Group Isomorphisms
Quotient Groups and
Fundamental Theorem of Homomorphisms

A Project Work Submitted By
Kimsie PHAN

in partial fulfillment of the requirements for being a member of
Mathematical Association of Cambodia

M. A. C.

Mathematical Association of Cambodia
15 March 2021

Abstract

In this work, we explore almost all parts of the basic concepts in algebra such as isomorphism groups, quotient groups, and fundamental theorem of homomorphisms. Firstly, we begin our studies with first chapter talking about isomorphism groups. There we introduce the main criterions to make two groups isomorphic with each other. And we prove Cayley's theorem in the next section. After that we study some properties and applications of isomorphism. Secondly, we study quotient groups. We introduce transforming from quotient sets to quotient groups and we study some applications of quotient groups. Thirdly, we work on fundamental theorem of homomorphisms. There we introduce some definitions that related to concept of homomorphisms. Moreover, we work on applications of fundamental theorem of homomorphisms.

Keywords: Isomorphisms, homomorphisms, and quotient.

Declaration

I hereby declare that the work presented in this project work, submitted to the Mathematical Association of Cambodia (MAC) in partial fulfillment of the requirements for being a member of MAC. I confirm that this project work is my original work, and that any work done by others or by myself previously has been acknowledged and referenced accordingly. This work was not previously presented to another examination board and has not been published.

Kimsie Phan
BSc. Student

Acknowledgements

First of all, I wish to express my sincere gratitude to the MAC, the non-government organization which let me be a part of this work.

Further, I would like to express my sincere appreciation to my patient and supportive advisor Doem Vanny who has supported me throughout this project work. Without his persistent help, the goal of this work would not have been realized.

I cannot end without thanking all those who helped me in one way or the other and whose names have not been mentioned here.

Kimsie Phan
BSc. Student

Contents

1
Introduction

Firstly, mathematicians start to study algebra by solving equation. Then they think that "Does an equation have an answer?" and "if it does, how many solution for this equation?". Starting this point, algebra is growing up until now. They observe that some subjects in mathematics such as Analysis, Probability, Topology, Differential Equation, and Complex Analysis, that's all contributed from Algebra. Algebra is divided into five part such as Pre-Algebra, Elementary Algebra, Abstract Algebra or Modern Algebra, Linear Algebra, and Universal Algebra. However, in our work, we only study some parts in abstract algebra.

In algebra, which is a broad division of mathematics, abstract algebra (occasionally called modern algebra) is the study of algebraic structures. Algebraic structures include groups, rings, fields, modules, vector spaces, lattices, and algebras. The term abstract algebra was coined in the early 20th century to distinguish this area of study from the other parts of algebra.

Algebraic structures, with their associated homomorphisms, form mathematical categories. Category theory is a formalism that allows a unified way for expressing properties and constructions that are similar for various structures.

Universal algebra is a related subject that studies types of algebraic structures as single objects. For example, the structure of groups is a single object in universal algebra, which is called variety of groups.

1.1 Brief Literature Review

Through the end of the nineteenth century, many perhaps most of these problems were in some way related to the theory of algebraic equations. Major themes include:

- Solving of systems of linear equations, which led to linear algebra
- Attempts to find formulas for solutions of general polynomial equations of higher degree that resulted in discovery of groups as abstract manifestations of symmetry
- Arithmetical investigations of quadratic and higher degree forms and diophantine equations, that directly produced the notions of a ring and ideal.

Numerous textbooks in abstract algebra start with axiomatic definitions of various algebraic structures and then proceed to establish their properties. This creates a false impression that in algebra axioms had come first and then served as a motivation and as a basis of further study. The true order of historical development was almost exactly the opposite. For example, the hypercomplex numbers of the nineteenth century had kinematic and physical motivations but challenged comprehension. Most theories that are now recognized as parts of algebra started as collections of disparate facts from various branches of mathematics, acquired a common theme that served as a core around which various results were grouped, and finally became unified on a basis of a common set of concepts. An archetypical example of this progressive synthesis can be seen in the history of group theory.

The end of the 19th and the beginning of the 20th century saw a shift in the methodology of mathematics. Abstract algebra emerged around the start of the 20th century, under the name modern algebra. Its study was part of the drive for more intellectual rigor in mathematics. Initially, the assumptions in classical algebra, on which the whole of mathematics (and major parts of the natural sciences) depend, took the form of axiomatic systems. No longer satisfied with establishing properties of concrete objects, mathematicians started to turn their attention to general theory. Formal definitions of certain algebraic structures began to emerge in the 19th century. For example, results about various groups of permutations came to be seen as instances of general theorems that concern a general notion of an abstract group. Questions of structure and classification of various mathematical objects came to forefront.

These processes were occurring throughout all of mathematics, but became especially pronounced in algebra. Formal definition through primitive operations and axioms were proposed for many basic algebraic structures, such as groups, rings, and fields. Hence such things as group theory and ring theory took their places in pure mathematics. The algebraic investigations of general fields by Ernst Steinitz and of commutative and then general rings by David Hilbert, Emil Artin and Emmy Noether, building up on the work of Ernst Kummer, Leopold Kronecker and Richard Dedekind, who had considered ideals in commutative rings, and of Georg Frobenius and Issai Schur, concerning representation theory of groups, came to define abstract algebra. These developments of the last quarter of the 19th century and the first quarter of 20th century were systematically exposed in Bartel van der Waerden's Moderne Algebra, the two-volume monograph published in 19301931 that forever changed for the mathematical world the meaning of the word algebra from the theory of equations to the theory of algebraic structures.

1.2 Objectives of the Study

The objectives of this project work are as follows:

- Chapter 1: We introduce group isomorphism, Cayley's theorem, properties of group isomorphism, and some applications of group isomorphism.
- Chapter 2: We study quotient groups and its applications.
- Chapter 3: We introduce fundamental theorem of homomorphisms and its applications.

1.3 Outline of the Thesis

In chapter 1, we start introducing some definitions related to group isomorphism, then we start testing whether two groups are isomorphic to each other or not. Moreover, we prove Cayley's theorem and study some applications of group isomorphism. In chapter 2, we study quotient groups and its applications. Finally, in chapter 3, we work on a special theorem. It is the fundamental theorem of homomorphisms and at the end we also include some of its applications.

1.4 Preliminaries

To achieve our main objectives we have set for our work, we first have to build up all the basic concepts needed then immediately we go ahead with our main theorems which are followed by some useful applications, for each work.

In chapter 1, we have to start from binary operation on two groups. Then we cannot study all groups, so we keep trying to find a function that is bijective and also preserve both operations of group. That is the definition of group isomorphism and we use its definition to study Cayley's theorem, properties, and its applications.

In chapter 2, before we know that quotient sets can be quotient groups, we take a concept of subgroup. However, it does not work even it satisfies with condition of groups. For this we need a concept of normal subgroups, then it works.

In chapter 3, we study quotient groups, homomorphism, image, and kernel of function, then we start working on fundamental theorem of homomorphisms, and further working to word its applications.

2
Group Isomorphisms

2.1 Introduction

Suppose an American and a German are asked to count a handful or objects. The American sat "one, two, three, four,..." whereas the German says "Eins, zwei, drei, vier,...". Are the two doing different thing? No. They are both counting the objects, but they are using different terminology to do so. An analogous situation often occurs with groups; the same group is describes with different terminology.

In mathematics, an isomorphism is a structure-preserving mapping between two structures of the same type that can be reversed by an inverse mapping. Two mathematical structures are isomorphic if an isomorphism exists between them. The word isomorphism is derived from the Ancient Greek: isos "equal", and morphe "form" or "shape".

The interest in isomorphisms lies in the fact that two isomorphic objects have the same properties (excluding further information such as additional structure or names of objects). Thus isomorphic structures cannot be distinguished from the point of view of structure only, and may be identified. In mathematical jargon, one says that two objects are the same up to an isomorphism.

Before we work on group isomorphism, we review some definition that involve our concept in this chapter.

Definition 2.1.1 (Groups)**.** *A group is a nonempty set G with a binary operation $*: G \times G \to G$, $(x, y) \mapsto x * y$ satisfying the following conditions:*

1. *G is associative: $(a * b) * c = a * (b * c), \quad \forall a, b, c \in G$.*
2. *There is an element e in G such that $a * e = a$ and $e * a = a, \quad \forall a \in G$.*
3. *$\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = e$ and $a^{-1} * a = e$.*
   If G be a group but it is also commutative i.e., $\forall a, b \in G, \quad a * b = b * a$, that is called Abelian group.

Definition 2.1.2 (Subgroups)**.** *Let G be a group and H a nonempty subset of G i.e.,*

$$\varnothing \neq H \leq G \Longleftrightarrow \begin{cases} h_1 h_2 \in H \\ h_1^{-1} \in H \end{cases}, \forall h_1, h_2 \in H$$

$$\Longleftrightarrow \quad \forall h_1, h_2 \in H, \quad h_1 h_2^{-1} \in H.$$

Definition 2.1.3 (Order of Groups and elements)**.** *Let G be a group. A number of elements in G is called the* ***order*** *of G and denoted by $|G|$. When G is infinite, we write $|G| = \infty$. Let $x \in G$ and $n \in \mathbb{N}$. We denote*

$$x^n = x \cdot x \cdot x \cdots x \quad (n \text{ times of } x)$$
$$x^{-n} = (x^{-1})^n = x^{-1} \cdot x^{-1} \cdot x^{-1} \cdots x^{-1} \quad (n \text{ time of } x^{-1})$$
$$x^0 = e$$

The smallest positive integer n such that $x^n = e$ is called the ***order of the element*** *x in G and denoted by $|x| = n$. If no such integer exists, we say that x has* ***infinite order*** *and denoted by $|x| = \infty$.*

Definition 2.1.4 (Cyclic groups)**.** *Let G be a group. G is a* ***cyclic group*** *if there exists $x \in G$ such that $G = \langle x \rangle$. The group $\langle x \rangle$ is called the* ***group generated by*** *x and x is called the* ***generator*** *of $\langle x \rangle$.*

Example 2.1.5. *We give some examples of groups.*

I. Infinite Groups

1. *Matrix groups:* $\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{R}), \mathrm{SO}(n), \mathrm{U}(n)$ *and* $\mathrm{SU}(n), ...$ *with multiplication operation.*
2. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ *are abelian group.*
3. $(S_X, \circ), S_X = \{f : X \to X, X \neq \varnothing | f \quad \text{is bijective}\}$ *is called permutation groups.*

II. Finite Groups

1. $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$ *with addition operation modulo n.*
2. $\mathbb{Z}_n^\times = \{m \in \mathbb{Z}_n | (m, n) = 1\}$ *with multiplication operation modulo n.*
   Example: $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$
3. *$G = \{1, -1, i, -i\}$ is a group under usual multiplication of complex number and it is an abelian group.*
4. *If the set $X = \{1, 2, ..., n\}$ we denote S_n is symmetric groups.*

2.2 Group Isomorphism

We start to observe $\mathbb{Z}_8^\times, \mathbb{Z}_4$, and $(G, \times)$. In binary operation of table shown that those groups are different. And if we work transformation between $\mathbb{Z}_8^\times$ and $\mathbb{Z}_4$ or G, then they are not correspondence each other.

- Table of $\mathbb{Z}_8^\times$

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

- Table of $(G, \times)$

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- Table of $\mathbb{Z}_4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

But for $\mathbb{Z}_4$ and G can be one-to-one correspondence between them which transforms $0 \longleftrightarrow 1, 1 \longleftrightarrow i, 2 \longleftrightarrow -1$ and $3 \longleftrightarrow -i$. They exists an isomorphism.

- Table of $\mathbb{Z}_4$

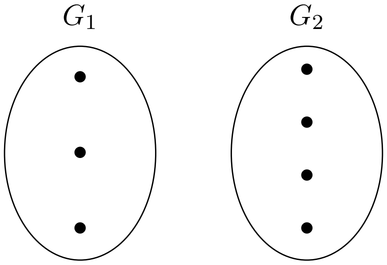
$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Table of G after changing order of element

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

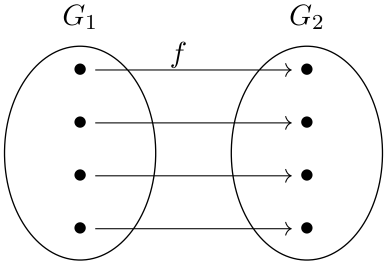
Remark: We cannot use table of operations to check whether two groups are the same or not.

Now consider:

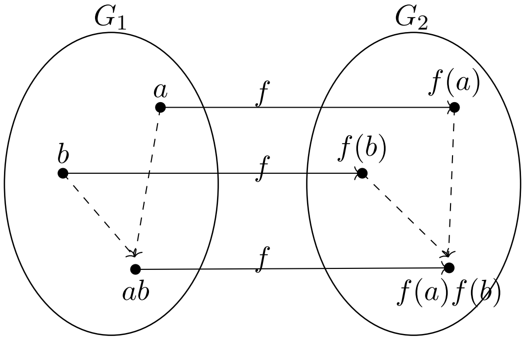


G_1 can not be the same as G_2 since $\text{card}(G_1) \neq \text{card}(G_2)$.

Consider if $\text{card}(G_1) = \text{card}(G_2)$, then



1. There exists $f : G_1 \to G_2$ such that f is bijective.



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

Definition 2.2.1 (isomorphism groups)**.** *Let G_1 and G_2 be two groups. We say that G_1 is* ***isomorphic*** *to G_2 there exists a function $f : G_1 \longrightarrow G_2$ which satisfies:*

1. *f is bijection.*

2. *f preserves operator, that is $f(ab) = f(a)f(b)$ for any $a, b \in G$.*

We symbolize this fact by writing,

$$G_1 \cong G_2 \quad \text{or} \quad G_1 \approx G_2.$$

Proposition 2.2.2. *Any infinite cyclic group is isomorphic to* $\mathbb{Z}$*.*

Proof. Let $G = \langle x \rangle$ where $|x| = \infty$.
Consider the map $f : G \to \mathbb{Z}$ given by $x^n \mapsto n$ where $n \in \mathbb{Z}$.
This map is well-defined and injective since for any $x^m, x^n \in G$

$$x^m = x^n \iff m = n$$

where $m, n \in \mathbb{Z}$.
Now f is surjective since for any $n \in \mathbb{Z}$, $\exists x^n \in G$ such that $f(x^n) = n$.
And f is operation preserving since for any $x^m, x^n \in G$, we have

$$f(x^m x^n) = f(x^{m+n}) = m + n = f(x^m) + f(x^n).$$

Therefore, any infinite cyclic group is isomorphic to $\mathbb{Z}$. □

Proposition 2.2.3. *Any finite cyclic group* $\langle x \rangle$ *such that card*$(\langle x \rangle) = n$ *is isomorphic to* $\mathbb{Z}_n$*.*

Proof. Let $G = \langle x \rangle$ where $|x| = n$.
Consider the map $f : G \longrightarrow \mathbb{Z}_n$ given by

$$f(x^p) = p \mod n$$

where $p \in \mathbb{Z}$.
Now f is injective since $\forall p, q \in \mathbb{Z}$

$$p(\mod n) = q(\mod n) \iff x^p = x^q.$$

And f is surjective since $\forall p(\mod n) \in \mathbb{Z}_n, \exists x^p \in G$ such that $f(x^p) = p$ mod n.
Furthermore f preserve group operation: Let $x^p, x^q \in G$ then
$f(x^p x^q) = f(x^{p+q})$
$= (p + q) \mod n$
$= (p \mod n) + (q \mod n)$
$= f(x^p) + f(x^q)$
Therefore,

$$\langle x \rangle \cong \mathbb{Z}_n.$$

□

Lemma 2.2.4. *How does one recognize if two groups are isomorphic to each other?*

1. *Make a smart guess on a function* $f : G_1 \longrightarrow G_2$ *which might be an isomorphism.*
2. *Check that* f *is injective and surjective, that is bijective.*
3. *Check that* f *satisfies the preserve operation* $f(ab) = f(a)f(b)$*.*

Lemma 2.2.5. *Show that two groups* G_1 *and* G_2 *are not isomorphic by observing:*

- *card*$(G_1) \neq$ *card*(G_2)*.*
- $|G_1| \neq |G_2|$*.*
- G_1 *is cyclic but* G_2 *is not.*
- G_1 *is abelian but* G_2 *is not.*

2.3 Cayley's Theorem

In the early days of modern algebra the word "group" had a different meaning from the meaning it has today. In those days a group always meant a group of permutation. The only groups mathematicians used were groups whose elements were permutations of some fixed set and whose operation was composition.

There are something comforting about working with tangible, concrete things, such as groups of permutations of a set. At all times we have a clear picture of what it is we are working with. Later, as the axiomatic method reshaped algebra, a group came to mean any set with any associative operation having a neutral element and allowing each element an inverse. The new notion of group pleases mathematicians because it is simpler and more lean and sparing than the old notion of groups of permutation; it is also more general because it allows many new things to be groups which are not groups of permutations. However, it is harder to visualize, precisely because so many different things can be groups.

It was therefore a great revelation when, about 100 years ago, **Arthur Cayley** discovered that *every group is isomorphic to a group of permutation*. Roughly, this means that the groups of permutations are actually all the groups there are! Every group is a group of permutations. This great result is a classic theorem of modern algebra. Its proof is not very difficult.

Theorem 2.3.1. *Every group is isomorphic to a group of permutations.*

Proof. Let G be an arbitrary group. Consider the permutation group S_G and for each $g \in G$, we define a map

$$\begin{aligned} f_g : G &\to G \\ x &\mapsto gx \end{aligned}$$

First, observe that $f_g \in S_G$ for all $g \in G$. Indeed,

$$f_g(x) = f_g(y) \iff gx = gy \iff x = y, \quad \forall x, y \in G.$$

$$\forall y \in G, \exists x = g^{-1}y \in G, f_g(x) = f_g(g^{-1}y) = gg^{-1}y = y.$$

In addition, the set $\overline{G} := \{f_g | g \in G\}$ is a subgroup of S_G since for any $g_1, g_2 \in G$ and $x \in G$, we have

$$\left(f_{g_1} \circ f_{g_2}\right)(x) = f_{g_1}(g_2 x) = g_1 g_2 x = f_{g_1 g_2}(x) \iff f_{g_1} \circ f_{g_2} = f_{g_1 g_2} \in \overline{G}.$$

$$f_{g_1} \circ f_{g_1^{-1}}(x) = f_{g_1}(g_1^{-1}x) = g_1 g_1^{-1} x = x.$$

$$\iff f_{g_1} \circ f_{g_1}^{-1} = Id \iff f_{g_1}^{-1} = f_{g_1^{-1}} \in \overline{G}.$$

We will prove that $G \cong \overline{G}$. Consider a map:

$$\begin{aligned} f : G &\to \overline{G} \\ g &\mapsto f_g. \end{aligned}$$

This map is well-defined and injective.
Let $g_1, g_2 \in G$,

$$g_1 = g_1 \iff g_1 x = g_2 x, \forall x \in G \iff f_{g_1} = f_{g_2}.$$

Now f is clearly surjective because $\forall y \in \overline{G}, \exists x = g^{-1}y \in G$ such that

$$f_g(x) = f_g(g^{-1}y) = gg^{-1}y = y.$$

And f preserves the operation: for any $g_1, g_2 \in G$, we have

$$f(g_1 g_2) = f_{g_1 g_2} = f_{g_1} \circ f_{g_2} = f(g_1) \circ f(g_2).$$

Therefore,

$$G \cong \overline{G} \leq S_G.$$

□

2.4 Properties of Group Isomorphism

After studying definition of group isomorphism, we now give a catalog of properties of isomorphisms and isomorphic groups.

1. Properties of Isomorphism Acting on Elements

   Theorem 2.4.1. *Suppose that f is an isomorphism from a group G onto a group $\overline{G}$.*

   (a) f carries the identity of G to the identity of $\overline{G}$.

   (b) For every integer n and for every group element a in G, $f(a^n) = [f(a)]^n$.

   (c) For any element a and b in G, a and b commute if and only if $f(a)$ and $f(b)$ commute.

   (d) $G = \langle a \rangle$ if and only if $\overline{G} = \langle f(a) \rangle$.

   (e) $|a| = |f(a)|$ for all a in G (isomorphism preserves orders).

   (f) For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same numbers of solutions in G as does the equation $x^k = f(b)$ in $\overline{G}$.

   (g) If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

2. Properties of Isomorphism Acting on Groups

   Theorem 2.4.2. *Suppose that f is an isomorphism from a group G onto a group $\overline{G}$.*

   (a) f^{-1} is an isomorphism from $\overline{G}$ onto G.

   (b) G is abelian if and only if $\overline{G}$ is abelian.

   (c) G is cyclic if and only if $\overline{G}$ is cyclic.

   (d) If K is a subgroup of G, then $f(K) = \{f(k) | k \in K\}$ is a subgroup of $\overline{G}$.

   (e) $f(Z(G)) = Z(\overline{G})$ where $Z(G)$ denotes the center of the group G.
   Note: $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$.

2.5 Application of Group Isomorphism

In algebra, isomorphisms are defined for all algebraic structures. Some are more specifically studied; for example:

- Linear isomorphisms between vector spaces; they are specified by invertible matrices.

- Group isomorphisms between groups; the classification of isomorphism classes of finite groups is an open problem.

Example: Suppose V is vector space on $\mathbb{R}$ and finite-dimensional.
Let $G = \{T : V \to V | T \quad \text{is bijective}, T, T^{-1} \quad \text{is linear}\}$.
Let $T : \mathbb{R}^3 \to \mathbb{R}^3$ be the linear transformation defined by

$$T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + 3x_2 - x_3 \\ 3x_1 - x_2 + 4x_3 \\ 2x_1 - 4x_2 + x_3 \end{pmatrix}$$

We get $\quad T \circ T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = T \begin{pmatrix} x_1 + 3x_2 - x_3 \\ 3x_1 - x_2 + 4x_3 \\ 2x_1 - 4x_2 + x_3 \end{pmatrix}$

$$= \begin{pmatrix} x_1 + 3x_2 - x_3 + 3(3x_1 - x_2 + 4x_3) - (2x_1 - 4x_2 + x_3) \\ 3(x_1 + 3x_2 - x_3) - (3x_1 - x_2 + 4x_3) + 4(2x_1 - 4x_2 + x_3) \\ 2(x_1 + 3x_2 - x_3) - 4(3x_1 - x_2 + 4x_3) + (2x_1 - 4x_2 + x_3) \end{pmatrix}.$$

We must instead again, it is too hard. But we can find $T \circ T \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ by using multiplication of matrix.

$$T(x) = \begin{pmatrix} 1 & 3 & -1 \\ 3 & -1 & 4 \\ 2 & -4 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Then $\quad T(T(x)) = \begin{pmatrix} 1 & 3 & -1 \\ 3 & -1 & 4 \\ 2 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & -1 \\ 3 & -1 & 4 \\ 2 & -4 & 1 \end{pmatrix}$

$$= T \circ T.$$

The set of linear transform has inverse on vector space of real number which has n-dimensions or vector space of complex number which has n-complex dimensions, they isomorphic matrix groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$. We can study properties of linear transformation that instead to properties of matrix. In fact, compositing of linear transformation is multiplication of matrix that correspondence and inverse of linear transformation is inverse of matrix that correspondence each other.

3
Quotient Groups

3.1 Introduction

A quotient group or factor group is a mathematical group obtained by aggregating similar elements of a larger group using an equivalence relation that preserves some of the group structure (the rest of the structure is "factored" out). For example, the cyclic group of addition modulo n can be obtained from the group of integers under addition by identifying elements that differ by a multiple of n and defining a group structure that operates on each such class (known as a congruence class) as a single entity. It is part of the mathematical field known as group theory.

3.2 Quotient Groups

Before we work on quotient groups, we recall some properties that involve in this section.

Definition 3.2.1 (Cosets)**.** *Let G be a group, and H a subgroup of G.*

1. *The right coset of H in G defined by $Ha = \{ha|h \in H\}, \forall a \in G$.*
2. *The left coset of H in G defined by $aH = \{ah|h \in H\}, \forall a \in G$.*
   Moreover, the set of left and right cosets are denoted respectively by

$$G/_{H} = \{aH|a \in G\} \quad \textit{and} \quad {}_{H}\backslash^{G} = \{Ha|a \in G\}.$$

Proving quotient sets to be quotient groups

We let G is group and $H \leq G$.
And let $G/_{H} = \{aH|a \in G\}$ (is a set).
We define an operation on $G/_{H}$ by coset multiplication:
$(G,*): \quad (aH)(bH) := (ab)H$

$$G/_{H} \times G/_{H} \longrightarrow G/_{H}$$

$$(aH, bH) \mapsto (ab)H$$

Is this operation well-defined?
Answer: If $H \leq G$ then operation is not well-defined.
Via counterexample: if $G = S_3 = \{\epsilon, (12), (13), (23), (123), (132)\}$
And let $H \leq G$ such that $H = \{\epsilon, (12)\}$

We get $\quad (13)H = \{(13), (123)\} = (123)H$

$(23)H = \{(23), (132)\} = (132)H$

We get $\quad ((13)H, (23)H) = ((123)H, (132)H)$
Then $\quad ((13)H)((23)H) = [(13)(23)]H = (132)H$
But $\quad ((123)H)((132)H) = [(123)(132)]H = (\epsilon)H$
It means that one element in the domain assign two elements in the range. So the above operation

is not well-defined.

Is the operation on ${}^{G}\!/_{H}$ satifies other conditions?

- Associative
  We have $[(aH)(bH)](cH) = [(ab)H](cH)$
  $$= (abc)H = (aH)(bc)H$$
  $$= (aH)[(bH)(cH)]$$
- The identity: $(eH = H)$
  We have $eH = \{eh|h \in H\} = \{h|h \in H\} = H$
  such that $(aH)(eH) = (ae)H = aH$
  $$(eH)(aH) = (ea)H = aH$$
- Inverse:
  $\forall aH \in {}^{G}\!/_{H}, \quad \exists a^{-1}H \in {}^{G}\!/_{H}$
  such that $(aH)(a^{-1}H) = (aa^{-1})H = eH = H$
  $$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H.$$

What condition on H that the operation on ${}^{G}\!/_{H}$ defined above well-defined?

Definition 3.2.2 (normal subgroups)**.** *A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. We denote this by $H \triangleleft G$.*

Theorem 3.2.3. *Let G be a group and $H \triangleleft G$. The set ${}^{G}\!/_{H} = \{aH|a \in G\}$ is a group under the operation*

$$(aH)(bH) = (ab)H, \forall a, b \in G.$$

*${}^{G}\!/_{H}$ is called the **factor group**, or **quotient group** of G by H.*
Notice that :
$(a + H)(b + H) = (a + b) + H$, we define $(\times)$ on ${}^{G}\!/_{H}$ if $(G, +)$.
$(a + H) + (b + H) = (a + b) + H$, we define $(+)$ on ${}^{G}\!/_{H}$ if $(G, +)$.

Proof. It is enough to prove that the operation is well-defined.
If $H \triangleleft G$ then coset multiplication (Operation) is well-defined. How?

$(aH, bH) \in {}^{G}\!/_{H} \times {}^{G}\!/_{H}$

$(cH, dH) \in {}^{G}\!/_{H} \times {}^{G}\!/_{H}$

If $\quad (aH, bH) = (cH, dH) \Longrightarrow (ab)H = (cd)H$?

If $\begin{cases} aH = cH & \text{then} \quad a \in cH \\ bH = dH & \text{then} \quad b \in dH. \end{cases}$

Then $\begin{cases} a = ch_1 \\ b = dh_2 \end{cases}$ for some $h_1, h_2 \in H$.

Thus $(ab)H = (ch_1)(dh_2)H$
$$= c(h_1d)h_2H, \quad \text{since, } Hd = dH$$
$$= cdh_3h_2H$$
$$= (cd)H \quad \text{,since} \quad h_3h_2H \Longleftrightarrow h_3h_2 \in H.$$

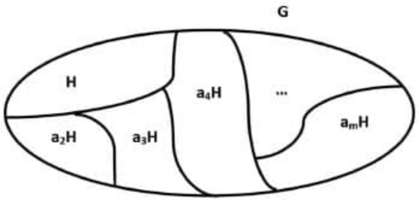
Therefore, $*$ on ${}^{G}\!/_{H}$ is well-defined. □

Example: From above counterexample $H \ntriangleleft S_3$ where $H = \{\epsilon, (12)\}$ because $(12)(123) \neq (123)(12)$ where $(123) \in S_3$.

3.3 Application of Quotient Groups

Remark: The set of left or right cosets are define respectively by
${}^{G}\!/_{H} = \{aH | \forall a \in G\}$ and ${}_{H}\backslash^{G} = \{Ha | \forall a \in G\}$.
By the theorem of Larange :

$$|G| = |G : H||H| = \left|{}^{G}\!/_{H}\right| |H|$$



Why are quotient groups important? Well, when G is finite and $H \neq \{e\}$, ${}^{G}\!/_{H}$ is smaller than G, and its structure is usually less complicated than that of G. At the same time, ${}^{G}\!/_{H}$ simulates G in many ways. In fact, we may think of a factor group of G as a less complicated approximation of G. What makes quotient groups important is that one can often deduce properties of G by examining the less complicated group ${}^{G}\!/_{H}$ instead.

Proposition 3.3.1. *Let G be a group and $H \triangleleft G$. If ${}^{G}\!/_{H}$ and H are finitely generated then G is finitely generated. (A group is said to be finitely generated if it is generated by a finite subset of its elements.).*

Proof. Let ${}^{G}\!/_{H} = \langle g_1H, g_2H, ..., g_mH\rangle$ and $H = \langle h_1, h_2, ..., h_n\rangle$ for some positive integer m, n.
Let $x \in G$ then $xH \in {}^{G}\!/_{H} = \langle g_1H, g_2H, ..., g_mH\rangle$.
$\implies xH = yH \quad \text{where} \quad y \in \langle g_1, g_2, ..., g_m\rangle$.
Then $\quad y^{-1}x \in H = \langle h_1, h_2, ..., h_n\rangle$
$\implies y^{-1}x = h, \quad h \in H.$
$\implies x = yh \in \langle g_1, ..., g_m, h_1, ..., h_n\rangle$.
Therefore, G is finitely generated. □

Proposition 3.3.2. *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. Recall that $Z(G) = \{x \in G | xg = gx, \forall g \in G\}$.
Let $g \in G$ then $gZ(G) \in {}^{G}\!/_{Z(G)} = \langle g_0Z(G)\rangle$.
Then $\exists n \in \mathbb{Z}$ such that $\quad gZ(G) = (g_0Z(G))^n = g_0^nZ(G)$

$$\iff g_0^{-n}g = x, \quad x \in Z(G)$$
$$\implies g = g_0^n x.$$

Thus, $\forall g_1, g_2 \in G, \exists m, n \in \mathbb{Z}$ such that $g_1 = g_0^m x, g_2 = g_0^n y$ for some $x, y \in Z(G)$.
Then $g_1g_2 = (g_0^m x)(g_0^n y) = g_0^m g_0^n xy = g_0^m g_0^n yx = g_2g_1$.
Therefore, G is Abelian. □

Proposition 3.3.3. *If every element of* ${}^{G}\!/_{H}$ *has a square root, and every element of* H *has a square root, then every element of* G *has a square root. (Assume* G *is abelian.)*

Proposition 3.3.4. *Let* p *be a prime number. If* ${}^{G}\!/_{H}$ *and* H *are* p*-groups, then* G *is a* p*-groups. A group* G *is called a* $p - group$ *if the order of every element* x *in* G *is a power of* p*.*

4
Fundamental Theorem of Homomorphisms

4.1 Introduction

In abstract algebra, the fundamental theorem on homomorphisms, also known as the fundamental homomorphism theorem, relates the structure of two objects between which a homomorphism is given, and of the kernel and image of the homomorphism.

Definition 4.1.1. *Let $G, G^{'}$ be groups. A map $f : G \longrightarrow G^{'}$ is said to be an **homomorphism** if it preserve the group operator; that is, $f(ab) = f(a)f(b)$ for all $a, b \in G$. In addition, if:*

- *f is one-one then f is called **monomorphsim**.*
- *f is onto then f is called **epimorphism**.*
- *f is bijective then f is called **isomorphism**.*
- *f is bijective and $G = G^{'}$ then f is called **automorphism**.*

Definition 4.1.2. *Let $f : G \longrightarrow G^{'}$ be a group homomorphism. Then the sets:*

- $\ker(f) = \{x \in G | f(x) = e_{G'}\} \subset G$ *is called **the kernel** of homomorphism f.*
- $\operatorname{Im}(f) = \{f(x) | x \in G\} \subset G^{'}$ *is called **the image** of G in $G^{'}$ via homomorphism f.*

Proposition 4.1.3. *Let f be a group homomorphism from G to $G^{'}$. Then*

1. $\operatorname{Im}(f) \leq G^{'}$.

2. $\ker(f) \triangleleft G$.

Proof. 1. Let $f(g_1), f(g_2) \in \operatorname{Im}(f)$, such that $g_1, g_2 \in G$.
We have $f(g_1)f(g_2) = f(g_1g_2) \in \operatorname{Im}(f)$.

$$\text{And} \quad [f(g_1)]^{-1} = f(g_1^{-1}) \in \operatorname{Im}(f).$$

$$\text{Thus,} \quad \operatorname{Im}(f) \leq G^{'}.$$

2. Let $x, y \in \ker(f)$ then $f(x) = e$ and $f(y) = e$.
We have
$$\begin{aligned} f(xy^{-1}) &= f(x)f(y^{-1}) \\ &= e[f(y)]^{-1} \\ &= ee^{-1} \\ &= e \end{aligned}$$
So, $xy^{-1} \in \ker(f)$ then $\ker(f) \leq G$.
From definition of normal subgroups is $aH = Ha, \forall a \in G$.
Observation that
$$\begin{aligned} aH = Ha &\Longleftrightarrow aHa^{-1} = H \\ &\Longleftrightarrow \forall a \in G, \forall h \in H, aha^{-1} \in H. \end{aligned}$$

If $a \in \ker(f)$ and $x \in G$.
Then $\quad f(xax^{-1}) = f(x)f(a)f(x^{-1})$

$$= f(x)f(a)[f(x)]^{-1}$$
$$= f(x)[f(x)]^{-1}, \quad \text{since } f(a) = e$$
$$= e.$$

So, $xax^{-1} \in \ker(f)$ then $\ker(f) \triangleleft G$.

□

Theorem 4.1.4 (Fundamental Theorem of Homomorphisms)**.** *Let f be a group homomorphism from G to $G^{'}$. Then the mapping from ${}^{G}\!/_{\ker(f)}$ to $G^{'}$, given by $g\ker(f) \mapsto \mathrm{Im}(f)$, is an isomorphism. In symbols, ${}^{G}\!/_{\ker(f)} \cong \mathrm{Im}(f)$.*

Proof. Consider the map $f^{'} : {}^{G}\!/_{\ker(f)} \longrightarrow \mathrm{Im}(f)$ defined by $f^{'}(g\ker(f)) = f(g), \quad g \in G$.
Now $f^{'}$ is well-defined and injective since

$$a\ker(f) = b\ker(f) \Longleftrightarrow b^{-1}a \in \ker(f) \Longleftrightarrow f(b^{-1}a) = e \Longleftrightarrow f(a) = f(b).$$

And $f^{'}$ is surjective: since

$$f^{'}\left({}^{G}\!/_{\ker(f)}\right) = \{f^{'}(g\ker(f))|g \in G\} = \{f(g)|g \in G\} = \mathrm{Im}(f).$$

Moreover $f^{'}$ is homomorphism:
$f^{'}[(a\ker(f))(b\ker(f))] = f^{'}(ab\ker(f))$

$$= f(ab) = f(a)f(b)$$
$$= f^{'}(a\ker(f))f^{'}(b\ker(f)).$$

□

4.2 Application of Fundamental Theorem of Homomorphisms

After proving the fundamental theorem of homomorphisms, we can work on its applications.

Proposition 4.2.1. *Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$. For each $n \in \mathbb{N}$ then ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathbb{Z}_n$.*

Note: $n\mathbb{Z} \triangleleft \mathbb{Z}$ and so ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{m + n\mathbb{Z}|m \in \mathbb{Z}\}$.

Proof. We have $f : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ given by $f(m) = m(\mod n)$.
Observe that f is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.
And f is clearly surjective.
Consider $\ker(f) = \{m \in \mathbb{Z} : m(\mod n) = 0\}$

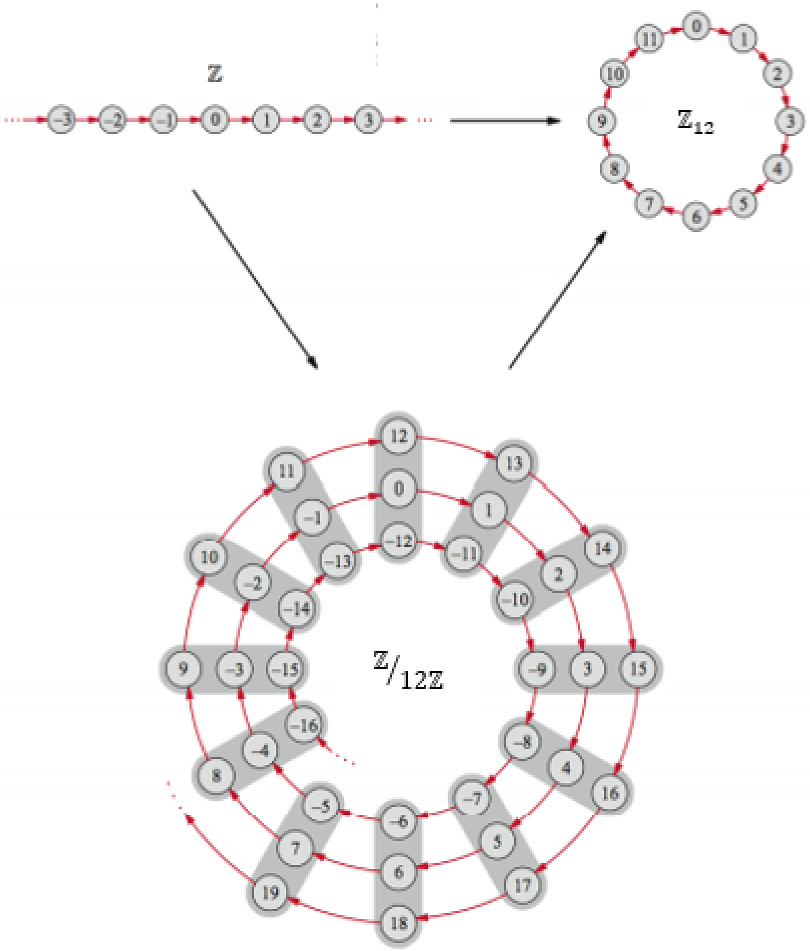
$$= \{m \in \mathbb{Z} : m = kn, k \in \mathbb{Z}\}$$
$$= n\mathbb{Z} = \langle n \rangle.$$

By Fundamental Theorem of Homomorphisms, we have that:

$${}^{\mathbb{Z}}\!/_{\ker(f)} = {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = {}^{\mathbb{Z}}\!/_{\langle n \rangle} \cong \mathrm{Im}(f) = \mathbb{Z}_n.$$

Therefore, ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathbb{Z}_n$. □

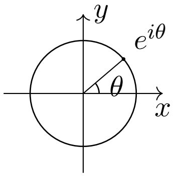
A picture of the isomorphism $f : \mathbb{Z}/_{12\mathbb{Z}} \longrightarrow \mathbb{Z}_{12}$:



Proposition 4.2.2. *Let $(\mathbb{R}, +)$ and $(\mathbb{Z}, +)$ be the additive group. And let $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ be the circle group. Prove that $\mathbb{R}/_{\mathbb{Z}} \cong \mathbb{T}$.*

Review: $(\mathbb{R}, +), (\mathbb{Z}, +)$ are abelian group. Then $\mathbb{Z} \triangleleft \mathbb{R}$ and $\mathbb{R}/_{\mathbb{Z}} = \{x + \mathbb{Z} | x \in \mathbb{R}\}$.

The circle group, denoted by $\mathbb{T}$, is the multiplicative group of all complex numbers with absolute value 1, that is, the unit circle in the complex plane or simply the unit complex numbers.



$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\} = \{e^{i2\pi x} | x \in \mathbb{R}\}.$$

Proof. $\mathbb{R}/_{\mathbb{Z}} \cong \mathbb{T}$. Let a map $f : \mathbb{R} \longrightarrow \mathbb{T}$ given by $f(x) = e^{2\pi ix}$.
Note that f is well-define since, $a, b \in \mathbb{R}$

$$a = b \Longleftrightarrow 2\pi ia = 2\pi ib \Longrightarrow e^{2\pi ia} = e^{2\pi ib} \Longleftrightarrow f(a) = f(b).$$

Now f is homomorphism because, let $a, b \in \mathbb{R}$ then

$$f(a + b) = e^{2\pi i(a+b)} = e^{2\pi ia} \cdot e^{2\pi ib} = f(a) \cdot f(b)$$

And f is surjective since $\forall y \in \mathbb{T}, \exists x \in \mathbb{R}$ such that $y = e^{i2\pi x}$
$\implies f(x) = e^{i2\pi x} = y$.
Moreover, $\ker(f) = \{x \in \mathbb{R} : e^{i2\pi x} = 1\}$
$= \{n : n \in \mathbb{Z}\}$.
Then $\ker(f) = \mathbb{Z}$. By Fundamental Theorem of Homomorphisms :

$$\mathbb{R}\big/_{\ker(f)} \cong \mathbb{T}.$$

Therefore

$$\mathbb{R}\big/_{\mathbb{Z}} \cong \mathbb{T}.$$

□

5
Thesis Summary and Future Work

5.1 Thesis Summary

In algebra, which is a broad division of mathematics, abstract algebra (occasionally called modern algebra) is the study of algebraic structures. Algebraic structures include groups, rings, fields, modules, vector spaces, lattices, and algebras. The term abstract algebra was coined in the early 20th century to distinguish this area of study from the other parts of algebra. And in this work we have studied some of them in detail, namely group isomorphism, quotient groups, and fundamental theorem of homomorphism.

We explored almost all parts of the basic concepts in group theory such as group isomorphism, quotient groups, and fundamental theorem of homomorphisms. Firstly, we began our studies with group isomorphism in chapter 1. In the content of this chapter, we recalled some definitions which involve with concept in this chapter. Then we introduced relative between two group that isomorphic each other and gave group isomorphism. And we proved Cayley's theorem which is interesting part. After that we studied some properties of isomorphism acting on elements and on groups. In the end of this chapter, we worked on some applications of isomorphism in linear algebra.

Furthermore, in the second chapter, we studied quotient groups. We introduced definition of cosets. And we started studying what to transform quotient sets to quotient groups through denoting operation on ${}^{G}\!/_{H}$ with H which is subgroup of G. We took conterexample, and then we took definition of normal subgroups which is special condition to work on quotient groups. In the end of chapter 2, we studied applications of quotient groups.

Finally, in the last chapter, we introduced fundamental theorem of homomorphism. We started with definition of homomorphism, image, and kernel. Then we worked on proposition of image and kernel. After that, we studied fundamental theorem of homomorphisms and also its application. In this section, we proved that ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \cong \mathbb{Z}_n$ and ${}^{\mathbb{R}}\!/_{\mathbb{Z}} \cong \mathbb{T}$ which are interesting parts in this section.

5.2 Future Work

There are many more interesting parts I am passionate about learning in abstract algebra. In the future, I am hoping to experience other tools such as field, ring, and trying to find some connections between them.

Bibliography

[1] **Charles C. Pinter**, *A Book of Abstract Algebra*. Second edition, McGraw-Hill Publishing Company, Inc., New York, 1982.

[2] **Joseph A. Gallian**, *Contemporary Abstract Algebra*. Eight edition, CENGAGE Learning, United State of America, 2017.

[3] **Vinod Moreshwar Vaz**, *A Comparative Study of Graph Isomorphism Applications*. (0975-8887), March 7 2017.

[4] **Ellis**, *Properties of Group Isomorphism*. 2011.

[5] **M.Machauley (Clemson)**, *Homomorphisms*. Math 4120. Spring 2014.

[6] **Mathematics Stack Exchange**, *Proof the First Isomorphism Theorem*. 2013.

[7] **Edmund F Robertson**, *The First Isomorphism Theorem*. 11 September 2006.

[8] **Proofwiki**, *Quotient Group of Reals by Integers is Circle Group*. 13 December 2019.