# GROUP THEORY 2

Lecture Notes

5th Edition, 2021

Nor Haniza Sarmin
Faiz Muhammad Khan
Hazzirah Izzati Mat Hassim

Department of Mathematical Sciences,
Faculty of Science,
Universiti Teknologi Malaysia

# Group Theory 2

## LECTURE NOTES

# Group Theory 2

## LECTURE NOTES

**Nor Haniza Sarmin**
**Faiz Muhammad Khan**
**Hazzirah Izzati Mat Hassim**

**Fifth Edition**
**March 2021**

**Department of Mathematical Sciences**
**Faculty of Science**
**Universiti Teknologi Malaysia**
**Johor, Malaysia**

Fifth Edition 2021


*Typeset by*
N. H. SARMIN & H. I. MAT HASSIM
Department of Mathematical Sciences,
Faculty of Science
Universiti Teknologi Malaysia
81310 UTM Johor Bahru
Johor Darul Takzim, Malaysia

F. M. KHAN
Department of Mathematics and Statistics,
University of Swat, Khyber Pakhtunkhwa, Pakistan

*Printed in Malaysia by*
JASAMAX Enterprise
55, Jalan Kebudayaan 2
Taman Universiti
81300 Skudai
Johor Darul Takzim, Malaysia

# CONTENTS


| CHAPTER | | PAGE NO |
|---|---|---|
| | **AUTHORS' PREFACE** | |
| **1** | **SIMPLE GROUPS** | **1** |
| | 1.0 Introduction | 1 |
| | 1.1 Some Properties of Simple Groups | 1 |
| | 1.2 Some Examples of Simple Groups | 3 |
| | 1.3 Maximal Normal Subgroups | 5 |
| | Exercise 1 | 7 |
| **2** | **SERIES OF GROUPS, GROUP ACTIONS ON A SET** | **8** |
| | 2.0 Introduction | 8 |
| | 2.1 Series of Groups | 8 |
| | 2.2 Refinement of Series | 10 |
| | 2.3 Isomorphic Series | 13 |
| | 2.4 Composition/ Principal Series | 14 |
| | 2.5 Solvable Groups | 16 |
| | 2.6 Isotropy Subgroups | 19 |
| | 2.7 Orbit | 19 |
| | Exercise 2 | 21 |
| **3** | **ISOMORPHISM THEOREM** | **22** |
| | 3.0 Introduction | 22 |
| | 3.1 Isomorphism Theorems | 22 |
| | 3.2 Examples on the Isomorphism Theorems | 28 |
| | Exercise 3 | 32 |

| | | |
|---|---|---|
| **4** | **FREE ABELIAN GROUPS** | **33** |
| | 4.0 Introduction | 33 |
| | 4.1 Theorems of Free Abelian Groups | 34 |
| | Exercise 4 | 37 |
| **5** | **FREE GROUPS** | **38** |
| | 5.0 Introduction | 38 |
| | 5.1 Words | 38 |
| | 5.2 Free Group | 39 |
| | 5.3 Homomorphism of Free Groups | 42 |
| | Exercise 5 | 44 |
| **6** | **GROUP PRESENTATIONS** | **45** |
| | 6.0 Introduction | 45 |
| | 6.1 Examples of Groups Presentation | 45 |
| | Exercise 6 | 51 |
| **7** | **RINGS AND INTEGRAL DOMAINS** | **52** |
| | 7.0 Introduction | 52 |
| | 7.1 Types of Rings | 53 |
| | 7.2 Characteristic of a Ring | 56 |
| | Exercise 7 | 58 |
| **8** | **RINGS OF POLYNOMIALS** | **60** |
| | 8.0 Introduction | 60 |
| | 8.1 Rings and Polynomials | 60 |
| | 8.2 The Evaluation Homomorphism | 62 |
| | 8.3 Zero of Polynomials | 64 |
| | Exercise 8 | 67 |

| | | |
|---|---|---|
| **9** | **HOMOMORPHISMS AND FACTOR RINGS** | **68** |
| | 9.0 Introduction | 68 |
| | 9.1 Properties of Ring Homomorphism | 69 |
| | 9.2 Factor (Quotient) Rings | 74 |
| | 9.3 Isomorphism Theorems for Rings | 77 |
| | Exercise 9 | 82 |
| **10** | **MAXIMAL AND PRIME IDEALS** | **83** |
| | 10.0 Introduction | 83 |
| | 10.1 Ideal | 83 |
| | 10.2 Maximal and prime Ideals | 84 |
| | 10.3 Prime Fields | 88 |
| | 9.3 Ideal Structure in $F[x]$ | 89 |
| | Exercise 10 | 91 |
| **11** | **GROBNER BASES FOR IDEALS** | **92** |
| | 11.0 Introduction | 92 |
| | 11.1 Definitions | 92 |
| | 11.2 Grobner Bases | 96 |
| | Exercise 11 | 100 |
| **12** | **INTRODUCTION TO EXTENSION FIELDS, VECTOR SPACE** | **101** |
| | 12.0 Introduction | 101 |
| | 12.1 Extension Fields | 101 |
| | 12.2 Vector Space | 104 |
| | Exercise 12 | 106 |
| **13** | **ALGEBRAIC EXTENSIONS** | **107** |
| | 13.0 Introduction | 107 |
| | 13.1 Extensions | 107 |

13.2 Examples of Algebraic Extensions 110
Exercise 13 111

**REFERENCES** **112**

# Authors' Preface

This is an advanced group theory course for master's level students. The lecture notes are written according to Universiti Teknologi Malaysia's curriculum. It is anticipated that the students have taken the first group theory course in their Master's level.

This lecture notes consist of three parts. The first part includes simple groups, series of groups, group action on a set, isomorphism theorems, free abelian groups, free groups and group presentations. The second part includes properties of rings and fields, integral domains, rings of polynomials, factor rings and ideals and Grobner bases for ideals. The last part includes some advanced topics in group theory which are extension fields, vector spaces and algebraic extensions.

As the reader will soon see, many examples are given in each chapter.

However, the authors feel that having these lecture notes only are not enough. Every student should have or should refer to at least one text book of Graduate Text in Advanced Group Theory.

Finally, the authors wish all readers a joyful voyage on the mathematical journey they are about to further embark into a beautiful realm of group theory.

***N. H. Sarmin, F. M. Khan & H. I. Mat Hassim***

*March 2021*

# CHAPTER 1

# SIMPLE GROUPS



## 1.0 INTRODUCTION

Simple groups are building blocks for all groups because they help to determine the structure of the groups. The term simple group was first used by Camille Jordan (1838-1921). The definition of a simple group is given as follows.

**Definition 1.1 (Simple Group)**

A group is **simple** if its only normal subgroups are the trivial subgroup and the group itself

*In other words, we say that a group is simple if it has no proper nontrivial normal subgroups.*

## 1.1 SOME PROPERTIES OF SIMPLE GROUPS

In this subsection, some important properties of simple groups are presented.

**Theorem 1.1** All abelian groups are not simple.

***Proof*** Since all subgroups of an abelian group are normal, therefore abelian groups are not simple. ■

**Theorem 1.2** Let $G$ be a group and $H$ is a proper subgroup of $G$ of index 2. Then $G$ is not simple.

***Proof*** Since $H$ is of index 2, $H$ is normal in $G$. Thus $G$ is not simple. ■

**Theorem 1.3** All cyclic groups of prime orders are simple.

***Proof*** Let $G$ be a cyclic group of prime order. By Lagrange's theorem, $G$ has no proper nontrivial subgroup and therefore has no proper normal nontrivial subgroup. Thus $G$ is simple. ■

Note that the class of cyclic groups of prime order is the only class of abelian simple groups.

**Theorem 1.4** An abelian group is simple if and only if it is finite and of prime order.

***Proof*** *(Exercise)*

**Theorem 1.5 2-Odd Test**

Suppose $G$ is a group of order $2 \cdot n$, where $n$ is an odd number greater than 1. Then $G$ is not simple.

**Example 1.1**

Let $G$ be a group of order 30. By Theorem 1.5, $G$ is not simple.

**Theorem 1.6 Index Theorem**

If $G$ is a finite group and $H$ is a proper subgroup of $G$ such that $|G|$ does not divide $|G:H|!$, then $H$ contains a nontrivial normal subgroup of $G$. In particular, $G$ is not simple.

**Example 1.2**

Let $G$ be a group of order 20 and $H$ is a subgroup of $G$ of order 5. By Theorem 1.6, since $|G| = 20$ does not divide $|G:H|! = 4! = 24$, then $G$ is not simple.

## 1.2 SOME EXAMPLES OF SIMPLE GROUPS

Some examples of simple groups are given in the following.

**Example 1.3**

The dihedral group of order 8 is not simple. Let $G = D_4$, the dihedral group of order 8. Let $H = \langle R_{90} \rangle$. Then, the index of $H$ in $G$ is

$$\frac{|G|}{|H|} = \frac{|D_4|}{|\langle R_{90} \rangle|} = \frac{8}{4} = 2.$$

By Theorem 1.2, $G$ is not simple. ■

**Example 1.4**

The quaternion group of order 8 is not simple. Let $G = Q$, the quaternion group of order 8. Let $H = \langle i \rangle = \langle j \rangle = \langle k \rangle$. Then, the index of $H$ in $G$ is given in the following :

$$\frac{|G|}{|H|} = \frac{|Q|}{|\langle i \rangle|} = \frac{8}{4} = 2.$$

By Theorem 1.2, $G$ is not simple. ■

Furthermore, we can also see that the quaternion group $Q$ is not simple since every subgroup of $Q$ is normal.

**Example 1.5**

The symmetric group of order 6 is not simple. Let $G = S_3$, the symmetric group of order 6. Let $H = \langle 123 \rangle$. Then, the index of $H$ in $G$ is

$$\frac{|G|}{|H|} = \frac{|S_3|}{|\langle 123 \rangle|} = \frac{6}{3} = 2.$$

By Theorem 1.2, $G$ is not simple. ■

**Example 1.6**

The alternating groups $A_n$ is simple for $n \geq 5$ (See exercise).

**Example 1.7**

A group of order 210 is not simple by Theorem 1.5.

**Example 1.8**

A group of order 80 is not simple. Let $G$ be a group of order 80. Suppose $H$ is a subgroup of $G$ or order 16. By Theorem 1.6, since 80 is not a divisor of 5!, then $G$ is not simple.

**Example 1.9**

There is no simple group of order 30. Assume that $G$ is simple. Then $|G| = 30 = 2 \cdot 3 \cdot 5.$ Since $n(Syl_5 G) = 1(5)$ and $n(Syl_5 G) = 30,$ thus $n(Syl_5 G) = 1$ or 6. Suppose $n(Syl_5 G) = 6$ and $n(Syl_3 G) = 10.$ We count the number of elements of $G$:

$$6(5-1)+1+10(3-1) = 25+20 = 45$$

elements which is greater than the order of $G$; a contradiction. We have to have at least one normal for $Syl_5 G$ or $Syl_3 G.$ So $G$ cannot be simple because there has to be a normal subgroup of $G$. ■

## 1.3 MAXIMAL NORMAL SUBGROUPS

To understand the series of groups in the next chapter, the readers need to understand the concepts of a maximal normal subgroup. The definition and some examples on maximal normal subgroup are included in this subsection.

**Definition 1.2 (Maximal Normal Subgroup)**

$H$ is a maximal normal subgroup of a group $G$ if $H$ is the largest normal subgroup of $G$ (there is no normal subgroup in between $H$ and $G$)

**Example 1.10**

Let $G = D_4$. Then $\langle R_{90} \rangle$ is the maximal normal subgroup of $G$. ■

**Example 1.11**

Let $G = Q$. Then $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$ are the maximal normal subgroups of $G$. ■

**Example 1.12**

Let $G = S_3$. Then $\langle (123) \rangle$ is the only normal subgroup of $G$ and it is also maximal. ■

**Theorem 1.7**

$H$ is a maximal normal subgroup of $G$ if and only if $G/H$ is simple.

***Proof*** *(Exercise)*

**Exercises 1 (Simple Groups)**

1. Show that a group of order 206 is not simple.
2. Prove that there is no simple group of 216.
3. Show that $M$ is a maximal normal subgroup of $G$ if and only if $G/M$ is simple.
4. Let $G$ be a group and $|G| = p$ where $p$ is prime, then $G$ is simple.
5. An abelian group is simple if and only if it is finite and of prime order.
6. Find an example of a non-abelian group that is simple.
7. Show that the alternating groups $A_n$ is simple for $n \geq 5$.

# CHAPTER 2

# SERIES OF GROUPS, GROUP ACTIONS ON A SET



## 2.0 INTRODUCTION

To give insights into the structure of a group $G$, we study a series of embedding subgroups of $G$. Meanwhile, a group action may be defined as a group homomorphism. Subgroup series can simplify the study of a group to the study of simpler subgroups and their relations. Some types of series of groups are given in this chapter.

## 2.1 SERIES OF GROUPS

A special sequence of subgroups of a group called subnormal series is introduced in the following.

**Definition 2.1 (Subnormal Series)**

Let $G$ be a group. If $G$ has a finite sequence of subgroups $H_0, H_1, H_2, ..., G$ such that $H_i \lhd H_{i+1}$ where $H_0 = \{0\}$ and $H_n = G$, then $\{H_i\}$ is a **subnormal series** of $G$.

We give an example of a subnormal series in the following.

**Example 2.1**

Let $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, V, H, D, D'\}$ be the dihedral group of order 8. Then $D_4$ has a subnormal series:

$$\{R_0\} < \{R_0, V\} < \{R_0, R_{180}, V, H\} < D_4. \quad \blacksquare$$

A special case where all subgroups are normal is called a normal series of a group, defined formally in the following.

**Definition 2.2 (Normal Series)**

Let $G$ be a group. If $G$ has a finite sequence of *normal* subgroups of $G$, namely $H_0, H_1, \ldots, H_n$ such that $H_i < H_{i+1}$ where $H_0 = \{e\}$ and $H_n = G$, then $\{H_i\}$ is a normal series of $G$.

Some examples of subnormal series are given in the following, including that which is not subnormal.

**Example 2.2**

Let $G = \mathbb{Z}$ (group of integers). Then the normal series of $G$ is given by

$$\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z} \text{ or } \{0\} < 8\mathbb{Z} < 4\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z}. \quad \blacksquare$$

**Example 2.3**

The series in Example 2.1 is not a normal series of $D_4$.

**Example 2.4**

The following are normal series of $D_4$:

(i) $\langle R_0 \rangle < \langle R_{180} \rangle < D_4$

(ii) $\langle R_0 \rangle < \langle R_{90} \rangle < D_4$

(iii) $\langle R_0 \rangle < \langle R_{180} \rangle < \langle R_{90} \rangle < D_4$

Some properties of subnormal and normal series are given in the following.

**Theorem 2.1** Every **normal** series is a **subnormal** series.

***Proof*** Direct from the definition of normal and subnormal series. ■

**Theorem 2.2** **Abelian groups** have both **subnormal** and **normal** series.

***Proof*** Since every abelian subgroup is normal, then abelian groups have both subnormal and normal series. ■

## 2.2 REFINEMENT OF SERIES

A refinement of a series is a series which contains all the subgroups of the original series, and may contain more. The definition of refinement of subnormal series and normal series are provided below.

**Definition 2.3 (Refinement of Subnormal Series)**

Let $G$ be a group and $\{H_i\}$ and $\{K_j\}$ are normal series of $G$. Then, the series $\{K_j\}$ is a **refinement of a subnormal series** $\{H_i\}$ of $G$ if $\{H_i\} \subseteq \{K_j\}$, that is $H_i$ is one of the $K_j$.

**Definition 2.4 (Refinement of Normal Series)**

Let $G$ be a group and $\{H_i\}$ and $\{K_j\}$ are subnormal series of $G$. Then, the series $\{K_j\}$ is a **refinement of a normal series** $\{H_i\}$ of $G$ if $\{H_i\} \subseteq \{K_j\}$, that is $H_i$ is one of the $K_j$.

An example of a refinement series is given in the following.

**Example 2.5**

Let $G = \mathbb{Z}$ with a normal series: $\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < \mathbb{Z}$.

Then, the refinement of the normal series is given in the following:

$$\{0\} < 72\mathbb{Z} < 24\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}. \quad \blacksquare$$

In mathematics, especially in the fields of group theory and Lie theory, a central series is a kind of normal series of subgroups or Lie subalgebras, expressing the idea that the commutator is nearly trivial. For groups, this is an explicit expression that the group is a nilpotent group, and for matrix rings, this is an explicit expression that in some basis the matrix ring consists entirely of upper triangular matrices with constant diagonal.

**Definition 2.5 (Central Series)**

A **central series** is a normal series in the form $\{e\} \lhd A_1 \lhd A_2 \lhd \ldots \lhd G$ where each successive quotient is central, i.e. $A_{i+1}/A_i \leq Z\left(G/A_i\right)$, where $Z\left(G/A_i\right)$ is the center of the factor group $G/A_i$.

If the series is ordered in the form $\{e\} \lhd A_1 \lhd A_2 \lhd \ldots \lhd G$, it is called an **upper central series**, and a series in the form $G \rhd A_1 \rhd A_2 \rhd \ldots \rhd \{e\}$ is called a **lower central series**.

Suppose $\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \ldots \lhd H_n = G$ is an upper central series for a group *G*. Then the **length** of the series is *n*.

Nilpotent groups arise in Galois theory, as well as in the classification of groups. They also appear prominently in the classification of Lie groups.

**Definition 2.6 (Nilpotent Group, Nilpotency Class)**

A group $G$ is said to be **nilpotent** if its central series is of finite length. A nilpotent group with a central series of shortest length $n$ is said to be **nilpotent of class *n***.

Some examples of nilpotent groups are given in the following.

**Example 2.6**

The symmetric group of order 6, $S_3$, is nilpotent of class 1, the dihedral group of order 8, $D_4$, and the quaternion group of order 5, $Q$, are nilpotent of class 2 (as an exercise, find their upper central series). ■

## 2.3 ISOMORPHIC SERIES

The definition and some examples of isomorphic series are provided in this section.

**Definition 2.7 (Isomorphic Series)**

Two subnormal / normal series $\{H_i\}$ and $\{K_j\}$ of the same group $G$ is isomorphic if there exists a one to one correspondence between the collections of factor group $\left\{H_{i+1}/H_i\right\}$ and $\left\{K_{j+1}/K_j\right\}$ such that the corresponding factor group is isomorphic to each other.

**Example 2.7**

Two series of $\mathbb{Z}_{15}$ are given as follows:

i) $\{0\} < \langle 5 \rangle < \mathbb{Z}_{15}$,

ii) $\{0\} < \langle 3 \rangle < \mathbb{Z}_{15}$.

Both are isomorphic as there exists a one to one corresponding factor group that are isomorphic to each other:

i) $\mathbb{Z}_{15}/\langle 5 \rangle$ and $\langle 3 \rangle/\{0\} \cong \mathbb{Z}_5$.

ii) $\mathbb{Z}_{15}/\langle 3\rangle$ and $\langle 5\rangle/\{0\} \cong \mathbb{Z}_3$.

A group of results known under the general name Jordan–Hölder theorem asserts that whenever normal series exist, the isomorphism classes of simple pieces and their multiplicities are uniquely determined. The definition of Jordan-Holder Theorem is given in the following.

**Theorem 2.3 The Jordan – Hölder Theorem**

Two subnormal or normal series of a group *G* have an isomorphic refinement.

**Example 2.8**

The series $\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$ is a refinement of the series $\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$, while $\{0\} < 72\mathbb{Z} < 18\mathbb{Z} < 9\mathbb{Z} < \mathbb{Z}$ is a refinement of $\{0\} < 9\mathbb{Z} < \mathbb{Z}$.

The series $\{0\} < 72\mathbb{Z} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$ is isomorphic to the series $\{0\} < 72\mathbb{Z} < 18\mathbb{Z} < 9\mathbb{Z} < \mathbb{Z}$ since there exists a one to one corresponding factor group that are isomorphic to each other, namely: $\mathbb{Z}_4$, $\mathbb{Z}_2$, and $\mathbb{Z}_9$.

■

## 2.4 COMPOSITION / PRINCIPAL SERIES

In abstract algebra, a composition series provides a way to break up an algebraic structure, such as a group or a module, into simple pieces. The

need for considering composition series in the context of modules arises from the fact that many naturally occurring modules are not semisimple, hence cannot be decomposed into a direct sum of simple modules.

**Definition 2.8 (Composition of Subnormal Series)**

A **subnormal** series $\{H_i\}$ of $G$ is a **composition** series if all the factor groups $\left\{ H_{i+1} / H_i \right\}$ are simple.

**Definition 2.9 (Composition of Normal Series)**

A **normal** series $\{H_i\}$ of $G$ is a **principal (or chief)** series if all the factor groups $\left\{ H_{i+1} / H_i \right\}$ are simple.

**Example 2.9**

i) Given the series $\{e\} < A_n < S_n$ :

The factor group:

a) $A_n / \{e\} \cong A_n$ which is only simple if $n \geq 5$,

b) $S_n / A_n \cong \mathbb{Z}_2$ which is simple.

Therefore, the series are both composition and principal series for $n \geq 5$.

■

## 2.5 SOLVABLE GROUPS

In the field of group theory, a solvable group (or is sometimes called soluble group) is a group that can be constructed from abelian groups using extensions. That is, a solvable group is a group whose derived series terminates in the trivial subgroup.

Historically, the word "solvable" arose from Galois theory and the proof of the general unsolvability of quantic equation. Specifically, a polynomial equation is solvable by radicals if and only if the corresponding Galois group is solvable.

**Definition 2.10 (Solvable Groups)**

A group $G$ is **solvable** if it has a composition series $\{H_i\}$ such that all factor groups $\left\{H_{i+1}/H_i\right\}$ are abelian.

**Theorem 2.4** All abelian groups are solvable.

***Proof*** All subgroups of abelian groups are abelian. Hence, all of its factor groups are also abelian, thus they are solvable. ■

**Example 2.10**

The symmetric group of order 6, $S_3$, is solvable. Given the composition series $\{e\} < A_3 < S_3$. Then both of the factor groups:

$$A_3/\{e\} \cong \mathbb{Z}_3 \text{ and } S_3/A_3 \cong \mathbb{Z}_2 \text{ are abelian.}$$

Therefore, $S_3$ is solvable. ■

**Example 2.11**

The symmetric group of order 120, $S_5$, is not solvable. Given the composition series $\{e\} < A_5 < S_5$. Then, the factor groups:

$$A_5/\{e\} \cong A_5 \text{ is not abelian although } S_5/A_5 \cong \mathbb{Z}_2 \text{ is abelian.}$$

Therefore, $S_5$ is not solvable. ■

Before discussing on the group actions on a set, recall the binary operation given as in the following.

**Definition 2.11 (Binary Operation)**

Let $G$ be a set. A binary operation $*$ on $G$ is a function that assigns each ordered pair of elements of $G$ an element of $G$ i.e.

$$*: G \times G \to G.$$

The theory of groups first dealt with permutation groups. Later on the notion of an abstract group was introduced in order to examine the properties of permutation groups which did not refer to the set on which the permutations acted. We extend the notion of a permutation on a set to a group action on a set.

In the following, we will be concerned with the case where $X$ is a set, $G$ is a group, and we have a map $*: G \times X \to X$. We will write $*(g, x)$ as $g * x$ or $gx$.

**Definition 2.12 (Group Action)**

Let $X$ be a set and $G$ be a group. An action $*$ of $G$ on $X$ is a map $*: G \times X \to X$ such that

1. $e * x = x$ for all $x \in X$,

2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, $X$ is a $G$-set.

**Example 2.12**

Let $X$ be any set and $H$ be a subgroup of the group $S_x$ of all permutations of $X$. Then $X$ is an $H$-set, where the action $\sigma \in H$ on $X$ is its action as an element of $S_x$, so that $\sigma x = \sigma(x)$ for all $x \in X$. ■

Condition 2 is a consequence of the definition of permutation multiplication as function composition, and Condition 1 is immediate from the definition of the identitiy permutation as the identity function. Note that, in particular, $\{1,2,3,\ldots,n\}$ is an $S_n$ set.

**Example 2.13**

Every group $G$ is itself a $G$-set, where the action on $g_2 \in G$ by $g_1 \in G$ is given by left multiplication. This means $*(g_1, g_2) = g_1 g_2$. If $H$ is a subgroup of $G$, we can also regard $G$ as an $H$-set, where $*(h, g) = hg$. ■

**Example 2.14**

Let $H$ be a subgroup $G$. Then $G$ is an $H$-set under conjugation where $*(h, g) = hgh^{-1}$ for $g \in G$ and $h \in H$. Condition 1 is obvious, and for Condition 2, note that

$$*(h_1 h_2, g) = (h_1 h_2) g (h_1 h_2)^{-1} = h_1 (h_2 g h_2^{-1}) h_1^{-1} = *(h_1, *(h_2, g)).$$ ■

## 2.6 ISOTROPY SUBGROUPS

The definition of isotropy subgroup is given in this section.

**Definition 2.13 (Isotropy Subgroup)**

Let $X$ be a $G$ set and let $x \in X$. The subgroup $G_x$ is the **isotropy subgroup** of $x$ where $X_g = \{x \in X \mid gx = x\} \subseteq X$ and $G_x = \{g \in G \mid gx = x\} \subseteq G$.

## 2.7 ORBITS

In mathematics, in the study of dynamical systems, an orbit is a collection of points related by the evolution function of the dynamical system. It can be understood as the subset of phase space covered by the trajectory of the dynamical system under a particular set of initial conditions, as the system evolves. As in Group Theory, the concepts of orbits are provided in the following.

**Definition 2.14 (Orbit)**

Let $X$ be a $G$ set. Each cell in the partition of the equivalent relation is an **orbit** in $X$ under $G$. If $x \in X$, the cell containing $x$ is the orbit of $x$.

**Theorem 2.5** Let $X$ be a $G$ set and $x \in X$. Then $|G_x| = (G : G_x)$.

If $|G|$ is finite, then $|G_x|$ is a divisor of $|G|$.

**Example 2.15**

Let $X = \{1,2,3,4\}$ be the $D_4$ set with $G = D_4$. Then we have $G_1 = \{1,2,3,4\}$ and $G_1 = \{R_0, D\}$. Since $|G| = 8$, we have $|G_1| = (G : G_1) = 4$. ■

**Theorem 2.6**

Let $X_i$ be an orbit of $X$. Then $\bigcup_{i=1}^{n} X_i = X$.

**Exercises 2 (Series of Groups, Group Actions on a Set)**

1. Let $G$ be a dihedral group of order 8, $D_4$. Find (if possible):

   i. all subnormal series which are not normal series.

   ii. all normal series.

   Which one is a refinement to the other one?

   iii. an upper central series of $G$ and thus state its nilpotency class.

2. Repeat Question 1 with the quaternion group of order 8, $Q$.

3. Repeat Question 1 with the symmetric group of order 24, $S_4$.

4. Give isomorphic refinements of the two series below

$$\{0\} < 10\mathbb{Z} < \mathbb{Z} \text{ and } \{0\} < 25\mathbb{Z} < \mathbb{Z}.$$

   Explain your answer.

5. Decide whether $D_4$ is solvable or not.

# CHAPTER 3

# ISOMORPHISM THEOREMS



## 3.0 INTRODUCTION

One of the main uses of the concept of an isomorphism is the classification of algebraic structures. Another important use of an isomorphism is the representation of one algebraic structure by means of another.

In this section, we continue our study of isomorphisms. Our objective is to prove the fundamental theorem of homomorphism, the isomorphism theorems and the correspondence theorem. These theorems replicate the relationship between homomorphisms and quotient groups.

There are several theorems concerning isomorphic factor group that are known as the isomorphism theorem in group theory.

## 3.1 ISOMORPHISM THEOREMS

In this subsection, some theorems on the concepts of isomorphism with their proofs are presented.

**Theorem 3.1 (The Fundamental Homomorphism Theorem)**

Let $\phi: G \to G'$ be a group homomorphism with kernel, $H$. Then $\phi[G]$ is a group and $\mu: G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is a homomorphism. If $\gamma_K: G \to G/H$ is an isomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu\gamma(g)$ for all $g \in G$.

***Proof*** We illustrate Theorem 3.1 in Figure 3.1.

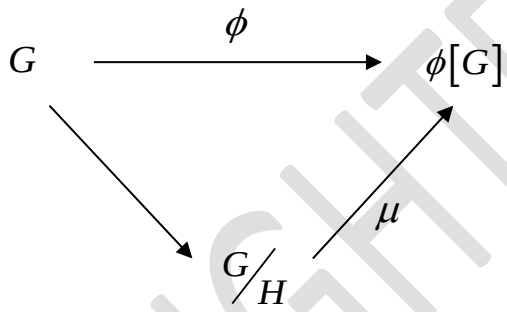


**Figure 3.1**

Define $\mu: G/H \to G'$ by $\mu(aH) = \phi(a)$ for all $aH \in G/H$. If $aH = bH$ then $b^{-1}aH = H$ implies $b^{-1}a \in H \subseteq Ker\,\phi$ and so $\phi(b^{-1}a) = e'$ implies

$$\phi(b^{-1})\phi(a) = e' \text{ or } [\phi(b)]^{-1}\phi(a) = e' \text{ or } \phi(a) = \phi(b)e' \text{ or } \phi(a) = \phi(b).$$

Hence, $\mu(aH) = \mu(bH)$ shows that $\mu$ is well defined. Let $a \in G$. Then

$$(\mu \circ \gamma_K)(a) = \mu(\gamma_K(a)) = \mu(aH) = \phi(a).$$

Therefore $\phi = \mu \circ \gamma_K$. Since $\phi$ maps $G$ onto $G'$, $\mu$ must map $G/H$ onto $G'$. Now

$$\mu((aH)(bH)) = \mu((ab)H) = \phi(ab) = \phi(a)\,f\,(b) = \mu(aH)\mu(bH).$$

Hence $\mu$ is homomorphism of $G/H$ onto $G'$ satisfying $\phi = \mu \circ \gamma_K$. To prove the uniqueness part, let us assume there exists a homomorphism $\mu' : G/H \xrightarrow{onto} G'$ such that $\phi = \mu' \circ \gamma_K$. Then

$$\mu(aH) = \phi(a) = (\mu' \circ \gamma_K)(a) = \mu'(\gamma_K(a)) = \mu'(aH)$$

for all $aH \in G/H$ and so $\mu = \mu'$. Hence, $\mu$ is the only homomorphism of $G/H$ onto $G'$ such that $\phi = \mu \circ \gamma_K$. Next $\mu$ is one-one since $H = Ker\,\phi$. ■

**Theorem 3.2 (First Isomorphism Theorem)**

Let $\phi : G \to G^*$ be a homomorphism with kernel $K$ and let $\gamma_K : G \to G/K$ be the canonical homomorphism. There is a unique isomorphism $\mu : G/K \to \phi[G]$ such that $\phi(x) = \mu(\gamma_K(x))$ for each $x \in G$.

***Proof*** We illustrate Theorem 3.2 in Figure 3.2.

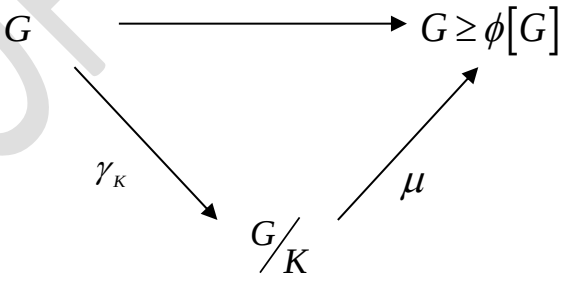


**Figure 3.2**

Since $G$ is a group, therefore $e \in G$ and hence $\phi(e) \in \phi(G)$ i.e. $\phi(G)$ is non-empty. Let $\phi(a), \phi(b) \in \phi(G)$, where $a, b \in G$.

Consider,

$$\phi(a)\cdot\left(\phi(b)\right)^{-1} = \phi(a)\cdot\phi\left(b^{-1}\right)$$
$$= \phi\left(ab^{-1}\right) \in \phi(G) \text{ (because } ab^{-1} \in G \text{ for all } a,b \in G).$$

This implies $\phi(a)\cdot\left(\phi(b)\right)^{-1} \in \phi(G)$ hence $\phi(G)$ is a subgroup of $G^*$.

For the second part, let $Ker\,\phi = K$ and define $\mu: {}^{G}\!/_{K} \to f(G)$ by $\mu(Kg) = \phi(g)$ for all $g \in G$. Let $Kg_1 = Kg_2$, then

$$(Kg_1)(Kg_2)^{-1} = (Kg_2)(Kg_2)^{-1}$$
$$= K\left(\text{Identity of } {}^{G}\!/_{K}\right).$$

Thus, this leads to the following:

$$\Rightarrow (Kg_1)\left(Kg_2^{-1}\right) = (Kg_2)\left(Kg_2^{-1}\right)$$
$$\Rightarrow Kg_1g_2^{-1} = Kg_2g_2^{-1}$$
$$\Rightarrow Kg_1g_2^{-1} = Ke$$
$$\Rightarrow Kg_1g_2^{-1} = K \ \left(\text{Identity of } {}^{G}\!/_{K}\right)$$
$$\Rightarrow g_1g_2^{-1} \in K$$
$$\Rightarrow \phi\left(g_1g_2^{-1}\right) = e^* \ \left(\text{Identity of } G^*\right)$$
$$\Rightarrow \phi(g_1).f(g_2^{-1}) = e^*$$
$$\Rightarrow \phi(g_1).f\left(g_2\right)^{-1} = e^*$$
$$\Rightarrow \phi(g_1) = f\left(g_2\right)$$
$$\Rightarrow \mu(Kg_1) = h(Kg_2).$$

This shows that $\mu: {}^{G}\!/_{K} \to \phi(G)$ is well defined.

Let $\mu(Kg_1) = \mu(Kg_2)$. Then

$$\Rightarrow \phi(g_1) = \phi(g_2)$$
$$\Rightarrow \phi(g_1).\phi(g_2)^{-1} = e^*$$
$$\Rightarrow \phi(g_1).\phi(g_2^{-1}) = e^*$$
$$\Rightarrow \phi(g_1 g_2^{-1}) = e^*$$
$$\Rightarrow g_1 g_2^{-1} \in K$$
$$\Rightarrow Kg_1 g_2^{-1} = K$$
$$\Rightarrow Kg_1 = Kg_2.$$

Hence $\mu : {}^{G}\!/_{K} \to \phi(G)$ is one-one.

Now, let $x \in \phi(G)$, then $x = \phi(g)$ for some $g \in G$. Therefore $\mu(Kg) = \phi(g) = x \in \phi(G)$ this shows that $\mu : {}^{G}\!/_{K} \to \phi(G)$ is onto.

Finally consider,

$$\begin{aligned}\mu\big((Kg_1)\cdot(Kg_2)\big) &= \mu(Kg_1 \cdot g_2)\\ &= \phi(g_1 \cdot g_2)\\ &= \phi(g_1)\cdot\phi(g_2) \ (\phi \text{ is homomorphism})\\ &= \mu(Kg_1)\cdot\mu(Kg_2).\end{aligned}$$

This shows that $\mu : {}^{G}\!/_{K} \to \phi(G)$ is homomorphism. Consequently ${}^{G}\!/_{Ker\phi} \cong \phi(G)$. ■

**Theorem 3.3 (Second Isomorphism Theorem)**

Let $H$ be a subgroup of $G$ and let $N$ be a normal subgroup of $G$. Then

$${}^{HN}\!/_{N} \cong {}^{H}\!/_{(H \cap N)}.$$

***Proof*** Let $\gamma : G \to {}^{G}\!/_{N}$ be a natural homomorphism and $H \le G$.

Then $\gamma[H]$ is a subgroup of ${}^{G}\!/_{N}$. *(By theorem: let $\varphi : G \to G'$ be a homomorphism. If $H \le G$ then $\varphi[H] \le G'$).*

Now consider

**Case I:** $\gamma$ restricted to $H$

These give us with a homomorphism mapping $H$ onto $\gamma[H]$ and Kernel is the intersection $H \cap N$. Theorem 3.2 shows that there is isomorphism

$$\mu_1 = {H}/{(H \cap N)} \to \gamma[H].$$

**Case II:** $\gamma$ restricted to $HN$

These give us with a homomorphism mapping $HN$ onto $\gamma[H]$, since $\gamma(n)$ is the identity $N$ of ${G}/{N}$ for all $n \in N$ and the kernel is $N$.

By Theorem 3.2, there is an isomorphism

$$\mu_2 = {(HN)}/{N} \to \gamma[H].$$

Since results are both isomorphic to $\gamma[H]$, they are isomorphic to each other.

Therefore ${(HN)}/{N} \cong {H}/{(H \cap N)}$. ■

**Example 3.1**

Let $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, $H = \mathbb{Z} \times \mathbb{Z} \times \{0\}$ and $N = \{0\} \times \mathbb{Z} \times \mathbb{Z}$. Then clearly $HN = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ and $H \cap N = \{0\} \times \mathbb{Z} \times \{0\}$. We have ${(HN)}/{N} \cong \mathbb{Z}$ and we also have ${H}/{(H \cap N)} \cong \mathbb{Z}$. ■

**Theorem 3.4 (Third Isomorphism Theorem)**

Let $H$ and $K$ be normal subgroups of group $G$ with $K \le H$. Then $G/H \cong \left(G/K\right)\Big/\left(H/K\right)$.

***Proof*** Let $\varphi : G \to \left(G/K\right)\Big/\left(H/K\right)$ be given by $\varphi(a) = (aK)\left(H/K\right)$ for all $a \in G$.

Clearly $\varphi$ is onto $\left(G/K\right)\Big/\left(H/K\right)$ and for $a,b \in G$,

$$\begin{aligned}\varphi(ab) &= \left[(ab)K\right]\left(H/K\right)\\ &= \left[(aK)(bK)\right]\left(H/K\right)\\ &= \left[(aK)\left(H/K\right)\right]\left[(bK)\left(H/K\right)\right]\\ &= \varphi(a)\varphi(b).\end{aligned}$$

So $\varphi$ is a homomorphism.

The kernel consists of those $x \in G$ such that $\varphi(x) = \left(H/K\right)$ and these $x$ are just the elements of $H$.

Then Theorem 3.1 shows that $G/H \cong \left(G/K\right)\Big/\left(H/K\right)$. ■

## 3.2 EXAMPLES ON THE ISOMORPHISM THEOREMS

In the following examples, we illustrate the First Isomorphism Theorem.

**Example 3.2**

Let $f$ be the homomorphism of $(\mathbb{Z},+)$ onto $(\mathbb{Z}_3,+_3)$ defined by $f(n)=[n]$ for all $n\in\mathbb{Z}$. Let $g$ be the natural homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}/\langle 6\rangle$. Now $\langle 6\rangle$ is normal subgroup of $\mathbb{Z}$ and $\langle 6\rangle\subset\langle 3\rangle = Ker\ f$. Thus, there exists a homomorphism $h$ of $\mathbb{Z}/\langle 6\rangle$ onto $\mathbb{Z}_3$ such that $f=h\circ g$.

The homomorphism $h$ is defined by $h(n+\langle 6\rangle)=[n]$, $n=0,1,2,\ldots,5$.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\ f\ } & \mathbb{Z}_3 \\ & {\scriptstyle g}\searrow \quad \nearrow{\scriptstyle h} & \\ & \mathbb{Z}/\langle 6\rangle & \end{array}$$

We illustrate the second isomorphism theorem with the help of the following example.

**Example 3.3**

Consider the group $(\mathbb{Z},+)$ and its subgroups $H=\langle 2\rangle$ and $N=\langle 3\rangle$. Then $H+N=\langle 2\rangle+\langle 3\rangle=\mathbb{Z}$ and $H\cap N=\langle 6\rangle$. Theorem 3.3 says that

$$(H+N)/N \cong H/(H\cap N),$$

i.e.,

$$\langle 2\rangle/\langle 6\rangle \cong \mathbb{Z}/\langle 3\rangle.$$

This isomorphism is evident if we notice that

$\langle 2\rangle/\langle 6\rangle=\{0+\langle 6\rangle,2+\langle 6\rangle,4+\langle 6\rangle\}$ while $\mathbb{Z}/\langle 3\rangle=\{0+\langle 3\rangle,1+\langle 3\rangle,2+\langle 3\rangle\}$.

The mapping

$$h: {\langle 2\rangle}/{\langle 6\rangle} \to {\mathbb{Z}}/{\langle 3\rangle}$$

defined by $h: 0+\langle 6\rangle \to 0+\langle 3\rangle,\ 2+\langle 6\rangle \to 2+\langle 6\rangle,\ 4+\langle 6\rangle \to 1+\langle 3\rangle$ is the desired homomorphism.

We illustrate the third isomorphism theorem with the help of the following example.

**Example 3.4:**

Consider the group $(\mathbb{Z},+)$ and the subgroups $\langle 6\rangle$ and $\langle 3\rangle$ of $\mathbb{Z}$. Then

$${\mathbb{Z}}/{\langle 3\rangle} = \{0+\langle 3\rangle,\ 1+\langle 3\rangle,\ 2+\langle 3\rangle\}.$$

$${\mathbb{Z}}/{\langle 6\rangle} = \{0+\langle 6\rangle,\ 1+\langle 6\rangle,\ 2+\langle 6\rangle,\ 3+\langle 6\rangle,\ 4+\langle 6\rangle,\ 5+\langle 6\rangle\}.$$

$${\langle 3\rangle}/{\langle 6\rangle} = \{0+\langle 6\rangle,\ 3+\langle 6\rangle\}.$$

Now,

$$\left({\mathbb{Z}}/{\langle 6\rangle}\right) \Big/ \left({\langle 3\rangle}/{\langle 6\rangle}\right) = \{\bar{0}, \bar{1}, \bar{2}\},$$

where

$$\bar{0} = 0+\langle 6\rangle + \left({\langle 3\rangle}/{\langle 6\rangle}\right)$$

$$\bar{1} = 1+\langle 6\rangle + \left({\langle 3\rangle}/{\langle 6\rangle}\right)$$

$$\bar{2} = 2+\langle 6\rangle + \left({\langle 3\rangle}/{\langle 6\rangle}\right).$$

It is now clear that

$$\mathbb{Z}/\langle 3\rangle \cong \left(\mathbb{Z}/\langle 6\rangle\right) \Big/ \left(\langle 3\rangle/\langle 6\rangle\right).$$

Since both are cyclic groups of order 3 and of course, by Theorem 3.4. ■

**Example 3.5**

Consider $K = 6\mathbb{Z} < H = 2\mathbb{Z} < G = \mathbb{Z}$. Then $G/H = \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$. Now $G/K = \mathbb{Z}/(6\mathbb{Z})$ have elements $6\mathbb{Z}$, $1+6\mathbb{Z}$, $2+6\mathbb{Z}$, $3+6\mathbb{Z}$, $4+6\mathbb{Z}$ and $5+6\mathbb{Z}$. Of these six cosets, $6\mathbb{Z}$, $2+6\mathbb{Z}$ and $4+6\mathbb{Z}$ lie in $2\mathbb{Z}/6\mathbb{Z}$.

Thus, have two elements and it isomorphic to $\mathbb{Z}_2$ also.

Alternatively, we see that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$, and $2\mathbb{Z}/6\mathbb{Z}$ correspond under this isomorphism to the cyclic subgroup $\langle 2\rangle$ of $\mathbb{Z}_6$.

Thus $\left(\mathbb{Z}/6\mathbb{Z}\right) \Big/ \left(2\mathbb{Z}/6\mathbb{Z}\right) \cong \mathbb{Z}_6/\langle 2\rangle \cong \mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z}$. ■

**Exercises 3 (Isomorphism Theorems)**

1. Let $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ be the homomorphism such that $\varphi(1) = 2$.

   (i) Find the kernel $K$ of $\phi$.

   (ii) List the cosets in $\mathbb{Z}_{12}/K$, showing the elements in each coset.

   (iii) Give the correspondence between $\mathbb{Z}_{12}/K$ and $\mathbb{Z}_3$ given by the map $\mu$ described in the First Isomorphism Theorem.

2. In the group $\mathbb{Z}_{24}$, let $H = \langle 4 \rangle$ and $N = \langle 6 \rangle$.

   (i) List the elements in $HN$ (which we might write $H + N$ for these additive groups) and in $H \cap N$.

   (ii) List the cosets in $HN/N$, showing the elements in each coset.

   (iii) List the cosets in $H/(H \cap N)$, showing the elements in each coset.

   (iv) Give the correspondence between $HN/N$ and $H/(H \cap N)$, described in the Second Isomorphism Theorem.

3. In the group $G = \mathbb{Z}_{24}$, let $H = \langle 4 \rangle$ and $K = \langle 8 \rangle$.

   (i) List the cosets in $G/H$, showing the elements in each coset.

   (ii) List the cosets in $G/K$, showing the elements in each coset.

   (iii) List the cosets in $H/K$, showing the elements in each coset.

   (iv) List the cosets in $(G/K)/(H/K)$, showing the elements in each coset.

   (v) Give the correspondence between $G/H$ and $(G/K)/(H/K)$, described in the Third Isomorphism Theorem.

# CHAPTER 4

# FREE ABELIAN GROUPS



## 4.0 INTRODUCTION

Free abelian groups have properties which make them similar to vector spaces and allow a general abelian group to be understood as a quotient of a free abelian group by "relations". Every free abelian group has a rank defined as the cardinality of a basis. The rank determines the group up to isomorphism, and the elements of such a group can be written as finite formal sums of the basis elements.

Every subgroup of a free abelian group is itself free abelian, which allows the description of a general abelian group as a co-kernel of an injective homomorphism between free abelian groups.

**Definition 4.1 (A Free Abelian Group)**

A free abelian group is an abelian group that has a basis. This means that every element of the group can be written in one and only one way as a finite linear combination of elements of the basis, with integer coefficients.

Suppose $G$ is an abelian group with a generating set $X$ and $X$ is a subset of nonzero abelian group $G$ that satisfies the following conditions:

1. Each nonzero element $a$ in $G$ can be uniquely expressed in the form $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ for $n_i \neq 0$ in $\mathbb{Z}$ and $x_i$ in $X$.
2. $X$ generates $G$, and $n_1x_1 + n_2x_2 + \ldots + n_rx_r = 0$ for $n_i \in \mathbb{Z}$ and distinct $x_i \in X$ if and only if $n_1 = n_2 = \cdots = n_r = 0$.

Then $G$ is a **free abelian group**, and $X$ is a basis of the group $G$.

**Example 4.1**

The group $\mathbb{Z} \times \mathbb{Z}$ is free abelian and $\{(1,0),(0,1)\}$ is a basis. In general, $\underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n \text{ times}}$ is free abelian with a basis

$$\{(1,0,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots,1)\}. \blacksquare$$

## 4.1 THEOREMS OF FREE ABELIAN GROUPS

In this subsection, some important theorems on the concept of free abelian groups are provided.

**Theorem 4.1** If $G$ is a nonzero free abelian group with a basis of $r$ elements, then $G$ is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for $r$ factors.

**Theorem 4.2** Let $G \neq \{0\}$ be a free abelian group with a finite basis. Then every basis of $G$ is finite, and all bases have the same number of elements.

***Proof*** Let $G$ have a basis $\{x_1, x_2, \cdots, x_n\}$, Then $G \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for $r$ factors. Let $2G = \{2g \,|\, g \in G\}$. We can show $2G$ is a subgroup of $G$. Since $G \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for $r$ factors,

$$G/2G \cong (\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}) / (2\mathbb{Z} \times 2\mathbb{Z} \times \cdots \times 2\mathbb{Z})$$

$$\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \text{ for } r \text{ factors}$$

Thus $\left|G/2G\right| = 2^r$.

The number of elements in any finite basis $X$ is $\log_2 \left|G/2G\right|$, i.e. $\log_2 2^r = r$. Thus any two finite bases have the same numbers of elements. It remains to show that $G$ cannot have an infinite basis.

Let $Y$ be any basis for $G$. Let $\{y_1, y_2, \cdots, y_s\}$ be distinct elements in $Y$. Let $H$ be the subgroup of $G$ generated by $\{y_1, y_2, \cdots, y_s\}$, and let $K$ be the subgroup of $G$ generated by the remaining elements of $Y$. It can be readily checked that

$$G \cong H \times K.$$

thus, $G/2G \cong (H \times K)/(2H \times 2K)$. Since $\left|H/2H\right| = 2^s$, then $\left|G/2G\right| \geq 2^r$.

Since we have $\left|G/2G\right| = 2^r$, thus $s \leq r$.

Then $Y$ cannot be an infinite set, for we could take $s > r$. ■

**Definition 4.2 (Rank)**

If $G$ is free abelian group, the **rank** of $G$, $r$ is the number of elements in a basis for $G$. (All bases have the same number of elements). The trivial group $\{0\}$ is a free abelian group of rank 0.

An example of rank of a group is given in the following.

**Example 4.2**

The rank of $\mathbb{Z}$ is 1, $\mathbb{Z}\times\mathbb{Z}$ is 2 and $\underbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n}$ is $n$. ■

**Theorem 4.3** Let $G$ be a finitely generated abelian group with generating set $\{a_1, a_2, \cdots, a_n\}$. Let

$$\varphi : \underbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n \text{ factors}} \to G$$

be defined by $\varphi(h_1, h_2, \cdots, h_n) = h_1a_1 + h_2a_2 + \cdots + h_na_n$. Then $\varphi$ is a homomorphism onto $G$.

***Proof*** Since $X = \{a_1, a_2, \cdots, a_n\}$ is the generating set of $G$

$\forall g \in G\ \exists c_1, c_2, \cdots, c_n \in \mathbb{Z}$ s.t. $g = c_1a_1 + c_2a_2 + \cdots + c_na_n$

thus $(x_1, x_2, \cdots, x_n) = (c_1, c_2, \cdots, c_n)$ (onto)

$\varphi : G \to H, g, h \in G$

$\varphi(g+h) = \varphi(g) + \varphi(h)$

$$\begin{aligned}
\varphi(g+h) &= \varphi((x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n)) \\
&= \varphi(x_1, x_2, \cdots, x_n) + \varphi(y_1, y_2, \cdots, y_n) \\
&= \varphi(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n) \\
&= (x_1 + y_1)a_1 + (x_2 + y_2)a_2 + \cdots + (x_n + y_n)a_n \\
&= (x_1a_1 + y_1a_1) + (x_2a_2 + y_2a_2) + \cdots + (x_na_n + y_na_n) \\
&= (x_1a_1 + x_2a_2 + \cdots + x_na_n) + (y_1a_1 + y_2a_2 + \cdots + y_na_n).
\end{aligned}$$

Thus $\varphi$ is a homomorphism onto $G$. ■

**Exercises 4 (Free Abelian Groups)**

1. Decide whether the following is a basis for $\mathbb{Z}\times\mathbb{Z}$. Give your reasons.

   (i) $\{(1,1),(-2,-2)\}$

   (ii) $\{(1,1),(1,-2)\}$

   (iii) $\{(2,1),(3,1)\}$

   (iv) $\{(2,1),(4,1)\}$.

2. Show that if $G$ and $G'$ are free abelian groups, then $G\times G'$ is free abelian.

3. Show that if $G_1, G_2, \cdots, G_n$ are free abelian groups, then $G_1\times G_2\times\cdots\times G_n$ is free abelian.

# CHAPTER 5

# FREE GROUPS



## 5.0 INTRODUCTION

Free groups first arose in the study of hyperbolic geometry, as examples of Fuchsian groups (discrete groups acting by isometries on the hyperbolic plane). A group is called a free group if no relation exists between its group generators other than the relationship between an element and its inverse required as one of the defining properties of a group. In this chapter, we discuss a portion of group theory that is of great interest not only in algebra but in topology as well.

## 5.1 WORDS

Words play an important role in the theory of free groups and presentations, and are central objects of study in combinatorial group theory. Therefore, the definition of a word is given as follows.

**Definition 5.1 (A Word)**

If $X$ is a subset of a group $G$, a **word** on $X$ is either 1 or an element $w$ of $G$ of the form

$$w = x_1^{e_1} \cdots x_n^{e_n},$$

where $x_i \in X$ and $e_i = \pm 1$.

Some examples of a word are given in the following.

**Example 5.1**

Let $A$ be any set of elements $a_i$, for $i \in I$. For example, $A = \{a_1, a_2, a_3\}$. Then,

$$a_2^{\,3} a_2^{\,-1} a_3 a_1^{\,2} a_1^{\,-7},\ a_1 a_3^{\,-4} a_2^{\,2} a_3 \text{ and } a_3^{\,2}$$

are all words, if we follow the convention of understanding that $a_i^{\,1}$ is the same as $a_i$. ■

There are two natural types of modifications of certain words, the **elementary contractions:**

a) Replacing an occurrence of $a_i^{\,m} a_i^{\,n} = a_i^{\,m+n}$

b) Replacing an occurrence of $a_i^{\,0} = 1$ i.e dropping it out of the word where 1 is an empty word called the identity element.

**Example 5.2**

The reduced form of the word $a_2^{\,3} a_2^{\,-1} a_3 a_1^{\,2} a_1^{\,-7}$ is $a_2^{\,2} a_3 a_1^{\,-5}$. ■

## 5.2 FREE GROUP

In this subsection, some important definitions and theorems on the concept of free groups are provided.

Let the set of all reduced words formed from our alphabet $A$ be $F[A]$. Now we make $F[A]$ into a group in a natural way. For $w_1$ and $w_2$ elements of $F[A]$, define $w_1 \cdot w_2$ to be reduced form of the word obtained by the juxtaposition $w_1 \cdot w_2$ of the two words.

Eg: if $w_1 = a_2 a_1^{-5} a_3^{\,2}$ and $w_2 = a_3^{-2} a_1^{\,2} a_3 a_2^{-2}$ then,

$w_1 \cdot w_2 = a_2 a_1^{-3} a_3 a_2^{-2} \rightarrow$ reduced form.

This operation is well defined and associative.

**Definition 5.2**

The group $F[A]$ is the **free group generated** by $A$.

**Theorem 5.1**

If $G$ is a group and $a_i \in G$ for $i \in I$, then the subgroup $H$ of $G$ generated by $\{a_i | i \in I\}$ has an element precisely those elements of $G$ that are finite products of integral powers of the $a_i$, where powers of a fixed $a_i$ may occur several times in the product.

**Proof**

Let $K$ denotes the set of all finite products of integral powers of the $a_i$. Then $K \subseteq H$. Observe that a product of the element $k$ in $K$, is again in $K$. Since $(a_i)^0 = e$, we have $e \in K$. For every element $k$ in $K$, if we form from the product giving $k$ a new product with the order of the $a_i$ reversed and the opposite sign of all exponents, we have $k^{-1}$ which is thus in $K$. For example,

$$\left[(a_i)^3(a_2)^2(a_1)^{-7}\right]^{-1} = (a_1)^7(a_2)^{-2}(a)^{-3},$$

which is again in $K$. ■

The definition and example of free generators are given as follows.

**Definition 5.3**

If $G$ is a group with a set $A=\{a_i\}$ of generators and if $G$ is isomorphic to $F[A]$ under a map $\phi(a_i)=a_i$, then $G$ is free on $A$ and $a_i$ are **free generators** of $G$. A group is free if it is free on some nonempty set $A$.

**Example 5.3**

Free group is $\mathbb{Z}$ which is free on one generator.

Note that, every free group is infinite. ■

**Definition 5.4**

If $G$ is free on $A$, the number of elements in $A$ is the **rank of the free group** $G$.

Three theorems on the free groups are introduced as follows.

**Theorem 5.2**

If a group $G$ is free on $A$ and also on $B$, then the sets $A$ and $B$ have the same cardinality.

**Theorem 5.3**

Two free groups are isomorphic iff they have the same rank.

**Theorem 5.4**

A nontrivial proper subgroup of a free group is free.

**Example 5.4**

Let $F\left[\{x,y\}\right]$ be the free group on $\{x,y\}$. Let $y_k = x^k y x^{-k}$ for $k \geq 0$. The $y_k$ for $k \geq 0$, are free generators for subgroup of $F\left[\{x,y\}\right]$ that they generate. This illustrates that although a subgroup of a free group is free, the rank of the subgroup maybe much greater than the rank of the whole group. ■

## 5.3 HOMOMORPHISM OF FREE GROUPS

**Theorem 5.5**

Let $G$ be generated by $A=\{a_i \mid i \in I\}$ and let $G'$ be any group. If $a_i'$ for $i \in I$ is any element in $G'$ then there exists at most one homomorphism $\phi(G) \to G' \ni \phi(a_i) = a_i'$. If $G$ is free on $A$, then there is exactly one such homomorphism.

**Theorem 5.6**

Every group $G'$ is a homomorphic image of a free group.

**Proof**

Let $G' = \{a_i' | i \in I\}$ and let $A = \{a_i | i \in I\}$ be a set with the same number of elements as $G'$. Let $G = F[A]$. Then by Theorem 5.5, there exists a homomorphism $\psi$ mapping $G$ into $G'$

$$\psi(a_i) = a_i'.$$

Clearly the image of $G$ under $\psi$ is all $G'$. ■

**Exercises 5 (Free Groups)**

1. Find the reduced form and the inverse of the reduced form of each of the following words:

   i) $a^2b^{-1}b^3a^3c^{-1}c^4b^{-2}$,

   ii) $a^2a^{-3}b^3a^4c^4c^2a^{-1}$.

2. Let $G$ be a finitely generated abelian group with identity 0. A finite set $\{b_1,\ldots,b_n\}$, where $b_i \in G$, is a basis for $G$ if $\{b_1,\ldots,b_n\}$ generates $G$ and $\sum_{i=1}^{n} m_i b_i = 0$ if and only if each $m_i b_i = 0$, where $m_i \in \mathbb{Z}$. Show that $\{2,3\}$ is not a basis for $\mathbb{Z}_4$. Find a basis for $\mathbb{Z}_4$.

# CHAPTER 6

# GROUP PRESENTATIONS

## 6.0 INTRODUCTION

In mathematics, one method of defining a group is by a presentation. One specifies a set $S$ of generators so that every element of the group can be written as a product of some of these generators, and a set $R$ of relations among those generators. We then say $G$ has presentation $\langle S|R\rangle$ or

$$G=\langle g_1, g_2, ..., g_n \mid r_1=r_2=...=r_t=e\rangle,$$

where $g_i$ generators and $r_j$ relations.

## 6.1 EXAMPLES OF GROUPS PRESENTATION

1. The cyclic group of order $n$ has the presentation $\langle a \mid a^n = e\rangle$

   where $e$ is the group identity.

2. The dihedral group of order 8 can be presented by $D_4 = \langle a,b \mid a^4 = b^2 = (ab)^2 = e \rangle$. Let $R = R_{90}$ where $H$ is the reflection across horizontal axis, then $D_4 = \langle R, H \rangle$ since $R^4 = H^2 = (RH)^2 = R_0$.

   (Note that there exists other relations in $D_4$, for example $HR = R^3H$ and $RHR = H$ )

3. $\mathbb{Z}_4 \oplus \mathbb{Z}_2 = \langle a,b \mid a^4 = b^2 = e,\ ab = ba \rangle$.

4. The quaternion group of order 8 can be written as $Q = \langle a,b \mid a^2 = b^2 = (ab)^2 \rangle$.

   Note that $b^2 = (ab)^2 = abab$ implies $b = aba$ and $a^2 = b^2 = (aba)(aba) = aba^2ba = abb^2ba = ab^4a$ implies $b^4 = e$.

5. The generalized quaternion group is a group of order $4n,\ n \geq 2,\ n \in \mathbb{N}$ and can be presented as

$$Q_{4n} = \langle a,b \mid a^{2n} = e,\ a^n = b^2,\ bab^{-1} = a^{-1} \rangle.$$

6. The quasidihedral group, also called semidihedral group, is a nonabelian group of order $2^n,\ n \geq 4,\ n \in \mathbb{N}$ and the group presentation is $QD_{2n} = \langle a,b \mid a^{2n-2} = b^2 = e,\ bab^{-1} = a^{2^{n-2}-1} \rangle$.

A presentation is said to be **finitely generated** if $S$ is finite and finitely related if $R$ is finite. If both are finite it is said to be a finite presentation. A group is finitely generated (respectively finitely related, finitely presented) if it has a presentation that is finitely generated (respectively finitely related, a finite presentation).

**Theorem 6.1**

Every group $G$ has a presentation.

**Proof**

Consider the free group $\langle G \rangle$ on $G$. Since $G$ clearly generates itself one should be able to obtain it by a quotient of $\langle G \rangle$. Indeed, by the universal property of free groups there exists a unique group homomorphism $\varphi : \langle G \rangle \to G$ which covers the identity map. Let $K$ be the kernel of this homomorphism. Then $G$ clearly has the presentation $\langle G | K \rangle$. Note that this presentation is highly inefficient as both $G$ and $K$ are much larger than necessary. Every finite group has a finite presentation. The negative solution to the word problem for groups states that there is a finite presentation $\langle S | R \rangle$ for which there is no algorithm which, given two words $u,v$ decides whether $u$ and $v$ describe the same element in the group. ■

**Theorem 6.2**

Let $G$ have a presentation

$$G = \langle x_1, \ldots, x_n | r_j(x_1, \ldots, x_n), j \in J \rangle$$

so that $G = F/R$, where $F$ is the free group with basis $\{x_1, \ldots, x_n\}$ and $R$ is the normal subgroup generated by the $r_j$. If $H = \langle y_1, \ldots y_n \rangle$ and if $r_j(y_1, \ldots y_n) = 1$ for all $j$, then there is a surjective homomorphism $G \to H$ with $x_i \mapsto y_i$ for all $i$.

Table 6.1 gives some examples of presentations for commonly studied groups.

**Table 6.1 : Some groups' presentations**

| No | Group | Presentation | Comments |
|---|---|---|---|
| 1. | The free group on $S$ | $\langle S \mid \phi \rangle$ | A free group is "free" in the sense that it is subject to no relations. |
| 2. | $C_n$, the cyclic group of order $n$ | $\langle a \mid a^n \rangle$ | |
| 3. | $D_{2n}$, the dihedral group of order $2n$ | $\langle r, f \mid r^n = f^2 = (rf)^2 = e \rangle$ | Here $r$ represents a rotation and $f$ a reflection |
| 4. | $D_\infty$, the infinite dihedral group | $\langle r, f \mid f^2 = (rf)^2 = e \rangle$ | |
| 5. | $\mathrm{Dic}_n$, the dicyclic group | $\langle r, f \mid r^{2n} = e,\ r^n = f^2,\ frf^{-1} = r^{-1} \rangle$ | The quaternion group is a special case when $n = 2$ |
| 6. | $\mathbb{Z} \times \mathbb{Z}$ | $\langle x, y \mid xy = yx \rangle$ | |
| 7. | $\mathbb{Z}_m \times \mathbb{Z}_n$ | $\langle x, y \mid x^m = y^n = e,\ xy = yx \rangle$ | $x^m = y^n = [x, y] = 1$ |
| 8. | The free abelian group on $S$ | $\langle S \mid R \rangle$ where $R$ is the set of all commutators of elements of the free group on $S$. | |

| | | | |
|---|---|---|---|
| 9. | The symmetric group, $S_n$ | Generators: $\sigma_1,\ldots,\sigma_{n-1}$<br>Relations:<br>• $\sigma_i^2=1$,<br>• $\sigma_i\sigma_j=\sigma_j\sigma_i$ if $j\neq i\pm1$<br>• $\sigma_i\sigma_{i+1}\sigma i=\sigma_{i+1}\sigma_i\sigma_{i+1}$<br>The last set of relations can be transformed into $(\sigma_i\sigma_{i+1})^3=1$ using $\sigma_i^2=1$. | Here $\sigma_i$ is the permutation that swaps the $i$th element with the $i+1$ one. The product $\sigma_i\sigma_{i+1}$ is a 3-cycle on the set $\{i,i+1,i+2\}$. |
| 10. | The quaternion group, $Q$ of order 8 | $\langle i,j \mid i^4=i^2j^2=1=ijij^{-1}\rangle$ | |
| 11. | $SL_2(\mathbb{Z})$ | $\langle a,b \mid aba=bab,(aba)^4=e\rangle$ | Topologically can visualize $a$ and $b$ as Dehn twists on the torus |
| 12. | $GL_2(\mathbb{Z})$ | $\left\langle a,b,j \middle\| \begin{matrix} aba=bab,(aba)^4=j^2= \\ (ja)^2=(jb)^2=e \end{matrix} \right\rangle$ | |
| 13. | $PSL_2(\mathbb{Z})$ Projective special linear group | $\langle a,b \mid a^2=b^3=e\rangle$ | $PSL_2(\mathbb{Z})$ is the free product of the cyclic groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$. |

A group presentation is not unique. Some examples are given below.

**Example 6.1**

Although $\mathbb{Z}_6$ is cyclic, we can also write its presentation as below :

$$\mathbb{Z}_6 = \left\langle x, y \;\middle|\; x^3 = 1,\ y^2 = 1,\ xyx^{-1}y^{-1} = 1 \right\rangle. \ \blacksquare$$

**Example 6.2**

The dihedral group $D_{2n}$ has a presentation

$$D_{2n} = \left\langle x, y \;\middle|\; x^n = y^2 = e,\ yxy = x^{-1} \right\rangle.$$

For example

$$D_4 = \left\langle x, y \;\middle|\; x^4 = y^2 = e,\ (xy)^2 = e \right\rangle. \ \blacksquare$$

**Example 6.3**

The group of quaternions has presentations

$$Q = \left\langle a, b \middle| a^2 = b^2 = (ab)^2 = e \right\rangle.$$

Note that $b^2 = (ab)^2 = abab$ implies $b = aba$ and $a^2 = b^2 = (aba)(aba) = aba^2ba = ab^4a$ implies $b^4 = e$. $\blacksquare$

**Example 6.4**

A free abelian group $G$ with basis $X$ has presentation

$$G = \left\langle X \middle| xyx^{-1}y^{-1} = 1 \text{ for all } xy \in X \right\rangle,$$

a free group $F$ with basis $X$ has presentation

$$F = \langle X \mid \phi \rangle. \ \blacksquare$$

**Exercises 6 (Group Presentations)**

1. Give a presentation of $S_3$ involving two generators.

2. Give a presentation of $S_3$ involving three generators.

3. Give a presentation of $\mathbb{Z}_4$ involving two generators.

4. Give the tables for both the octic group, $O_8$,

$$O_8 = \left\langle a, b \middle| a^4 = 1, b^2 = 1, ba = a^3 b \right\rangle$$

and the quaternion group, $Q_8$,

$$Q_8 = \left\langle a, b \middle| a^4 = 1, b^2 = a^2, ba = a^3 b \right\rangle.$$

Decide whether they are isomorphic.

5. Given $G = \left\langle a, b \middle| a^3 = 1, b^2 = 1, ba = a^2 b \right\rangle$ with order 6. Write out the Cayley table for $G$.

# CHAPTER 7

# RINGS AND INTEGRAL DOMAINS



## 7.0 INTRODUCTION

A ring is an algebraic structure consisting of a set together with two binary operations (usually called addition and multiplication) where each operation combines two elements to form a third element. To qualify as a ring, the set together with its two operations must satisfy certain conditions — namely, the set must be an abelian group under addition and a monoid under multiplication such that multiplication distributes over addition.

The concept of a ring first arose from attempts to prove Fermat's last theorem, starting with Richard Dedekind in the 1880s. After contributions from other fields, mainly number theory, the ring notion was generalized and firmly established during the 1920s by Emmy Noether and Wolfgang Krull.

We define a ring formally as follows:

**Definition 7.1**

A ring $<R,+,\cdot>$ is a set $R$ together with two binary operations + and $\cdot$, defined on $R$ such that

1. $<R,+>$ **is an Abelian group.**
2. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ for $a,b,c\in R$.
3. $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ and $(a+b)\cdot c=(a\cdot c)+(b\cdot c)$ for $a,b,c\in R$.

**Example 7.1**

Some examples of rings are given in the following.

1. $<\mathbb{Z},+,\cdot>$, $<\mathbb{Q},+,\cdot>$, $<\mathbb{R},+,\cdot>$ and $<\mathbb{C},+,\cdot>$.
2. $<M_2(\mathbb{R}),+,\cdot>$ and $<M_n(\mathbb{Z}),+,\cdot>$.
3. $<F,+,\cdot>$ where *F* is a set of all continuous function.
4. $<n\mathbb{Z},+,\cdot>$.
5. $<\mathbb{Z}_n,+,\cdot>$.

## 7.1 TYPES OF RINGS

Some types of rings are introduced in this section.

**Definition 7.2 (Commutative Ring)**

A ring $\langle R,+,\cdot\rangle$ is called a commutative ring if $a\cdot b = b\cdot a \ \ \forall a,b\in R$.

**Definition 7.3 (Ring with Unity)**

Identity under multiplication of a ring $R$ is called a unity denoted by $I$. A ring with unity is a ring with multiplicative identity.

**Definition 7.4 (Unit, Division Ring & Field)**

Let $R$ be a ring with unity $I \neq 0$. An element $r \in R$ is a **unit** if it has a multiplicative inverse in $R$. If every non zero element is a unit, then $R$ is called a **division ring**. A **field** is a commutative division ring.

**Definition 7.5 (Divisors of 0)**

If $a$ and $b$ are nonzero elements such that $a \cdot b = 0$, then we called $a$ and $b$ as divisors of 0.

**Definition 7.6 (Integral Domain)**

A commutative ring with unity $1 \neq 0$ and containing no divisors of 0 is called an integral domain.

We illustrate the definitions with some examples in the following.

**Example 7.2**

The ring $\mathbb{Z}_p$, which is isomorphic to $\mathbb{Z}/\mathbb{Z}_p$ is a field for $p$, a prime. Thus a factor ring of an integral domain maybe a field. ■

**Example 7.3**

The ring $\mathbb{Z} \times \mathbb{Z}$ is not an integral domain, for

$$(0,1)(1,0) = (0,0),$$

showing that $(0,1)$ are 0 divisors. Let $N=\{(0,n)|n\in\mathbb{Z}\}$. Now $N$ is an ideal of $\mathbb{Z}\times\mathbb{Z}$ and $(\mathbb{Z}\times\mathbb{Z})/N$ is isomorphic to $\mathbb{Z}$ under the correspondence $[(m,0)+N]\leftrightarrow m$, where $m\in\mathbb{Z}$. Thus, the factor ring of a ring maybe an integral domain, even though the original ring is not. ■

**Example 7.4**

The subset $N=\{0,3\}$ of $\mathbb{Z}_6$ is easily seen to be an ideal of $\mathbb{Z}_6$ and $\mathbb{Z}_6/N$ has three elements, $0+N$, $1+N$ and $2+N$. These add and multiply in such a fashion as to show that $\mathbb{Z}_6/N\cong\mathbb{Z}_3$ under the correspondence

$$(0+N)\leftrightarrow 0\quad(1+N)\leftrightarrow 1\quad(2+N)\leftrightarrow 2.$$ ■

This example shows that if $R$ is not even an integral domain, i.e if $R$ has zero divisors, it is still possible for $R/N$ to be a field.

**Example 7.5**

Note that $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}/6\mathbb{Z}\cong\mathbb{Z}_6$ is not. The preceding examples showed that a factor ring may have a structure that seems better than the original ring. This example indicates that the structure of a factor ring may seem worse than that of the original ring. ■

## 7.2 CHARACTERISTIC OF A RING

If $\exists n \in \mathbb{Z}^+$ such that $n \cdot a = 0 \ \ \forall a \in R$ then the least $n$ is called a **characteristic of a ring *R***. If not, the characteristic is 0. We denote the characteristic of a ring $R$ as char($R$).

**Example 7.6**

1. Let $R = \mathbb{Z}_n$. Then char($R$) = $n$.
2. Let $R = \mathbb{Z}$. Then char($R$) = 0.
3. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have characteristic zero. The ring $\mathbb{Z}_n$ ( $n = 1, 2, 3, ...$ ) has characteristic $n$.

*Note:*

In $\mathbb{Z}_6$, $3[2] = [6] = [0]$ and $2[3] = [6] = [0]$. However $6$, is the smallest positive integer such that $6[a] = [0]$ for all $[a] \in \mathbb{Z}_6$. In particular, $[1]$ has additive order $6$.

**Theorem 7.1**

A ring $R$ has characteristic $n > 0$ if and only if $n$ is the smallest positive integer such that $n \cdot 1 = 0$.

**Proof**

Let $R$ has characteristic $n > 0$, then $na = 0$ for all $a \in R$ and hence in particular $n \cdot 1 = 0$. If $m \cdot 1 = 0$ for $0 < m < n$, then $ma = m(1 \cdot a) = (m \cdot 1)a = 0 \cdot a = 0$. However, this contradicts the minimility of $n$. Hence $n$ is the smallest positive integer such that $n \cdot 1 = 0$.

Conversely; Suppose $n$ is the smallest positive integer such that $n \cdot 1 = 0$. Then for all $a \in R$, $na = n(1 \cdot a) = (n \cdot 1)a = 0 \cdot a = 0$. By the minimility of $n$ for $1$, $n$ must be the characteristic of $R$.

**Theorem 7.2**

The characteristic of an integral domain $R$ is either zero or a prime.

**Proof**

If there does not exist a positive integer $n$ such that $na = 0$ for all $a \in R$, then $R$ is of characteristic zero. Suppose there exist a positive integer $n$ such that $na = 0$ for all $a \in R$, and let $m$ be the smallest positive integer such that $ma = 0$ for all $a \in R$. Then $m \cdot 1 = 0$. If $m$ is not a prime number, then there exist integers $m_1, m_2$ such that $m = m_1 \cdot m_2$ where $0 < m_1, m_2 < m$. Hence,

$$\begin{aligned} 0 &= m \cdot 1 \\ &= (m_1 m_2) \cdot 1 \\ &= (m_1 \cdot 1)(m_2 \cdot 1), \\ \Rightarrow (m_1 \cdot 1)(m_2 \cdot 1) &= 0. \end{aligned}$$

Since $R$ is an integral domain therefore $R$ has no zero divisors, consequently, $(m_1 \cdot 1)(m_2 \cdot 1) = 0$ implies, $m_1 \cdot 1 = 0$ or $m_2 \cdot 1 = 0$. This contradicts the minimility of $m$, thus $m$ is a prime.

**Exercises 7 (Rings and Integral Domains)**

1. The set $\{0, 2, 4\}$ under addition and multiplication modulo 6 has a unity. Find it.

In Exercise 2 through 4, find the characteristic of the given ring.

2. $\mathbb{Z} \oplus \mathbb{Z}$ 3. $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ 4. $\mathbb{Z}_6 \oplus \mathbb{Z}_{15}$

5. Let $R$ be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^9$ for $a, b \in R$.

6. Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.

7. Verify a through g below are as claimed.

   a) The ring of integers is an integral domain.
   b) The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is an integral domain.
   c) The ring $Z[x]$ of polynomials with integer coefficients is an integral domain.
   d) The ring $Z[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in Z\}$ is an integral domain.
   e) The ring $\mathbb{Z}_p$ of integers modulo a prime $p$ is an integral domain.
   f) The ring $\mathbb{Z}_n$ of integers modulo $n$ is *not* an integral domain when $n$ is not prime.
   g) The ring $M_2(\mathbb{Z})$ of $2 \times 2$ matrices over the integers is not an integral domain.

8. Which of a through e in Exercise 7 are fields?

9. List all zero-divisors in $\mathbb{Z}_{20}$. Can you see a relationship between the zero-divisors of $\mathbb{Z}_{20}$ and the units of $\mathbb{Z}_{20}$?

10. Show that every nonzero element of $\mathbb{Z}_n$ is a unit or a zero-divisor.

11. Prove that every field is an integral domain.

12. Prove that a ring $R$ is commutative if and only if $(a+b)^2 = a^2 + b^2 + 2ab$ for all $a,b \in R$.

13. Give an example of a commutative ring without zero-divisors that is not an integral domain.

14. If $x^2 = x$ for all $x$ belonging to a ring $R$. Then prove the following,

    i. $2x = 0$ for all $x \in R$.

    ii. $R$ is commutative.

15. Is $\mathbb{Z} \oplus \mathbb{Z}$ an integral domain? Explain.

# CHAPTER 8

# RINGS OF POLYNOMIALS

## 8.0 INTRODUCTION

The study of polynomials dates back to 1650 B.C., when Egyptians were solving certain linear polynomial equations. In 1600 B.C., Hindus had learned how to solve quadratic equations. However, polynomials, as we know them today, i.e., polynomials written in our notation, did not exist until approximately 1700 A. D.

About 400 A. D., the use of symbolic algebra began to appear in India and Arabia. Some mark the use of symbols in algebra as the first level of abstraction in mathematics.

## 8.1 RINGS AND POLYNOMIALS

The definitions of subring and polynomials are given in the following.

**Definition 8.1 (Subring)**

A subset $S$ of a ring $R$ is a subring of $R$ if $S$ itself is a ring with the same operations as in $R$.

An example of subring is given in the following.

**Example 8.1**

The subset $\{0,2,4\}$ is a subring of the ring $\mathbb{Z}_6$. Besides, for each integer $n$, the set $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ is a subring of the integers $\mathbb{Z}$. ■

**Definition 8.2 (Polynomial)**

Let $R$ be a ring. A polynomial $f(x)$ with coefficients in $R$ is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of $i$. The term $a_i$ is called the coefficients of $f(x)$.

If $i > 0$ and it is true that $a_i \neq 0$, then the largest value of $I$ is the **degree** of $f(x)$.

If $a_i = 0$, then the degree of $f(x)$ is undefined.

If $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ has $a_i = 0$ for $i > n$, then $f(x) = a_0 + a_1 x + \ldots + a_n x^n ..$

**Definition 8.3 (Addition of Polynomials)**

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ and $g(x) = b_0 + b_1 x + \ldots + b_n x^n + \ldots$, then $f(x) + g(x) = c_0 + c_1 x + ... + c_n x^n + ...$, where $c_n = a_n + b_n$.

**Definition 8.4 (Multiplication of Polynomials)**

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ and $g(x) = b_0 + b_1 x + \ldots + b_n x^n + \ldots$ then

$$f(x)\cdot g(x)=d_0+d_1x+\ldots+d_nx^n+\ldots, \text{ where } d_n=\sum_{i=0}^{n}a_ib_{n-i}.$$

**Note:**

The summation $d_n=\sum_{i=0}^{n}a_ib_{n-i}\neq\sum_{i=0}^{n}b_ia_{n-i}$ if $R$ is not commutative.

**Theorem 8.1**

The set $R[x]$ of all polynomial in an indeterminate $x$ with coefficients in a ring $R$ is a ring under polynomial addition and multiplication. If $R$ is commutative, then $R[x]$ is also commutative and if $R$ has unity $1\neq 0$, then 1 is also unity of $R[x]$.

**Example 8.2**

Let $R[x]=Z_2[x]$, then

$(x+1)+(x+1)=2x+2=0x+0=0.$

$(x+1)^2=(x+1)(x+1)=x^2+(1+1)x+1=x^2+2x+1=x^2+1.$ ■

## 8.2 THE EVALUATION HOMOMORPHISM

**Theorem 8.2**

Let $F$ be a subfield of a field $E$. Let $\alpha$ be any element of $E$ and $x$ be an indeterminate:

$$\Phi_\alpha : F[x]\to E$$

defined by $\Phi(a_0+a_1x+\ldots+a_nx^n)=a_0+a_1\alpha+\ldots+a_n\alpha^n.$ Then $(a_0+a_1x+\ldots+a_nx^n)\in F[x]$ is a homomorphism of $F[x]$ into $E$, in

which $\Phi_\alpha(x)=\alpha$ and $\Phi_\alpha$ maps $F$ isomorphically by identity mapping $\Phi_\alpha(a)=a$ for $a\in F$.

The homomorphism $\Phi_\alpha$ is an evaluation at $\alpha$.

Some examples related to evaluation homomorphism are given below.

**Example 8.3**

Let $F$ be $Q$ and $E$ be $R$. Consider the evaluation homomorphism $\Phi_0 : Q[x]\to R$ where

$$\Phi\left(a_0+a_1x+\ldots+a_nx^n\right)=a_0+a_10+\ldots+a_n0^n=a_0.$$

Thus every polynomial is mapped onto its constant term.

**Example 8.4**

Let $\Phi_2 : Q[x]\to R$ in which

$$\Phi_2\left(a_0+a_1x^1+\ldots+a_nx^n\right)=a_0+a_12+\ldots+a_n2^n.$$

**Example 8.5**

$$\begin{aligned}\Phi_2\left(x^2+x-6\right)&=2^2+2-6\\&=0\end{aligned}$$

Therefore, $\left(x^2+x-6\right)$ is the kernel, $N$ of $\Phi_2$.

**Example 8.6**

Let $F$ be $Q$ and $E$ be $C$, and $\Phi_i : Q[x]\to C$.

Here

$$\Phi_i\left(a_0+a_1x+\ldots+a_nx^n\right)=a_0+a_1i+\ldots+a_ni^n \text{ and } \Phi_i(x)=i.$$

**Example 8.7**

$$\Phi_i\left(x^2+1\right) = i^2+1$$
$$= 0.$$

Thus $x^2+1$ is the kernel $N$ of $\Phi_i$.

**Example 8.8**

Let $F$ be $Q$ and $E$ be $R$, and $\Phi_\pi : Q[x] \to C$.

Here $\Phi_\pi\left(a_0 + a_1x + ... + a_nx_n\right) = a_0 + a_1\pi + ... + a_n\pi_n$.

We can prove that

$$a_0 + a_1\pi + ... + a_n\pi_n = 0 \text{ iff } a_i = 0 \text{ for } i = 0,1,...,n.$$

Therefore, Kernel of $\Phi_\pi = \{0\}$ and $\Phi_\pi$ is a one to one mapping.

## 8.3 ZERO OF POLYNOMIALS

The definition of the zero of polynomials is given in the following.

**Definition 8.5 (A Zero of a Polynomial)**

Let $F$ be a subfield of a field $E$, and let $\alpha$ be an element of $E$. Let $f(x) = a_0 + a_1x + ... + a_nx_n$ be in $F[x]$ and let $\Phi_\alpha : F[x], E$ be an evaluation homomorphism.

Then, $f(\alpha)$ is denoted by $\Phi_\alpha\left[f(x)\right] = a_0 + a_1\alpha + ... + a_n\alpha_n$.

If $f(\alpha) = 0$, then $\alpha$ is the zero of $f(x)$.

**Example 8.9**

Let $f(x)=x^2+x-6,$ then $\Phi_\alpha\left(x^2+x-6\right)=0.$ This gives

$$\alpha^2+\alpha-6=0$$

which implies $(\alpha+3)(\alpha-2)=0.$ So, $\alpha=-3,\ \alpha=2.$

Therefore, 2 and -3 are the zeroes of $f(x)$.

Next, we will be discussing on the Fermat's Little Theorem. This is a fundamental theorem in elementary number theory, which helps compute powers of integers modulo prime numbers. The definition and examples of Fermat's Little Theorem are given as follows.

**Theorem 8.3 Fermat's Little Theorem**

Let *a* be an integer, *p* is a prime number. If *p* does not divide *a*, then $a^{p-1}\equiv 1(\text{mod}\,p)$. In other words, $a^{p-1}-1$ is an integer multiple of *p* or $a^p\equiv a(\text{mod}\,p).$

**Example 8.10**

Let *a*=2, *p*=7. Then $2^{p-1}-1=2^6-1=64-1=63$ is an integer multiple of 7. Thus $2^{7-1}\equiv 1(\text{mod}\,7).$

**Example 8.11**

Let *a*=20, *p*=71. Then $20^{71}\equiv 20(\text{mod}\,71).$

**Example 8.12**

Use Fermat's Theorem to find all the zeros of $f(x)=2x^{132}+4x^{43}+3x^{21}$ in the ring $\mathbb{Z}_5$.

**Solution**

Clearly $x = 0$ is a solution. Note that every nonzero element of $\mathbb{Z}_5$ is relatively prime to 5. Therefore if $x \neq 0$ is in $\mathbb{Z}_5$ we can use Fermat's Little Theorem to simplify.

$$f(x) = 2x^{132} + 4x^{43} + 3x^{21} = 2(x^{33})^4 + 4x^3(x^{10})^4 + 3x(x^5)^4$$
$$\equiv 2(1) + 4x^3(1) + 3x(1) \pmod 5$$

Now we just apply the evaluation homomorphism for each nonzero value in $\mathbb{Z}_5$.

$$f(1) \equiv 2 + 4(1)^3 + 3(1) \equiv 4 \pmod 5$$
$$f(2) \equiv 2 + 4(2)^3 + 3(2) \equiv 0 \pmod 5$$
$$f(3) \equiv 2 + 4(3)^3 + 3(3) \equiv 4 \pmod 5$$
$$f(4) \equiv 2 + 4(4)^3 + 3(4) \equiv 0 \pmod 5$$

Therefore the zeros in $\mathbb{Z}_5$ are $\{0,2,4\}$.

**Exercises 8 (Ring of Polynomials)**

1. Given $f(x) = 2x^3 + 4x^2 + 3x + 2$ and $g(x) = 3x^4 + 2x + 4$ in $\mathbb{Z}_5[x]$. Find
   (i) $f + g$
   (ii) $f \cdot g$
2. Compute the evaluation homomorphism of
$$\phi_5\left[\left(x^3 + 2\right)\left(4x^2 + 3\right)\left(x^7 + 3x^2 + 1\right)\right]$$
3. Find all zeros in the indicated field of studies of the given polynomial with coefficients in that field
   (i) $P_1(x) = x^3 + 2x + 2$ in $\mathbb{Z}_7$
   (ii) $P_2(x) = x^5 + 3x^3 + x^2 + 2x$ in $\mathbb{Z}_5$.
4. Use Fermat's Theorem to find all the zeros in $\mathbb{Z}_5$ of $f(x) = 2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$.
5. Let $\phi_a : \mathbb{Z}_5[x] \to \mathbb{Z}_5$ be an evaluation homomorphism. Use Fermat's theorem to evaluate
$$\phi_3\left(x^{231} + 3x^{117} - 2x^{53} + 1\right).$$
6. (a) Define a zero of a polynomial $f(x)$.
   (b) Find all zeroes of the polynomial $x^2 + 3x + 2$ in $\mathbb{Z}_6$.

# CHAPTER 9

# HOMOMORPHISMS AND FACTOR RINGS



## 9.0 INTRODUCTION

In this chapter we introduce the idea of homomorphisms of rings. This concept is the analogs of homomorphisms for groups. The definition of ring homomorphism is given as follows.

**Definition 9.1**

A map $\varphi$ of ring $R$ into a ring $R'$ is a homomorphism if

$$\varphi(a+b)=\varphi(a)+\varphi(b)$$

and

$$\varphi(ab)=\varphi(a)\varphi(b)$$

for all $a,b\in R$.

A homomorphism $\varphi$ of a ring $R$ into a ring $R'$ is called

i. a **monomorphism** if $\varphi$ is one-one,

ii. an **epimorphism** if $\varphi$ is onto $R'$, and

iii. an **isomorphism** if $\varphi$ is one-one and maps $R$ onto $R'$.

An isomorphism of a ring $R$ onto $R$ is called an **automorphism**.

**Example 9.1**

Let $R_1, R_2, \cdots, R_n$ be rings, for all $i$, $\pi_i : R_1 \times R_2 \times \cdots \times R_n \to R_i$ defined by $\pi_i(r_1, r_2, \cdots, r_n) = r_i$ is a homomorphism, projection onto the $i^{\text{th}}$ component.

The properties of homomorphism hold for $\pi_i$, since both addition and multiplication in the direct product are computed by addition and multiplication in each individual component.

## 9.1 PROPERTIES OF RING HOMOMORPHISM

Some important concepts on the ring homomorphisms are discussed in this section.

**Theorem 9.1**

Let $\varphi$ be the homomorphism of a ring $R$ into a ring $R'$.

1. If 0 is the additive identity in $R$, then $\varphi(0) = 0'$ is the additive identity on $R'$.
2. If $a \in R$ then $\varphi(-a) = -\varphi(a)$.
3. If $S$ is subring of $R$, then $\varphi(S)$ is a subring of $R'$.
4. If $S'$ is a subring of $R'$ then $\varphi^{-1}[S']$ is a subring of $R$.
5. If $R$ has unity 1 then $\varphi(1)$ is unity for $\varphi[R]$.

On the other word, subrings correspond to subrings, and ring with unity correspond to ring with unity under ring homomorphism.

**Proof**

Let $\varphi$ be a homomorphism of a ring $R$ into a ring $R'$.

Since $\varphi$ can be viewed as a group homomorphism of $\langle R,+\rangle$ into $\langle R,+'\rangle$;

For 1 and 2, we can apply the properties of group homomorphism $\varphi(0)=0'$ is the additive identity element of $R'$ and that $\varphi(-a)=-\varphi(a)$.

For 3, it follows from the properties of group homomorphism. If $S$ is a subring of $R$, then considering the additive group $\langle S,+\rangle$, the set $\langle \varphi[S],+'\rangle$ gives a subgroup of $\langle R',+'\rangle$.

If $\varphi(s_1)$ and $\varphi(s_2)$ are two elements of $\varphi[S]$, then $\varphi(s_1)\varphi(s_2)=\varphi(s_1s_2)$ and $\varphi(s_1s_2)\in\varphi[S]$. Thus $\varphi(s_1)\varphi(s_2)\in\varphi[S]$ is closed under multiplication. Consequently, $\varphi[S]$ is a subring of $R'$.

For 4, by properties of group homomorphism, we can show that:

If $S'$ is a subring of $R'$, then $\langle \varphi^{-1}[S'],+\rangle$ is a subring of $\langle R,+\rangle$.

Let $a,b\in\varphi^{-1}[S']$ so that $\varphi(a)\in S'$ and $\varphi(b)\in S'$. Then $\varphi(ab)=\varphi(a)\varphi(b)$ since $\varphi(a)\varphi(b)\in S'$. Thus $\varphi^{-1}[S']$ is closed under multiplication. Hence it is a subring of $R$.

For 5, if $R$ has unity 1, then for all $r\in R$.

$$\varphi(r)=\varphi(1r)=\varphi(1)\varphi(r)=\varphi(r)\varphi(1).$$

So $\varphi(1)$ is a unity of $\varphi[R]$. ■

Now we recall the definition of an ideal in a ring *R*.

**Definition 9.2 (Ideal)**

An additive subgroup $N$ of a ring $R$ satisfying the properties

$$aN\subseteq N \text{ and } Nb\subseteq N \text{ for all } a,b\in R$$

is an **ideal**.

**Example 9.2**

$n\mathbb{Z}$ is an ideal in the ring since $n\mathbb{Z}$ is a subring and $a(n\mathbb{Z}) = n(a\mathbb{Z}) \subseteq n\mathbb{Z}$ and $(n\mathbb{Z})b = n(b\mathbb{Z}) \subseteq n\mathbb{Z}$. ■

**Example 9.3**

Let $F$ be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$, and let $C$ be the subring of $F$ consisting of all the constant functions in $F$. Is $C$ an ideal in $F$? Why?

**Solution**

It is not true that the product of a constant function with every function is a constant function. For example, the product of $\sin x$ and 2 is the function $2\sin x$. Thus $C$ is not an ideal of $F$. ■

**Example 9.4**

Let $F$ be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$ and let $N$ be a subring of all functions $f$ such that $f(2) = 0$. Is $N$ an ideal in $F$? Why or why not?

**Solution**

Let $f \in N$ and let $g \in F$. Then

$(fg)(2) = f(2)g(2) = 0g(2) = 0$

$fg \in N$ and $gf \in N$. Hence $N$ is an ideal of $F$. ■

Next, the kernel of homomorphism is introduced in the following definition.

**Definition 9.3**

Let a map $\varphi: R \to R'$ be a homomorphism of rings, the subring $\varphi^{-1}[0'] = \{r \in R \mid \varphi(r) = 0'\}$ is the **kernel of** $\varphi$**,** denoted by ker $(\varphi)$.

**Example 9.5**

The identity map of a ring $R$ is a homomorphism (an isomorphism). Its kernel is $\{0\}$. Let $R$ and $R'$ be rings and $\varphi: R \to R'$ be defined by $f(a) = 0'$ for all $a \in R$. Then $\varphi$ is homomorphism of $R$ into $R'$ and $Ker\ f = R$. ■

The relationship between ring homomorphism and ideal is defined in the following theorem.

**Theorem** 9**.2**

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring $R$ onto a ring $R'$, then $Ker\ f$ is an ideal of $R$.

**Proof**

Since $0 \in R$ and $f(0) = 0$, then $0 \in Ker\ f$ which implies that $Ker\ f \neq \phi$.

Let $a, b \in Ker\ f$ and $r \in R$. Consider,

$$\begin{aligned} f(a-b) &= f(a+(-b)) = f(a) + f(-b) && (f \text{ being homomorphism}) \\ &= f(a) - f(b) = 0 - 0 && (\text{since } a, b \in Ker\ f) \\ &= 0. \end{aligned}$$

Thus $a-b \in Ker\ f$.

Also consider,

$$\begin{aligned} f(ra) &= f(r)f(a) \quad (f \text{ being homomorphism}) \\ &= f(r)\cdot 0 \qquad (\text{since } a \in Ker\ f) \\ &= 0 \end{aligned}$$

Thus $ra \in Ker\ f$. Hence $Ker\ f$ is an ideal of $R$. ■

**Exercise 9.6**

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism, then we show that,

(i) $f(na) = nf(a)$ for all $a \in R$ and $n \in Z$.

(ii) $f(a^n) = \left(f(a)\right)^n$ for all $a \in R$ and $n \in Z$.

**Exercise 9.7**

Prove that the composition of two ring homomorphisms is a ring homomorphism.

**Theorem 9.3**

Let $\varphi : R \to R'$ be a ring homomorphism and let $H = \ker(\varphi)$. Let $a \in R$, then $\varphi^{-1}\left[\varphi(a)\right] = a + H = H + a$ is a coset containing $a$ of the commutative additive group $\langle H, + \rangle$.

**Corollary 9.1**

A ring homomorphism $\varphi : R \to R'$ is a one to one map if only if $\ker(\varphi) = \{0\}$.

## 9.2 FACTOR (QUOTIENT) RINGS

We now give the analogue of quotient groups for rings. Let $I$ be an ideal of a ring $R$. Then since $(I,+)$ is a sub-group of $(R,+)$ and $(R,+)$ is commutative, therefore $(I,+)$ is normal in $(R,+)$. Hence, if $R/I$ denotes the set of all cosets, $r+I=\{r+a : a\in I \text{ for all } r\in R\}$.

Then $R/(I,+)$ is commutative group, where addition and multiplication is defined on $R/I$ by $(r+I)+(r'+I)=(r+r')+I$ and $(r+I)\cdot(r'+I)=rr'+I$ for all $(r+I),(r'+I)\in R/I$. Then $R/(I,+,\cdot)$ is a ring.

**Definition 9.4 (Quotient Ring)**

If $I$ is an ideal of a ring $R$, then the ring $R/(I,+,\cdot)$ is called the quotient ring of $R$ by $I$.

**Theorem 9.4**

Let $\varphi: R\to R'$ be a ring homomorphism with the kernel $H$. Then the additive cosets of $H$ from a ring, $R/H$, whose binary operations are defined by choosing a representative.

i.e. the sum of two cosets is defined by

$$(a+H)+(b+H)=(a+b)+H,$$

and the product of two cosets is defined by

$$(a+H)(b+H)=(ab)+H.$$

Also, the map $\mu : {}^{R}\!/_{H} \to \varphi[R]$ defined by

$$\mu(a+H) = \varphi(a)$$

is an isomorphism.

**Theorem 9.5**

Let $H$ be a subring of the ring $R$. Multiplication of additive cosets of $H$ is well defined by the equation

$$(a+H)(b+H) = ab+H$$

if and only if $ah \in H$ and $hb \in H$ for all $a,b \in R$ and $h \in H$.

**Proof**

Suppose that $ah \in H$ and $hb \in H$ for all $a,b \in R$ and $h \in H$. Let $h_1, h_2 \in H$ so that $a+h_1$ and $a+h_2$ are also representative of the cosets $a+H$ and $b+H$ containing $a$ and $b$. Then

$$(a+h_1)(b+h_2) = ab + ah_2 + h_1 b + h_1 h_2.$$

Since $ah_2$ and $h_1 b$ and $h_1 h_2$ are all in $H$, thus $(a+h_1)(b+h_2) \in ab+H$.

Conversely, suppose multiplication of additive cosets by representative is well defined. Let $a \in R$ and consider the coset product $(a+H)H$. Choosing $a \in (a+H)$ and $0 \in H$, then

$$(a+H)H = a0 + H = 0 + H = H.$$

Since we can also compute $(a+H)H$ by choosing $a \in (a+H)$ and any $h \in H$, we see that $ah \in H$ for any $h \in H$. A similar argument starting with the product $(b+H)H$ shows that $hb \in H$ for any $h \in H$.

**Definition 9.5**

Let $N$ be an ideal of a ring $R$, then the additive cosets of $N$ form a ring $R/N$ with the binary operation defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=(ab)+N.$$

Thus $R/N$ is the **factor ring** of $R$ by $N$.

**Theorem 9.6**

Let $I$ be an ideal of a ring $R$, then the mapping $g : R \to R/I$ defined by $g(a)=a+I$ for all $a \in R$, is a homomorphism, called the natural homomorphism of $R$ onto $R/I$. Furthermore, $Ker\, g = I$.

**Proof**

Let $a,b \in R$, then

$$g(a+b)=(a+b)+I=(a+I)+(b+I)=g(a)+g(b)$$

and

$$g(a\cdot b)=(a\cdot b)+I=(a+I)\cdot(b+I)=g(a)\cdot g(b)$$

for all $a,b \in R$.

Hence $g : R \to R/I$ is a homomorphism.

Next as,

$$\begin{aligned} Ker\, g &= \{a \in R : g(a)=I\} \\ &= \{a \in R : a+I=I\} \\ &= \{a \in R : a \in I\} \\ &= R \cap I = I \end{aligned}.$$

Hence, $Ker\, g = I$. ■

## 9.3 ISOMORPHISM THEOREMS FOR RINGS

**Theorem 9.7 (First Isomorphism Theorem)**

Let $f$ be a homomorphism of a ring $R$ into a ring $R'$. Then $f(R)$ is an ideal of $R'$ and $R/Ker\, f \cong f(R)$ .

**Proof**

Let $f : R \xrightarrow{\text{into}} R'$ be a ring homomorphism of a ring $R$ onto a ring $R'$. To show that $f(R)$ is an ideal of $R'$, we let $f(a)$, $f(b) \in f(R)$, where $a, b \in R$ and consider,

$$\begin{aligned} f(a) - f(b) &= f(a) + \big(-f(b)\big) \\ &= f(a) + f(-b) && \text{(because } -f(b) = f(-b)) \\ &= f\big(a + (-b)\big) && (f \text{ being a homomorphism}) \\ &= f(a-b) \in f(R) && (\text{as } a - b \in R). \end{aligned}$$

Thus $f(a) - f(b) \in f(R)$.

Now let $r' \in R'$, then $r' = f(r)$ for some $r \in R$. Consider,

$$\begin{aligned} r'f(a) &= f(r) \cdot f(a) \\ &= f(ra) \in f(R) \quad \big(f \text{ being a homomorphism and } ra \in R\big) \end{aligned}$$

Thus $r'f(a) \in f(R)$.

Similarly, $f(a)r' \in f(R)$. Hence $f(R)$ is an ideal of $R'$.

Next, we suppose $Ker\, f = I$ and define

$$h : R/I \to f(R)$$

by

$$h(r+I)=f(r)$$

for all $r+I\in R/I$.

Now to show that this mapping is well defined, we consider, $r+I=r'+I$

$\Leftrightarrow -r'+r+I=-r'+r'+I$

$\Leftrightarrow -r'+r+I=0+I$

$\Leftrightarrow -r'+r+I=I$

$\Leftrightarrow -r'+r\in I=K\text{er } f$

$\Leftrightarrow f(-r'+r)=0$

$\Leftrightarrow f(-r')+f(r)=0$ ($f$ being a homomorphism)

$\Leftrightarrow -f(r')+f(r)=0$ (because $f(-b)=-f(b)$)

$\Leftrightarrow f(r)=f(r')$

$\Leftrightarrow h(r+I)=h(r'+I)$ (by definition of $h: R/I\to f(R)$)

This shows that $h$ is well defined and one-one.

To show that $h$ is onto, let $x\in f(R)$, then $x=f(r)$ for some $r\in R$ and hence $h(r+I)=f(r)=x$, this shows that $h$ is onto.

Finally, we have to show that $h$ is a homomorphism. To do this we consider,

$$\begin{aligned} h((r+I)+(r'+I)) &= h((r+r')+I) \\ &= f(r+r') && \text{(by definition)} \\ &= f(r)+f(r') && (f \text{ being homomorphism}) \\ &= h(r+I)+h(r'+I) && \text{(by definition).} \end{aligned}$$

This implies $h((r+I)+(r'+I))=h(r+I)+h(r'+I)$.

Also consider,

$$\begin{aligned} h((r+I)\cdot(r'+I)) &= h(v)=f(r\cdot r') && \text{(by definition)} \\ &= f(r)\cdot f(r') && (f \text{ being homomorphism}) \\ &= h(r+I)\cdot h(r'+I) && \text{(by definition).} \end{aligned}$$

Thus $h((r+I)\cdot(r'+I)) = h(r+I)\cdot h(r'+I)$. This shows that $h$ is a homomorphism and hence $R/Ker\ f \cong f(R)$. ■

**Theorem 9.8 (Second Isomorphism Theorem)**

If $I$ and $J$ are ideals of a ring $R$, then $I/I\cap J \cong (I+J)/J$.

**Proof**

Let us define a mpping $f: I \to (I+J)/J$ by $f(i) = i + J$.

Let $i + j + J \in (I+J)/J$, then $j + J = J$. Thus $i + j + J = i + J = f(i)$. This implies $(i + j + J)$ is the image of some $i \in I$ under $f$ and hence $f$ is onto.

Next, we consider,

$$\begin{aligned} f(i_1 + i_2) &= (i_1 + i_2) + J \text{ for all } i_1, i_2 \in I \\ &= (i_1 + J) + (i_2 + J) \\ &= f(i_1) + f(i_2). \end{aligned}$$

Also,

$$\begin{aligned} f(i_1 \cdot i_2) &= (i_1 \cdot i_2) + J \text{ for all } i_1, i_2 \in I \\ &= (i_1 + J)\cdot(i_2 + J) \\ &= f(i_1)\cdot f(i_2). \end{aligned}$$

This shows that $f$ is a homomorphism and hence by Theorem 8.7, $I/Ker\ f \cong (I+J)/J$.

Finally, we need to show that $Ker\ f = I \cap J$, consider,

$$\begin{aligned} Ker\ f &= \{i \in I\ :\ f(i) = J\} \\ &= \{i \in I\ :\ i + J = J\} \\ &= \{i \in I\ :\ i \in J\} \\ &= I \cap J \end{aligned}$$

Consequently, $I/I \cap J \cong I/Ker\ f$. ■

**Theorem 9.9 (Third Isomorphism Theorem)**

If $I$ and $J$ are ideals of a ring $R$, such that $I \subseteq J$ then $\left(R/I\right)\Big/\left(J/I\right) \cong R/J$.

**Proof**

Define a mapping, $f : R/I \to R/J$ by $f(r+I) = r + J$ for all $r \in R$. To show that $f$ is well defined, let $r_1 + I, r_2 + I \in R/I$ such that

$$\begin{aligned} & r_1 + I = r_2 + I \\ & \Rightarrow -r_2 + r_1 + I = -r_2 + r_2 + I \\ & \Rightarrow -r_2 + r_1 + I = 0 + I \\ & \Rightarrow -r_2 + r_1 + I = I \\ & \Rightarrow -r_2 + r_1 \in I \subseteq J \\ & \Rightarrow -r_2 + r_1 \in J \\ & \Rightarrow -r_2 + r_1 + J = J \\ & \Rightarrow r_1 + J = r_2 + J \\ & \Rightarrow f(r_1 + I) = f(r_2 + I). \end{aligned}$$

This shows that $f$ is well defined.

Next to show that $f$ is a homomorphism, let $r_1 + I, r_2 + I \in R/I$ and consider

$$\begin{aligned} f\left((r_1+I)+(r_2+I)\right) &= f\left((r_1+r_2)+I\right) \\ &= (r_1+r_2)+J \\ &= (r_1+J)+(r_2+J) \\ &= f(r_1+I)+f(r_2+I). \end{aligned}$$

This implies $f\left((r_1+I)+(r_2+I)\right) = f(r_1+I)+f(r_2+I).$

Also,

$$\begin{aligned} f\left((r_1+I)\cdot(r_2+I)\right) &= f\left((r_1\cdot r_2)+I\right) \\ &= (r_1\cdot r_2)+J \\ &= (r_1+J)\cdot(r_2+J) \\ &= f(r_1+I)\cdot f(r_2+I). \end{aligned}$$

Thus $f$ is shown to be a homomorphism.

If $x \in R/J$, then $x = r+J = f(r+I)$ for some $r \in R$.

This implies that $f$ is onto. Hence by Theorem 8.7, $\left(R/I\right)/Ker\, f \cong R/J$.

Finally, we need to show that $Ker\, f = J/I$, consider

$$\begin{aligned} Ker\, f &= \{x \in R/I : f(x) = J\} \\ &= \{x = r+I \ : \ f(r+I) = J\} \\ &= \{r+I \ : \ r+J = J\} \\ &= \{r+I \ : \ r \in J\} \\ &= J/I. \end{aligned}$$

Hence $\left(R/I\right)/\left(J/I\right) \cong R/J$.

**Exercises 9 (Homomorphisms and Factor Rings)**

1. Find all ideals $N$ of $\mathbb{Z}_{12}$. In each case compute the $\mathbb{Z}_{12}/N$.

2. Give the addition and multiplication tables for $2\mathbb{Z}/8\mathbb{Z}$. Are $2\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}_4$ isomorphic rings?

3. Let $f: R \xrightarrow{into} R'$ be a ring homomorphism, show that,

   (i) for all $f(na) = nf(a)$ for all $a \in R$ and $n \in \mathbb{Z}$.

   (ii) for all $f(a^n) = (f(a))^n$ for all $a \in R$ and $n \in \mathbb{Z}$.

4. Prove that the composition of two ring homomorphisms is a ring homomorphism.

5. Prove: A ring homomorphism $\varphi: R \to R'$ is a one to one map if and only if $\ker(\varphi) = \{0\}$.

6. Let $\varphi: \mathbb{Z}_{12} \to \mathbb{Z}_3$ be the homomorphism where $\varphi(1) = 2$.

   (i) Find the kernel $K$ of $\phi$.

   (ii) List the cosets in $\mathbb{Z}_{12}/K$, showing the elements in each coset.

   (iii) Give the correspondence between $\mathbb{Z}_{12}/K$ and $\mathbb{Z}_3$ given by the map $\mu$ described in the First Isomorphism Theorem.

# CHAPTER 10

# MAXIMAL AND PRIME IDEALS



## 10.0 INTRODUCTION

In algebra, a prime ideal is a subset of a ring that shares many important properties of a prime number in the ring of integers. Meanwhile, a maximal ideal is an ideal that is maximal (with respect to set inclusion) amongst all proper ideals.

## 10.1 IDEAL

Every nonzero ring $R$ has at least two ideals, the **improper ideal** $R$ and the **trivial ideal** $\{0\}$. For these ideals, the factor rings are $R/R$, which has only one element, and $R/\{0\}$, which is isomorphic to $R$. These are uninteresting cases. Just as for a subgroup of a group, a **proper nontrivial ideal** of a ring $R$ is an ideal $N$ of $R$ such that $N \neq R$ and $N \neq \{0\}$.

**Theorem 10.1**

If $R$ is a ring with unity, and $N$ is an ideal of $R$ containing a unit, then $N = R$.

**Proof**

Let $N$ be an ideal of $R$, and suppose that $u \in N$ for some unit $u$ in $R$. Then the condition $rN \subseteq N$ for all $r \in R$ implies, if we take $r = u^{-1}$ and $u \in N$, that $1 = u^{-1}u$ is in $N$. But then $rN \subseteq N$ for all $r \in R$ implies that $r1 = r$ is in $N$ for all $r \in R$, so $N = R$. □

**Corollary 10.1**

A field contains no proper nontrivial ideals.

**Proof**

Since every nonzero element of a field is unit, it follows at once from Theorem 10.1 that an ideal of a field $F$ is either $\{0\}$ or all of $F$.

## 10.2 MAXIMAL AND PRIME IDEALS

In this particular section we are especially interested in certain ideals of commutative rings. These ideals give us special types of factor rings. The definition and example of maximal ideal are given in the following.

**Definition 10.1 (Maximal Ideal)**

A **maximal ideal of a ring** $R$ is an ideal $M$ different from $R$ such that there is no proper ideal $N$ of $R$ properly containing $M$.

**Example 10.1**

Let $p$ be a prime positive integer. We know that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}_p$. Since $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $\mathbb{Z}_p$ as additive groups, we know that $\mathbb{Z}_p$ is a simple group, and consequently $p\mathbb{Z}$ must be a maximal normal subgroup of $\mathbb{Z}$ by Theorem 1.5. Since $\mathbb{Z}$ is an abelian group and every subgroup is a normal subgroup, we see that $p\mathbb{Z}$ is a maximal proper subgroup of $\mathbb{Z}$. Since $p\mathbb{Z}$ is an ideal of a ring $\mathbb{Z}$, it follows that $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$. We know that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}_p$, and that $\mathbb{Z}_p$ is actually a field. Thus $\mathbb{Z}/p\mathbb{Z}$ is a field. This illustrates the next theorem. ■

**Theorem 10.2**

Let $R$ be a commutative ring with unity. Then $M$ is a maximal ideal of $R$ iff $R/M$ is a field.

**Proof**

Suppose $M$ is a maximal ideal in $R$. Observe that if $R$ is a commutative ring with unity, then $R/M$ is also a nonzero commutative ring with unity if $M \neq R$, which is the case if $M$ is maximal.

Let $(a+M) \in R/M$ with $a \notin M$, so that $a+M$ is not the additive identity element of $R/M$. Suppose $a+M$ has no multiplicative inverse in $R/M$. Then the set $(R/M)(a+M) = \{(r+M) \in R/M\}$ does not contain

$1+M$. We easily see that $\left(R/M\right)(a+M)$ is an ideal of $R/M$. It is nontrivial because $a \notin M$, and it is a proper ideal because it does not contain $1+M$. If $\gamma : R \to R/M$ is the canonical homomorphism, then $\gamma^{-1}\left[\left(R/M\right)(a+M)\right]$ is a proper ideal of $R$ properly containing $M$. But this contradicts our assumption that $M$ is maximal ideal, so $a+M$ must have multiplicative inverse in $R/M$.

Conversely, suppose that $R/M$ is a field. If $N$ is any ideal of $R$ such that $M \subset N \subset R$ and $\gamma$ is the canonical homomorphism of $R$ onto $R/M$, then $\gamma[N]$ is an ideal of $R/M$ with $\{(0+M) \subset \gamma[N] \subset R/M\}$. But this is contrary to the fact that the field $R/M$ contains no proper nontrivial ideals. Hence if $R/M$ is a field, $M$ is maximal. ■

**Example 10.2**

Since $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ and $\mathbb{Z}_n$ is a field iff $n$ is a prime, we see that the maximal ideals of are precisely the ideals $p\mathbb{Z}$ for prime positive integers $p$. ■

**Corollary 10.2**

A commutative ring with unity is a field iff it has no proper nontrivial ideals.

**Example 10.3**

All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. For $n=0$ we have $n\mathbb{Z}=\{0\}$, and $\mathbb{Z}/\{0\}\cong\mathbb{Z}$, which is an integral domain. For $n>0$, we have $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$ and $\mathbb{Z}_n$ is an integral domain iff $n$ is a prime. Thus the nonzero ideals $n\mathbb{Z}$ such that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain are of the form $p\mathbb{Z}$, where $p$ is a prime. Of course, that $\mathbb{Z}/p\mathbb{Z}$ is actually a field, so that $p\mathbb{Z}$ is a maximal ideal of that $\mathbb{Z}$. Note that for a product $rs$ of integers to be in that $p\mathbb{Z}$, the prime $p$ must divide either $r$ or $s$. ■

Next, the definition and example of prime ideal are given in the following.

**Definition 10.2 (Prime Ideal)**

An ideal $N\neq R$ in a commutative ring $R$ is a **prime ideal** if $ab\in N$ implies that either $a\in N$ or $b\in N$ for $a,b\in R$.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$, and indeed, in any integral domain.

**Example 10.4**

Given that $R=\mathbb{Z}_{12}$. Then the ideals are $\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 6\rangle$.

The prime ideals are the same as the maximal ideals, namely $\langle 2\rangle$ and $\langle 3\rangle$.

**Example 10.5**

Note that $\mathbb{Z}\times\{0\}$ is a prime ideal of $\mathbb{Z}\times\mathbb{Z}$, for if $(a,b)(c,d)\in\mathbb{Z}\times\{0\}$, then we must have $bd=0$ in $\mathbb{Z}$. This implies that either $b=0$ so $(a,b)\in\mathbb{Z}\times\{0\}$ or $d=0$ so $(c,d)\in\mathbb{Z}\times\{0\}$.

Note that $(\mathbb{Z}\times\mathbb{Z})/(\mathbb{Z}\times\{0\})$ is isomorphic to $\mathbb{Z}$ which is an integral domain. ■

**Theorem 10.3**

Let $R$ be a commutative ring with unity, and let $N\neq R$ be an ideal in $R$. Then $R/N$ is an integral domain iff $N$ is a prime ideal in $R$.

**Corollary 10.3**

Every maximal ideal in a commutative ring $R$ with unity is a prime ideal.

In summary, we have the following result:

For a commutative ring $R$ with unity:

1. An ideal $M$ of $R$ is maximal iff $R/M$ is a field.
2. An ideal $N$ of $R$ is prime iff $R/N$ is an integral domain.
3. Every maximal ideal of $R$ is a prime ideal.

## 10.3 PRIME FIELDS

A field is called a prime field if it has no proper (for example strictly smaller) subfields. Some important theorems and corollary are given in this section.

**Theorem 10.4**

If $R$ is a ring with unity 1, then the map $\phi:\mathbb{Z}\to R$ given by

$$\phi(n)=n\cdot 1$$

for $n\in\mathbb{Z}$ is a homomorphism of $\mathbb{Z}$ into $R$.

**Corollary 10.4**

If $R$ is a ring with unity and characteristic $n>1$, then $R$ contains a subring isomorphic to $\mathbb{Z}_n$. If $R$ has characteristic 0, then $R$ contains a subring isomorphic to $\mathbb{Z}$.

**Theorem 10.5**

A field $F$ is either of prime characteristic $p$ and contains a subfield isomorphic to $\mathbb{Q}$.

**Definition 10.3**

The fields $\mathbb{Z}_p$ and $\mathbb{Q}$ are prime fields.

## 10.4 IDEAL STRUCTURE IN $F[x]$

Some definition and examples of the ideal structure in the $F[x]$ are given in the following.

**Definition 10.4 (Principal Ideal Generated by $a$)**

If $R$ is a commutative ring with unity and $a \in R$ the ideal $\{ra | r \in R\}$ of all multiples of $a$ is the **principal ideal generated by** $a$ and is denoted by $\langle a \rangle$. An ideal $N$ of $R$ is a **principal ideal** if $N = \langle a \rangle$ for some $a \in R$.

**Example 10.6**

Every ideal of the ring $\mathbb{Z}$ is of the form $n\mathbb{Z}$, which is generated by $n$, so every ideal of $\mathbb{Z}$ is a principal ideal. ■

**Example 10.7**

The ideal $\langle x \rangle$ in $F[x]$ consists of all polynomials in $F[x]$ having zero constant term. ■

**Theorem 10.6**

If $F$ is a field, every ideal in $F[x]$ is principal.

**Theorem 10.7**

An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal iff $p(x)$ is irreducible over $F$.

**Example 10.8**

We can show that $x^3 + 3x + 2$ is irreducible in $\mathbb{Z}_5[x]$, so $\mathbb{Z}_5[x] / \langle x^3 + 3x + 2 \rangle$ is a field. Similarly, we can show that $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ so $\mathbb{Q}[x] / \langle x^2 - 2 \rangle$ is a field. ■

**Exercises 10 (Prime and Maximal Ideals)**

1. Let $G = \mathbb{Z}_{24}$. Find all prime and maximal ideals of $G$.

2. Repeat Question 1 with $G = \mathbb{Z}_2 \times \mathbb{Z}_4$.

3. Find $c \in \mathbb{Z}_3$ such that $\mathbb{Z}_3(x)\big/_{x^3+x^2+c}$ is a field.

4. (i) Find all ideals $N$ of $\mathbb{Z}_{18}$.

   (ii) For each case, compute $\mathbb{Z}_{18}\big/_{N}$, and find a known ring to which the quotient ring is isomorphic.

# CHAPTER 11

# GROBNER BASES FOR IDEALS



## 11.0 INTRODUCTION

Gröbner bases are primarily defined for ideals in a polynomial ring $R = K[x_1,\ldots,x_n]$ over a field $K$. Although the theory works for any field, most Gröbner basis computations are done either when $K$ is the field of rationals or the integers modulo a prime number.

## 11.1 DEFINITIONS

Some important definitions and theorems on the Grobner bases are given in this subsection.

**Definition 11.1** (**Algebraic Variety**)

Let $S$ be a finite subset of $F[x]$. The **algebraic variety** $V(S)$ in $F^n$ is the set of all common zeros in $F^n$ of the polynomials in $S$.

**Example 11.1**

Let $S=\{2x+y-2\}\subset R[x,y]$. The algebraic variety $V(S)$ in $\mathbb{R}^2$ is the line with $x-$intercept 1 and $y-$ intercept 2.

$$I=\{c_1f_1+c_2f_2+\cdots+c_rf_r : c_i\in R \text{ for } i=1,\cdots,r\}$$

Let $R=F[x]$ where all the $c_i$ and all the $f_i$ are polynomials in $F[x]$ where $c_i$ as coefficient polynomials. By its construction, this ideal $I$ is the smallest ideal containing $f_1, f_2,\cdots, f_r$; it can described as the intersection of all ideals containing these $r$ polynomials. ■

**Definition 11.2 (Basis for an Ideal)**

Let $I$ be an ideal in a commutative ring $R$ with the unity. A subset $\{b_1,b_2,\cdots,b_r\}$ of $I$ is a basis for $I$ if

$$I=\langle b_1,b_{2,}\cdots,b_r\rangle.$$

**Theorem 11.1**

Let $f_1, f_{2,}\cdots, f_r\in F[x]$. The set of common zeros in $F^n$ of the polynomials $f_i$ for $i=1,2,\cdots,r$ is the same as the set if common zeros in $F^n$ of all the polynomials in the entire Ideal $I=\langle f_1, f_2,\cdots, f_r\rangle$.

**Proof**

Let

$$f=c_1f_1+c_2f_2+\cdots+c_rf_r \qquad (1)$$

be any element of $I$, and let $a\in F^n$ be a common zero of $f_1, f_2,\cdots$ and $f_r$. Applying the evaluation homomorphism $\phi_a$ to (1), we obtain

$$\begin{aligned} f(a)&=c_1(a)f_1(a)+c_2(a)f_2(a)+\cdots+c_r(a)f_r(a)\\ &=c_1(a)0+c_2(a)0+\cdots+c_r(a)0=0 \end{aligned}$$

Showing that $a$ is also a common zero of the polynomial $f$ in $I$. Of course, a zero of every polynomial in $I$ will be a zero of each $f_i$ because each $f_i \in I$.

For an ideal $I$ in $F[x]$, we let $V(I)$ be the set of all common zeros of all elements of $I$. Then we can summarize Theorem 11.1 as

$$V(\{f_1, f_2, \cdots, f_r\}) = V(\langle f_1, f_2, \cdots, f_r \rangle). \square$$

**Theorem 11.2 (Hilbert Basis Theorem)**

Every ideal in $F[x_1, x_2, \cdots, x_n]$ has a finite basis.

The objective of this theorem is given a basis for an ideal $I$ in $F[x]$, modify it if possible become a basis that better exhibits the structure of $I$ and the geometry of the associated algebraic variety $V(I)$.

**Theorem 11.3 (Property of the Division Algorithm)**

Let $f(x), g(x), q(x)$ and $r(x)$ be polynomials in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$. The common zeros in $F^n$ of $f(x)$ and $g(x)$ are the same as the common zeros of $g(x)$ and $r(x)$. Also the common divisors in $F[x]$ of $f(x)$ and $g(x)$ are the same as the common divisors of $g(x)$ and $r(x)$.

**Proof**

If $a \in F^n$ is a common zero of $g(x)$ and $r(x)$, then applying $\phi_a$ to both sides of the equation $f(x) = g(x)q(x) + r(x)$, we obtain

$$\begin{aligned} f(a) &= g(a)q(a)+r(a) \\ &= 0q(a)+0 \\ &= 0. \end{aligned}$$

So, $a$ is a zero of both $f(x)$ and $g(x)$.

If $b \in F[x]$ is a common zero of $f(x)$ and $g(x)$, then applying $\phi_a$ yields

$$f(b) = g(b)q(b)+r(b)$$

so that $0 = 0q(b)+r(b)$ and we see that $r(b)=0$ as well as $g(b)$.

Let $B$ be a basis for an ideal $I$, let $f(x), g(x) \in B$, and let $f(x) = g(x)q(x)+r(x)$.

Let $B'$ be the set obtained by replacing $f(x)$ and $r(x)$ in $B$, and let $I'$ be the ideal having $B'$ as a basis.

Let $S$ be the set obtained from $B$ by adjoining $r(x)$ to $B$. Note that $S$ can also be obtained by adjoining $f(x)$ to $B'$.

The equation $f(x) = g(x)q(x)+r(x)$ shows that $f(x) \in I'$, so we have $B' \subseteq S \subseteq I'$. Thus $S$ is a basis for $I'$.

The equation $r(x) = f(x) - q(x)g(x)$ shows that $r(x) \in I$, so we have $B \subseteq S \subseteq I$.

Thus $S$ is a basis for $I$. Therefore $I = I'$ and $B'$ is a basis for $I$. □

## 11.2 GROBNER BASES

Our polynomials in $F[x]$ have terms of the form $ax_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$, where $a \in F$. Lets consider a power product in $F[x]$ to be an expression $P = x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ where all the $m_i \geq 0$ in $\mathbb{Z}$.

For example, in $F[x, y, z]$, $xz^2 = xy^0z^2$. We define a total ordering < on the set of all power products. We denote by 1 the power products with all exponents 0. In $ax_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}$ $F[x]$, we have $1 < x$. Multiplying repeatedly by *x* gives $x < x^2$, $x^2 < x^3$, etc.

**Properties for an Ordering of Power Products**

1. $1 < P$ for all power products $P \neq 1$.
2. For any two power products $P_i$ and $P_j$, exactly one of $P_i < P_j, P_j < P_i$, $P_i = P_j$.
3. If $P_i < P_j$ and $P_j < P_k$, then $P_i < P_k$.
4. If $P_i < P_j$, then $PP_i < PP_j$ for any power product *P*.

There are a number of possible orderings for power products in $F[x]$ with *n* determinates. One of them is called *the lexicographical order* (denoted by "lex"). In lex, we define

$$x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n} < x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n}$$

if and only if $s_i < t_i$ for the first subscript *i*.

Thus in $F[x, y]$, if we write the power products in the order $x^n y^m$, then we have $y = x^0y^1 < x^1y^0 = x$ and $xy < xy^2$. Furthermore, we have

$$1 < y < y^2 < y^3 < \ldots < x < xy < xy^2 < xy^3 < \ldots < x^2 < x^2y < x^2y^2 < \ldots$$

Next, we denote by 1t(*f*) the leading term of *f* and by 1p(*f*) the power product of the leading term.

Now we are ready to define a Grobner basis.

**Definition 11.3 (Grobner Basis)**

A set $\{g_1, g_{2,\cdots,} g_r\}$ of nonzero polynomials in $F[x_1, x_2, \cdots, x_r]$, with term ordering $<$ is a **Grobner Basis** for the ideal $I = \langle g_1, g_2, \cdots, g_r \rangle$ if and only if for each nonzero $f \in I$, there exists some $i$ where $1 \le i \le r$ such that $1p(g_i)$ divides $1p(f)$.

**Example 11.2**

By division, reduce the basis $\{xy^2, y^2 - y\}$ for the ideal $I = \langle xy^2, y^2 - y \rangle$ in $\mathbb{R}[x, y]$ to one with smaller maximum term size, assuming the order lex with $y < x$.

**Solution**

We see that $y^2$ divides $xy^2$ and compute

$$\begin{array}{r|l} & x \\ \hline y^2 - y & xy^2 \\ & xy^2 - xy \\ \hline & xy \end{array}$$

Because $y^2$ does not divide $xy$, we cannot continue the division. Note that $1p(xy) = xy$ is not less than $1p(y^2 - y) = y^2$. However, we do have $1p(xy) < 1p(xy^2)$. Our new basis for $I$ is $\{xy, y^2 - y\}$. ■

**Example 11.3**

Consider the ideal $I = \langle x^2y - 2, xy^2 - y \rangle$ in $R[x, y]$. The polynomials in the basis shown cannot be reduced further. However, the ideal $I$ contains

$$y(x^2y - 2) - x(xy^2 - y) = xy - 2y,$$

whose leading power product $xy$ is not divisible by other of the leading power product $x^2y$ or $xy^2$ of the given basis. Thus, $\{x^2y - 2, xy^2 - y\}$ is not a Grobner basis for $I$, according to Definition 11.3. ■

**Theorem 11.4**

A basis $G = \{g_1, g_2, \cdots, g_r\}$ is a Grobner basis for the ideal $\langle g_1, g_2, \cdots, g_r \rangle$ if and only if, for all $i \neq j$, the polynomial $S(g_i, g_j)$ can be reduced to zero by repeatedly dividing remainders by elements of $G$, as in the division algorithm.

**Example 11.4**

Let $g_1 = x^2y - 2$, $g_2 = xy^2 - y$, and $I = \langle g_1, g_2 \rangle$ in $\mathbb{R}^2$. In Example 11.3, we obtained the polynomial $S(g_1, g_2) = xy - 2y$ which cannot be reduced to zero using $g_1$ and $g_2$. We proceed to reduce the basis $\{x^2y - 2, xy^2 - y, xy - 2y\}$, indicating each step.

$\{x^2y - 2, xy^2 - y, xy - 2y\}$ augmented basis

$\{2xy-2, xy^2-y, xy-2y\}$ by adding $(-x)$ (third) to the first

$\{2xy-2, 2y^2-y, xy-2y\}$ by adding $(-y)$ (third) to the second

$\{4y-2, 2y^2-y, xy-2y\}$ by adding $(-2)$ (third) to the first

$\{4y-2, 0, xy-2y\}$ by adding $\left(-\frac{y}{2}\right)$ (first) to second

$\left\{4y-2, 0, \frac{1}{2}x-2y\right\}$ by adding $\left(-\frac{x}{4}\right)$ (first) to third

$\left\{4y-2, 0, \frac{1}{2}x-1\right\}$ by adding $\left(\frac{1}{2}\right)$ (first) to third

So $\left\{y-\frac{1}{2}, x-2\right\}$ is a Grobner basis. Note that if $f = y-\frac{1}{2}$ and $g = x-2$, then

$$S(f,g) = xf - yg = \left(xy-\frac{x}{2}\right)-(xy-2y) = -\frac{x}{2}+2y$$

which can readily be reduced to zero by adding $\frac{1}{2}(x-2)$ and $-2\left(y-\frac{1}{2}\right)$.

## Exercises 11 (Grobner Bases for Ideals)

1. Let power products in $R\left[x, y, z\right]$ have order lex where $z < y < x$. If possible, perform a single-step division algorithm reduction that changes the given ideal basis to one having smaller maximum term order.

   (i) $\left\langle xy^2 - 2x, x^2y + 4xy, xy - y^2 \right\rangle$

   (ii) $\left\langle xyz - 3z^2, x^3 + y^2z^3, x^2yz^3 + 4 \right\rangle$.

2. Let the Order of power product in $R\left[w, x, y, z\right]$ be lex with $z < y < x < w$. Find a Grobner basis for the ideal below:

   $$\left\langle w + x - y + 4z - 3, 2w + x + y - 2z + 4, w + 3x - 3y + z - 5 \right\rangle.$$

3. Find a Grobner basis for the ideal below:

   (i) $\left\langle x^4 + x^3 - 3x^2 - 4x - 4, x^3 + x^2 - 4x - 4 \right\rangle$

   (ii) $\left\langle x^5 + x^2 + 2x - 5, x^3 - x^2 + x - 1 \right\rangle$.

4. Find a Grobner basis for the given ideal in $R\left[x, y\right]$. Consider the order of power products to be lex with $y < x$. If you can describe the corresponding algebraic variety in $R\left[xy\right]$

   (i) $\left\langle x^2y + x, xy^2 - x \right\rangle$

   (ii) $\left\langle x^2y + xy^2, xy - x \right\rangle$

   (iii) $\left\langle x^2y + x, x^2y - x \right\rangle$.

# CHAPTER 12

# INTRODUCTION TO EXTENSION FIELDS, VECTOR SPACE



## 12.0 INTRODUCTION

In the first part of this chapter, extension fields are introduced. The main goal is so that all polynomials can be reduced. In other words, their zeros can be found.

In the second part of this chapter, the notions in vector space which have been learned before in linear algebra class is extended in such that the scalars are elements of a field.

## 12.1 EXTENSION FIELDS

The formal definition of an extension field is given in the following.

**Definition 12.1 (Extension Field)**

A field $E$ is called an extension field of a field $F$ if $F \leq E$.

**Example 12.1**

The set of complex numbers is an extension of the set of real numbers, $\mathbb{R} \leq \mathbb{C}$.

Next are the definitions of algebraic and transcendental elements.

**Definition 12.2 (Algebraic, Transcendental)**

An element $\alpha$ of an extension field $E$ of a field $F$ is algebraic over $F$ if $f(\alpha)=0$ for some nonzero $f(x)\in F[x]$. If $\alpha$ is not algebraic over $F$, then $\alpha$ is transcendental over $F$.

**Example 12.2**

Let $F=\mathbb{R}$ and let $f(x)=x^2+1$, which have no zeros in $\mathbb{R}$. Then $\langle x^2+1\rangle$ is a maximal ideal in $R[x]$, so $R[x]/\langle x^2+1\rangle$ is a field. Identifying $r\in R$ with $r+\langle x^2+1\rangle$ in $R[x]/\langle x^2+1\rangle$, we can view $R$ as a subfield of $E=R[x]/\langle x^2+1\rangle$. Let $\alpha = x+\langle x^2+1\rangle$. Computing in $R[x]/\langle x^2+1\rangle$, we find

$$\begin{aligned}\alpha^2+1 &= \left(x+\langle x^2+1\rangle\right)^2+\left(1+\langle x^2+1\rangle\right)\\ &= \left(x^2+1\right)+\left(x^2+1\right)=0.\end{aligned}$$

Thus $\alpha$ is a zero of $x^2+1$. ■

**Example 12.3**

$\mathbb{Z}\subseteq\mathbb{C}$ is an extension field of $\mathbb{Q}$. Since $\sqrt{2}$ is a zero of $x^2-2$, we see that $\sqrt{2}$ is an algebraic element over $\mathbb{Z}$. Also $i$ is an algebraic element over $\mathbb{Q}$ being zero of $x^2+1$. ■

**Example 12.4**

It is easy to see that the real number $\sqrt{1+\sqrt{3}}$ is algebraic over $\mathbb{Q}$. For if $\alpha=\sqrt{1+\sqrt{3}}$ then $\alpha^2=1+\sqrt{3},$ so $\alpha^2-1=\sqrt{3}$ and $\left(\alpha^2-1\right)^2\neq 3.$ Therefore $\alpha^4-2\alpha^2-2=0,$ so $\mathbb{Q}$ is a zero of $x^4-2x^2-2,$ which in $\mathbb{Q}[x].$ ■

The following are definitions of algebraic and transcendental numbers.

**Definition 12.3 (Degree of an Extension Field)**

Let $E$ be an extension field of a field $F$ and $a$ is algebraic over $F$. Then $\deg(a,f)=\deg f(x)\in F[x]$ such that $f(a)=0$.

**Definition 12.4 (Algebraic and Transcendental Numbers)**

An element of $\mathbb{Q}$ that is algebraic over $\mathbb{Q}$ is an algebraic number. A transcendental number is an element of $\mathbb{Q}$ that is transcendental over $\mathbb{Q}$.

**Theorem 12.1 (Kronecker's Theorem)**

Let $F$ be a field and let $f(x)$ be a non constant polynomial in $F[x]$. Then there exists an extension field $E$ of $F$ and an $\alpha\in E$ such that $f(\alpha)=0.$

**Theorem 12.2**

Let $E$ be an extension field of a field $F$ and let $\alpha\in E.$ Let $\phi_\alpha: F[x]\to E$ be the evaluation homomorphism of $F[\alpha]$ into $E$ such that $\phi_\alpha(a)=a$ for $\alpha\in F$ and $\phi_\alpha(x)=\alpha.$ Then $\alpha$ is transcendental over $F$ if and only if $\phi_\alpha$ is a one-to-one mapping.

**Proof**

Now $\alpha$ is transcendental over $F$ if and only if $F(\alpha) \neq 0$ for all nonzero $f(x) \in F[x]$ which is true if and only if the kernel of $\phi_\alpha$ is $\{0\}$, that is if and only if $\phi_\alpha$ is a one-to-one mapping. ■

## 12.2 VECTOR SPACE

Abstract algebra has three basic components: groups, rings, and fields. To explore fields more deeply, we need some basic principles of vector space theory that are covered in a linear algebra course. In this subsection, a concise review on vector space is provided.

**Definition 12.5 (Vector Space)**

Let $F$ be a field. A vector space over $F$ ($F$-vector space) consists of an abelian group $V$ under addition together with an operation of scalar multiplication of each element of $V$ by each element of $F$ on the left such that for all $c, c_1, c_2 \in F$ and $v, v_1, v_2 \in V$, the following conditions are satisfied:

a) $cv \in V$.

b) $c_1(c_2 v) = (c_1 c_2)v$.

c) $(c_1 + c_2)v = c_1 v + c_2 v$.

d) $c(v_1 + v_1) = cv_1 + cv_2$.

e) $1 \cdot v = v$.

The elements of $V$ are vectors and the elements of $F$ are scalars.

**Example 12.5**

Consider the abelian group $\langle \mathbb{R}^n, + \rangle = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times ... \times \mathbb{R}$ for $n$ factors, which consists of ordered $n$-tuples under addition by components. Define scalar multiplication for scalars in by

$$r\alpha = (ra_1, ..., ra_n)$$

for $r \in \mathbb{R}$ and $\alpha = (a_1, ..., a_n) \in \mathbb{R}^n$. With these operations, $\mathbb{R}^n$ becomes a vector space over $\mathbb{R}$. The axioms for a vector space are readily checked. In particular, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ as a vector space over $\mathbb{R}$ can be viewed as all vectors whose starting points are origin of Euclidean plane. ■

**Theorem 12.3**

If $V$ is a vector space over $F$, then $0\alpha = 0$, $\alpha 0 = 0$ and $(-a)\alpha = a(-\alpha) = -(a\alpha)$ for all $a \in F, \alpha \in V$.

**Proof**

Take $(0\alpha) = (0+0)\alpha = (0\alpha) + (0\alpha)$. This equation is in the abelian group $\langle V, + \rangle$, so by the group cancellation law, $0 = 0\alpha$. Likewise, from $a0 = a(0+0) = a0 + a0$. We conclude that $a0 = 0$. Then

$$0 = 0\alpha = (a + (-a))\alpha = a\alpha + (-a)\alpha \text{ so } (-a)\alpha = -(a\alpha).$$

Likewise, from $0 = a0 = a(\alpha + (-\alpha)) = a\alpha + a(-\alpha)$. We can conclude that $a(-\alpha) = -(a\alpha)$. ■

**Exercises 12 (Introduction to Extension Fields, Vector Space)**

In Exercises 1 through 3, show that the given number $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ by finding $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$.

1. $1+\sqrt{2}$.

2. $1+i$.

3. $\sqrt{\sqrt[3]{2}-i}$.

4. Given $\alpha = \sqrt{3-\sqrt{6}} \in \mathbb{C}$. Find $\deg(\alpha, \mathbb{Q})$.

In Exercises 5 through 7, classify the given $\alpha \in \mathbb{C}$ as algebraic or transcendental over the given field $F$. If $\alpha$ is algebraic over $F$, find $\deg(\alpha, F)$.

5. $\alpha = 1+i, F = \mathbb{R}$.

6. $\alpha = \pi^2, F = \mathbb{Q}$.

7. $\alpha = \pi^2, F = \mathbb{Q}(\pi^3)$.

8. Show that the polynomial $x^2+1$ is irreducible in $\mathbb{Z}_3[x]$.

# CHAPTER 13

# ALGEBRAIC EXTENSIONS



## 13.0 INTRODUCTION

Recall from Chapter 12 that an element $\alpha$ of an extension field $E$ of a field $F$ is algebraic over $F$ if $f(\alpha)=0$ for some nonzero $f(x)\in F[x]$. If $\alpha$ is not algebraic over $F$, then $\alpha$ is transcendental over $F$. In other words, $\alpha$ is a root or a zero of the polynomial $f(x)$. In studying zeros of polynomials in $F[x]$, we shall be interested almost exclusively in extensions of $F$ containing only elements algebraic over $F$.

## 13.1 EXTENSIONS

**Definition 13.1 (Algebraic Extension)**

An extension field $E$ of a field $F$ is an algebraic extension of $F$ if every element in $E$ is algebraic over $F$.

**Definition 13.2 (Finite Extension)**

If an extension field $E$ of a field $F$ is of finite dimension $n$ as vector space over $F$, then $E$ is a finite extension of degree $n$ over $F$. The $[E:F]$ be the degree $n$ of $E$ over $F$.

**Theorem 13.1**

Let $S=\{\alpha_1,\alpha_2,\ldots,\alpha_r\}$ be a finite set of linearly independent vectors of a finite-dimensional vector space $V$ over a field $F$. Then $S$ can be enlarged to a basis for $V$ over $F$. Furthermore, if $B=\{\beta_1,\beta_2,\ldots,\beta_n\}$ is any basis for $V$ over $F$, then $r\le n$.

**Theorem 13.2**

A finite extension field $E$ of a field $F$ is an algebraic extension of $F$.

**Proof**

We must show that for $\alpha\in E$, $\alpha$ is algebraic over $F$. By Theorem 13.1, if $[E:F]=n$, then $1,\alpha,...,\alpha^n$ cannot be linearly independent elements, so there exist $\alpha_i\in F$ such that

$$a_n\alpha^n+\cdots+a_1\alpha+a_0=0,$$

and not all $a_i=0$. Then

$$f(x)=a_nx^n+\cdots+a_1x+a_0$$

is a nonzero polynomial in $F[x]$, and $f(\alpha)=0$. Therefore, $\alpha$ is algebraic over $F$. ■

**Corollary 13.1**

If $f_i$ is a field for $i=1,...,r$ and $f_{i+1}$ is a finite extension of $f_i$, then $f_r$ is a finite extension of $f_1$ and

$$[f_r:f_1]=[f_r:f_{r-1}][f_{r-1}:f_{r-2}]...[f_2:f_1].$$

**Theorem 13.3**

Let $E$ be an extension field of $F$, and let $\alpha \in E$ be algebraic over $F$. If $\deg(\alpha, F) = n$, then $F(\alpha)$ is an $n-$dimensional vector space over $F$ with basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Furthermore, every element $\beta$ of $F(\alpha)$ is algebraic over $F$, and $\deg(\beta, F) \leq \deg(\alpha, F)$.

**Corollary 13.2**

If $E$ is a finite extension field of a field $F$, and $K$ is a finite extension field of $E$, then $K$ is a finite extension of $F$, and

$$[K : F] = [K : E][E : F].$$

**Theorem 13.4**

If $E$ is an extension field of $F$, $\alpha \in E$ is algebraic over $F$, and $\beta \in F(\alpha)$, then $\deg(\beta, F)$ divides $\deg(\alpha, F)$.

**Proof**

By Theorem 13.3, $\deg(\alpha, F) = [F(\alpha) : F]$ and $\deg(\beta, F) = [F(\beta) : F]$. We have $F \leq F(\beta) \leq F(\alpha)$, so by Theorem 13.4, $[F(\beta) : F]$ divides $[F(\alpha) : F]$. ■

## 13.2 EXAMPLES OF ALGEBRAIC EXTENSIONS

**Example 13.1**

By Corollary 13.2, there is no element of $\mathbb{Q}\left(\sqrt{2}\right)$ that is a zero of $x^3-2$. Note that $\deg\left(\sqrt{2},\mathbb{Q}\right)=2,$ while a zero of $x^3-2$ is of degree 3 over $\mathbb{Q}$, but 3 does not divide 2. ■

**Example 13.2**

Consider $\mathbb{Q}\left(\sqrt{2}\right)$. Theorem 13.3 shows that $\left(1,\sqrt{2}\right)$ is a basis for $\mathbb{Q}\left(\sqrt{2}\right)$ over $\mathbb{Q}$. Then, $\sqrt{2}+\sqrt{3}$ is a zero of $x^4-10x^2+1$. We can show that this polynomial is irreducible in $\mathbb{Q}[x]$. Thus $\text{irr}\left(\sqrt{2}+\sqrt{3},\mathbb{Q}\right)=x^4-10x^2+1,$ so $\left[\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right):Q\right]=4$. Thus $\left(\sqrt{2}+\sqrt{3}\right)\notin\mathbb{Q}\left(\sqrt{2}\right),$ so $\sqrt{3}\notin\mathbb{Q}\left(\sqrt{2}\right)$. Consequently, $\left\{1,\sqrt{3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)=\left(\mathbb{Q}\left(\sqrt{2}\right)\right)\left(\sqrt{3}\right)$ over $\mathbb{Q}\left(\sqrt{2}\right)$. From the Theorem 13.4 shows that $\left\{1,\sqrt{2},\sqrt{3},\sqrt{6}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ over $\mathbb{Q}$. ■

**Theorem 13.5**

Let $E$ be an algebraic extension of a field $F$. Then there exist a finite number of elements $\alpha_1,...,\alpha_n$ in $E$ such that $E=F\left(\alpha_1,...,\alpha_n\right)$ if and only if $E$ is a finite-dimensional vector space over $F,$ that is if and only if a finite extension of $F$.

**Exercises 13 (Algebraic Extensions)**

In Exercises 1 through 5, find the degree and a basis for the given field extension. Justify your answers.

1. $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ over $\mathbb{Q}$.

2. $\mathbb{Q}\left(\sqrt[3]{2},\sqrt{3}\right)$ over $\mathbb{Q}$.

3. $\mathbb{Q}\left(\sqrt{2}+\sqrt{3}\right)$ over $\mathbb{Q}$.

4. $\mathbb{Q}\left(\sqrt{2},\sqrt[3]{5}\right)$ over $\mathbb{Q}$.

5. $\mathbb{Q}\left(\sqrt{2},\sqrt{6}\right)$ over $\mathbb{Q}\left(\sqrt{3}\right)$.

6. Prove in detail that $\mathbb{Q}\left(\sqrt{3}+\sqrt{7}\right)=\mathbb{Q}\left(\sqrt{3},\sqrt{7}\right)$.

## REFERENCES


1. Fraleigh J.B., 2003, *A First Course in Abstract Algebra*, 7th Ed. USA : Addison Wesley.
2. Ledermann W. , 1973, *Introduction to Group Theory* . Longman.
3. Alexandroff , 1959, *Theory of Groups* . Springer.
4. Rotman J. J., 1988, *An Introduction to the Theory of Groups*, 3rd Edition, Wm.C.Brown.
5. Malik, D. S., Mordeson, J. M and Sen, M. K., 1997, *Fundamentals of Abstract Algebra*, International Editions, McGraw-Hill Book Co-Singapore.
6. Gallian, J.A., 1994, *Contemporary Abstract Algebra*, 3rd Edition, Lexington, Massachusetts: D.C. Heath and Company.
7. Gilbert, J. and Gilbert, L., 2005, *Elements of Modern Algebra*, 6th Edition, Belmont, California: Thomson Brooks/Cole.
8. Gilbert, W.J. and Nicholson, W.K., 2004, *Modern Algebra with Applications*, 3rd Edition, New Jersey: John Wiley & Sons.
9. Robinson, D.J.S., 2005, *A Course in the Theory of Groups* (Graduate Texts in Mathematics), 2nd Edition, Springer.