“Homomorphisms and Isomorphisms in Abstract Algebra: Structure, Properties and Applications”

Dissertation submitted to the Department of Mathematics in partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

Submitted By:

Pankaj Bonia

Roll No: MAT-06/23

Registration No: MSSV-0023-101-001354

Department of Mathematics MSSV, Nagaon

Under The Guidance:

Dr. Raju Bordoloi, HOD

Department of Mathematics, MSSV, Nagaon

Mahapurusha Srimanta Sankaradeva Viswavidyalaya

Department of Mathematics

DISSERTATION

on

"Homomorphisms and Isomorphisms in Abstract Algebra: Structure, Properties and Applications"

Submitted in partial fulfillment of the requirements
for M.Sc in Mathematics
Masters of science

Submitted by:
Pankaj Bonia
Roll No.: MAT-06/23
Registration No.: MSSV-0023-101-001354
Session: 2023–2025

Under the supervision of:
Dr. Raju Bordoloi
HOD, Department of Mathematics MSSV, Nagaon

July 2025

Certificate

This is to certify that the dissertation entitled **"Homomorphisms and Isomorphisms in Abstract Algebra: Structure, Properties and Applications"**, submitted by **Pankaj Bonia**, Roll No. **MAT-06/23**, Registration No. **MSSV-0023-101-001354**, in partial fulfillment for **M.Sc in Mathematics**, is a bonafide record of original work carried out under my supervision and guidance.

To the best of my knowledge, the work has not been submitted earlier to any other institution for the award of any degree or diploma.

Dr. Raju Bordoloi
HOD
Department of Mathematics
MSSV, Nagaon

Date: Signature of Guide
Place:

Declaration

I, **Pankaj Bonia**, hereby declare that the dissertation titled **"Homomorphisms and Isomorphisms in Abstract Algebra: Structure, Properties and Applications"**, submitted to the Department of Mathematics, **Mahapurusha Srimanta Sankaradeva Viswavidyalaya**, is a record of original work carried out by me under the supervision of **Dr. Raju Bordoloi**, HOD of Department of Mathematics.

This work has not been submitted earlier to any other institution or university for the award of any degree or diploma.

Place: Pankaj Bonia
Date: Roll No.: MAT-06/23

Acknowledgment

First and foremost, I would like to express my sincere gratitude to my guide, **Dr. Raju Bordoloi**, HOD, Department of Mathematics,Mahapurusha Srimanta Sankaradeva Viswavidyalaya, Nagaon, for his valuable guidance, continuous support, and encouragement throughout the course of this dissertation.

I also extend my heartfelt thanks to the faculty members of the Department of Mathematics for their constant academic support and the friendly learning environment they provided.

I am deeply grateful to my family and friends for their unwavering moral support and motivation throughout my academic journey. Their encouragement gave me the strength to successfully complete this work.

Lastly, I thank all those who directly or indirectly helped me during this project.

Place: Pankaj Bonia
Date: Roll No.: MAT-06/23

Table of Contents

Chapter 1

Introduction

Abstract Algebra is a fundamental area of mathematics that focuses on the study of algebraic structures such as groups, rings, and fields. These structures provide a framework for understanding various mathematical systems that appear across pure and applied mathematics.

One of the central ideas in abstract algebra is that of **structure-preserving mappings**, which allow us to compare and connect different algebraic systems. These mappings are known as **homomorphisms** and, in more specific cases, **isomorphisms**. Homomorphisms provide a way to map one algebraic structure to another while preserving operations, while isomorphisms are special kind of homomorphism that are bijective, indicating that the two structures are essentially the same, differing only in the names of their elements.

Motivation

Understanding homomorphisms and isomorphisms is crucial for analyzing the deeper properties of algebraic systems. They are the fundamental concept of algebra that help revealing how different mathematical objects are related, classify structures up to equivalence, and simplify complex systems by breaking them down into understandable parts.

These concepts are not just theoretical, they have widespread applications in computer science, physics, cryptography, and coding theory.

Objectives of the Study

The main objectives of this dissertation are:

- To define, understand and explore the concepts of homomorphism and isomorphism in various algebraic structures.

- To explore and examine the properties, types, and key theorems associated with these mappings.
- To examine how these concepts are applied in algebra and beyond.
- To highlight the structural differences and similarities between homomorphisms and isomorphisms.

Structure of the Dissertation

This dissertation is organized into the following chapters:

- **Chapter 1: Introduction** – Overview, motivation, and structure of the dissertation.
- **Chapter 2: Preliminaries** – Fundamental concepts of sets, binary operations, and algebraic structures.
- **Chapter 3: Homomorphisms** – Definitions, types, properties, and the Fundamental Homomorphism Theorem.
- **Chapter 4: Isomorphisms** – Definitions, examples, structural implications, and classification.
- **Chapter 5: Applications** – Practical relevance in mathematics and real-world domains.
- **Chapter 6: Comparative Study** – Key differences and connections between homomorphisms and isomorphisms.
- **Chapter 7: Case Studies and Worked Examples** – Illustrative examples and step-by-step verifications.
- **Chapter 8: Conclusion and Future Work** – Summary and scope for further research.

Chapter 2

Preliminaries

This chapter focuses on the basic concepts and algebraic structures that are crucial for understanding homomorphisms and isomorphisms. These definitions and properties form the framework for analyzing the structures and mappings of abstract algebra.

2.1 Sets and Binary Operations

A **set** is a well-defined collection of distinct elements. In algebra, we often define operations on sets.

Binary operation: A binary operation on a set S is a function that takes two elements from S and returns a single element that is also in S. i.e.,

$$* : S \times S \to S$$

that assigns to each pair $(a, b) \in S \times S$ an element $a * b \in S$.

Examples of binary operations include the addition and multiplication on $\mathbb{Z}$, the set of integers.

2.2 Groups

A **group** is a set G equipped with a binary operation $*$ satisfying the following properties:

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

2. **Associativity:** For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

3. **Identity element:** There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

4. **Inverse element:** For every $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

If a group also satisfies:

$$a * b = b * a \quad \forall a, b \in G$$

then it is called an **Abelian group**.

Example: $(\mathbb{Z}, +)$ is an Abelian group.

2.3 Rings

A **ring** is a set R equipped with two binary operations: addition $(+)$ and multiplication $(\cdot)$, such that:

- $(R, +)$ is an Abelian group.
- $(R, \cdot)$ is a semigroup (associative multiplication).
- Multiplication is distributive over addition:

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

  for all $a, b, c \in R$.

Example: $(\mathbb{Z}, +, \cdot)$ is a ring.

2.4 Fields

A **field** is a ring F in which:

- $(F, +)$ is an Abelian group.
- $(F \setminus \{0\}, \cdot)$ is an Abelian group.
- Multiplication is distributive over addition.

Example: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are all fields.

2.5 Substructures

- A **subgroup** H of a group G is a subset of G that forms a group under the same operation.
- A **subring** of a ring R is a subset that is itself a ring.
- A **subfield** is a subset of a field that is also a field under the same operations.

These substructures are important for defining homomorphisms and analyzing how structure is preserved under mappings.

Chapter 3

Homomorphisms

Homomorphisms are fundamental in abstract algebra because they allow us to relate different algebraic structures in a way that respects their operations. They capture the idea of *structure preservation*, which helps in classifying and understanding algebraic objects such as groups, rings, and fields.

3.1 Definition and Intuition

Let $(A, *)$ and $(B, \circ)$ be two algebraic structures. A function $f : A \to B$ is called a **homomorphism** if:

$$f(a_1 * a_2) = f(a_1) \circ f(a_2), \quad \forall a_1, a_2 \in A$$

Remark 3.1. This condition ensures that the operation in A maps to the corresponding operation in B without breaking the algebraic structure. Homomorphisms can be thought of as "translations" that preserve the essential behavior of the elements.

3.2 Group Homomorphism

Let $(G, \cdot)$ and $(H, *)$ be groups. A function $f : G \to H$ is a **group homomorphism** if:

$$f(x \cdot y) = f(x) * f(y), \quad \forall x, y \in G$$

Example 1: Identity Homomorphism

Let $f : G \to G$ be defined by $f(x) = x$. This is trivially a homomorphism.

Example 2: Modulo Homomorphism

Let $f : \mathbb{Z} \to \mathbb{Z}_6$ be defined as $f(a) = a \mod 6$. Then:

$$f(a+b) = (a+b) \mod 6 = (a \mod 6 + b \mod 6) \mod 6 = f(a) +_6 f(b)$$

Hence, f is a group homomorphism.

3.3 Kernel and Image

For a group homomorphism $f : G \to H$:

- The **kernel** of f is:
  $$\ker(f) = \{g \in G \mid f(g) = e_H\}$$
  where e_H is the identity in H.
- The **image** of f is:
  $$\text{Im}(f) = \{f(g) \in H \mid g \in G\}$$

Remark 3.2. The kernel tells us "what collapses to identity" under the homomorphism, while the image tells us "what is covered" in the codomain.

Example 3:

For $f : \mathbb{Z} \to \mathbb{Z}_6$, $f(a) = a \mod 6$:

$$\ker(f) = \{a \in \mathbb{Z} \mid a \equiv 0 \mod 6\} = 6\mathbb{Z}$$

$$\text{Im}(f) = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$$

3.4 Ring Homomorphisms

Let $(R, +, \cdot)$ and $(S, \oplus, \otimes)$ be rings. A function $f : R \to S$ is a **ring homomorphism** if:

$$f(a+b) = f(a) \oplus f(b), \quad f(a \cdot b) = f(a) \otimes f(b)$$

Example 4: Polynomial Ring Homomorphism

Define $f : \mathbb{Z}[x] \to \mathbb{Z}_3[x]$ by reducing all coefficients modulo 3.

$$f(2x^2 + 5x + 4) = 2x^2 + 2x + 1$$

This map respects addition and multiplication, hence it is a ring homomorphism.

3.5 Field Homomorphisms

A **field homomorphism** $f : F \to K$ satisfies:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad f(1) = 1$$

Note: Nonzero field homomorphisms are always injective due to the lack of non-trivial ideals in fields.

Example 5:

Let $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(x) = x$ is the identity field homomorphism. It's clearly structure-preserving.

3.6 Properties of Homomorphisms

- $\ker(f)$ is always a normal subgroup of G.
- $\operatorname{Im}(f)$ is a subgroup (or subring, etc.) of H.
- f is injective if and only if $\ker(f) = \{e_G\}$.

Remark 3.3. This injectivity condition gives a powerful way to check whether the structure is faithfully preserved.

3.7 Fundamental Theorem of Homomorphisms

Let $f : G \to H$ be a group homomorphism. Then:

$$G/\ker(f) \cong \operatorname{Im}(f)$$

Sketch of Proof. Define $\phi : G/\ker(f) \to \operatorname{Im}(f)$ by $\phi(g\ker(f)) = f(g)$. This is well-defined, a homomorphism, and bijective.

Therefore, the quotient group $G/\ker(f)$ is isomorphic to the image of f. □

3.8 Further Examples and Applications of Homomorphisms

In this section, we explore additional examples and counterexamples of homomorphisms, solve small problems, and highlight some applications of the concept in broader mathematics and real-world systems.

3.8.1 More Examples of Homomorphisms

Example 3.4. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be defined by $\phi(n) = 2n$. Then for all $a, b \in \mathbb{Z}$,

$$\phi(a+b) = 2(a+b) = 2a + 2b = \phi(a) + \phi(b),$$

so ϕ is a homomorphism. It is injective, but not surjective since odd integers are not in the image.

Example 3.5. Define $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(x) = 0$ for all $x \in \mathbb{R}$. Then:

$$\phi(x+y) = 0 = 0 + 0 = \phi(x) + \phi(y).$$

This is a homomorphism, though it is neither injective nor surjective. The kernel is all of $\mathbb{R}$, and the image is just $\{0\}$.

3.8.2 A Non-Example

Example 3.6. Let $\phi : \mathbb{R} \to \mathbb{R}$ be defined by $\phi(x) = x^2$. This is **not** a group homomorphism from $(\mathbb{R}, +)$ to itself because:

$$\phi(x+y) = (x+y)^2 \neq x^2 + y^2 = \phi(x) + \phi(y) \text{ in general.}$$

3.8.3 Worked Problems

Example 3.7. Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_3$ be defined by $\phi([a]_6) = [a]_3$. Show that this is a group homomorphism and compute its kernel and image.

Solution: This is well-defined and operation preserving:

$$\phi([a+b]_6) = [a+b]_3 = [a]_3 + [b]_3 = \phi([a]_6) + \phi([b]_6).$$

So it's a homomorphism. The kernel is:

$$\ker(\phi) = \{[0]_6, [3]_6\}, \quad \text{and} \quad \mathrm{Im}(\phi) = \mathbb{Z}_3.$$

Example 3.8. Let $\phi : \mathbb{Z} \to \mathbb{Z}_5$ be given by $\phi(n) = [2n]_5$. Is ϕ a homomorphism?

Solution: Yes, because:

$$\phi(a+b) = [2(a+b)]_5 = [2a+2b]_5 = [2a]_5 + [2b]_5 = \phi(a) + \phi(b).$$

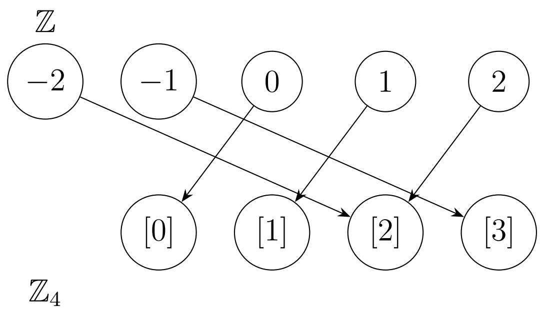


Figure 3.1: Homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_4$ defined by $\phi(n) = n \mod 4$

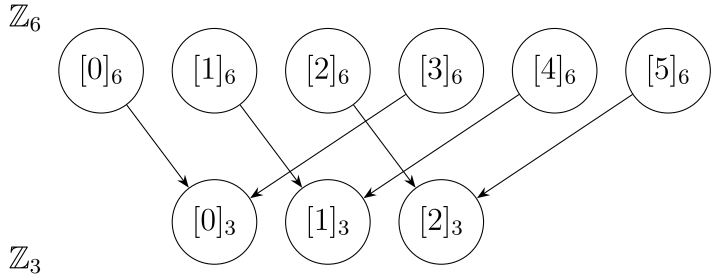


Figure 3.2: Homomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_3$ with nontrivial kernel $\{[0], [3]\}$

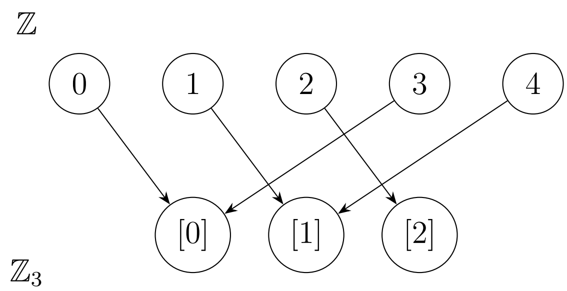


Figure 3.3: Surjective homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_3$

Example 3.9.

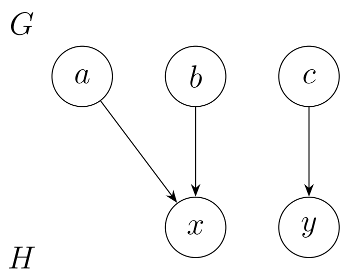


Figure 3.4: Homomorphism $\phi : G \to H$ that is not injective

3.8.4 Applications of Homomorphisms

Homomorphisms allow us to:

- Construct quotient groups and understand their structure.
- Classify finite groups up to isomorphism using kernels and images.
- Model symmetry in physics and computer science.
- Encrypt and encode information in cryptography by mapping structures.

Remark 3.10. Homomorphisms are the foundation of many abstract concepts in mathematics, including category theory and module theory, and appear in algebraic topology, algebraic geometry, and number theory.

3.9 Conclusion

Homomorphisms provide a way to understand the structural behavior of algebraic systems. The concepts of kernel and image are crucial to studying how much structure is preserved or collapsed. it preserve the structure of the operations. These ideas lead naturally to the study of isomorphisms and classification of structures, which we explore in the next chapter.

Chapter 4

Isomorphisms

An **isomorphism** is a special type of homomorphism that is both one-to-one (injective) and onto (surjective). If two algebraic structures are isomorphic, they are essentially the same in structure, even if their elements look different.

4.1 Definition of Isomorphism

Definition 4.1. Let $(G, *)$ and $(H, \cdot)$ be two groups. A function $\phi : G \to H$ is called an **isomorphism** if:

- ϕ is a group homomorphism: $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G$, and
- ϕ is bijective (i.e., one-to-one and onto).

If such a ϕ exists, we say that G and H are **isomorphic**, and we write $G \cong H$.

Remark 4.2. Isomorphic groups have the same algebraic structure. Properties like being abelian, cyclic, or order of elements are preserved.

4.2 Examples of Isomorphic Groups

Example 4.3. The group $(\mathbb{R}^+, \times)$ of positive real numbers under multiplication is isomorphic to the group $(\mathbb{R}, +)$ under addition via the logarithmic map:

$$\phi(x) = \log(x)$$

with inverse $\phi^{-1}(y) = 10^y$ (or e^y in natural log).

Example 4.4. The group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition modulo 4 is isomorphic to the group $\{1, i, -1, -i\} \subset \mathbb{C}$ under multiplication.

4.3 Properties Preserved Under Isomorphism

Theorem 4.5. *Let G and H be groups such that $G \cong H$. Then:*

- *G is abelian if and only if H is abelian.*
- *G is cyclic if and only if H is cyclic.*
- *The order of G equals the order of H.*
- *The number of elements of a given order is the same in G and H.*

Proof. Follows from the fact that isomorphisms are bijective and operation-preserving. □

4.4 Cyclic Group Classification via Isomorphism

Theorem 4.6. *Every finite cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n$.*

Proof. Let $G = \langle g \rangle$ be a finite cyclic group of order n. Define $\phi : \mathbb{Z}_n \to G$ by $\phi(k) = g^k$. This is a well-defined isomorphism. □

4.5 Automorphisms

Definition 4.7. An **automorphism** is an isomorphism from a group G to itself. That is, $\phi : G \to G$ is an automorphism if it is bijective and operation-preserving.

Example 4.8. Let $G = \mathbb{Z}$. Define $\phi(n) = -n$. This is an automorphism of $\mathbb{Z}$.

Remark 4.9. The set of all automorphisms of a group G, denoted $\mathrm{Aut}(G)$, forms a group under composition of functions.

4.6 Further Examples and Applications of Isomorphisms

This section explores additional examples of isomorphisms, demonstrates cases that are not isomorphisms, and provides insight into their importance in mathematical reasoning and structure.

4.6.1 More Examples of Isomorphisms

Example 4.10. Let $\phi : (\mathbb{Z}, +) \to (2\mathbb{Z}, +)$ be defined by $\phi(n) = 2n$. This is an injective and surjective homomorphism:

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b),$$

and for every $m \in 2\mathbb{Z}$, there exists $n = \frac{m}{2} \in \mathbb{Z}$ such that $\phi(n) = m$. Thus, ϕ is an isomorphism.

Example 4.11. The additive group $(\mathbb{R}, +)$ and the multiplicative group $(\mathbb{R}^+, \times)$ are isomorphic via:

$$\phi(x) = e^x \quad \text{with inverse} \quad \phi^{-1}(y) = \ln(y).$$

It preserves the operation: $\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x)\phi(y)$.

4.6.2 Non-Examples (Not Isomorphisms)

Example 4.12. Let $\phi : \mathbb{Z} \to \mathbb{Z}$ be defined by $\phi(n) = 0$. Although this is a homomorphism, it is neither injective nor surjective. Hence, ϕ is not an isomorphism.

Example 4.13. Let $\phi : \mathbb{R} \to \mathbb{R}$ be defined by $\phi(x) = x^3$. This is bijective, but not an isomorphism if considered from $(\mathbb{R}, +)$ to $(\mathbb{R}, \times)$, because it does not preserve the group operation. For example:

$$\phi(x + y) = (x + y)^3 \neq x^3 + y^3 = \phi(x) + \phi(y).$$

So it's not an isomorphism between these group structures.

4.6.3 Worked Problems

Example 4.14. Let $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ be defined by $\phi([a]_5) = [2a]_5$. Is ϕ an isomorphism?

Solution: It is a homomorphism: $\phi([a + b]) = [2(a + b)] = [2a + 2b] = \phi([a]) + \phi([b])$. It is injective: $\phi([a]) = \phi([b]) \Rightarrow [2a] = [2b] \Rightarrow [a] = [b]$ (since 2 has inverse mod 5). It is surjective as ϕ maps to all elements of $\mathbb{Z}_5$. So ϕ is an isomorphism.

Example 4.15. Let $\phi : \mathbb{R} \to \mathbb{R}$ be defined by $\phi(x) = 3x + 1$. Is ϕ an isomorphism of $(\mathbb{R}, +)$?

Solution: No. Although ϕ is bijective, it is not a homomorphism because:

$$\phi(x + y) = 3(x + y) + 1 = 3x + 3y + 1,$$

but $\phi(x) + \phi(y) = (3x + 1) + (3y + 1) = 3x + 3y + 2 \neq \phi(x + y)$. Not an isomorphism.

4.6.4 Isomorphism Diagrams

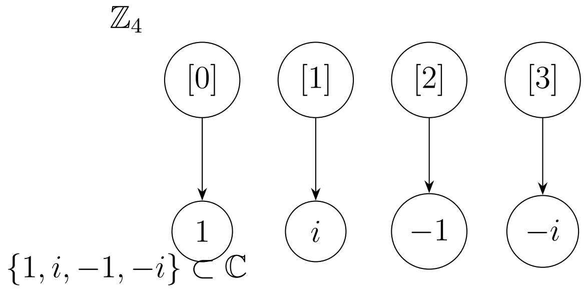


Figure 4.1: An isomorphism from $(\mathbb{Z}_4, +)$ to the 4th roots of unity under multiplication

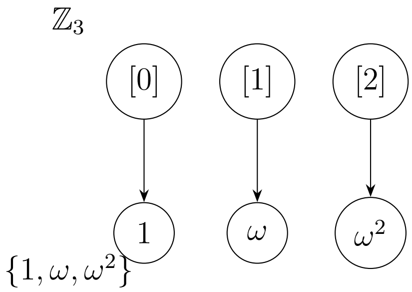


Figure 4.2: Isomorphism between $(\mathbb{Z}_3, +)$ and $\{1, \omega, \omega^2\} \subset \mathbb{C}$ under multiplication

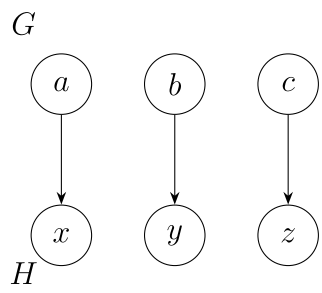


Figure 4.3: Abstract isomorphism $\phi : G \to H$ preserving structure bijectively

4.6.5 Applications of Isomorphisms

- Isomorphisms are used to classify groups: two isomorphic groups are structurally the same.
- In physics, isomorphisms help relate symmetry groups of molecules or crystal structures.
- In algebraic coding theory, structures like $\mathbb{Z}_n$ and vector spaces are mapped via isomorphisms to simplify computations.
- Computer algebra systems often reduce problems by replacing structures with isomorphic, simpler ones.

Remark 4.16. If $G \cong H$, then any theorem about G also holds for H. Studying abstract properties through isomorphism avoids redundancy.

Chapter 5

Applications of Homomorphisms and Isomorphisms

Homomorphisms and isomorphisms are not only central to the structure of abstract algebra but also serve as bridges to numerous applications within and beyond pure mathematics. Their importance lies in their ability to preserve algebraic structure, enabling deep insights into the behavior of algebraic systems through simplified or equivalent models.

5.1 Applications in Group Theory

5.1.1 Structure Classification

Group isomorphisms allow for the classification of groups up to structural similarity. Two isomorphic groups are considered "essentially the same" from an algebraic standpoint.

Theorem 5.1 (Cyclic Group Classification). *Every finite cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n$.*

Example 5.2. Let $G = \langle a \rangle$ be a cyclic group of order 4. Then $G \cong \mathbb{Z}_4$, as the mapping $\phi(a^k) = [k]_4$ defines an isomorphism.

5.1.2 Cayley's Theorem

Theorem 5.3 (Cayley's Theorem). *Every group G is isomorphic to a subgroup of the symmetric group Sym(G).*

Idea of Proof. Define $\phi : G \to \mathrm{Sym}(G)$ by $\phi(g)(x) = gx$, the left multiplication map. This mapping is injective and preserves group operation:

$$\phi(g_1 g_2)(x) = g_1 g_2 x = \phi(g_1)(\phi(g_2)(x)).$$

Thus, ϕ is an embedding of G into $\mathrm{Sym}(G)$. □

Remark 5.4. Cayley's Theorem shows that every abstract group can be viewed as a group of permutations.

5.2 Applications in Ring Theory

5.2.1 Quotient Rings and Homomorphisms

Ring homomorphisms naturally lead to the concept of quotient rings.

Theorem 5.5. *Let $\phi : R \to S$ be a surjective ring homomorphism with kernel K. Then $R/K \cong S$.*

Example 5.6. Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(a) = [a]_n$. Then $\ker(\phi) = n\mathbb{Z}$, and $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

5.3 Applications in Field Theory

5.3.1 Field Extensions and Automorphisms

In field theory, homomorphisms that are bijective are isomorphisms and are especially important in understanding algebraic extensions and Galois theory.

Definition 5.7. A field automorphism is an isomorphism from a field to itself. The set of all automorphisms of a field F forms a group under composition, denoted $\mathrm{Aut}(F)$.

Example 5.8. The complex conjugation map $\phi(a + bi) = a - bi$ is an automorphism of the field $\mathbb{C}$.

5.4 Applications in Linear Algebra and Modules

Linear transformations are homomorphisms between vector spaces. An isomorphism between vector spaces implies structural equivalence (same dimension over the same field).

Example 5.9. Let $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T(x, y) = (x + y, x - y)$. This transformation is linear, bijective, and hence a vector space isomorphism.

5.5 Applications in Cryptography

Many cryptographic protocols utilize the algebraic properties of groups and rings, especially their homomorphic characteristics.

5.5.1 RSA and Group Homomorphism

In RSA, the mapping:

$$\phi(m) = m^e \mod n$$

is a homomorphism from the multiplicative group $\mathbb{Z}_n^*$ to itself under modular exponentiation. The security of RSA is based on the difficulty of computing the inverse homomorphism (decryption) without knowing the factorization of n.

Remark 5.10. Though RSA is not a full isomorphism due to lack of bijection without the private key, its homomorphic structure is what enables secure computation.

5.6 Applications in Symmetry and Physics

Groups are used to model physical symmetries. For example, the symmetry group of a regular polygon is a dihedral group.

Example 5.11. The symmetry group of a square is isomorphic to the dihedral group D_4. Each rotation and reflection corresponds to a group element, and their composition mirrors group multiplication.

Remark 5.12. Group isomorphisms in this context allow mathematicians and physicists to abstract physical symmetries into algebraic operations for easier analysis.

5.7 Summary

The concepts of homomorphism and isomorphism are deeply embedded in the study of algebraic structures. From abstract theory to cryptographic applications and symmetry in nature, these mappings offer the language to compare, classify, and compute across mathematical domains.

Chapter 6

Comparative Study of Homomorphisms and Isomorphisms

Homomorphisms and isomorphisms are both structure-preserving mappings between algebraic systems, but they serve very different roles in mathematics. This chapter explores their similarities, differences, and deeper interpretations to gain a comprehensive understanding of these foundational concepts.

6.1 Foundational Definitions and Properties

Definition 6.1. A **homomorphism** between two algebraic structures is a function that preserves the relevant operations. For groups, a function $\phi : G \to H$ is a homomorphism if:

$$\phi(ab) = \phi(a)\phi(b), \quad \forall a, b \in G.$$

Definition 6.2. An **isomorphism** is a bijective homomorphism. That is, $\phi : G \to H$ is an isomorphism if it is a homomorphism and also a bijection.

Basic Summary Table

Feature	Homomorphism	Isomorphism
Operation preservation	Yes	Yes
One-to-one (injective)?	Not necessarily	Yes
Onto (surjective)?	Not necessarily	Yes
Has inverse?	Not always	Yes, and it is also a homomorphism
Structural equivalence?	No	Yes

6.2 Visual Interpretation and Intuition

A homomorphism can be imagined as a "shadow" projection — it transfers structure but may collapse or compress parts of it. An isomorphism, on the other hand, is like a perfect translation: nothing is lost, and every detail of the structure is preserved.

Example 6.3. Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\phi(a) = [a]_n$. This is a homomorphism but not an isomorphism, as it is not injective (many integers map to the same residue class).

Example 6.4. The mapping $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$ defined by $\phi([a]) = [3a]_4$ is an isomorphism, as it is bijective and preserves addition modulo 4.

6.3 Philosophical and Structural Significance

Homomorphism as a "Structure Observer"

A homomorphism respects structure — but not identity. It shows that certain behaviors are preserved under transformation, even if the structures are not identical.

Isomorphism as "Structural Sameness"

When two algebraic objects are isomorphic, they are not just similar — they are essentially the same. Isomorphism is the mathematical expression of "different forms, same essence".

Category Theory Viewpoint

In category theory, homomorphisms are called morphisms. Isomorphisms are special morphisms that have inverses. From this viewpoint:

- **Homomorphisms** = arrows that preserve operations. - **Isomorphisms** = reversible arrows → the objects they connect are indistinguishable in the category.

6.4 Implications in Algebraic Studies

6.4.1 Classification of Structures

Isomorphisms help classify algebraic structures by grouping them into equivalence classes. For example:

$$\text{All groups of prime order } p \cong \mathbb{Z}_p.$$

Homomorphisms, on the other hand, help analyze internal structure — such as kernels and images — and lead to important results like:

- The First Isomorphism Theorem
- Decomposition of modules and vector spaces
- Quotient groups and rings

6.5 Real-World and Cross-Disciplinary Analogies

Language Analogy

A homomorphism is like translating the grammar of a sentence correctly, but not necessarily every word. An isomorphism is a perfect translation — every word and its role are preserved.

Software Analogy

- Homomorphism: Copying the behavior of a system (e.g., an app's backend logic) but not its UI or exact state. - Isomorphism: A perfect software clone, identical in logic and appearance.

6.6 The Fine Line Between Homomorphism and Isomorphism

The distinction often lies in the **bijectivity** of the mapping. Many homomorphisms can become isomorphisms when restricted to image sets or quotient structures. For instance:

$$\phi : G \to \phi(G) \quad \text{is an isomorphism if } \ker(\phi) = \{e\}.$$

Worked-Out Problem

Problem: Let $\phi : \mathbb{Z} \to \mathbb{Z}_6$ be defined by $\phi(n) = [n]_6$. Determine whether ϕ is a homomorphism, isomorphism, or neither.

Solution:

We check each condition:

- $\phi(m + n) = [m + n]_6 = [m]_6 + [n]_6 = \phi(m) + \phi(n)$ for all $m, n \in \mathbb{Z}$. So ϕ preserves addition.

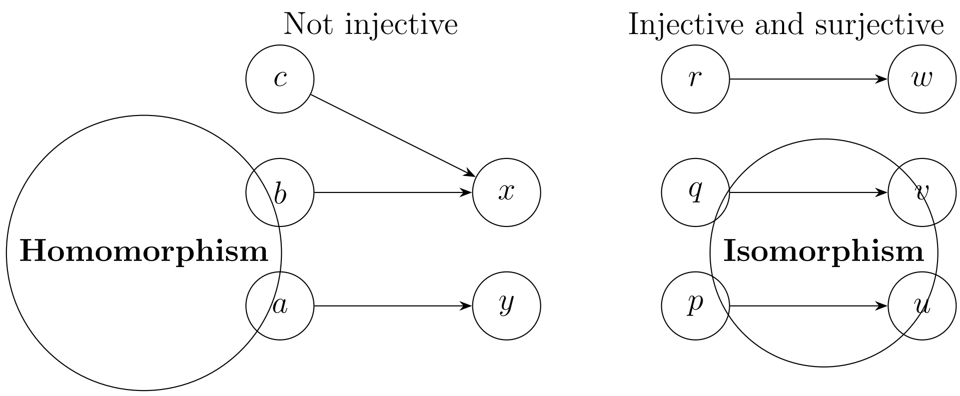


Figure 6.1: Homomorphism vs Isomorphism: Structure compression vs perfect structure preservation

- Hence, ϕ is a group homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_6, +)$.
- However, ϕ is not injective: $\phi(0) = \phi(6) = [0]_6$.
- It is not surjective either: e.g., elements of $\mathbb{Z}_6$ like $[1]_6$ are not unique images since infinitely many integers map to them.

Conclusion: ϕ is a homomorphism but not an isomorphism.

6.7 Summary

While all isomorphisms are homomorphisms, not all homomorphisms are isomorphisms. The study of their differences is more than just technical — it is foundational to understanding structure, classification, transformation, and equivalence in algebra and beyond.

Chapter 7

Case Studies and Key Theorems

7.1 Case Study 1: Group Homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$

Let us consider the homomorphism:

$$\phi : \mathbb{Z} \to \mathbb{Z}_n, \quad \phi(a) = [a]_n.$$

Here, $\mathbb{Z}$ is the additive group of integers and $\mathbb{Z}_n$ is the additive group of integers modulo n.

Homomorphism Check

We verify that ϕ is a homomorphism:

$$\phi(a + b) = [a + b]_n = [a]_n + [b]_n = \phi(a) + \phi(b).$$

Hence, ϕ preserves addition.

Kernel and Image

- **Kernel:** The kernel of ϕ is the set of all integers that map to $[0]_n$:

$$\ker(\phi) = \{a \in \mathbb{Z} \mid [a]_n = [0]_n\} = n\mathbb{Z}.$$

- **Image:** Since ϕ maps every integer to its equivalence class modulo n, the image is:

$$\mathrm{Im}(\phi) = \mathbb{Z}_n.$$

Is ϕ an Isomorphism?

To be an isomorphism, ϕ must be:

- A homomorphism
- Injective

  Since $\ker(\phi) = n\mathbb{Z} \neq \{0\}$, the mapping is not injective.
- Surjective

  Every element in $\mathbb{Z}_n$ has a preimage in $\mathbb{Z}$.

Conclusion: ϕ is a surjective homomorphism but not an isomorphism.

Visual Diagram (Optional)

$$\mathbb{Z} \xrightarrow{\quad \phi(a) = [a]_n \quad} \mathbb{Z}_n$$

Infinite group　　　　Finite cyclic group

Figure 7.1: Group Homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$

7.2 Case Study 2: Ring Isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

Let us consider the ring homomorphism:

$$\phi : \mathbb{Z} \to \mathbb{Z}_n, \quad \phi(a) = [a]_n.$$

This is the natural map sending an integer to its equivalence class modulo n. It preserves both addition and multiplication:

$$\phi(a + b) = [a + b]_n = [a]_n + [b]_n = \phi(a) + \phi(b),$$

$$\phi(ab) = [ab]_n = [a]_n \cdot [b]_n = \phi(a) \cdot \phi(b).$$

Hence, ϕ is a ring homomorphism.

Kernel and Image

- **Kernel:** $\ker(\phi) = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{n}\} = n\mathbb{Z}$.
- **Image:** The image of ϕ is $\mathbb{Z}_n$, since every equivalence class has a preimage in $\mathbb{Z}$.

Use of First Isomorphism Theorem

Theorem 7.1 (First Isomorphism Theorem for Rings)**.** *Let* $\phi : R \to S$ *be a ring homomorphism. Then:*

$$R/\ker(\phi) \cong Im(\phi).$$

Applying the theorem:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

This is a fundamental and elegant result in ring theory.

Interpretation

- $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring formed by factoring out the ideal $n\mathbb{Z}$ from $\mathbb{Z}$. - $\mathbb{Z}_n$ is the ring of integers modulo n. - The isomorphism confirms these two structures are algebraically identical in terms of ring operations.

Example for $n = 6$

Let $a = 10 \in \mathbb{Z}$. Then $\phi(10) = [10]_6 = [4]_6$.

The class [10] in $\mathbb{Z}/6\mathbb{Z}$ maps directly to [4] in $\mathbb{Z}_6$, preserving both ring operations.

Visual Map

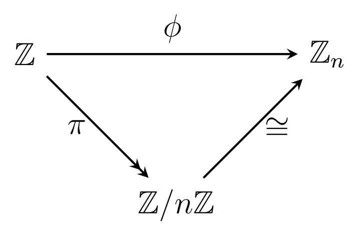


Figure 7.2: Isomorphism: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ via First Isomorphism Theorem

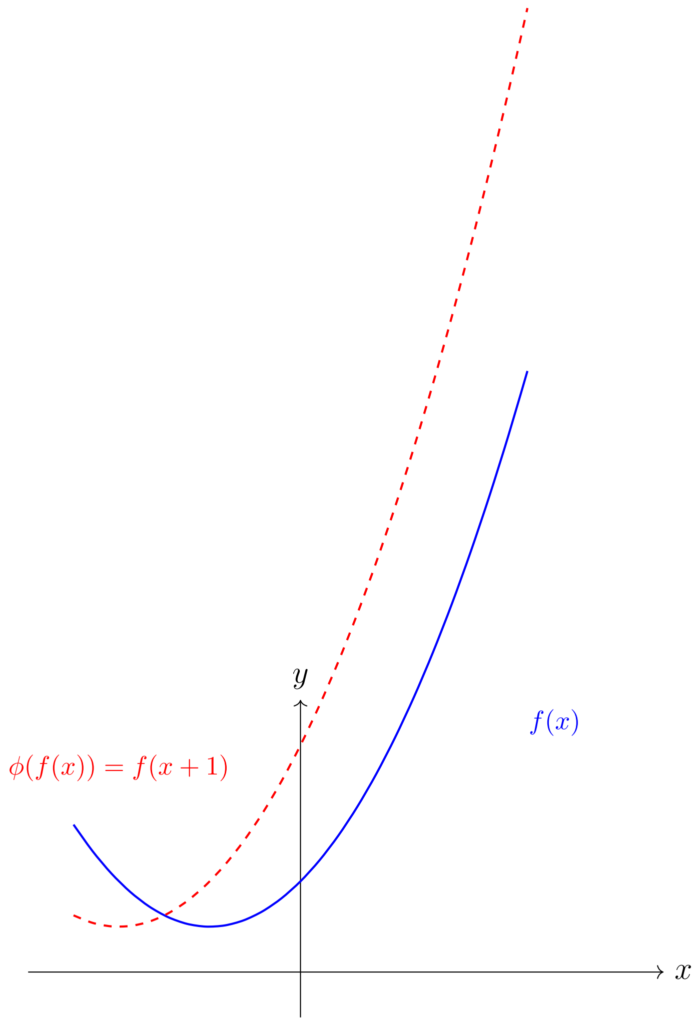


Figure 7.3: Polynomial shift: $f(x)$ vs $f(x+1)$

Object	**Description**
$\ker(\phi)$	Elements mapping to identity in H
$G/\ker(\phi)$	Cosets that form a quotient group
$\mathrm{Im}(\phi)$	Subgroup of H actually reached by ϕ

7.3 Theorem 1: First Isomorphism Theorem (Groups)

Theorem 7.2 (First Isomorphism Theorem). *Let $\phi : G \to H$ be a group homomorphism. Then the quotient group $G/\ker(\phi)$ is isomorphic to the image of ϕ:*

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

Proof Sketch

Let $\phi : G \to H$ be a homomorphism.

- Define the mapping:

$$\psi : G/\ker(\phi) \to \mathrm{Im}(\phi), \quad \psi(g\ker(\phi)) = \phi(g).$$

- **Well-defined:** If $g_1\ker(\phi) = g_2\ker(\phi)$, then $g_1^{-1}g_2 \in \ker(\phi)$, so $\phi(g_1) = \phi(g_2)$.
- **Homomorphism:**

$$\psi(g_1\ker(\phi) \cdot g_2\ker(\phi)) = \psi((g_1g_2)\ker(\phi)) = \phi(g_1g_2) = \phi(g_1)\phi(g_2).$$

- **Bijective:** ψ is injective (kernel of ψ is trivial) and surjective (image is $\mathrm{Im}(\phi)$).

Thus, ψ is an isomorphism, and we conclude:

$$G/\ker(\phi) \cong \mathrm{Im}(\phi).$$

Example

Let:

$$\phi : \mathbb{Z} \to \mathbb{Z}_6, \quad \phi(n) = [n]_6.$$

- $\ker(\phi) = 6\mathbb{Z}$
- $\mathrm{Im}(\phi) = \mathbb{Z}_6$

Then by the theorem:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$$

Diagram Illustration

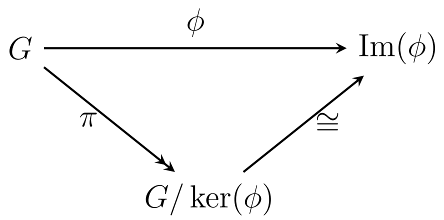


Figure 7.4: Structure of the First Isomorphism Theorem

7.4 Case Study 4: Automorphism Group of $\mathbb{Z}_6$

Let $G = \mathbb{Z}_6$, the additive group of integers modulo 6.

An **automorphism** of G is a group isomorphism from G to itself:

$$\phi : G \to G, \quad \text{such that } \phi(a+b) = \phi(a) + \phi(b) \text{ and } \phi \text{ is bijective.}$$

Step 1: Find All Group Automorphisms

Fact: $\mathbb{Z}_6$ is a cyclic group generated by 1.

So any automorphism ϕ is completely determined by the image of the generator.

To preserve structure:

$$\phi(1) = k \in \mathbb{Z}_6 \text{ such that } \gcd(k, 6) = 1.$$

The valid choices of k are:

$$k \in \{1, 5\}, \text{ since } \gcd(1, 6) = \gcd(5, 6) = 1.$$

Each such k defines a homomorphism:

$$\phi_k(n) = k \cdot n \mod 6.$$

So we define:

- $\phi_1(n) = n \mod 6$ (identity automorphism)
- $\phi_5(n) = 5n \mod 6$

Step 2: Structure of Aut($\mathbb{Z}_6$)

- $\text{Aut}(\mathbb{Z}_6)$ is a group under composition of functions.
- It has 2 elements: ϕ_1 and ϕ_5.
- Thus:

$$\text{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2.$$

Visualization

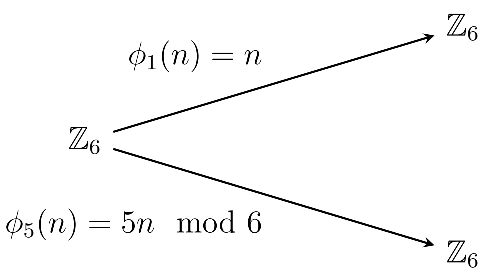


Figure 7.5: Two automorphisms of $\mathbb{Z}_6$: Identity and ϕ_5

Conclusion

- $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$ (the multiplicative group modulo n).
- For $n = 6$, $\mathbb{Z}_6^\times = \{1, 5\} \cong \mathbb{Z}_2$.
- So:

$$\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2.$$

7.5 Case Study 5: Automorphisms of $\mathbb{Z}_p$, where p is Prime

Let p be a prime number. Then $\mathbb{Z}_p$ is a finite field under addition and multiplication modulo p.

We consider $\mathbb{Z}_p$ as an additive group:

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}, \quad \text{under } + \quad \text{mod } p.$$

Automorphisms of $\mathbb{Z}_p$

Fact: Since $\mathbb{Z}_p$ is a cyclic group of order p, generated by 1, any automorphism is determined by where 1 is sent.

Let:

$$\phi_k(n) = kn \mod p, \quad \text{for } k \in \mathbb{Z}_p^\times.$$

Each ϕ_k is a group automorphism if $\gcd(k, p) = 1$ (which is always true for $k \in \{1, 2, ..., p-1\}$ because p is prime).

Structure of Aut($\mathbb{Z}_p$)

$$\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1},$$

the multiplicative group of units modulo p.

Example: $\mathbb{Z}_7$

$$\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}, \quad \phi_k(n) = kn \mod 7.$$

There are $\varphi(7) = 6$ automorphisms:

k	Automorphism $\phi_k(n) = kn \mod 7$
1	$\phi_1(n) = n$
2	$\phi_2(n) = 2n \mod 7$
3	$\phi_3(n) = 3n \mod 7$
4	$\phi_4(n) = 4n \mod 7$
5	$\phi_5(n) = 5n \mod 7$
6	$\phi_6(n) = 6n \mod 7$

Conclusion

For any prime p:

$$\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$$

- Each automorphism is a multiplication map ϕ_k with $k \in \mathbb{Z}_p^\times$.
- The automorphism group has order $p - 1$ and is cyclic.

7.6 Theorem 2: First Isomorphism Theorem for Rings

Theorem 7.3 (First Isomorphism Theorem for Rings)**.** *Let $f : R \to S$ be a ring homomorphism. Then the quotient ring $R/\ker(f)$ is isomorphic to the image of f, i.e.,*

$$R/\ker(f) \cong \text{Im}(f).$$

Sketch of Proof. Define a map $\phi : R/\ker(f) \to \text{Im}(f)$ by

$$\phi(r + \ker(f)) = f(r).$$

This map is well-defined, a homomorphism, and bijective:

- Well-defined: If $r + \ker(f) = r' + \ker(f)$, then $r - r' \in \ker(f)$, so $f(r) = f(r')$.
- Homomorphism: $\phi((r_1 + \ker(f)) + (r_2 + \ker(f))) = f(r_1 + r_2) = f(r_1) + f(r_2)$, and similarly for multiplication.
- Surjective: By construction, ϕ maps onto $\text{Im}(f)$.
- Injective: If $\phi(r + \ker(f)) = 0$, then $f(r) = 0$, so $r \in \ker(f)$ and hence $r + \ker(f) = \ker(f)$, the identity.

Hence, ϕ is an isomorphism. □

Example

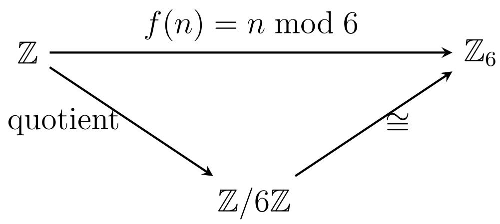
Let us consider the canonical ring homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}_6 \quad \text{defined by } f(n) = n \mod 6.$$

Here, $\ker(f) = \{n \in \mathbb{Z} \mid n \equiv 0 \mod 6\} = 6\mathbb{Z}$, and $\mathrm{Im}(f) = \mathbb{Z}_6$.

So, by the theorem:

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6.$$



This diagram shows the factorization of f via the isomorphism $\mathbb{Z}/\ker(f) \cong \mathrm{Im}(f)$.

7.7 Theorem 3: A Homomorphism is Determined by Its Action on Generators

Theorem 7.4. *Let G and H be groups, and let $f : G \to H$ be a group homomorphism.*

If G is generated by a set $S = \{g_1, g_2, \ldots, g_n\}$, and the values $f(g_1), f(g_2), \ldots, f(g_n)$ in H are known, then f is completely determined by these images.

Sketch of Proof. Every element $g \in G$ can be written as a finite product of elements from S and their inverses. Since f is a homomorphism, it respects products and inverses:

$$f(g_1^{a_1} g_2^{a_2} \cdots g_n^{a_n}) = f(g_1)^{a_1} f(g_2)^{a_2} \cdots f(g_n)^{a_n}$$

Therefore, knowing $f(g_i)$ for all i determines $f(g)$ for any $g \in G$. □

Example

Let $G = \mathbb{Z}_4 = \langle 1 \rangle$ and $H = \mathbb{Z}_2$.

Define $f : \mathbb{Z}_4 \to \mathbb{Z}_2$ by:

$$f(1) = 1 \in \mathbb{Z}_2 \Rightarrow f(2) = f(1{+}1) = f(1){+}f(1) = 0 \Rightarrow f(3) = f(1{+}2) = f(1){+}f(2) = 1 \Rightarrow f(0) = 0$$

So the homomorphism is completely known just by defining $f(1)$.

Visual Illustration

$$\mathbb{Z}_4 \xrightarrow{f(1) = 1 \text{ determines all}} \mathbb{Z}_2$$

Summary

In this chapter, we explored several concrete case studies and foundational theorems that highlight the essential role of homomorphisms and isomorphisms in different algebraic structures.

We began by examining specific examples of group and ring homomorphisms, demonstrating how kernels, images, and structure-preserving properties manifest in concrete settings such as $\mathbb{Z}_n$, polynomial rings, and automorphism groups. These case studies provided practical illustrations which will enrich our understanding of abstract definitions.

Following this, we presented three key theorems:

- **Theorem 1: First Isomorphism Theorem for Groups** – demonstrating the isomorphism between the quotient group and the image of a homomorphism.
- **Theorem 2: First Isomorphism Theorem for Rings** – extending the group theorem to ring structures, showing how quotient rings relate to images of ring homomorphisms.
- **Theorem 3: A Homomorphism is Determined by Its Action on Generators** – a powerful result defining a homomorphism on a generating set fully determines the entire map.

Throughout, we have used diagrams and worked examples to visualize the structure-preserving nature of homomorphisms and the classification role of isomorphisms. These insights help us to understand how algebraic systems relate to one another through well-defined mappings.

Chapter 8

Conclusion and Future Work

Conclusion

In this dissertation, we have prsented a comprehensiveexplorations of homomorphisms and isomorphisms in the realm of abstract algebra. These concepts serve as the bridge between alebric structuresand acts as a foundational tools for comparing and analyzing algebraic structures, enabling us to map complex relationships in a structured and meaningful way.

We began foundational definitions and proceeds through properties of group, ring, and field homomorphisms. The study extended to classifications and visual representations of isomorphisms — bijective homomorphisms that preserve the entire algebraic structure — and their pivotal role in classifying algebraic objects up to structural equivalence.

Through a combination of theoretical exposition, diagrams, and case studies, we observed how structure-preserving maps behave in various contexts, such as:

- Mappings between cyclic groups like $\mathbb{Z}_n$,
- Quotient constructions and kernel-image relationships,
- Automorphism groups and symmetry transformations.

The theorems presented — including both versions of the First Isomorphism Theorem and the generator-based homomorphism principle — emphasized the elegance and depth of algebraic logic. Together, these ideas form the bedrock of modern algebra and its many applications.

Future Work

While this work focused on classical group and ring theory, several rich directions remain open for further exploration:

1. **Module Theory:** A generalization of vector spaces and abelian groups, module homomorphisms lead to deeper results in representation theory and homological algebra.

2. **Homomorphisms in Field Extensions:** Understanding embeddings and isomorphisms between fields plays a crucial role in Galois theory and cryptographic constructions.

3. **Category Theory Perspective:** Viewing homomorphisms as morphisms in algebraic categories (such as **Grp**, **Ring**, or **Mod**) offers an abstract, unified viewpoint that connects disparate mathematical fields.

4. **Computational Algebra Systems:** Implementation of isomorphism checking algorithms and homomorphism mapping in systems like GAP, SageMath, or Magma helps providing hands-on applications in pure and applied mathematics.

5. **Real-World Applications:** From cryptographic protocols and coding theory to symmetry analysis in physics and chemistry, homomorphisms remain deeply relevant beyond the theoretical realm.

This study of homomorphisms and isomorphisms opens the door to a world of abstraction and logical clarity. It is a theme that resonates across mathematics — from the integers we count with, to the fields and structures that shape our universe.

Bibliography

[1] John B. Fraleigh, *A First Course in Abstract Algebra*, 7th Edition, Pearson Education, 2003.

[2] Joseph A. Gallian, *Contemporary Abstract Algebra*, 9th Edition, Cengage Learning, 2016.

[3] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd Edition, Wiley, 2004.