Introduction to Group and Ring Theory: The Foundations of Algebraic Structures

Jianing Huang, Sylvia Lee

May 21, 2025

Abstract

This expository paper aims to offer an introduction to some fundamental concepts of group theory, which is a central part of abstract algebra, or the study of algebraic structures. Beginning with the definition and properties of groups, illustrated by examples involving symmetries, number systems, and modular arithmetic, we then proceed to introduce a category of groups called rings, as well as mappings from one ring to another. We conclude by proving the First Isomorphism Theorem, as well as an example of an isomorphism between a quotient ring and a polynomial ring.

1 Introduction

Abstract algebra is the mathematical study of algebraic systems, which can be generally viewed as sets involving operations. Despite the word "abstract", it is a branch of math that powers real-world technologies in everything from cryptography to the structure of chemical molecules with its language of patterns and symmetry. Acquiring its central discoveries and concrete examples from other branches of math such as number theory, elementary algebra, and geometry, abstract algebra was distilled into formal, axiomatic definitions in the 19th to 20th century as its own area of study.

One prominent type of algebraic structure is groups, the early formalization of which can be attributed to several areas of mathematics– for instance, Lagrange's study of quintic solutions inspired the Galois group of polynomials in 1770, and Fermat's Little Theorem led to studies of modulo groups [2]. After Galois coined the term "group" in 1832, group theory continued to be developed and expanded by mathematicians like Cayley, Frobenius, and Burnside, who refined the definition and properties of groups and operations, studying specialized quotient groups, mapping between groups, etc [3].

On the other hand, rings are another type of algebraic structure. Their history traces back to the extensions of the complex hypercomplex numbers in the early 19th century [2]. The study to understand other exotic number systems soon followed as specialized branches of ring theory diverged. For commutative rings, Gauss formulated the Gaussian integers and proved the law of quadratic reciprocity. With a consistent tinge of number theory, the drilling into Fermat's last theorem drove into the algebraic integers. Meanwhile, the intersection with analysis and p-adics opened a new realm for ring theory.

Today, group theory and ring theory have become central to many areas of mathematics and physical sciences. Its applications range from the Lie groups modeling particle physics and spatial symmetry to modulo groups used in cryptography [2]. This expository paper largely sources from Gallian's textbook on abstract algebra [1] and aims to provide an introduction to the fundamental, elementary concepts involving groups and rings and to begin investigating the properties and relationships between the elements and operations of these abstract systems.

2 Preliminaries

Before moving on to discuss algebraic structures, we will review some notations and concepts used in future references. To begin with, since both groups and rings involve sets of elements, it is natural to consider some common sets in mathematics:

1. **Integers** are numbers with no decimal or fractional parts, including positive numbers, negative numbers, and 0. The set of all integers is denoted as $\mathbb{Z}$.

2. **Real numbers** can be interpreted as any number that can be expressed on one number line; it includes sets like integers, rational numbers, and irrational numbers. The real numbers are denoted as $\mathbb{R}$.

3. **Complex numbers** are numbers that can be written in the form $a + bi$, where $a, b \in \mathbb{Z}$, and i, the imaginary unit, is defined to be $i = \sqrt{-1}$.

4. **Modular arithmetic** is a system of arithmetic operations for integers that focuses on the residue or remainder. Suppose today is Monday, and you would like to know what day it will be 15 days later. Most likely, you did not add 15 days to today, instead, you thought of 15 as $15 = 2 \cdot 7 + 1$ and realized that, after two full weeks, the "remainder" is 1 day. This system can be viewed as "mod 7".
   When two integers a, b have the same remainder when divided by c, we say that a is congruent to b mod c, denoted $a \equiv b \mod c$. Here are some other examples:

$$13 \equiv 6 \text{ mod } 7 \text{ since } 13 = 1 \cdot 7 + 6 = 2 \cdot 7 - 1$$
$$14 \equiv 4 \text{ mod } 5 \text{ since } 14 = 2 \cdot 5 + 4$$

   Note that, in general:

$$(a \text{ mod } c) + (b \text{ mod } c) = (a + b) \text{ mod } c$$
$$(a \text{ mod } c) \cdot (b \text{ mod } c) = ab \text{ mod } c$$

   For example:

$$3 \cdot 13 \text{ mod } 7 = (3 \text{ mod } 7) \cdot (13 \text{ mod } 7) = 3 \cdot (-1) = -3 = 4 \text{ mod } 7.$$

   We can verify this by checking directly:

$$3 \cdot 13 = 39 \equiv 4 \text{ mod } 7.$$

   We use the notation $\mathbb{Z}/n\mathbb{Z}$ to denote the set of all integers mod an integer n. This set would include all possible remainders under division by n, that is $\{0, 1, 2, ..., n - 1\}$.

3 Groups

This section introduces our first algebraic structure: groups. We will define what a group is, examine subgroups as smaller structures within a group, inspect the homomorphism as correspondences between groups, and conclude with quotient groups, which embed the idea of "modding out" by subgroups.

3.1 Definition and Examples

Imagine cutting a square off of a piece of paper and labeling its four corners in different colors. You pick up this square and move it in some way before putting it back in its original place on the paper. The resulting square may have each corner—and every point in between—in their original positions, or it may not. As you will see shortly, the set of potential transformations on the square can be viewed as a group.

3.1.1 Definitions

Definition 1. A **group** is a set G associated with an operation $\cdot$ that satisfies the following axioms:

1. *Closure.* For all elements $a, b \in G$, $ab \in G$.

2. *Associativity.* $(ab)c = a(bc)$ for all $a, b, c \in G$.

3. *Identity.* There exists an identity $e \in G$ such that $ae = ea = a$.

4. *Inverse.* For all $a \in G$, there is an element $b \in G$ such that $ab = ba = e$. b is the inverse of a, denoted $b = a^{-1}$.

Definition 2. The **order of a group** G, denoted $|G|$, is the number of elements in G.

Definition 3. The **order of an element** of an element a, denoted $|a|$, is the smallest natural number n such that $a^n = e$.

Now we will look at some examples.

3.1.2 Examples

1. The set of integers $\mathbb{Z}$ under addition.
   The sum of two integers is always an integer, satisfying closure. Regular addition is associative. The additive identity is 0, and the inverse of an integer n is $-n$. $\mathbb{Z}$ has infinite order.

2. Let's return to the set of transformations G on a square. This set is denoted as the dihedral group D_4 consisting of all symmetries of a regular 4-gon (most commonly known as a square). The set D_4 includes the identity, vertical and horizontal reflections, reflections about the two diagonals, and rotations of $90°$, $180°$, and $270°$:
   $G = \{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$. The order of this group is 8 since there are 8 elements. The operation here is composition; in other words, by $V \cdot R_{90}$, we simply reflect the square vertically first,

then rotate it by 90 degrees. The transformations preserve the shape of the square and are closed. Exhaustive checking can confirm associativity. I, or not transforming the square at all, is the identity, and each transformation has an inverse to "undo" it:

$$I \cdot I = I$$

$$V \cdot V = I$$

$$H \cdot H = I$$

$$D_1 \cdot D_1 = I$$

$$D_2 \cdot D_2 = I$$

$$R_{90} \cdot R_{270} = I$$

$$R_{180} \cdot R_{180} = I$$

As shown above, the orders of all reflections and R_{180} are 2. R_{90} and R_{270}, on the other hand, have order 4, as the square has to be rotated 4 times to return to original position.

3. $\mathbb{Z}/7\mathbb{Z}^{\times}$, the set of integers mod by 7, excluding 0. i.e. 1, 2, 3, 4, 5, 6, under multiplication.
   This is a modulo group of 7. Multiplying two numbers results in their product mod 7, which is less than 7. Note that the remainder also cannot be 0 since 0 is not in the original group, and no two nonzero numbers can multiply to 0 mod 7, which guarantees closure. Multiplication is associative, and the identity is 1. Furthermore, 1, 6, 7 are inverses of themselves, 2 and 4 are inverses, 3 and 5 are inverses.

3.1.3 Non-Examples

1. The set of integers $\mathbb{Z}$ under division.
   The quotient of two integers is not necessarily an integer, so closure is violated.

2. $\mathbb{Z}/6\mathbb{Z}$ excluding 0 under multiplication.
   This can raise some problems with inverses, for example, let's look at the element 2:

$$1 \cdot 2 = 2$$

$$2 \cdot 2 = 4$$

$$3 \cdot 2 = 6 \longmapsto 0$$

$$4 \cdot 2 = 8 \longmapsto 2$$

$$5 \cdot 2 = 10 \longmapsto 4$$

Note that the product of 2 with any other element is always even and cannot be 1. For a number to be equivalent to 1 mod 6, it must be in the form $6k + 1$ for some integer k. Since $6k$ is always even, $6k + 1$ must be odd. Unfortunately, the product of 2 and any other number would be in the form $2m$ for some

integer m, which is even and cannot be equal to the odd $6k+1$.
The element 3 has the same problem. $6k+1$ gives a remainder of 1 when divided by 1, but 3 multiplying by any number would result in a remainder 0 mod 3. Therefore, 3 also has no inverse.
2 and 3 both have common divisors with 6 that are greater than 1. The same problem holds for any element not coprime with the modulo of the group (which is 6 here). Thus, in general, $\mathbb{Z}/p\mathbb{Z}$ is only a group if p is prime.

3.1.4 Theorems

Theorem 3.1. *In a group G, there is only one unique identity.*

Proof. Assume that e_1 and e_2 are both identities in G. Then $e_1e_2 = e_1$ and $e_1e_2 = e_2$ by the definition of identity.
Thus, $e_1 = e_2$, so the two identities are actually the same. □

Theorem 3.2. *For every element a in a group G, there is only one unique inverse for a.*

Proof. Assume that b and c are both inverses of a. Then

$$ba = ca = e,$$

$$eb = (ba)b = (ca)b = c(ab) = ce,$$

$$b = c.$$

The two inverses of a are actually identical. □

Theorem 3.3. *In a finite group G, every element a has finite order.*

Proof. Since G has finitely many elements, by the Pigeonhole Principle, there must exist finite positive integers i, j such that $a^i = a^j$ and $i > j$. Then $a^{i-j} = e$. Note that $i - j$ is a finite positive integer, and the $|a| \leq i - j$ by the definition of order. So $|a|$ is also finite. □

3.2 Subgroups

Groups are essentially sets with an operation. A natural question to ask is if a subset of the elements of a group could also be groups. For example, the set of integers $\mathbb{Z}$ is a subset of the set of all real numbers $\mathbb{R}$. It happens that both are groups under addition. But when does this hold for other groups? The following definition outlines a test for determining if a subset of elements of a group is a group, or *subgroup* in its own right.

3.2.1 Definition

Definition 4. A subgroup H of a group G is a group such that all elements of H are also elements of G, and the operation is the same. To test if a nonempty subset H of a group G is a subgroup, it is sufficient to check the following conditions:

1. *Closure.* For all elements $a, b \in H$, $ab \in H$.

2. *Inverse.* For all elements $a \in H$, $a^{-1} \in H$.

These two conditions imply the other necessary conditions for H to be a group. Since H uses the same operation of the larger group G, it is associative. By the inverse and closure properties, H also contains the identity e since there exists an element a such that $a, a^{-1} \in H$ and $aa^{-1} = e$.

3.2.2 Examples

1. The set $6\,\mathbb{Z}$ representing the integer multiples of 6 is a subgroup of $\mathbb{Z}$ under addition. All integer multiples of 6 are in $\mathbb{Z}$, and $6\,\mathbb{Z}$ satisfies all the conditions of a group including closure and inverses.

2. The set of integers $\mathbb{Z}$ under addition is a subgroup of the set of complex numbers $\mathbb{C}$ under addition.

3. The set of rotations $\{I, R_{90}, R_{180}, R_{270}\}$ in the group of transformations $\{I, V, H, D_1, D_2, R_{90}, R_{180}, R_{270}\}$ on a square is a subgroup. The set of rotations is a subset of all transformations, each rotation has an inverse that is also a rotation. Closure is guaranteed since composing any two rotations always results in another rotation.

4. The set $\{1, 2, 4\}$ under multiplication is a subgroup of $\mathbb{Z}/7\,\mathbb{Z}^{\times} = \{1, 2, 3, 4, 5, 6\}$. Clearly, the elements of $\{1, 2, 4\}$ all belong to $\mathbb{Z}/7\,\mathbb{Z}^{\times}$. For inverses, $1^{-1} = 1$, $2^{-1} = 4$, and $4^{-1} = 2$. For closure, multiplying any two elements of $\{1, 2, 4\}$ will result in another element in $\{1, 2, 4\}$. Alternatively, one could notice that $1 \equiv 2^0$, $2 \equiv 2^1$, and $4 \equiv 2^2$ in mod 7, which are all the possible remainders of powers of 2 mod 7 since $2^3 \equiv 8 \equiv 1 \mod 7$. So the product of any two elements will be equivalent to a power of 2 mod 7, and thus the subgroup $\{1, 2, 4\}$ satisfies closure.

3.3 Cyclic Groups

3.3.1 Definitions

Definition 5. A group G is **cyclic** if $G = \{a^n \mid a \in G, n \in \mathbb{Z}\}$, i.e. the powers of one element a in G covers the whole group. We can denote this as $G = \langle a \rangle$, where element a is a **generator** of G.

3.3.2 Examples

1. The integers $\mathbb{Z}$ under addition is an infinite cyclic group.
   $\mathbb{Z} = \langle 1 \rangle$. Negative integers can be generated by the element $1^{-1} = -1$.
   The order of $\mathbb{Z}$ is infinite.

2. $\mathbb{Z}/7\mathbb{Z}^{\times} = G = \langle 3 \rangle$, verify this by listing the powers of 3:
   $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$.
   We can confirm that the powers of 3 covers all elements in the group, and the powers after 6 circle back, since 3^6 is the identity. Since there are 6 elements in this finite cyclic group, it has order 6.

3.3.3 Theorems

Theorem 3.4. *Let G be a group, and a is an element in G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order n, then then $a^i = a^j$ if and only if n divides $i - j$.*

Proof. $a^i = a^j$ implies that $a^{i-j} = e$, the identity.
If a has infinite order, there is no nonzero integer n such that $a^n = e$. Thus, $i - j = 0$, so $i = j$.
If $|a| = n$, where n is finite, let $i - j = k$, we can write k as.

$$k = nq + r,\ 0 \leq r < n.$$

Then,

$$e = a^{i-j} = a^k = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r.$$

Therefore,

$$e = a^r.$$

Since $r < n$, and there are no positive integer r less than n for which $a^r = e$ by the definition of order, it must be that $r = 0$. Then $k = nq$, which implies n divides k and n divides $i - j$. □

3.4 Group Isomorphism and Homomorphism

So far, we have examined the patterns and operations within a group. In this section, we will introduce group isomorphism and homomorphism, which are correspondences between two different groups. Sometimes, two groups drastically different in appearance may be similar in structure.

3.4.1 Definitions

Definition 6. A **bijection** is a function(mapping) where every element of the domain(starting set) is mapped uniquely to an element of the codomain(resulting set), and every element in the codomain has exactly one corresponding element in the domain.

Definition 7. A **homomorphism** ϕ from a group G to a group $\overline{G}$ is a mapping that is operation-preserving, i.e.

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

Definition 8. An **isomorphism** ϕ from a group G to a group $\overline{G}$ is a bijective homomorphism from G to $\overline{G}$. If an isomorphism exists between two groups, we say they are isomorphic, denoted by $G \approx \overline{G}$.

Definition 9. The **kernel** of a homomorphism ϕ from a group G to another group with identity e is the set $\{a \in G \mid \phi(a) = e\}$, denoted as $\ker \phi$.

3.4.2 Examples

1. The mapping from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ for any natural number n is a homomorphism. $\phi(a) = a$ mod n. However, this is not an isomorphism because more than one element of $\mathbb{Z}$ maps to the same element in $\mathbb{Z}/n\mathbb{Z}$. The kernel is the set of all multiples of n, denoted $n\mathbb{Z}$.
2. The group $\mathbb{Z}/7\mathbb{Z}^{\times}$ under multiplication is isomorphic to $\mathbb{Z}/6\mathbb{Z}$ under addition. Consider the powers of 3 listed in section 3.3 and note that multiplying powers of 3 is the equivalence of adding the exponents. Therefore, an isomorphism $\mathbb{Z}/7\mathbb{Z}^{\times} \longmapsto \mathbb{Z}/6\mathbb{Z}$ is as follows:

$$\begin{aligned} 3^1 &\longmapsto 1 \\ 3^2 &\longmapsto 2 \\ 3^3 &\longmapsto 3 \\ 3^4 &\longmapsto 4 \\ 3^5 &\longmapsto 5 \\ 3^6 &\longmapsto 6 \end{aligned}$$

3.4.3 Theorems

Theorem 3.5. *A homomorphism ϕ carries the identity of G to the identity of $\overline{G}$.*

Proof. Let the identify of G be e and that of $\overline{G}$ be $\overline{e}$. For any $a \in G$,

$$\begin{aligned} \phi(a)\phi(e) &= \phi(ae), \\ \phi(a)\phi(e) &= \phi(a), \\ \phi(e) &= \overline{e}, \end{aligned}$$

by the definition of identity. □

Theorem 3.6. *Let ϕ be a homomorphism from G to $\overline{G}$. For any integer n and any $a \in G$, $\phi(a^n) = (\phi(a))^n$.*

Proof. This statement can be shown with mathematical induction. First, when $n = 1$, $\phi(a) = \phi(a)$, so the base case is true. For the inductive step, assume that $\phi(a^k) = (\phi(a))^k$. Then

$$\begin{aligned} \phi(a^k)\phi(a) &= (\phi(a))^k\phi(a), \\ \phi(a^k)\phi(a) &= (\phi(a))^{k+1}, \\ \phi(a^k a) = \phi(a^k)\phi(a) &= (\phi(a))^{k+1}, \\ \phi(a^k a) &= (\phi(a))^{k+1}, \\ \phi(a^{k+1}) &= (\phi(a))^{k+1}. \end{aligned}$$

Therefore, homomorphism preserves operation. □

3.5 Quotient Groups

So far, we have used the notation $\mathbb{Z}/6\,\mathbb{Z}$ with a division symbol to represent the integers mod 6. But what does this really mean?

3.5.1 Definitions

We begin by defining a coset.

Definition 10. Let G be a group and H be a nonempty subset of G. The left coset of H in G containing an element a is the set $aH = \{ah \mid h \in H\}$. Similarly, the right coset of H in G containing an element a is the set $Ha = \{ha \mid h \in H\}$. In both cases, a is called the *coset representative.* There can be multiple coset representatives for a coset, as we will see in the following example.

3.5.2 Examples

1. If we consider the integers $\mathbb{Z}$ and the set of integer multiples of 6 denoted by $6\,\mathbb{Z}$, then there are 6 possible cosets:

   - $0+6\,\mathbb{Z}$, the set of all integers equivalent to 0 mod 6. The coset representative here is 0, as we operated on each element of $6\,\mathbb{Z}$ with 0 on the left. However, the coset representative could also be 6, 12, 18, or any multiple of 6.
   - $1+6\,\mathbb{Z}$, the set of all integers equivalent to 1 mod 6. The coset representative here is 1, as we operated on each element of $6\,\mathbb{Z}$ with 1 on the left. However, the coset representative could also be 7, 13, 19, etc.
   - $2+6\,\mathbb{Z}$, the set of all integers equivalent to 2 mod 6. Similarly, the coset representative can be 2, 8, 14, or any integer equivalent to 2 mod 6.
   - $3+6\,\mathbb{Z}$, the set of all integers equivalent to 3 mod 6. Similarly, the coset representative can be 3, 9, 15, or any integer equivalent to 3 mod 6.
   - $4+6\,\mathbb{Z}$, the set of all integers equivalent to 4 mod 6. Similarly, the coset representative can be 4, 10, 16, or any integer equivalent to 4 mod 6.
   - $5+6\,\mathbb{Z}$, the set of all integers equivalent to 5 mod 6. Similarly, the coset representative can be 5, 11, 17, or any integer equivalent to 5 mod 6.

We see with Example 1 that we can divide $\mathbb{Z}$ into 6 infinite sets of integers that leave the same remainder when divided by 6.

Definition 11. A subgroup H of a group of G is a *normal subgroup* of G if $aH = Ha$ for all $a \in G$. In other words, the left and right cosets are the same set for all coset representatives chosen from G.

For groups where the operation is commutative (e.g. addition of integers), the following corollary follows naturally.

Corollary 3.7. *All subgroups of commutative groups are normal.*

It follows that the group $6\,\mathbb{Z}$ from Example 1 is a normal subgroup of $\mathbb{Z}$. But what is so special (or normal...) about normal subgroups? It happens that we can define a new group called the *quotient group*.

Definition 12. If H is a normal subgroup of a group G, the quotient group denoted by G/H is the group of all the left (or right) cosets. For every normal subgroup H, there always exists a corresponding quotient group. Note that if H is *not* a normal subgroup, then we cannot form a quotient group. In this case, the operation on cosets is no longer well-defined. Normality is crucial to ensure that, regardless of which element is chosen to represent a closet, the composition of two cosets would stay constant.

At long last, we can finally name the mysterious $\mathbb{Z}/6\,\mathbb{Z}$ as the quotient group of $\mathbb{Z}$ and its normal subgroup $6\,\mathbb{Z}$! This quotient group allows us to simplify the integers by considering each element as part of a coset, rather than as an individual element. For example, in modulo 6, we can simply consider large numbers such as 1297 and 355 as part of the coset $1 + 6\,\mathbb{Z}$, or the set of integers with remainder 1 when divided by 6. So if we ever need to calculate the remainder of $1297 + 355$ when divided by 6, we can just add the two cosets $(1 + 6\,\mathbb{Z}) + (1 + 6\,\mathbb{Z})$ to get a sum in the coset $2 + 6\,\mathbb{Z}$.

4 Rings

In this section, we will turn to the study of rings, algebraic structures similar to groups that include two operations on a set of elements instead of one. Beginning with basic definitions and examples, we will move on to explore ideals, which play a similar role as subgroups in group theory. Next, we will define homomorphisms again as they act on rings and finally end with quotient rings.

4.1 Definitions and Examples

4.1.1 Definitions

Definition 13. A **ring** R is a set with two operations, addition and multiplication that satisfies the following axioms:

1. Additive commutativity. $a + b = b + a$.

2. Additive associativity. $a + (b + c) = (a + b) + c$.

3. R contains additive identity 0, where $a + 0 = a$ for $a \in R$.

4. For every $a \in R$, there is an inverse $-a$ such that $a + (-a) = 0$.

5. Multiplicative associativity. $a(bc) = (ab)c$.

6. Distributive property. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Note that multiplication is not necessarily commutative. If it is in a ring R, R is a commutative ring. Also, a ring need not have a multiplicative identity; if it does, we call the identity the **unity**. An element needs not have a multiplicative inverse, and, if it does, it is a **unit**. Interestingly, rings without a multiplicative identity are called "rngs", with the missing "i" standing for "identity"!

4.1.2 Examples

1. The integers $\mathbb{Z}$ under regular addition and multiplication form a commutative ring. The additive identity is 0 and unity 1. The units are 1 and -1, each of which is its own inverse.
2. The set $\mathbb{Z}/n\mathbb{Z}$ under addition and multiplication mod n is a commutative ring with additive identity 0 and unity 1. The units are all numbers less than n and coprime with n.
3. The even integer, $2\mathbb{Z}$, is a commutative ring under regular addition and multiplication, but has no multiplicative identity.

4.1.3 Theorems

Theorem 4.1. *The additive identity in a ring is unique. The additive inverse of an element is unique. If unity and multiplicative inverses exist, they are also unique.*

This can be proven analogously to the proof for uniqueness of identity and inverses in groups in section 3.1.

4.2 Subrings

Similarly to subgroups within groups, we can define subrings within rings.

Definition 14. A subring S of a ring R is a ring such that all elements of S are also elements of R, and the operation is the same.

4.3 Ideals

Subrings are great, but not all of them are very ideal...
In this section, we will define a type of subring called an *ideal*.

4.3.1 Definitions

Definition 15. A subring A of a ring R is an *ideal* of ring R if for all $a \in A$ and all $r \in R$, both ar and ra belong to A.

Corollary 4.2. *By this definition, A is a normal subgroup of the group R under addition, since the left coset $aR = \{ar \mid r \in R\}$ and right coset $Ra = \{ra \mid r \in R\}$ are both equivalent to A.*

Some of the most straightforward examples include:

1. $2\,\mathbb{Z}$, or the set of all even integers, is an ideal of $\mathbb{Z}$ because multiplying an even integer with any other integer always results in an even product, which is in the ideal $2\,\mathbb{Z}$.
2. An even more straightforward example is the ring $\{0\}$ and the ring R itself. Multiplying any element in R with the element 0 results in 0, so for that reason $\{0\}$ is called the *trivial ideal*, and it is part of every ring. Similarly, multiplying any element in R with any element in the ideal R always results in an element in R by the closure property. Thus R is also an ideal of R, and since it is not very interesting, R itself is also called the *trivial ideal*.
3. Similar to the first example, the set of all polynomials with integer coefficients and an even constant term (e.g. x^2+3x+2, $69x^{13}+42$, etc.) is an ideal of $\mathbb{Z}[x]$, the set of all polynomials with integer coefficients. This is because multiplying a polynomial with an even constant term with any other polynomial always results in an even constant term of the resulting polynomial.

4.3.2 Prime ideals

Rings were originally made to mimic the integers. A very important part of the integers is the prime numbers. So naturally, mathematicians had to put the notion of primes somewhere in there.

In the regular integers, prime numbers are normally defined as any number that is only divisible by 1 and itself. However, they also have an alternative definition: given two integers x and y such that xy is divisible by a prime p, we must have that either x or y is divisible by p. The following definition of a *prime ideal* is modeled on the latter definition.

Definition 16. An ideal A is *prime* if for all $a, b \in R$, we have $ab \in A$ if and only if $a \in A$ or $b \in A$.

A natural example is the following:

1. The ring $n\,\mathbb{Z}$ denoting all integer multiples of an integer n is prime in the ring of integers $\mathbb{Z}$ if and only if n is a prime number.

Ideals in rings are essentially the normal subgroups in groups. We will see more of their properties in Section 4.5.

4.4 Ring Homomorphisms

Ideals are substructures in a ring that often has a structural correspondence with the greater ring. To address parallel structures like these, we will cover ring isomorphism and homomorphism as mappings between rings in this section.

4.4.1 Definitions

Definition 17. A **homomorphism** ϕ from a ring R to a ring $\overline{R}$ is a mapping that is operation-preserving, that is:

$$\phi(a) + \phi(b) = \phi(a+b) \text{ and } \phi(a)\phi(b) = \phi(ab).$$

Definition 18. An **isomorphism** ϕ from a ring R to a ring $\overline{R}$ is a bijective homomorphism.

4.4.2 Examples

1. The mapping from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ for any natural number n is a homomorphism. $\phi(a) = a$ mod n.
2. The mapping $a + bi \longmapsto a - bi$ is an isomorphism from the complex numbers $\mathbb{C}$ onto itself. It can be verified that this function is bijective and preserves operation.
3. $f(x) \longmapsto f(1)$ is a homomorphism between $\mathbb{R}[x]$, the set of all polynomials in terms of x with real coefficients, and $\mathbb{Z}$, the set of all real numbers. However, this is not a isomorphism, because more than one element in $f(x) \longmapsto f(1)$ can have the same value evaluated at 1 and map to the same real number. In other words, this mapping is subjective and not injective, with every element in the codomain corresponding to at least one element in the domain, but not the other way around.

4.4.3 Theorems

Properties similar to group homomorphism apply to ring homomorphism.

Theorem 4.3. *Let ϕ be a homomorphism from ring R to $\overline{R}$. Then* $\ker\phi = \{r \in R \mid \phi(r) = 0\}$ *is an ideal of R.*

Proof. By the ideal test, to show $\ker\phi$ is an ideal of R, we must first show closure. $a, b \in \ker\phi$ implies that $\phi(a) = \phi(b) = 0$. Then $\phi(a+b) = \phi(a) + \phi(b) = 0$, which means $a - b \in \ker\phi$. Then, it remains to show absorption. For all $a \in \ker\phi$, $\phi(a) = 0$, so $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$ for all $r \in R$. Thus $ar, ra \in \ker\phi$ for all $r \in R$. □

4.5 Quotient Rings

4.5.1 Definitions

Similar to quotient groups, we can define quotient rings. However, instead of using a normal subgroup, we use an ideal of the ring to generate the cosets.

Definition 19. Let A be a subring of R. The set of cosets $\{r + A \mid r \in R\}$ is a ring under addition and multiplication if and only if A is an ideal of R. Otherwise, the set of cosets is just a quotient group.

4.5.2 Examples

1. Our favorite quotient group $\mathbb{Z}\,/6\,\mathbb{Z}$ is also a quotient ring because $\mathbb{Z}$ is a ring under addition and multiplication, and $6\,\mathbb{Z}$ is its ideal. To see how addition and multiplication in $\mathbb{Z}\,/6\,\mathbb{Z}$ works, consider the following examples:

   $$(2+6\,\mathbb{Z})+(5+6\,\mathbb{Z})=7+6\,\mathbb{Z}=1+(6+6\,\mathbb{Z})=1+6\,\mathbb{Z}\,.$$

   $$(2+6\,\mathbb{Z})\cdot(5+6\,\mathbb{Z})=10+6\,\mathbb{Z}=4+(6+6\,\mathbb{Z})=4+6\,\mathbb{Z}\,.$$

   Note that this is essentially basic arithmetic in mod 6.

2. Another example is $\mathbb{Z}[x]/\langle x\rangle$, which represents the quotient of the ring of all polynomials with integer coefficients with the ideal of all polynomials that are a multiple of x (i.e. it has constant term 0). However, it might not be immediately obvious what the coset representatives look like. To simplify this issue, consider a polynomial $p(x)\in\mathbb{Z}[x]$. Since the ideal is $\langle x\rangle$, any two polynomials in the same coset will differ by a multiple of x. Therefore, each polynomial $p(x)$ in is equivalent to its constant term, since the difference between $p(x)$ and its constant term $p(0)$ is equal to some polynomial times x. Thus, the coset representatives are simply the set of all possible constant terms, which is just $\mathbb{Z}$. So $\mathbb{Z}[x]/\langle x\rangle$ is actually isomorphic to $\mathbb{Z}$, the ring of integers!

5 First Isomorphism Theorem

This section presents the application of previous concepts and definitions in the First Isomorphism Theorem, which draws connections between factor groups and homomorphism or holomorphic images.

5.1 Definition and Proof

Theorem 5.1 (First Isomorphism Theorem)**.** *Let ϕ be a group homomorphism from G to $\overline{R}$. Then the mapping from $G/\ker\phi$ to $\phi(G)$, where the coset $g\ker\phi$ maps to $\phi(g)$, is an isomorphism. i.e. $G/\ker\phi$ is isomorphic to $\phi(G)$.*

To prove the First Isomorphism Theorem, let's begin with a lemma:

Lemma 5.2. *Let H be a subgroup of group G, and a, b elements in G, then the coset $aH = bH$ if $a \in bH$.*

Proof. Given $a\in bH$, then a must be equal to bh for some element $h\in H$. Then

$$aH=(bh)H=b(hH).$$

Note that $hH=H$ because, by closure in H, $hh'\in H$ for any other element $h'\in H$. Thus

$$aH=b(hH)=bH.$$

□

Now, we suggest a proof of the First Isomorphism Theorem:

Proof. Let ψ be the mapping $g \ker \phi \longmapsto \phi(g)$.
It can be verified that ψ is operation-preserving by considering $\psi(x \ker \phi \cdot y \ker \phi)$

$$\psi(x \ker \phi \cdot y \ker \phi) = \psi(xy \ker \phi)$$

$$\psi(xy \ker \phi) = \phi(xy) \text{ by the definition of } \psi$$

$$\phi(xy) = \phi(x) \cdot \phi(y) \text{ due to the operation-preserving property of homomorphism } \phi$$

$$\phi(x) \cdot \phi(y) = \psi(x \ker \phi) \cdot \psi(y \ker \phi) \text{ by the definition of } \psi \text{ again.}$$

Therefore,

$$\psi(xker\phi \cdot y \ker \phi) = \psi(x \ker \phi) \cdot \psi(y \ker \phi)$$

Now that it has been shown that ψ is operation-preserving, it remains to confirm that ψ is one-to-one. In other words, $\phi(a) = \phi(b)$ if and only if $a \ker \phi = b \ker \phi$.

Let $\phi(a) = \phi(b)$, then

$$e = (\phi(b))^{-1}\phi(a) = \phi(b^{-1})\phi(a) = \phi(b^{-1}a)$$

Therefore, $b^{-1}a \in \ker \phi$ by the definition of kernel, so

$$a \in b \ker \phi$$

Now, it directly follows from 5.2 that $a \ker \phi = b \ker \phi$. Reversing this argument verifies that the converse is true. □

We will now look at some examples.

5.2 Examples

1. Let ϕ be a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$, where $\phi(x) = x \pmod{n}$. Then $\ker \phi$ is any multiple of n, which would be mapped to 0, denoted by $\langle n \rangle$. The First Isomorphism Theorem guarantees that $\mathbb{Z}/\langle n \rangle \approx \mathbb{Z}/n\mathbb{Z}$. Consider the example when $n = 3$:
   $\mathbb{Z}/\langle 3 \rangle = \{x + \langle 3 \rangle\}$, and $\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$. There exists an isomorphism ψ from $\mathbb{Z}/\langle 3 \rangle$ to $\mathbb{Z}/3\mathbb{Z}$ such that $\psi(x + \langle 3 \rangle) \longmapsto x (\text{mod } n)$.

2. Consider the homomorphism ϕ from an Abelian group G to G^k, where G^k is defined as the subgroup $x^k \mid x \in G$. Then $\ker \phi = \{x \in G \mid x^k = e\}$, denoted as $G^{(k)}$. It can be concluded that $G/G^{(k)} \approx G^k$.

6 Polynomial Rings

So far we have been dealing with mostly integers and numbers in our rings. However, we have also briefly seen in previous examples that we can construct rings with polynomials. In this section we explore some more properties of polynomial rings.

6.1 Example

In this section, we present an interesting example about the quotient ring $\mathbb{R}[x]/\langle x^2+1\rangle$. We show that $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to the ring $\mathbb{R}[\sqrt{-1}]$, which is how the ring of complex numbers $\mathbb{C}$ is defined. The ring $\mathbb{R}[x]$ corresponds to all polynomials with real coefficients, and $\mathbb{R}[\sqrt{-1}]$ corresponds to the ring of all complex numbers that are the evaluation of a real polynomial at $x=\sqrt{-1}$ under addition and multiplication. More simply, every element of $\mathbb{R}[-1]$ can be expressed as $a+b\sqrt{-1}$ for real coefficients a and b, so we use $\mathbb{R}[\sqrt{-1}]$ and $\mathbb{C}$ interchangeably.

First, let us gain a better understanding of the cosets. Consider a polynomial $p(x)\in\mathbb{R}[x]$. We can write $p(x)$ as follows:

$$p(x)=q(x)(x^2+1)+r(x),$$

where $(q(x),r(x))$ is the unique pair of real polynomials in $\mathbb{R}[x]$ such that the degree of $r(x)$ is one or less. It follows that $r(x)$ is either a linear polynomial or a constant term, which can be expressed as $ax+b$ for any real coefficients a and b. We know that $p(x)$ and $r(x)$ belong to the same coset, since they differ by a multiple of x^2+1. This is similar to how we can "reduce" an integer to its mod 6 remainder by subtracting multiples of 6, but in this case we subtract multiples of x^2+1 to "reduce" a polynomial to a linear or constant remainder polynomial. Therefore we can consider the set of all $r(x)$ as the coset representatives.

Now define the mapping ϕ as the evaluation at $x=\sqrt{-1}$. In order to verify that the mapping $\phi:\mathbb{R}[x]/\langle x^2+1\rangle\to\mathbb{R}[\sqrt{-1}]$ is indeed a isomorphism, we must first check the following two properties necessary for homomorphisms:

1. Addition is preserved: for all $a,b\in\mathbb{R}[x]/\langle x^2+1\rangle$, $\phi(a+b)=\phi(a)+\phi(b)$.

2. Multiplication is preserved: for all $a,b\in\mathbb{R}[x]/\langle x^2+1\rangle$, $\phi(ab)=\phi(a)\phi(b)$.

First, we show that for all $a,b\in\mathbb{R}[x]/\langle x^2+1\rangle$, we have $\phi(a+b)=\phi(a)+\phi(b)$. Let the first element a be a coset with coset representative $p(x)$, and let the second element b be a coset with coset representative $q(x)$. The choice of the coset representative does not matter because any difference that is a multiple of x^2+1 evaluates to 0 when we plug in $x=\sqrt{-1}$. Then

$$\phi(a+b)=\phi(p(x)+q(x))=p(\sqrt{-1})+q(\sqrt{-1})=\phi(p(x))+\phi(q(x))=\phi(a)+\phi(b),$$

as desired. So addition is preserved.

Next, we show that for all $a,b\in\mathbb{R}[x]/\langle x^2+1\rangle$, we have $\phi(ab)=\phi(a)\phi(b)$. We define $p(x)$ and $q(x)$ as coset representatives to cosets a and b similarly to before. Then

$$\phi(ab)=\phi(p(x)q(x))=p(\sqrt{-1})q(\sqrt{-1})=\phi(p(x))\phi(q(x))=\phi(a)\phi(b),$$

as desired. So multiplication is also preserved, and ϕ is officially a homomorphism!

Now to prove that the homomorphism ϕ is an isomorphism, we turn to the First Isomorphism Theorem in Section 5, which states that for any homomorphism ϕ that maps a ring G to $\phi(G)$, the quotient ring $G/\ker\phi$ is isomorphic to $\phi(G)$. We would like to show that $G/\ker\phi$ is $\mathbb{R}[x]/\langle x^2+1\rangle$ and $\phi(G)$ is $\mathbb{R}[\sqrt{-1}]$ so that we can apply the First Isomorphism Theorem.

First, we show that $G/\ker\phi$ is $\mathbb{R}[x]/\langle x^2+1\rangle$. Let G be the ring $\mathbb{R}[x]$. The kernel of ϕ is $\langle x^2+1\rangle$ since any real polynomial that evaluates to 0 when $x=\sqrt{-1}$ must be a multiple of x^2+1, the smallest real polynomial that has $\sqrt{-1}$ as a factor. So $G/\ker\phi$ is indeed $\mathbb{R}[x]/\langle x^2+1\rangle$.

Next, we know that $\phi(G)$ is $\mathbb{R}[\sqrt{-1}]$ since $\phi(G)$ is the ring of all elements $g \in G$ evaluated at $x=\sqrt{-1}$, which is defined by the ring $\mathbb{R}[\sqrt{-1}]$.

So by the First Isomorphism Theorem, we know that ϕ is an isomorphism that sends $\mathbb{R}[x]/\ker\phi = \mathbb{R}[x]/\langle x^2+1\rangle$ to $\phi(\mathbb{R}[x]) = \mathbb{R}[\sqrt{-1}]$.

Thus we have shown that $\mathbb{R}[x]/\langle x^2+1\rangle$ is isomorphic to $\mathbb{C}$. This unexpected relationship is one of many interesting results in group theory that the First Isomorphism Theorem can help demonstrate.

References

[1] Joseph A. Gallian. *Contemporary Abstract Algebra*. Brooks/Cole, 2010.

[2] Israel Kleiner. “A History of Abstract Algebra”. 2007.

[3] Edmund Robertson and John J. O’Connor. *Abstract Groups*. MacTutor History of Mathematics Archive: University of St. Adrews.