$, the polynomial $t - a \in F[t]$ splits completely over F , and F is its splitting field. Thus, K/F is a Galois extension.

Problem 7.5. Let $F = \mathbb{R}$ and $K = \mathbb{C}$. Show that K/F is a Galois extension and determine its Galois group.

Solution 7.5. Consider the map

$$\tau : \mathbb{C} \rightarrow \mathbb{C}, \quad \tau(a + bi) = a - bi \quad (a, b \in \mathbb{R}),$$

which is complex conjugation. This map is a field automorphism of $\mathbb{C}$ that fixes $\mathbb{R}$.

The only $\mathbb{R}$ -automorphisms of $\mathbb{C}$ are the identity map $1_{\mathbb{C}}$ and τ . Thus,

$$\text{Gal}(K/F) = \{1_{\mathbb{C}}, \tau\}.$$

Since $\mathbb{C} = \mathbb{R}(i)$ and $i^2 + 1 = 0$, the field $\mathbb{C}$ is the splitting field of the polynomial $t^2 + 1 \in \mathbb{R}[t]$. Hence, K/F is a normal and separable extension.

Therefore, K/F is Galois and

$$[K : F] = 2 = |\text{Gal}(K/F)|.$$

Problem 7.6. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$. Show that K/F is a Galois extension and determine its Galois group.

Solution 7.6. Define a map

$$\sigma : K \rightarrow K, \quad \sigma(a + b\sqrt{2}) = a - b\sqrt{2}, \quad (a, b \in \mathbb{Q}).$$

Then σ is a field automorphism of K that fixes $\mathbb{Q}$. The only $\mathbb{Q}$ -automorphisms of K are the identity map 1_K and σ . Thus,

$$\text{Gal}(K/F) = \{1_K, \sigma\}.$$

Since $\sqrt{2}$ is a root of $t^2 - 2 \in \mathbb{Q}[t]$, and

$$t^2 - 2 = (t - \sqrt{2})(t + \sqrt{2})$$

splits completely over K , the field K is the splitting field of $t^2 - 2$ over $\mathbb{Q}$.

Therefore, K/F is a Galois extension and

$$[K : F] = 2 = |\text{Gal}(K/F)|.$$

8. The Fundamental Theorem of Galois Theory

In this section, we bring together the group-theoretic and field-theoretic aspects of Galois theory developed so far. Our goal is to describe the precise correspondence between subgroups of the Galois group and intermediate fields of a finite Galois extension. As an application, we will later use this correspondence to prove the Fundamental Theorem of Algebra.

Lemma 8.1. Let K/F be a finite Galois extension, and let $H_i \subseteq \text{Gal}(K/F)$ be subgroups with corresponding fixed fields $E_i = K^{H_i}$ for $i = 1, 2$. If $\sigma \in \text{Gal}(K/F)$, then

$$\sigma|_{E_1} : E_1 \rightarrow E_2$$

is an F -isomorphism if and only if $H_2 = \sigma H_1 \sigma^{-1}$.

Equivalently, E_1 and E_2 are conjugate over F (via σ) if and only if H_1 and H_2 are conjugate subgroups of $\text{Gal}(K/F)$.

PROOF. Since K/E_i is Galois, we have $H_i = \text{Gal}(K/E_i)$ and $[K : E_i] = |H_i|$ for $i = 1, 2$. Thus, $|H_1| = |H_2|$.

First, we assume $\sigma|_{E_1} : E_1 \rightarrow E_2$ is an F -isomorphism. For any $\tau \in H_1$ and $y \in E_2$, we have $\sigma^{-1}(y) \in E_1$, hence

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

Thus, $\sigma\tau\sigma^{-1} \in \text{Gal}(K/E_2) = H_2$ and so $\sigma H_1 \sigma^{-1} \subseteq H_2$. Since both subgroups have the same order, equality holds.

Conversely, assume $H_2 = \sigma H_1 \sigma^{-1}$. For $x \in E_1$ and $\tau \in H_1$, we have

$$(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma\tau(x) = \sigma(x),$$

and thus $\sigma(x)$ is fixed by H_2 . Hence, $\sigma(x) \in K^{H_2} = E_2$, and σ maps E_1 into E_2 . Since $[K : E_1] = [K : E_2]$, it follows that the restriction $\sigma|_{E_1}$ is an isomorphism. $\square$

Notations: For an algebraic extension K/F , we denote

$$\mathcal{F}(K/F) := \{E \mid F \subseteq E \subseteq K\} \quad \text{and} \quad \mathcal{G}(K/F) := \{H \mid H \subseteq \text{Gal}(K/F) \text{ is a subgroup}\}.$$

Theorem 8.1 (Fundamental Theorem of Galois Theory). Let K/F be a finite Galois extension. Then there exists an order-reversing bijection

$$i : \mathcal{G}(K/F) \rightarrow \mathcal{F}(K/F), \quad H \mapsto K^H,$$

with inverse

$$j : \mathcal{F}(K/F) \rightarrow \mathcal{G}(K/F), \quad E \mapsto \text{Gal}(K/E).$$

Moreover,

- (1) The correspondence is order-reversing

$$H_1 \subseteq H_2 \iff K^{H_1} \supseteq K^{H_2}.$$

- (2) For any intermediate field E , the extension E/F is normal (and hence Galois) if and only if $\text{Gal}(K/E)$ is a normal subgroup of $\text{Gal}(K/F)$.
 (3) If E/F is normal, then the canonical epimorphism

$$\Phi : \text{Gal}(K/F) \longrightarrow \text{Gal}(E/F), \quad \Phi(\sigma) = \sigma|_E,$$

induces an isomorphism

$$\text{Gal}(K/F)/\text{Gal}(K/E) \cong \text{Gal}(E/F).$$

- (4) For every subgroup $H \subseteq \text{Gal}(K/F)$, we have

$$|H| = [K : K^H],$$

and K/K^H is Galois with $\text{Gal}(K/K^H) = H$.

- (5) For every subgroup $H \subseteq \text{Gal}(K/F)$, we have

$$[\text{Gal}(K/F) : H] = [K^H : F].$$

PROOF. The correspondence $i(H) = K^H$ is injective because distinct subgroups of $\text{Gal}(K/F)$ fix different subfields of K . For any intermediate field E , K/E is Galois, and $\text{Gal}(K/E)$ fixes precisely E and so i is surjective.

- (1) Follows immediately from the definition of fixed fields.

- (2) By Lemma 8.1, E/F is normal if and only if $\sigma(E) = E$ for all $\sigma \in \text{Gal}(K/F)$, which holds exactly when $\text{Gal}(K/E)$ is normal in $\text{Gal}(K/F)$.

- (3) When E/F is normal, the restriction map Φ is well-defined and surjective. Since $\ker \Phi = \text{Gal}(K/E)$, the First Isomorphism Theorem gives

$$\text{Gal}(K/F)/\text{Gal}(K/E) \cong \text{Gal}(E/F).$$

- (4) and (5) follow from Artin's Theorem, since K/K^H is Galois with group H and $[K : K^H] = |H|$. $\square$

The bijection in Theorem 8.1,

$$H \longleftrightarrow K^H,$$

is called the *Galois correspondence*. It provides a one-to-one, order-reversing relationship between the subgroups of $\text{Gal}(K/F)$ and the intermediate fields of K/F .

If E/F is normal, then we have a group isomorphism

$$\text{Gal}(K/F)/\text{Gal}(K/E) \cong \text{Gal}(E/F).$$

Corollary 8.1. Let K/F be a finite Galois extension of fields. Then the set of intermediate fields

$$\mathcal{F}(K/F) = \{ E \mid F \subseteq E \subseteq K \}$$

is finite. In other words, there are only finitely many intermediate fields E with $K/E/F$.

PROOF. By the Fundamental Theorem of Galois Theory, there is a bijection between $\mathcal{F}(K/F)$ and the set of subgroups of $\text{Gal}(K/F)$. Since $\text{Gal}(K/F)$ is finite, it has only finitely many subgroups, and hence $\mathcal{F}(K/F)$ is finite. $\square$

Corollary 8.2. Let K/F be a finite separable field extension. Then $\mathcal{F}(K/F)$ is finite.

PROOF. Let L be a normal closure of K/F . Then L/F is finite, separable, and normal, that is, L/F is Galois. Since $\mathcal{F}(K/F) \subseteq \mathcal{F}(L/F)$ and $\mathcal{F}(L/F)$ is finite by Corollary 8.1, the result follows. $\square$

Problem 8.1. Illustrate the Fundamental Theorem of Galois Theory for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ by describing its Galois group, intermediate fields, and corresponding subgroups.

Solution 8.1. Let

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \quad f(t) = (t^2 - 2)(t^2 - 3) \in \mathbb{Q}[t].$$

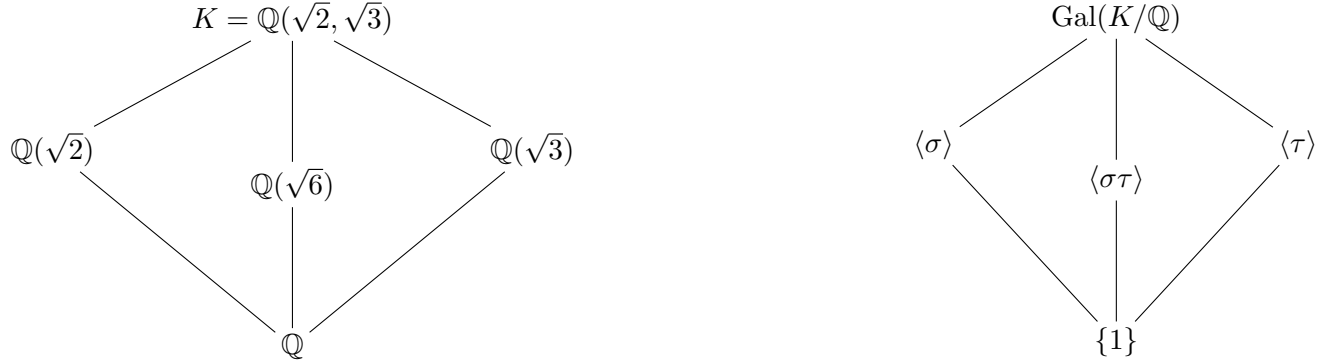
Then K is the splitting field of $f(t)$ over $\mathbb{Q}$, hence $K/\mathbb{Q}$ is Galois. We have

$$\text{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

where

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}, \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}.$$

The intermediate fields and corresponding subgroups are as follows.



Hence, there are precisely four intermediate fields, each corresponding to one of the four subgroups of the Galois group.

Problem 8.2. Illustrate the Fundamental Theorem of Galois Theory for the splitting field of the polynomial $t^4 - 2$ over $\mathbb{Q}$ by describing its Galois group, intermediate fields, and subgroup lattice.

Solution 8.2. Let

$$K = \mathbb{Q}(\sqrt[4]{2}, i), \quad i^2 = -1.$$

Then K is the splitting field of $t^4 - 2$ over $\mathbb{Q}$ and $[K : \mathbb{Q}] = 8$. Define automorphisms

$$\sigma : i \mapsto -i, \quad \sqrt[4]{2} \mapsto \sqrt[4]{2}, \quad \tau : i \mapsto i, \quad \sqrt[4]{2} \mapsto i\sqrt[4]{2}.$$

Then

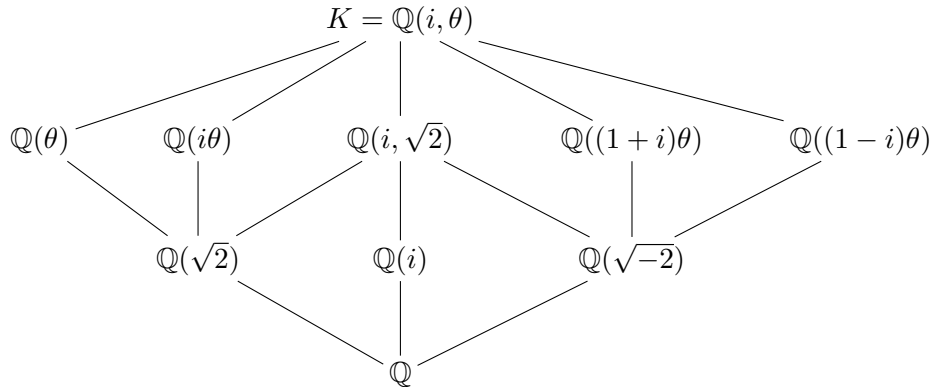
$$|\langle \sigma \rangle| = 2, \quad |\langle \tau \rangle| = 4, \quad \sigma\tau\sigma^{-1} = \tau^3,$$

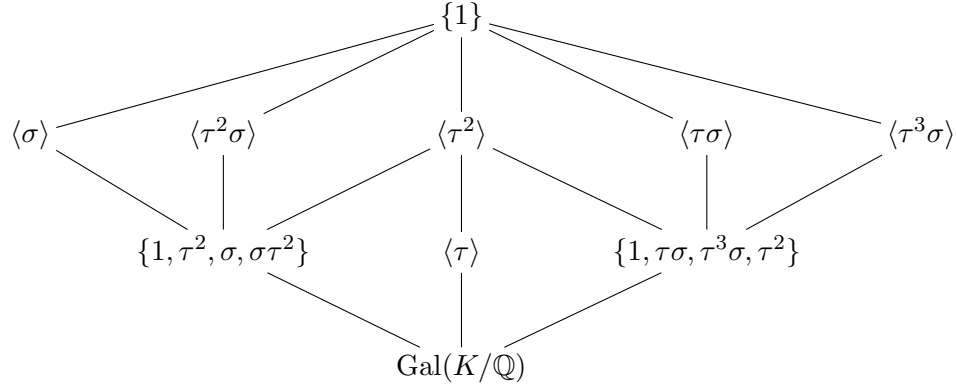
and hence

$$\text{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4,$$

the dihedral group of order 8.

The intermediate fields and corresponding subgroups are given schematically below.





Thus, the subgroup lattice of D_4 mirrors precisely the lattice of intermediate fields of the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.

Open Problem (Inverse Galois Problem). Let H be a finite group. Does there exist a Galois extension $L/\mathbb{Q}$ such that

$$G(L/\mathbb{Q}) \cong H?$$

This question, known as the *Inverse Galois Problem*, asks whether every finite group can appear as the Galois group of some extension of $\mathbb{Q}$.

The problem has been solved for several important classes of groups, including

- cyclic and abelian groups,
- solvable groups,
- the symmetric and alternating groups S_n and A_n .

However, the general case remains open and is one of the central unsolved problems in modern algebra.

Theorem 8.2 (Primitive Element Theorem). Let K/F be a finite field extension. If the set of intermediate fields $\mathcal{F}(K/F)$ is finite, then there exists an element $\alpha \in K$ such that

$$K = F(\alpha).$$

In particular, this holds whenever K/F is a separable extension. In other words, every finite separable field extension is *simple*, i.e., generated by a single element.

PROOF. If F is finite, then K is also a finite field. Since the multiplicative group $K^\times$ is cyclic, there exists an element $\alpha \in K$ such that $K^\times = \langle \alpha \rangle$. Hence, $K = F(\alpha)$, and clearly $\mathcal{F}(K/F)$ is finite.

Next, assume that F is infinite. Choose $\alpha \in K$ such that $[F(\alpha) : F]$ is maximal. If $F(\alpha) \neq K$, then there exists $\beta \in K \setminus F(\alpha)$. For each $a \in F$, consider the intermediate field

$$F(\alpha + a\beta) \subseteq F(\alpha, \beta) \subseteq K.$$

Since $\mathcal{F}(F(\alpha, \beta)/F) \subseteq \mathcal{F}(K/F)$ is finite, but F is infinite, there exist distinct elements $c, d \in F$ such that

$$F(\alpha + c\beta) = F(\alpha + d\beta).$$

Also,

$$(c - d)\beta = (\alpha + c\beta) - (\alpha + d\beta) \in F(\alpha + c\beta),$$

and since $c - d \in F^\times$, it follows that $\beta \in F(\alpha + c\beta)$. Therefore, $\alpha \in F(\alpha + c\beta)$ as well, implying that

$$F(\alpha, \beta) \subseteq F(\alpha + c\beta).$$

This contradicts the maximality of $[F(\alpha) : F]$. Hence, $K = F(\alpha)$, completing the proof. $\square$

8.1. The Fundamental Theorem of Algebra. Our exploration of field theory and Galois extensions culminates in one of the most profound and classical results in mathematics, the *Fundamental Theorem of Algebra*. This theorem provides an algebraic characterization of the complex field $\mathbb{C}$, showing that it is, in a sense, the ultimate destination for all algebraic equations.

In essence, it asserts that the field of complex numbers contains all the roots of any non-constant complex polynomial. Equivalently, every polynomial in $\mathbb{C}[x]$ factors completely into linear factors over $\mathbb{C}$. The result was conjectured as early as the seventeenth century and later proved rigorously using tools from both algebra and analysis.

Theorem 8.3 (Fundamental Theorem of Algebra). The field of complex numbers $\mathbb{C}$ is algebraically closed. That is, for every non-constant polynomial $f(x) \in \mathbb{C}[x]$, there exists an element $a \in \mathbb{C}$ such that

$$f(a) = 0.$$

Equivalently, every polynomial $f(x) \in \mathbb{C}[x]$ can be expressed as a product of linear factors as

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n),$$

where $c, a_1, a_2, \dots, a_n \in \mathbb{C}$.

Remark 8.1. (1) This theorem implies that $\mathbb{C}$ serves as an algebraic closure of $\mathbb{R}$.

(2) In the framework of Galois theory, this theorem ensures that every polynomial with real coefficients splits in $\mathbb{C}$, making $\mathbb{C}$ a complete and algebraically closed field.

Problem 8.3. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then prove that there exists an element $\alpha \in K$ such that

$$K = \mathbb{Q}(\alpha).$$

Solution 8.3. Since $K/\mathbb{Q}$ is a finite separable extension, the Primitive Element Theorem applies. Therefore, there exists an element $\alpha \in K$ such that

$$K = \mathbb{Q}(\alpha).$$

We prove that $\alpha = \sqrt{2} + \sqrt{3}$ is a primitive element for the extension. Clearly $\mathbb{Q}(\alpha) \subseteq K$. Next, we compute

$$\alpha^2 = 5 + 2\sqrt{6}.$$

Hence,

$$\sqrt{6} = \frac{\alpha^2 - 5}{2} \in \mathbb{Q}(\alpha).$$

Observe that $(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$. Thus,

$$\sqrt{3} - \sqrt{2} = \frac{1}{\alpha} \in \mathbb{Q}(\alpha).$$

It follows that

$$\sqrt{2} = \frac{\alpha - (\sqrt{3} - \sqrt{2})}{2} \quad \text{and} \quad \sqrt{3} = \frac{\alpha + (\sqrt{3} - \sqrt{2})}{2}$$

belong to $\mathbb{Q}(\alpha)$. Hence, $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$.

Therefore, $K \subseteq \mathbb{Q}(\alpha)$. Combining this with the reverse inclusion, we conclude that

$$K = \mathbb{Q}(\alpha).$$

Problem 8.4. Let $f(t) \in \mathbb{R}[t]$ be a polynomial of odd degree. Show that $f(t)$ has at least one real root.

Solution 8.4. Let

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0,$$

where n is odd and $a_n \neq 0$.

By the Fundamental Theorem of Algebra, the polynomial $f(t)$ has exactly n roots in $\mathbb{C}$, counted with multiplicity.

Since the coefficients of $f(t)$ are real, non-real roots occur in complex conjugate pairs. That is, if $\alpha \in \mathbb{C} \setminus \mathbb{R}$ is a root of $f(t)$, then its complex conjugate $\bar{\alpha}$ is also a root, with the same multiplicity.

Thus, the non-real roots of $f(t)$ contribute an even number to the total number of roots of $f(t)$, counted with multiplicity.

Since n is odd, it follows that not all roots of $f(t)$ can be non-real. Therefore, at least one root of $f(t)$ must be real. Hence, every polynomial in $\mathbb{R}[t]$ of odd degree has at least one real root.

Bibliography

- [1] Gary Chartrand. "Mathematical proofs: A transition to advanced mathematics". In: (2018).
- [2] Richard Elman. *Lectures on Abstract Algebra Preliminary Version*. 2019.
- [3] Joseph Gallian. *Contemporary abstract algebra*. Chapman and Hall/CRC, 2021.
- [4] G. H. Hardy. *A Mathematician's Apology*. Cambridge: Cambridge University Press, 1940.
- [5] Anthony W Knapp. *Basic algebra*. Springer Science & Business Media, 2006.
- [6] Henri Poincaré. *The Value of Science*. Trans. by George Bruce Halsted. New York: The Science Press, 1907.
- [7] Hermann Weyl. *Symmetry*. Princeton University Press, 2015.