A STUDY ON
SEMISIMPLE RINGS AND MODULES

By

FATEMA SIDDIQUA

Student No. 1017092502F

Session: October, 2017

MASTER OF SCIENCE
IN
MATHEMATICS

DEPARTMENT OF MATHEMATICS
BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY
DHAKA-1000
August, 2021

A STUDY ON
SEMISIMPLE RINGS AND MODULES

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree
of
MASTER OF SCIENCE
In
MATHEMATICS

By
FATEMA SIDDIQUA
Student No. 1017092502F, Registration No. 1017092502
Session: October, 2017
Department of Mathematics
Bangladesh University of Engineering and Technology
Dhaka-1000

Under the supervision of
Dr. Khandker Farid Uddin Ahmed
Professor
Department of Mathematics
BUET, Dhaka-1000August, 2021

The thesis entitled "A STUDY ON SEMISIMPLE RINGS AND MODULES", submitted by FATEMA SIDDIQUA, Student No. 1017092502F, Registration No. 1017092502, Session: October-2017, to the Department of Mathematics, has been accepted as satisfactory in partial fulfillment of the requirements for the award of the degree of Master of Science in Mathematics approved as to its style and contents on August 14, 2021.

BOARD OF EXAMINERS

1. Dr. Khandker Farid Uddin Ahmed
Professor
Department of Mathematics, BUET, Dhaka — Chairman (Supervisor)

2. Dr. Khandker Farid Uddin Ahmed
Professor and Head
Department of Mathematics, BUET, Dhaka — Member (Ex-Officio)

3. Dr. Mohammed Forhad Uddin
Professor
Department of Mathematics, BUET, Dhaka — Member

4. Dr. Rehena Nasrin
Professor
Department of Mathematics, BUET, Dhaka — Member

5. Salma Nasrin
Dr. Salma Nasrin
Professor
Department of Mathematics
University of Dhaka, Dhaka-1000 — Member (External)

DEDICATED

TO

MY PARENTS

CANDIDATE'S DECLARATION

I, Fatema Siddiqua, declare that the work presented in this thesis titled "A STUDY ON SEMISIMPLE RINGS AND MODULES" is the outcome of the investigation and research carried out by me under the supervision of Dr. Khandker Farid Uddin Ahmed, Professor, Department of Mathematics, BUET, Dhaka-1000, in accordance with the requirement of the University's Regulations and Code of Practice for research degree programs and that it has not been submitted anywhere for any other academic award of any degree or diploma.

Fatema Siddiqua

(Fatema Siddiqua)

ACKNOWLEDGEMENTS

First of all, I would like to express my sincerest gratitude and appreciation to my supervisor Dr. Khandker Farid Uddin Ahmed, Professor, Department of Mathematics, BUET, for his invaluable suggestion, constant inspiration and supervision that has enabled me to finish this dissertation successfully.

I am greatly indebted to the Head of the Department Dr. Khandker Farid Uddin Ahmed for providing me with all kinds of generous help and support during the period of my study.

I am highly grateful to the honorable members of the Board of Examiners, Prof. Dr. Mohammed Forhad Uddin and Prof. Dr. Rehena Nasrin, for their thoughtful and fruitful comments in preparing and writing this thesis.

I wish to thank the external examiner of the Board of Examiners, Dr. Salma Nasrin**,** Professor, Department of Mathematics, University of Dhaka.

My special thanks go to all of my respected teachers and staffs of the Department of Mathematics, BUET, for their help and support.

Last, first and always, I am grateful to my parents and my family members for their prayers and unstinting support throughout my study period.

Above all, I am grateful to Almighty Allah for giving me patience and strength to finish this program.

August 14, 2021 Fatema Siddiqua

ABSTRACT

In this thesis, we characterize semisimple modules over noncommutative rings and investigate their properties. We discuss noncommutative rings and their modules based on the Wedderburn-Artin structure theorem. Focusing on the basic concept of a semisimple module, we prove that a module over a semisimple ring is again semisimple. Considering the modular law, we prove that every submodule of a semisimple module contains a simple submodule. Some characterizations of semisimple modules over associative rings are also available in this study. We study some characterizations of regular rings. We show that every semisimple module is a quasi-projective module. Establishing the structure of endomorphism rings, we prove that the endomorphism ring of a semisimple module is regular. Finally, we prove that if M is a regular module and S is an endomorphism ring, then for any $\alpha \in S$, $\alpha(M)$ is a direct summand of M; conversely, when M is quasi-projective and $\alpha(M)$ is a direct summand of M for any $\alpha \in S$, then M is regular.

CONTENTS

CHAPTER I
INTRODUCTION

Ring theory is a subject of central importance in algebra. Historically, some of the major discoveries in ring theory have helped shape the course of development of modern abstract algebra. In view of these basic connections between ring theory and other branches of mathematics, it is perhaps no exaggeration to say that a course in ring theory is an indispensable part of education for any fledgling algebraist.

1.1 Background and present state of the problem

Modern ring theory began when Wedderburn in 1907 proved his celebrated classification theorem from finite dimensional semisimple algebras over fields. Twenty years later, Emmy Noether and Emil Artin introduced the ascending chain conditions and the descending chain conditions as substitutes for finite dimensionality. In 1927, Emil Artin proved the analog of Wedderburn's theorem for semisimple rings. The Wedderburn-Artin theorem is the cornerstone of noncommutative ring theory.

Wedderburn-Artin Theorem

Let R be a ring and let M be a right R-module. Then the following conditions are equivalent:

i) R_R is a semisimple ring;

ii) Every right R-module M is semisimple;

iii) Every right R-module M is injective;

iv) Every right R-module M is projective;

v) Every cyclic right R-module M is injective;

vi) Every cyclic right R-module M is projective;

vii) Every simple right R-module M is projective;

viii) $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_k}(D_k)$ where $i \in \{1, \ldots, k\}$, $M_{n_i}(D_i)$ is the ring of all $n_i \times n_i$ matrices over some skew-field D_i.

Wedderburn-Artin characterization theorem will be used to characterize semisimple modules over noncommutative rings. This characterization theorem will be used to develop some properties of semisimple modules over endomorphism rings.

1.2 Literature Review

Ring theory is an indispensable part of Algebra. It has been widely applied in Electrical and Computer Engineering [1]. Module theory appeared as a generalization of theory of vector spaces over a field. Every field is a ring and every ring may be considered as a module. Semisimple rings and modules have been studied extensively in many texts [2-4]. An Artinian ring is initially understood via its largest semisimple quotient rings. The structure of Artinian semisimple rings is well understood by the Artin-Wedderburn theorem, which exhibits these rings as finite direct product of matrix rings [5]. Asgari *et al.* [6] investigated various characterizations of right T-semisimple rings. Every semisimple ring is regular. Lee *et al.* [7] extensively investigated abelian groups whose endomorphism rings are von Neumann regular. They also studied modules whose endomorphism rings are von Neumann regular and provided characterizations of endoregular modules. Agayev *et al.* [8] showed that R is an R-semisimple ring if and only if it is a direct sum of simple rings and investigated the structure of modules whenever R is an R-semisimple ring.

The rigorous characterization theorem of Sanh *et al.* [9] will be used to develop some properties of semisimple modules over endomorphism rings. Artin [10] showed that the result of Wedderburn [11] depends only on the descending chain condition which gave birth to noncommutative ring theory.

Hadi and Shyaa [17] introduced the notions of strongly t-semisimple modules and strongly t-semisimple rings as a generalization of semisimple modules and rings, respectively. They also investigated many characterizations and properties of each of these concepts. Dung and Garcia [18] studied preinjective left modules over an arbitrary left pure semisimple ring R. They proved that R is of finite representation type if and only if every finitely presented right R-module is endofinite, if and only if every finitely presented right R-module has a left artinian endomorphism ring and obtained new criteria for a right pure semisimple ring to be of finite representation type [19].

Mozaffarikhah *et al.* [20] introduced the concept of p-semisimple modules and showed that a large family of abelian groups are p-semisimple. Bennis and Wang [21] investigated 2-strongly Gorenstein projective-semisimple rings which are a particular kind of quasi-Frobenius rings over which all modules are periodic of period 2.1. Namely, they showed that local 2-strongly Gorenstein projective-semisimple rings are the same as the known Artinian valuation rings. Guo and Shum [22] proved that a ring R is a Baer ring if and only if R itself, regarded as a regular R-module, is Baer semisimple. They have also introduced the concept of right perpetual ideals and consequently, reduced pp rings are characterized by using right perpetual submodules. Hadi and Shyaa [23] introduced the notions of Fi-semisimple, Fi-t-semisimple and strongly Fi-t-semisimple modules. This is a generalization of semisimple modules. Hirano and Tsutsui [24] investigated a ring R with the property that for every right R-module M and every ideal I of R the annihilator of I in M is a direct summand of M, and they introduced conditions under which such a ring is semisimple Artinian.

Boulagouaz and Oukhtite [25] proved that for the left artinian rings with involution, this new definition coincides with the classical definition of semisimple rings. Dinh and Huynh [26] proved a ring-direct decomposition theorem for right and left $\wp*$-semisimple rings. Moreover, they described the structure of each direct summand in the obtained decomposition of these rings. Engin *et al*. [27] investigated the various properties of RD-modules and RS-modules. They proved that M is an RD-module if and only if $M = Rad(M) \oplus X$, where X is semisimple and showed that a finitely generated RS-module is semisimple which gives us the characterization of semisimple rings in terms of RS-modules. Abed and Ahmad [28] introduced new conditions over semisimple, simple modules and discussed some of the basic characterizations of these modules which show many relations between these modules and length property. Jenkins and Smith [31] defined the prime radical of M to be the intersection of M and all prime submodules of M.

McCasland and Moore [33] studied prime submodules and their various properties. Several authors extended the notion of prime left ideals to modules. McCasland and Smith [34] investigated properties of prime submodules of Noetherian module. Behboodi and Bigdeli [35] studied rings and modules in which every prime submodule is isomorphic to a direct summand and they called them prime virtually (or $\wp$-virtually) semisimple modules. Behboodi *et al.* [36] showed that the left R-module R is completely virtually semisimple if and only if R has a unique decomposition as a finite direct product of matrix rings over principal left ideal domains. They carried out a study of virtually semisimple modules over a commutative ring R [37]. As an application of their "structure theorem", they gave a characterization of commutative rings for which each proper ideal is virtually semisimple.

1.3 Organization of the Thesis

In this thesis, Chapter I deals with the early history of simple and semisimple rings and semisimple modules.

All the essential basic definitions, examples and their properties are given in Chapter II. In this chapter, we have some nice diagrams which help us to establish the main theorem of this research work.

Chapter III deals with the basic properties of simple and semisimple rings. In this Chapter, we describe some properties of prime and semi-prime ideals in associative arbitrary rings modifying the results on simple and semisimple modules investigated in [8]. Some properties of regular rings are investigated in associative arbitrary rings. The structure of endomorphism ring is also available as a generalization of arbitrary rings in this chapter. Based on the structure, a theorem on regular modules is established because every semisimple ring is regular.

In Chapter IV, conclusion of the thesis and its future scopes are available.

CHAPTER II
BASIC KNOWLEDGE

The subject of our study is ring theory. Throughout this thesis, all rings are associative with identity and all modules are unitary right R-modules. Ring admit a valuable and natural representation theory, analogous to the permutation representation theory for groups. As we shall see, each ring admits a vast horde of representation as an endomorphism ring of an abelian group. Each of these representations is called a module. A substantial amount of information about a ring can be learned from a study of the class of modules it admits. Modules actually serve as a generalization of both vector spaces and abelian groups and their basis behavior is quite similar to that of the more special systems.

We denote by R an arbitrary ring and by $Mod\text{-}R,$ the category of all right R-modules. The notation M_R indicates a right R-module M, which is assumed to be unity when $1 \in R$. The set $Hom_R(M, N)$ denotes the set of right R-module homomorphisms between two right R-modules M and N and if further emphasis is needed, the notation $Hom_R(M, N)$ is used. The kernel of any $f \in Hom_R(M, N)$ is denoted by $Ker\ f$ and the image of f by $Im\ f.$ In particular, $End_R(M)$ denotes the ring of endomorphisms of a right R-module $M.$

In this chapter, we introduce the fundamental tools of this study. Section 2.1 reviews the basic facts about ring, subring, zero divisors, quotient ring and their examples. Section 2.2 reviews the basic facts about ideals and different kinds of ideal. Section 2.3 reviews the basic fact about ring homomorphisms and other notions. Section 2.4 reviews the basic facts about modules, submodules and different kinds of submodules. It also introduces some of the notation and the examples that will be needed later.

2.1 Rings, Basic Definitions

Before dealing with deeper results on the structure of rings with the help of module theory, we provide first some essential elementary definitions, examples and properties.

Definition 2.1.1

A triple $(R, +, \cdot)$, where + and $\cdot$ are two binary operations on R, is called a ***ring*** if the following axioms are satisfied: For any $x, y, z \in R$

(R1) $(x + y) + z = x + (y + z)$ (Associativity of addition)

(R2) $x + y = y + x$ (Commutativity of addition)

(R3) There exists $0 \in R$, called the zero such that $x + 0 = 0 + x = x$

(Existence of an additive identity)

(R4) There exists $(-x) \in R$ such that $x + (-x) = (-x) + x = 0$.

(Existence of an additive inverse)

(R5) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(Associativity of multiplication)

(R6) There exists $1 \in R$ such that $1 \cdot x = x \cdot 1 = x$

(Existence of multiplicative identity)

(R7) $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$

(Law of distributivity)

In addition, the ring $(R, +, \cdot)$ is called a ***commutative ring*** if

(R8) $x \cdot y = y \cdot x$ for all $x, y \in R$

(Commutativity of multiplication)

For example, the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all commutative rings with identity under the appropriate addition and multiplication. In these, every non-zero element has an inverse. Also the integers $\mathbb{Z}$ with the usual addition and multiplication is a commutative ring with identity. The only elements with (multiplicative) inverses are ± 1. Again, if $a, b, c \in \mathbb{Z}$ (or $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) then the system $(R, +, \cdot)$ does not form a ring, where $R = \left\{\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}\right\}$, because $A, B \in R$ such that $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & 0 \end{bmatrix}$ imply $AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 \\ c_1a_2 & c_1b_2 \end{bmatrix}$. Here, AB is not a matrix of the form $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$ and therefore, $AB \notin R$. The set of all $n \times n$ square matrices with real coefficients forms a ring $(M_n(R), +, \cdot)$ which is not commutative if $n > 1$, because matrix multiplication is not commutative. Here, the set of all 2×2 real matrices forms a ring under the usual matrix addition and multiplication. This is a non-commutative ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Definition 2.1.2

Axioms (R1)-(R4) are equivalent to saying that $(R, +)$ is an ***abelian group*** and the axioms (R5) and (R6) are equivalent to saying that $(R,\cdot)$ is a ***monoid or semigroup***.

For example, the real numbers are an abelian group under addition and the non-zero real numbers are an abelian group under multiplication. For the integers $\mathbb{Z}$, the abelian group denoted by $(\mathbb{Z}, +)$, where the addition operation $+$ combines any two integers to form a third integer, addition is associative, zero is the additive identity, every integer n has an additive inverse $-n$ and the addition operation is commutative since $m + n = n + m$ for any two integers m and n.

Definition 2.1.3

Let the set R contains only the zero element. That is $R = \{0\}$, then $(R, +,\cdot)$ is called a ***zero ring***.

Again, if there exists an element $1 \in R$ such that $1 \neq 0$ and $1 \cdot a = a \cdot 1 = a$ for each element $a \in R$, we say that R is a ring with unity or identity and 1 is called the ***multiplicative identity or unity***.

For example, the system $(R, +,\cdot)$ is a zero ring, where $R = \left\{\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right\}$. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all rings with unity where the integer 1 is the identity element of $\mathbb{Z}$. Also, the ring $M_2(\mathbb{Z})$ is a ring with identity. The identity element of $M_2(\mathbb{Z})$ is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Again, let $E = \{\dots, -4, -2, 0, 2, 4, \dots\}$ be a set of even integers. Then E is a ring without unity.

Theorem 2.1.4

Let R be the set of all functions $f: \mathbb{R} \to \mathbb{R}$. Then $(R, +,\cdot)$ is a commutative ring with identity.

Proof: Let R be the set of all functions $f: \mathbb{R} \to \mathbb{R}$ for all f, g in R and $a \in f$ define by $+$ and $\cdot$ as

$$(f + g)(a) = f(a) + g(a)$$

$$(f \cdot g)(a) = f(a) \cdot g(a)$$

Since $+$ and $\cdot$ are binary operations on R, using the associativity of $\mathbb{R}$, for all f, g, h in R and $\forall a \in \mathbb{R}$, we have $\big((f + g) + h\big)(a) = (f + g)(a) + h(a)$

$$= (f(a) + g(a)) + h(a)$$

$$= f(a) + \big(g(a) + h(a)\big) = \big(f + (g + h)\big)(a)$$

Thus, $(f + g) + h = \ f + (g + h)$ which shows that $+$ is associative.

In a similar manner, we can show that the other properties of a ring hold for R by using the fact that they hold for $\mathbb{R}$. Thus, $(R, +,\cdot)$ is a ring.

The function $i_0: \mathbb{R} \to \mathbb{R}$ defined by $i_0(a)$ $\forall a \in \mathbb{R}$, is the additive identity of R and $i \in R$ defined by $i_1(a) = 1$ for all $a \in \mathbb{R}$ is the identity of R. Also, $\forall f, g$ in R, and $\forall a \in \mathbb{R}$, $(f \cdot g)(a) = f(a)g(a) = g(a)f(a) = (g \cdot f)(a)$. Thus, $\forall f, g \in R, f \cdot g = g \cdot f$. Consequently, $(R, +, \cdot)$ is a commutative ring with identity.

Example 2.1.5

If $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$, then $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ is a commutative ring.

Proof: The set $\mathbb{Q}(\sqrt{2})$ is a subset of $\mathbb{R}$ and the addition and multiplication is the same as that of real numbers. First, we check that $+$ and $\cdot$ are binary operators on $\mathbb{Q}(\sqrt{2})$. If $a, b, c, d \in \mathbb{Q}$, we have

$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, since $(a + c)$ and $(b + d) \in \mathbb{Q}$.

Also $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, since $(ac + 2bd)$ and $(ad + bc) \in \mathbb{Q}$.

We now check that $\mathbb{Q}(\sqrt{2})$ is satisfied all the axioms of a commutative ring

i. Addition of real numbers is associative: For any $a, b, c, d, e, f \in \mathbb{Q}$, we have

$$[(a + b\sqrt{2}) + (c + d\sqrt{2})] + (e + f\sqrt{2}) = (a + b\sqrt{2}) + [(c + d\sqrt{2}) + (e + f\sqrt{2})] \in \mathbb{Q}(\sqrt{2})$$

ii. Addition of real numbers is commutative: For any $a, b, c, d \in \mathbb{Q}$, we have

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2})] \in \mathbb{Q}(\sqrt{2})$$

iii. The zero $0 + 0\sqrt{2}$ is an additive identity on $\mathbb{Q}(\sqrt{2})$.

iv. The additive inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

v. Multiplication of real numbers is associative: For any $a, b, c, d, e, f \in \mathbb{Q}$, we have

$$[(a + b\sqrt{2}) \cdot (c + d\sqrt{2})] \cdot (e + f\sqrt{2}) = (a + b\sqrt{2})[(c + d\sqrt{2}) \cdot (e + f\sqrt{2})] \in \mathbb{Q}(\sqrt{2})$$

vi. For any $(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$, there exists a $(1 + 0\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ such that

$$(a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = (1 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = (a + b\sqrt{2}),$$

where $(1 + 0\sqrt{2})$ is the multiplicative identity of $\mathbb{Q}(\sqrt{2})$.

vii. The distributive axioms hold for elements of $\mathbb{Q}(\sqrt{2})$: For any $a, b, c, d, e, f \in \mathbb{Q}$, we have

$$[(a + b\sqrt{2}) + (c + d\sqrt{2})] \cdot (e + f\sqrt{2})$$
$$= [(a + b\sqrt{2}) \cdot (e + f\sqrt{2})] + [(c + d\sqrt{2}) \cdot (e + f\sqrt{2})] \in \mathbb{Q}(\sqrt{2})$$

And $\left[\left(c+d\sqrt{2}\right)+\left(e+f\sqrt{2}\right)\right]\cdot\left(a+b\sqrt{2}\right)$

$$=\left[\left(c+d\sqrt{2}\right)\cdot\left(a+b\sqrt{2}\right)\right]+\left[\left(e+f\sqrt{2}\right)\cdot\left(a+b\sqrt{2}\right)\right]\in\mathbb{Q}\left(\sqrt{2}\right)$$

viii. Multiplication of real numbers is commutative: For any $a,b,c,d\in\mathbb{Q}$, we have

$$\left(a+b\sqrt{2}\right)\cdot\left(c+d\sqrt{2}\right)=\left(c+d\sqrt{2}\right)\cdot\left(a+b\sqrt{2}\right)\in\mathbb{Q}\left(\sqrt{2}\right)$$

Thus $\mathbb{Q}\left(\sqrt{2}\right)$ is a commutative ring where $\mathbb{Q}\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\in\mathbb{R}\middle|a,b\in\mathbb{Q}\right\}$.

□

Definition 2.1.6

Let $(R,+,\cdot)$ be a ring. Then a subset P of R is called a ***subring*** of R if it is itself a ring with the same operations as R.

For example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and $\mathbb{Q}$ is a subring of $\mathbb{R}$. The set of even integers $E=\{\dots,-4,-2,0,2,4,\dots\}$ is a subring of the ring of integers $\mathbb{Z}=\{\dots,-2,-1,0,1,2,\dots\}$. More generally, if n is any integer, then the set of all multiples of n is a subring $n\mathbb{Z}$ of $\mathbb{Z}$. The odd integers do not form a subring of $\mathbb{Z}$. $M_2(\mathbb{Z})$ is a subring of $M_2(\mathbb{Q})$. Also, $2\mathbb{Z}$ is not a subring of $M_2(\mathbb{Z})$.

Note. A subring of a ring with identity need not have an identity. All results for a ring without identity are true for rings with identity.

Proposition 2.1.7 (Subring Test)

A subset $P\subseteq R$ of a ring R is called a subring of R if the following conditions hold:

i) $0\in P$;

ii) $1\in P$;

iii) If $r,p\in P$, then $(r+p)$, rp and $-p$ are all in P.

Note. All results for a ring without identity are true for rings with identity. A subring of a ring with identity need not have an identity.

Definition 2.1.8

A relation R on a set S is called an ***equivalence relation*** if the following conditions hold:

i) Reflexive condition: For any $\in S$, aRa.

ii) Symmetric condition: For $a,b\in S$, if aRb then bRa.

iii) Transitive condition: For $a,b,c\in S$, if aRb and bRc then aRc.

Definition 2.1.9

If R is an equivalence relation on a set S and $a \in S$ then $\bar{a}$ or $[a] = \{x \in S | xRa\} = \{x \in S | (x, a) \in R\}$ is called the ***equivalence class*** containing a. The set of all equivalence classes is called the ***quotient set*** of S by R and is denoted by $S \,/\, R$. Hence $S \,/\, R = \{[a]: a \in S\}$.

The set of equivalence classes is called the ***set of integers modulo n*** and is denoted by $\mathbb{Z}_n$.

In the congruence relation modulo 3, we have the following equivalence classes:

$$[0] = 0 + 3\mathbb{Z} = \{\dots, -3, 0, 3, 6, 9, \dots\}$$
$$[1] = 1 + 3\mathbb{Z} = \{\dots, -2, 1, 4, 7, 10, \dots\}$$
$$[2] = 2 + 3\mathbb{Z} = \{\dots, -1, 2, 5, 8, 11, \dots\}$$
$$[3] = 3 + 3\mathbb{Z} = \{\dots, 0, 3, 6, 9{,}12, \dots\} = [0]$$

Any equivalence class must be one of [0], [1] or [2]. So $\mathbb{Z}_3 = \{[0], [1], [2]\}$. In general, $\mathbb{Z}_n = \{[0], [1], [2], .., [n-1]\}$. Since any integer is congruent modulo n to its remainder when divided by n.

Definition 2.1.10

Let R be a ring if there exist a smallest positive integer n such that $na = 0, \forall a \in \mathbb{R}$. Then n is called the ***characteristics*** of $\mathbb{R}$.

For example, the ring $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ has characteristic 6. Since

$$6 \cdot 0 \equiv 0(mod\ 6),$$
$$6 \cdot 1 \equiv 0(mod\ 6),$$
$$6 \cdot 2 \equiv 0(mod\ 6),$$
$$6 \cdot 3 \equiv 0(mod\ 6),$$
$$6 \cdot 4 \equiv 0(mod\ 6),$$
$$6 \cdot 5 \equiv 0(mod\ 6).$$

Definition 2.1.11

A non-zero element of a ring R is called a ***zero divisor*** in R if the product of two non-zero elements of R is zero. That is, if $ab = 0$ then $a \neq 0$ and $b \neq 0$ for $a, b \in R$.

For example, [2] and [3] are zero divisors in $\mathbb{Z}_6$ since $[2] \neq [0], [3] \neq [0], [2][3] = [6] = [0]$. The ring $R = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}: a, b, c, d \in \mathbb{Z}\}$ is a ring with zero divisors. Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in R$, B$= \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} \in R$, where $a \neq 0$ and $b \neq 0$, there $AB = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$, where A$\neq 0$ and $B \neq 0$.

Definition 2.1.12

A ring R is called a ring ***without zero divisor*** if it is not possible to find two non-zero elements for $a, b \in R$ such that if $ab = 0$ then $a = 0$ or $b = 0$.

For example, let $R = \mathbb{Z}_5$, the ring of integers modulo 5. Then $\mathbb{Z}$ is a commutative ring with unit. In fact, it is a field. Also its non-zero element are $[1], [2], [3], [4]$ and $[2][3] = [6] = [1]$ and $[1]$ and $[4]$ are their own inverses, so every non-zero element in $\mathbb{Z}_5$ has an inverse in $\mathbb{Z}_5$. All the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are rings without zero divisors.

Definition 2.1.13

Let $(R; +; \cdot)$ be a ring. Then R is called a **domain** if it has no zero divisors. An ***integral domain*** is a commutative ring with unity and without zero divisors. More easily speaking, a commutative domain is called an integral domain.

For example, the rings $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{R}, +, \cdot)$ all are integral domains. The ring $(I, +, \cdot)$ is an integral domain where I is the set of all irrational numbers. $M_2(\mathbb{Z})$ is not an integral domain since $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Theorem 2.1.14

If a is a non-zero elements of an integral domain R and $a \cdot \mathrm{b} = \mathrm{a} \cdot \mathrm{c}$, then prove that $b = c$.

Proof: If $a \cdot \mathrm{b} = \mathrm{a} \cdot \mathrm{c}$ then $a \cdot (\mathrm{b} - \mathrm{c}) = a \cdot \mathrm{b} - \mathrm{a} \cdot \mathrm{c} = 0$. Since R is an integral domain, it has no zero divisors. Since $a \neq 0$, it follows that $(b - c) = 0$. Hence $b = c$.

Generally speaking, it is possible to add, subtract and multiply elements in a ring, but it is not always possible to divide. Even in an integral domain, where elements can be canceled, it is not always possible to divide by non-zero elements.

□

Definition 2.1.15

Let R be a ring. Then a ***division ring or skew-field*** is a ring R with an identity in which every nonzero element in R is a unit. A division ring is a ring in which every non-zero element has an inverse. The most important class of division rings are the commutative ones, which are called **fields**. A division ring is generally a noncommutative ring. It is commutative if and only if it is a field.

For example, all fields are division rings. The quaternions form a noncommutative division ring.

Note. A ring R is a division ring if and only if $(R\backslash\{0\},\cdot)$ is a group. Therefore if R is a division ring, then for all $a \in R$ with $a \neq 0$, there exists a unique element, denoted by $a^{-1} \in R$ such that $a^{-1} \cdot a = a \cdot a^{-1} = 1$. We call a^{-1} the multiplicative inverse of a.

Proposition 2.1.16

R is a division ring if and only if every non-zero element has a left inverse.

Proof: If every $a \neq 0 \in R$ has a left inverse b (so that $b = 1$). Then b also has a left inverse c with $cb = 1$. But then $c = c(ba) = (cb)a = a$. So b is a two-sided inverse for a, making R a division ring.

□

Definition 2.1.17

A ring R is called a ***field*** if it is a commutative ring with unity and every non-zero element has a multiplicative inverse. That is, a field is a commutative ring with identity in which every non-zero element form an abelian group under multiplication or has its multiplicative inverse.

For example, the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields with respect to addition and multiplication. The set $\mathbb{Z}$ of all integers is not a field, because all non-zero elements have not multiplicative inverses except 1 and -1. $\mathbb{Z}$ is not a field because the number $2 \in \mathbb{Z}$ but its multiplicative inverse is $\frac{1}{2}$ is not in $\mathbb{Z}$. Let $R = \mathbb{Z}_5$, the ring of integers modulo 5. Then $\mathbb{Z}$ is a commutative ring with unit. In fact, it is a field. Also its non-zero element are $[1]$, $[2]$, $[3], [4]$ and $[2][3] = [6] = [1]$ and $[1]$ and $[4]$ are their own inverses, so every non-zero element in $\mathbb{Z}_5$ has an inverse in $\mathbb{Z}_5$.

Theorem 2.1.18

Every field is an integral domain. It has no zero divisors.

Proof: Let, $a \cdot \mathrm{b} = 0$ in a field F. If $a \neq 0$, there exists an inverse $a^{-1} \in F$ and

$$b = (a^{-1} \cdot \mathrm{a}) \cdot \mathrm{b} = a^{-1}(\mathrm{a} \cdot \mathrm{b}) = a^{-1} \cdot 0 = 0$$

Hence either $a = 0$ or $b = 0$, and F is an integer. □

Corollary 2.1.19

A field is an integral domain.

Proof: Suppose $a \neq 0$ and $ab = 0$. Since $a \neq 0, a^{-1}$ exists and $a^{-1}ab = a^{-1}0$ implies that $1b = 0$. Hence, $b = 0$. Thus we have an integral domain.

□

Note. One can think of ab^{-1} as $\frac{a}{b}$ in the same way we think of $a + (-b) = a - b$. In a field, addition, subtraction, multiplication, and division (except by 0) are closed.

Theorem 2.1.20

A finite integral domain is a field.

Proof: Let, $D = \{x_0, x_1, \dots, x_n\}$ be a finite integral domain with x_0 as 0 and x_1 as 1. We have to show that every non-zero element of D has a multiplicative inverse. If x_i is non-zero, we show that the set $x_iD = \{x_ix_0, x_ix_1, \dots, x_ix_n\}$ is the same as the set D. If $x_ix_j = x_ix_k$ then by the cancellation property $x_j = x_k$. Hence all the elements $x_ix_0, x_ix_1, \dots, x_ix_n$ are distinct and x_iD is a subset of D with the same number of elements. Therefore, $x_iD = D$, but there is some element x_j such that $x_ix_j = x_1 = 1$. Hence $x_j = {x_i}^{-1}$ and D is a field.

□

Example 2.1.21

Prove that, $\mathbb{Z}(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$ is an integral domain but is not a field.

Proof: Here, we can see that

i) $0 + 0\sqrt{3}$ is the additive identity.

ii) $1 + 0\sqrt{3}$ is the multiplicative identity.

iii) Take $\sqrt{3} \in \mathbb{Z}(\sqrt{3})$. Suppose $\sqrt{3}$ is a unit in $\mathbb{Z}(\sqrt{3})$. Then $\left(\sqrt{3}\right)^{-1} = a + b\sqrt{3}$ for some a, b in $\mathbb{Z}$. In $a = 0$, then $\left(\sqrt{3}\right)^{-1} = b\sqrt{3}$ implying that $1 = 3b$, which is a contradiction because this equation has no solutions in $\mathbb{Z}$. Thus, $a \neq 0$, so $\left(\sqrt{3}\right)^{-1} = a + b\sqrt{3} \Longrightarrow 1 = a\sqrt{3} + 3b \Longrightarrow \sqrt{3} = \frac{1-3b}{a} \in \mathbb{Q}$. Hence, $\sqrt{3}$ is not a unit.

Hence, $\mathbb{Z}(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$ is not a field. Therefore the set $\mathbb{Z}(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in \mathbb{Z}\}$ is an integral domain.

□

Definition 2.1.22

The ***characteristic of an integer domain*** D is either 0 or a positive integer n according to the order the unity element e of D is 0 or n. When e is regarded as an element of the additive group of D. i.e., n is the least positive integer such that $ne = 0$. The ***characteristic of a field*** is defined to be the characteristic of an integral domain.

For example, let, $I_7 = \{[0], [1], [2], \dots, [5], [6]\}$ then the characteristic of the field $(I_7, +_7, \times_7)$ is 7.

2.2 Ideals, Different Kinds of Ideal

Definition 2.2.1

Let $(R, +, \cdot)$ be a ring and let $I \subseteq R$, a subset. Then I is called a ***left ideal*** of R if $(I, +)$ is an additive subgroup and $\forall\, x \in I,\ \forall\, r \in R$, we have $rx \in I$. Equivalently, $I \subseteq R$ is a left ideal of R if and only if

i) I is an additive subgroup of R. i.e., $\forall\, x, y \in I$, we have $x + y \in I$ and

ii) $\forall\, x \in I,\ \forall\, r \in R$, we have $rx \in I$

For example, let $R = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}\right\}$ is a ring. Then $I = \left\{\begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} : a, c \in \mathbb{Z}\right\}$ is a left ideal, but $T = \left\{\begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} : b, d \in \mathbb{Z}\right\}$ is not a left ideal of R.

Definition 2.2.2

Let $(R, +, \cdot)$ be a ring and let $I \subseteq R$, a subset. Then I is called a ***right ideal*** of R if $(I, +)$ is an additive subgroup and $\forall\, x \in I,\ \forall\, r \in R$, we have $xr \in I$. Equivalently, $I \subseteq R$ is a right ideal of R if and only if

i) I is an additive subgroup of R. i.e., $x, y \in I$, we have $x + y \in I$ and

ii) $\forall\, x \in I,\ \forall\, r \in R$, we have $xr \in I$.

For example, In the ring R of 2×2 matrices with entries in $\mathbb{R}$, the subset $J = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R}\right\}$ is a right ideal.

Definition 2.2.3

Again, a nonempty subset I of a ring R is called an ***ideal (two-sided ideal)*** of R if I is a subring of R and $xr \in I$ and $rx \in I, \forall\, x \in I, \forall\, r \in R$.

Remark. In any ring R, the subsets $\{0\}$ and R are ideals. These ideals are called trivial ideals. All other ideals are called nontrivial.

Example 2.2.4

Let $R = M_2(\mathbb{Z})$ where M a ring of 2×2 matrices with integer entries. Consider four subsets I_1, I_2, I_3 and I_4 of R. Prove that the subset I_1 is a left ideal but not a right ideal; the subset I_2 is a right ideal but not a left ideal; the subset I_3 is a two-sided ideal and the subset I_4 is a subring but not an ideal of R.

Proof: Consider the ring $R = M_2(\mathbb{Z})$. Let $I_1 = \left\{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}, I_2 = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in \mathbb{Z}\right\}$,

$$I_3 = \left\{\begin{pmatrix} a & c \\ b & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z}\right\}, I_4 = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{Z}\right\}$$

Because $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I_1, I_1 \neq \emptyset$. Let $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} \in I_1$ and $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in R$. Then

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} - \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a-c & 0 \\ b-d & 0 \end{pmatrix} \in I_1 \text{ and}$$

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} xa+yb & 0 \\ za+wb & 0 \end{pmatrix} \in I_1$$

which is proving that I_1 is a left ideal of R. Similarly, we can prove that I_2 is a right ideal of R, but not a left ideal. That is, $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I_1$ and $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in R$ but $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin I_1$.

Hence, I_1 is not a right ideal of $M_2(\mathbb{Z})$. Similarly, I_2 is a right ideal of $M_2(\mathbb{Z})$, but not a left ideal, I_3 is an ideal of $M_2(\mathbb{Z})$, and I_4 is a subring, but not an ideal of $M_2(\mathbb{Z})$.

□

Definition 2.2.5

An ideal e of a ring R is called an ***idempotent*** if $e^2 = e$. A right ideal of a ring R is called an idempotent if $I^2 = I$. Again, a right ideal I of a ring R is called ***nilpotent*** if there exist a natural number n such that $I^n = (0)$. The element 0 (zero) of a ring is trivially nilpotent.

For example, In any ring R, the elements 0 and 1 are idempotents and 0 is nilpotent. Let, any ideal $2\mathbb{Z}_8 = \{[0], [2], [4], [6]\}$ where $\mathbb{Z}_8 = \{[0], [1], [2], \dots, [7]\}$. Then $I = 2\mathbb{Z}_8$ is a nil ideal of $\mathbb{Z}_8$. Again, the nilpotent elements of $\mathbb{Z}_8 = \{[0], [1], \dots, [7]\}$, integers modulo 8 are $0,\ 2,\ 4,\ 6$. Since $2^3 = 0$, $4^2 = 0, 6^3 = 0$. In $M_2(\mathbb{R})$ we have,

Idempotent elements : $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{bmatrix}$, ... and

Nilpotent elements: $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ -2 & 0 \end{bmatrix}$, ...

Remarks. Every nilpotent ideal is a nil ideal, since if I is a nilpotent ideal, then there exists a positive integer n such that $I^n = (0)$. So for each $a \in I$, $a^n \in I^n$=(0) implies that $a^n = 0$. Hence I is a nil ideal. But the converse is not true. The notion of a nil ideal has a connection with that of a nilpotent ideal and in some classes of rings, the two notions coincide. If an ideal is nilpotent, it is of course nil. There are two main barriers for nil ideals to be nilpotent.

a) There need not be an upper bound on the exponent required to annihilate the elements. Arbitrarily high exponents may be required.

b) The product of n nilpotent elements may be non-zero for arbitrarily high n.

Both of these barriers must be avoided for a nil ideal to qualify as nilpotent.

Definition 2.2.6

Every ring R has at least two ideals which are:R itself (Unit ideal) and $\{0\}$ itself (Null ideal).

These two ideals are called ***improper*** or trivial.

Definition 2.2.7

The ideals other than these two is called proper or non-trivial ideals of R. An ***proper ideal*** J of a ring R is an ideal such that J is a proper subset of R. That is, $J \subseteq R$ and $J \neq R$. An ideal I in a commutative ring R is termed as proper ideal if it satisfies the following equivalent statements: (i) $1 \notin I$ (ii) $I \neq R$. For example, $2\mathbb{Z}$ is a proper ideal of the ring of integers $\mathbb{Z}$, since $1 \notin 2\mathbb{Z}$. Also $3\mathbb{Z} = \{\dots, -3, 0, 3, 6, 9, \dots\}$ is an ideal in $\mathbb{Z}$. It's proper because that isn't all of $\mathbb{Z}$. The only ideal of $\mathbb{Z}$ that isn't proper is $\mathbb{Z}$ itself.

Definition 2.2.8

An ideal I of a ring R, generated by a single element a of I, is called a ***principal ideal*** of ring R and we denote this by $I = \langle a \rangle$ or $I = (a)$.

The principal ideal generated by 0 is the ring $\{0\}$ is called null ideal, while the principal ideal generated by the unity element 1 in the ring R, called unit ideal and we write $(1) = R$.

For example, the ring $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, the ideal $I = (5)$ is a principal ideal. Here, the ideal generated by 5 of commutative ring $\mathbb{Z}$ of integers is $(5) = \{\dots, -10, -5, 0, 5, 10, \dots\}$.

Definition 2.2.9

Let R be a ring and an ideal I of a ring R is said to be a ***maximal ideal*** in R if for any ideal J of R, $I \subseteq J \subseteq R$ implies that $I = J$ or $J = R$ and $I \neq R$.

Let R be a ring and let I be a right ideal of R. We say that I is a ***maximal right ideal*** if for any right ideal J of R, if $I \subset J \subset R$, then we must have $J = I$ or $J = R$. That is, there are no ideals strictly in between I and R. Similarly, we can define maximal left ideals.

For example, let R be a ring of integers and choose $I = (6) = \{\dots,-18,-12,-6,0,6,12,18,\dots\}$. If we choose $J = (3) = \{\dots,-9,-6,-3,0,3,6,9,\dots\}$, then I is not maximal ideal as there exist an ideal J which lies between I and R. But if we choose $I' = (5) = \{\dots,-15,-10,-5,0,5,10,15,\dots\}$. Then I' is a maximal ideal because the only ideal containing I' is R itself. Thus, there are no ideals between I and R.

Definition 2.2.10

A right ideal I of a ring R is called ***minimal*** if $I \neq 0$ and for any right ideal J of R, if $0 \subset J \subset I$, then we must have $J = 0$ or $J = I$. Similarly, we can define minimal left ideals.

For example, In a commutative artinian ring, every maximal ideal is a minimal prime ideal. In an integral domain, the only minimal prime ideal is the zero ideal.

Definition 2.2.11

Let R be a ring and I be an ideal of R. Then the ring $({}^{R}/_{I},+,\cdot)$ is called the ***quotient ring*** of R defined by ${}^{R}/_{I} = \{\bar{x} = x + I : x \in R\}$, if for any $x + I, y + I$ in ${}^{R}/_{I}$, the following conditions are satisfied:

i) $(x + I) + (y + I) = (x + y) + I$ and

ii) $(x + I)(y + I) = (xy) + I$

The quotient ring ${}^{R}/_{I}$ is also denoted by $\bar{R}$.

For example, the quotient ring $\mathbb{Z}/4\mathbb{Z}$ consists of the elements $\{0 + 4\mathbb{Z},\ 1 + 4\mathbb{Z},\ 2 + 4\mathbb{Z},\ 3 + 4\mathbb{Z}\}$ with obvious operations.

$+$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$

$\times$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$

$(2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}\,, (2 + 4\mathbb{Z})(3 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z}$.

Theorem 2.2.12

$({}^{R}/_{I},+,\cdot)$ is a ring where R is a ring and I is an ideal of R.

Proof: Let ${}^{R}/_{I}$ be a quotient ring and denote the set ${}^{R}/_{I} = \{x + I : x \in R\}$. Under the $+$ and $\cdot$ binary operations $({}^{R}/_{I},+,\cdot)$ satisfies the properties of a ring. Let us verify some of these properties.

By definition, a quotient ring must satisfy the following conditions:

$$(x+I)+(y+I)=(x+y)+I \text{ and } (x+I)(y+I)=(xy)+I$$

Let $(x+I),(y+I),(z+I) \in {}^{R}/_{I}$. Then, $\big((x+I)+(y+I)\big)+(z+I)=\big((x+y)+I\big)+(z+I)$

$= ((x+y)+z)+I = \big(x+(y+z)\big)+I$ [Since associative ring holds in the ring]

$= (x+I)+\big((y+z)+I\big) = (x+I)+((y+I)+(z+I))$

This shows that $'+'$ is associative in ${}^{R}/_{I}$. Similarly $'+'$ is commutative in ${}^{R}/_{I}$. We have,

a) Additive Identity: Here, $I = 0 + I \in {}^{R}/_{I}, \forall 0 \in R$ where 0 is an additive identity.

b) Additive Inverse: For any $x + I \in {}^{R}/_{I}$, $(-x)+I$ is the additive inverse in ${}^{R}/_{I}$.

As in the case of the associativity for $+$, we can show that $\cdot$ is associative. Next, let us verify that one of the distributive law.

Now $(x+I)\big((y+I)\big)+(z+I)) = (x+I)\cdot((y+z)+I)$

$= \big(x(y+z)\big)+I = (x\cdot y + x\cdot z)+I$ [because distributivity holds in R]

$= (x\cdot y+I)+(x\cdot z+I) = ((x+I)\cdot(y+I))+((x+I)\cdot(z+I))$

In a similar manner, we can verify the right distributive law in R. Hence $({}^{R}/_{I},+,\cdot)$ is a ring.

□

Definition 2.2.13

An ideal I of a ring R is called a ***prime ideal*** if for any $ab \in I$ implies that $a \in I$ or $b \in I$.

For example, In the ring $\mathbb{Z}$, the ideal $I = (10) = \{\dots,-30,-20,-10,0,10,20,30,\dots\}$ is not a prime ideal since $30 = 5 \times 6$ but $5 \notin I$ or $6 \notin I$. In the ring $\mathbb{Z}$, the ideal $I = (5) = \{\dots,-15,-10,-5,0,5,10,15,\dots\}$ is a prime ideal since $10 = 5 \times 2 \in I$ implies that $2 \notin I$ but $5 \in I$.

Proposition 2.2.14 [2]

For a proper ideal P in a ring R, the following conditions are equivalent:

i) P is a prime ideal.

ii) If I and J are any ideals of R properly containing P, then $IJ \not\subset P$.

iii) R/P is a prime ring.

iv) If I and J are any right ideals of R such that $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.

v) If I and J are any left ideals of R such that $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.

vi) If $x, y \in R$ with $xRy \subseteq P$, then either $x \in P$ or $y \in P$.

vii) For any $x \in R$ and any ideal of R such that $xI \subset P$, then either $xR \subset P$ or $I \subset P$.

By induction, we know that if P is a prime ideal in a ring and $J_1, .., J_n$ are right ideals of R such that $J_1, .., J_n \subset P$, then some $J_i \subset P$. Recall that, a maximal ideal in a ring is meant a maximal proper ideal, i.e., an ideal which is maximal element in the collection of proper ideals.

Proposition 2.2.15 [2]

Every maximal ideal M of a ring R is a prime ideal.

2.3 Homomorphism and Endomorphism

We provide some essential definitions, examples and properties related to ring homomorphisms.

Definition 2.3.1

A mapping f from a ring R into a ring S is called a ***ring homomorphism*** if $\forall a, b \in R$

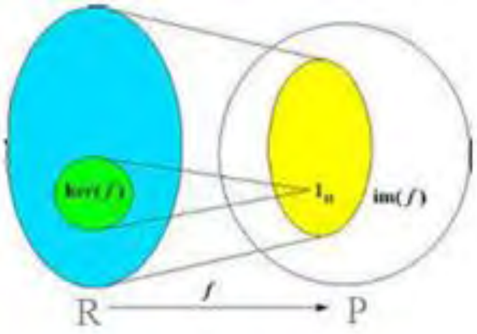
i) $f(a + b) = f(a) + f(b)$

ii) $f(ab) = f(a)f(b)$

The homomorphism f is said to be an ***isomorphism*** if it is a one-one and onto. If there exists an isomorphism from a ring R to a ring P then we say that R and P are isomorphic and we write $R \cong P$. For example, let S be a subring of a ring R (a subring may not have an identity), then $\iota: S \to R$, $\iota(x) = x$, $\forall x \in S$, is a ring homomorphism. Let $\mathbb{Z}$ be the ring of all integers and let $2\mathbb{Z}$ is a subring of $\mathbb{Z}$. Then the map $\iota: 2\mathbb{Z} \to \mathbb{Z}$ defined by $\iota(x) = x, \forall x \in 2\mathbb{Z}$ is a ring homomorphism. Let $\iota: \mathbb{Z} \to \mathbb{Q}$, $\iota(x) = x, \forall x \in \mathbb{Z}$. Then ι is a ring homomorphism.

Definition 2.3.2

Let $f: R \longrightarrow P$ be a ring homomorphism. The ***kernel*** of f is $Ker\, f = \{r \in R : f(r) = 0\} \subset R$, where 0 is the additive identity of P.

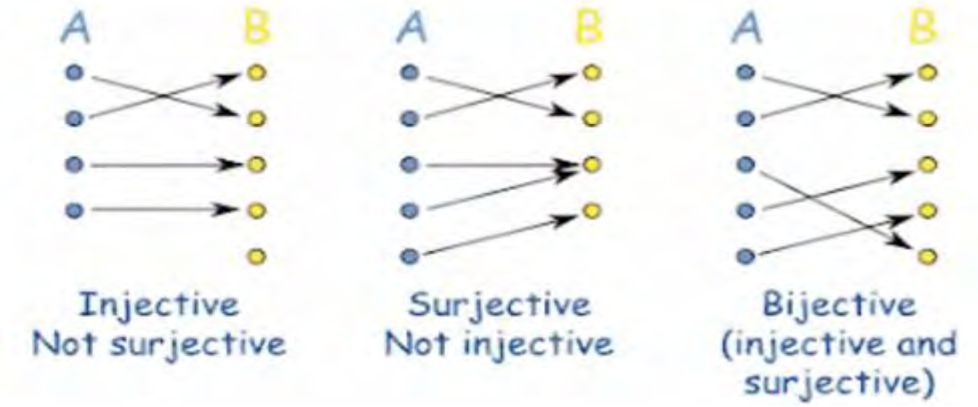


Let $f: R \longrightarrow P$ be a ring homomorphism. Then the ***image*** of f is $Im\, f = \{p \in P : f(r) = p$, for some $r \in R\} \subset P$.

Definition 2.3.3

For a pair of sets A and B, a map $f: A \longrightarrow B$ is called ***injective*** if and only if it has a left inverse, which means that there is a map $g: B \longrightarrow A$ such that $g \circ f = 1_A$, the identity map of A.

Dually, for a pair of sets A and B, a map $f: A \longrightarrow B$ is called ***surjective*** if and only if it has a right inverse. This means that there exists a map $g: B \longrightarrow A$ such that $f \circ g = 1_B$, the identity map of B.



If I is a proper right ideal of R and $f: I \rightarrow R_R$ is an R-homomorphism, then f need not be a left multiplication. If a ring R such that every $f: I \rightarrow R_R$ with I any right ideal of R is a left multiplication, then R is called a ***right self-injective ring***. For any $x \in I$, we have $f(x) = \bar{f}(x) = \bar{f}(1x) = \bar{f}(1)x = \bar{a}x$, where $\bar{a} = \bar{f}(1)$.

Theorem 2.3.4 (First Isomorphism Theorem)

Statement: Let R and P be rings and let $\phi: R \longrightarrow P$ be a homomorphism. Then,

(i) The kernel of ϕ is an ideal of R,

(ii) The image of ϕ is a subring of P,

(iii) The map $\varphi: R/Ker\,\phi \rightarrow Im\,\phi \subset S, r + Ker\,\phi \mapsto \phi(r)$ is a well-defined isomorphism.

Proof: The image of ϕ is a subring. Let us prove that $Ker\,\phi$ is an ideal and $\phi(0) = 0$, so $0 \in Ker\,\phi$ and hence the kernel is nonempty. Let $a, b \in Ker\,\phi$ and let $r \in R$. Then since ϕ is a homomorphism, we have

$$\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0,$$
$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0,$$
$$\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0.$$

Thus $a + b, ra$ and ar are in $Ker\ \phi$ and so $Ker\ \phi$ is an ideal. Consider the map φ. We first show that it is well-defined. Let $r, s \in R$ be such that $r - s \in Ker\ \phi$, i.e., such that $r + Ker\ \phi = s + Ker\ \phi$. Then, $\phi(r) = \phi\big(s + (r - s)\big) = \phi(s) + \phi(r - s) = \phi(s) + 0 = \phi(s)$. So φ is well defined.

Let $r + I, s + I \in R/I$. Then since ϕ is a homomorphism we have:

$\varphi(r + I + s + I) = \varphi(r + s + I) = \phi(r + s) = \phi(r) + \phi(s) = \varphi(r + I) + \varphi(s + I)$

$\varphi\big((r + I)(s + I)\big) = \varphi(rs + I) = \phi(rs) = \phi(r)\phi(s) = \varphi(r + I)\varphi(s + I)$

$\varphi(1 + I) = \phi(1) = 1.$

Therefore φ is a homomorphism. Let us prove that φ is bijective. If $r + Ker\ \phi \in Ker\ \varphi$, then $\varphi(r + I) = \phi(r) = 0$ and so $r \in Ker\ \phi$ or equivalently $r + Ker\ \phi = Ker\ \phi$. Thus $Ker\ \varphi$ is trivial and φ is injective. Let $s \in Im\ \phi$. Then there exists an $r \in R$ such that $\phi(r) = s$ or equivalently that $\varphi(r + Ker\ \phi) = s$. Thus $s \in Im\ \varphi$ and so φ is surjective. Hence φ is an isomorphism as desired.

□

Theorem 2.3.5 (Second Isomorphism Theorem)

Statement: Let R be a ring, let $P \subset R$ be a subring, and let I be an ideal of R. Then,

i) $P + I := \{s + a : s \in P, a \in I\}$ is a subring of R,

ii) $P \cap I$ is an ideal of S, and

iii) $(P + I)/I$ is isomorphic to $P/(P \cap I)$.

<u>Proof of (i)</u>: P is a subring and I is an ideal so $1 + 0 \in P + I$. Let $s_1 + a_1$ and $s_2 + a_2$ be elements of $P + I$. Then, $(s_1 + a_1) - (s_2 + a_2) = s_1 - s_2) + (a_1 - a_2)$ and $(s_1 + a_1)(s_2 + a_2) = s_1 s_2 + s_1 a_2 + a_1 s_2 + a_1 a_2$. Hence $P + I$ is a subring of R.

<u>Proof of (ii)</u>: The intersection $P \cap I$ is non-empty since 0 is contained in I and P. Let $a_1, a_2 \in P \cap I$ and let $s \in P$. Then $a_1 + a_2 \in P \cap I$ since P and I are both closed under addition. Furthermore, sa_1 and $a_1 s$ are in $P \cap I$ since I is closed under multiplication from $R \supset P$ and P is closed under multiplication. Therefore $P \cap I$ is an ideal of P.

<u>Proof of (iii)</u>: Consider the map $\phi: P \rightarrow (P + I)/I$ which sends an element s to $s + I$. This is a ring homomorphism by definition of addition and multiplication in quotient rings. We claim that it is surjective with kernel $P \cap I$, which would complete the proof by the first isomorphism theorem 2.3.4. Consider, elements $s \in P$ and $a \in I$. Then $s + a + I = s + I$ since $a \in I$, so $s + a + I \in im\ \phi$ and hence ϕ is surjective. Let $s \in P$ be an element of $Ker\ \phi$. Then $s + I = I$ which holds if and only if $s \in I$ or equivalently if $s \in P \cap I$. Thus $Ker\ \phi = P \cap I$ and we have our desired result.

□

Theorem 2.3.6 (Third Isomorphism Theorem)

Let R be a ring and let $J \subset I$ be ideals of R. Then I/J is an ideal of R/J and $\frac{R/J}{I/J} \cong R/I$.

Proof: Since I and J are ideals, they are nonempty and so $I/J = \{a + J : a \in I\}$ is also nonempty. Let $a_1, a_2 \in I$ and let $r \in R$. By definition of addition and multiplication of cosets, we have

$$(a_1 + J) + (a_2 + J) = (a_1 + a_2) + J,$$
$$(r + J)(a_1 + J) = ra_1 + J$$
$$\text{and } (a_1 + J)(r + J) = a_1r + J.$$

Since I is an ideal, $a_1 + a_2, ra_1$, and a_1r are contained in I, so I/J is an ideal of R/J.

Consider the map $\phi: R/J \to R/I$ that sends $r + J$ to $r + I$. We claim that, this is a well-defined surjective homomorphism with kernel equal to I/J. Then $\frac{R/J}{I/J}$ is isomorphic to R/I by the first isomorphism theorem 2.3.4.

□

Theorem 2.3.7 (Chinese Remainder Theorem)

Statement: Let R be a ring and let A, B be two ideals of R such that $A + B = R$. Then,

$$R/(A \cap B) \cong (R/A) \times (R/B).$$

Proof: Consider the map $f: R \to (R/A) \times (R/B)$, $f(r) = (r + A, r + B)$. For $r, s \in R$ we have

$$f(1) = (1 + A, 1 + B) = 1_{(R/A)\times(R/B)},$$

$f(r + s) = (r + s + A, r + s + B)$

$\quad = (r + A, r + B) + (s + A, s + B) = f(r) + f(s)$

And $f(rs) = (rs + A, rs + B)$

$\quad = ((r + A)(s + A), (r + B)(s + B)) = (r + A, r + B)(s + A, s + B)$

$\quad = f(r)f(s)$

Thus, f is a ring homomorphism.

We next show that, f is surjective. Since $A + B = R$. We have $1 = a + b$ for some $a \in A$ and $b \in B$. Now choose $r_1, r_2 \in R$ and set $r = r_1b + r_2a$. Then,

$r_1 - r = r_1 - (r_1b + r_2a) = r_1(1 - b) - r_2a = r_1a + r_2a \in A$

$\Rightarrow r_1 + A = r + A$

And $r_2 - r = r_2 - (r_1b + r_2a) = r_2(1 - a) - r_1b = r_2b + r_1b \in B$

$\Rightarrow r_2 + B = r + B$

Thus, $f(r) = (r + A, r + B) = (r_1 + A, r_2 + B)$. Since $r_1, r_2 \in R$ were arbitary, this implies that f is surjective.

Finally, $f(r) = (0 + A, 0 + B)$

$\Leftrightarrow (r + A = 0 + A \text{ and } r + B = 0 + B)$

$\Leftrightarrow (r \in A \; and \; r \in B)$

$\Leftrightarrow (r \in A \cap B)$

So, $Ker \; f = A \cap B$. The result then follows from the first Isomorphism theorem 2.3.4.

□

2.4 Modules and Different Kinds of Module

In mathematics, a module is one of the fundamental algebraic structures used in abstract algebra.

Definition 2.4.1

Let R be a ring with identity. Then a subset M is called a ***right R-module*** if for any $m, m' \in M$ and for any $r, r', s \in R$, the following conditions are satisfied-

i. $(M, +)$ is an abelian group.

ii. There exists a map $f: M \times R \to M$ defined by $f(m, r) = mr$ such that we have

   a) $(m + m')r = mr + m'r$

   b) $m(r + r' \,) = mr + mr'$

   c) $(mr)s = m(rs)$

   d) $m \cdot 1 = 1 \cdot m = m$

If M is a right R-module, we write M_R.The class of all right R-modules is not a set. We denote this class by mod-R. So R-mod is used for left R-modules. We call mod-R (resp. R-mod), the category of right (resp. left) R-modules.

For example, let R be a ring and let M be a left ideal of R, then M is an R-module. Every ring R is an R-module over itself. Again, every additive group is a module over the ring of integers.

Definition 2.4.2

Let M be a right R-module and let $A \subseteq M$, a subset of M. Then A is called a **submodule** of M, if $(A, +)$ is a subgroup of $(M, +)$ and A is a right R-module. That is, A is submodule of M equivalent that $\forall a, a' \in A, a + a' \in A$ and $\forall a \in A, \forall r \in R, ar \in A$.

Definition 2.4.3

Let M be a right R-module and let A is a submodule of M_R. Then A is called a ***direct summand*** of M_R if we can find an another submodule B of M_R such that $M = A + B$ and $A \cap B = \{0\}$.

In this case, we write $M = A \oplus B$ and we call, M is a ***direct sum*** of A and B or the sum $A + B$ is direct. Generally, let $i \in I$ and A_i is a submodule of M_R. Then the sum $\sum_{i\in I} A_i$ is direct if for any $j \in I$ such that $A_i \cap \sum_{i\neq j} A_j = \{0\}$. Let $M \in R$-mod and A, B are submodules of M_R. If $A \cap B = \{0\}$ then $A + B = A \oplus B$. Moreover, if $x \in A \oplus B$, then $x = a + b$ where $a \in A$ and $b \in B$.

Definition 2.4.4

A subset $X \subseteq M_R$, is called a ***free set or linearly independent*** set if for any $x_1, x_2, \dots, x_k$ in X and for any $c_1, c_2, \dots, c_k$ in R. We have, $\sum_{i=1}^{k} c_i\, x_i = 0 \Rightarrow c_i = 0\ \forall\ i$. Moreover, if $X = \{m_1, m_2, \dots, m_k\}$ then $M = |X) = \sum_{i=1}^{k} m_i R = m_1R + m_2R + \cdots + m_kR$. The subset $X \subseteq M_R$ is called a ***basis*** of M_R if $M = |X)$ and if X is a free set. If M_R has a basis then this right R-module is called the ***free module***. Then, Submodule of M generated by $|X)$ is defined by

$$|X) = \{\textstyle\sum_{i=1}^{n} x_i\, r_i | x_i \in X, r_i \in R, i = 1,2, \dots, n, n \in \mathbb{N}\}$$

This submodule is the ***smallest submodule*** of M_R containing X. This submodule $|X)$ is called the submodule generated by X.

Generally, For each $i \in I$, let A_i is a right R-module of M_R. Then $\bigcup_{i\in I} A_i$ may not be a right R-submodule of M_R. The sum of all submodules $A_i, i \in I$ is a submodule of M_R defined by, $|\bigcup_{i\in I} A_i) = \left\{\sum_{k=1}^{n} a_{i_k} \middle| a_{i_k} \in A_{i_k}; k = 1,2, \dots, n; n \in \mathbb{N}\right\}$. Let M be a right R-module and $X \subseteq M$, a subset. Then X is generated by M if $M = |X)$. If X is a finite subset, then M is ***finitely generated***.

Definition 2.4.5

A right R-module M is called a ***finitely generated right R-module*** if M is generated by a finite number of elements, i.e., there exist $m_1, m_2, \dots, m_k \in M$ such that

$$M = |\{m_1, m_2, \dots, m_k\}) = \sum_{i=1}^{k} m_i R.$$

A right R-module M is called a ***finitely generated right R-module*** if for any family $\{A_i, i \in I\}$ of submodules of M such that $\bigcap_{i\in I} A_i = 0$, there is a finite subset $I_0 \subset I$ such that $\bigcap_{i\in I_0} A_i = 0$.

Theorem 2.4.6

A right R-module M is finitely generated if and only if for any family $\{A_i, i \in I\}$ of submodules of M such that $\sum_{i\in I} A_i = M$, there is a finite subset $I_0 \subset I$ such that

$$\sum_{i\in I_0} A_i = M.$$

Proof: Suppose that M is finitely generated. Then by definition, $M = \sum_{i=1}^{k} m_i R = |\{m_1, m_2, \dots, m_k\})$. Now $m_1 \in \sum_{i\in I} A_i$, $m_1 = a_{i_1} + \cdots + a_{i_{n_1}} = \sum_{i\in I_1} a_i$, $I_1 = \{i_1, \dots, i_{n_1}\}$. Similarly $m_2 \in \sum_{i\in I} A_i$, $m_2 = \sum_{i\in I_2} a_i$, with I_2 finite and $a_j \in A_j$ for $j = i_1, \dots, i_{n_1}$. Continuing this process, $m_k = \sum_{i\in I_k} a_i$, I_k is finite. We can see that $m_1, m_2, \dots, m_k \in \sum_{i\in I_0} A_i$, where $I_0 = \bigcup_{j=1}^{k} I_j$. Then $M = |\{m_1, m_2, \dots, m_k\}) \subset \sum_{i\in I_0} A_i \subset \sum_{i\in I} A_i = M$. Hence $M = \sum_{i\in I_0} A_i$.

Conversely, note that $M = \sum_{m\in M} mR$. By assumption, we can find $m_1, m_2, \dots, m_k$ such that $M = \sum_{i=1}^{k} m_i R$, proving that M is finitely generated.

□

Definition 2.4.7

Let M be a right R-module and let $m \in M$. Then the set $mR = \{mr | r \in R\}$ is a submodule of M, called the ***cyclic submodule*** of M. We can see that

$$M = \sum_{m\in M} mR.$$

A right R-module M is called a ***cyclic right R-module*** if M is generated by a single element, i.e., there exists $m \in M$ such that $M = mR$. A cyclic right ideal is called a principal right ideal. The following theorem gives us a characterization of finitely generated right R-modules.

Theorem 2.4.8

The homomorphic image of a (cyclic) finitely generated right R-module is again (cyclic) finitely generated.

Proof: Let $f: M \to N$ be an epimorphism, i.e., $Im(f) = N$. Suppose that M is cyclic. Then $M = mR$ (say). Then for any $n \in N$, we can find $x \in M$ such that $n = f(x)$. Hence $n = f(x) = f(mr) = f(m)r$ where $x = mr$. It shows that $N = |\{f(m)\}) = f(m)R$.

Similarly, if M is finitely generated, then $M = m_1 R + \cdots + m_k R$ (say). Then $Im(f) = N = f(m_1)R + \cdots + f(m_k)R$, proving that N is finitely generated. As an application, let M be a finitely generated right R-module. Then for any submodule X of M, we have M/X is finitely generated. □

Theorem 2.4.9

A right R-module M is cyclic if and only if M is isomorphic to R/I for some right ideal I of R.

Proof: Suppose that M is cyclic, i.e., $M = mR = \{mr | r \in R\}$ for some $m \in M$. Consider the map $f: R \to mR, r \mapsto mr$. This map is well-defined and is an R-homomorphism.

Moreover, f is an epimorphism. By the First Isomorphism Theorem 2.3.4, $mR \cong R/ker(f)$, where $ker(f)$ is a right ideal of R. Since $R = 1R$, we have R/I is cyclic (generated by $\bar{1} = 1 + I$).

□

Definition 2.4.10

Let X be a submodule of a right R-module M. Then X is called a ***minimal submodule*** of M if $X \neq 0$ and for any submodule $Y \subset_{>} M$, if $0 \neq Y \subset X$, then $Y = X$.

Definition 2.4.11

Let X be a submodule of a right R-module M. Then X is called a ***maximal submodule*** of M or maximum in M if $X \neq M$ and for any submodule $Y \subset_{>} M$, if $X \subset_{>} Y$, then $Y = X$.

Properties 2.4.12

For a right R-module M, the following conditions are true:

i) Let X be a maximal submodule of M and let $m \in M - X$. If $X \subsetneq_{>} X + mR \subset_{>} M$, then $X + mR = M$.

ii) Let $X \subset_{>} M$. Suppose that for any $m \in M - X$, $X + mR = M$. If $X \subsetneq_{>} Y \subset_{>} M$ and $Y \neq X$ then there exists $X \subsetneq_{>} X + mR \subset_{>} Y \subset_{>} M$. Hence $Y = M$.

Thus X is maximal.

Theorem 2.4.13 (Zorn's Lemma)

Let $\mathcal{F}$ be a partially ordered set. If every totally ordered subset of $\mathcal{F}$ has an upper bound in $\mathcal{F}$, then $\mathcal{F}$ contains a maximal element.

To understand Zorn's lemma, we need to know four terms: partially ordered set, totally ordered subset, upper bound, and maximal element. The ways we apply Zorn's lemma in this note are typical applications of this result in algebra.

Theorem 2.4.14

If M is a finitely generated right R-module, then every proper submodule of M is contained in a maximal submodule of M. Especially, if M is finitely generated, then M contains at least one maximal submodule.

Proof: Suppose that $M = \sum_{i=1}^{k} m_i R$ and U is a proper submodule of M. If U is maximal in M, then we are done. Suppose that U is not maximal in M. Then there is $U \subset_{>}\neq X \subset_{>}\neq M$. Consider the family $\mathcal{F} = \{X \subset_{>} M | U \subset_{>}\neq X \subset_{>}\neq M\}$. Then $\mathcal{F} \neq \phi$. Consider any chain $X_1 \subset_{>} X_2 \subset_{>} \dots$ in $\mathcal{F}$ and put $C = \bigcup_{i=1}^{\infty} X_i$. Then $C \subset_{>} M$. We want to show that $C \neq M$.

Suppose on the contrary that $C = M$. Then $\{m_1, \dots, m_k\} \subset C$. Take any $m_1 \in C \bigcup_{i=1}^{\infty} X_i$. Then there is i_1 such that $m_1 \in X_{i_1}$. Again, take any $m_2 \in C \bigcup_{i=1}^{\infty} X_i$. Then there is i_2 such that $m_2 \in X_{i_2}$ with $i_2 > i_1$. Continuing this process, we get $m_1, \dots, m_k \in X_{i_k}$. Hence $M = X_{i_k}$, a contradiction. So, $C \neq M$ or $C \in \mathcal{F}$. By Zorn's Lemma 2.4.13, $\mathcal{F}$ contains a maximal element, D (say).

We now show that D is a maximal submodule of M. Take any $m \in M \backslash D$. Then $D \subset_{>}\neq mR + D \subset_{>} M$. If $mR + D \neq M$, then $mR + D \in \mathcal{F}$. This contradicts the maximality of D in F. Hence $mR + D = M$, proving that D is maximal in M.

□

Definition 2.4.15

Let M be a right R-module and X be a submodule of M. Then the relation xRy is an equivalence relation if and only if $x - y \in X$ and we consider M/R, the quotient set. We denote $M/X \equiv M/R$, where M/X is defined by

$$M/X = \{\bar{m} = m + X | m \in M\}$$

On M/X, we define $\bar{m} + \overline{m'} = \overline{m + m'}$ and $\bar{m} \cdot \bar{r} = \overline{mr}$ $\forall m, m' \in M$, $\forall\, r \in R$. Then M/X becomes a right R-module, called a ***factor module*** of M by X.

Theorem 2.4.16

Let M be a right R-module and let $X \subset_{>} M$. Then X is maximal in M if and only if for any $m \in M \backslash X$, $X + mR = M$.

Proof: Suppose that X is maximal in M. Take any $m \in M \backslash X$. Then $X \subset_{>}\neq X + mR \subset_{>} M$. By definition, $X + mR = M$. Conversely, assume that $X \subset_{>}\neq Y \subset_{>} M$. Then we can find $y \in Y \backslash X$. So, $y \in M \backslash X$. By assumption, $X + yR = M$. Since $X \subset_{>} Y$, and $y \in Y$, we have $X + yR \subset_{>} Y$, proving that $M = X + yR \subset_{>} Y \subset_{>} M$. This shows that $Y = M$ or X is maximal in M. □

Definition 2.4.18

Let R be a ring and M, N be right R-modules. Then a map $f: M \to N$ is called a ***right R-module homomorphism*** if for any m, m' in M and $r \in R$ we have,

i) $f(m + m') = f(m) + f(m')$ and

ii) $f(mr) = f(m)r$.

Definition 2.4.19

i) Let $M \in M_R$ and let X be its submodule. Then the map $\iota: X \hookrightarrow M$ defined by $x \mapsto x$ is an R-homomorphism called an ***embedding***.

ii) Let $M \in M_R$ and let $X \subset_{>} M$, a submodule. Then, the map $\nu: M \to M/A$ defined by $\nu(m) = m + x$ is an R-homomorphism, called the ***natural or canonical homomorphism***.

iii) The map $0: M_R \to N_R$ defined by $0(M) = 0_N$ is called the ***zero map***.

iv) The map $1: M_R \to M_R$ defined by $1(M) = M$ is called the ***identity map***.

Definition 2.4.20

An R-homomorphism $f: M_R \to N_R$ is called a ***monomorphism*** if for any $X \in M_R$ and for any homomorphism $h, g: X \to M$, $f \circ h = f \circ g$ such that $h = g$.

An R-homomorphism $f: M_R \to N_R$ is called a ***epimorphism*** if for any $X \in M_R$ and for any homomorphism $h, g: N \to X$, $h \circ f = g \circ f$ such that $h = g$.

Remarks: (i) $f: M_R \to N_R$ is a monomorphism iff f is one-one.

(ii) $f: M_R \to N_R$ is an epimorphism iff f is onto.

The ***endomorphism ring*** $End_R(M)$ of a right R-module M is the set of all R-module homomorphism $f : M \to M$ with multiplication is defined by composition of functions: $f \cdot g = f \circ g$ and point wise addition: $(f + g)(x) = f(x) + g(x)$. A homomorphism (resp. isomorphism) from a ring to itself is called an ***endomorphism*** (resp. *automorphism*). For example, the map $f: \mathbb{C} \to \mathbb{C}$ given by $f(\mathbb{Z}) = \overline{\mathbb{Z}}$ is an automorphism of $\mathbb{C}$.

Definition 2.4.21

Let M be a right R-module and $M_1, M_2, M_3, \ldots$ are submodules of M_R. Then M satisfies ***ascending chain condition (A.C.C)*** on submodules if the chain $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ stabilizes, i.e., there exists integer i such that $M_i = M_{i+1} = M_{i+2} = \cdots$.

Definition 2.4.22

Let M be a right R-module and $M_1, M_2, M_3, \dots$ are submodules of M_R. Then M satisfies ***descending chain condition (D.C.C)*** on submodules if the chain $M_1 \supseteq M_2 \supseteq M_3 \supseteq \cdots$ stabilizes, i.e., there exists integer i such that $M_i = M_{i+1} = M_{i+2} = \cdots$.

Definition 2.4.23

A right R-module M_R is called ***Noetherian*** if M is finitely generated and M satisfies the A.C.C. on submodules.

Definition 2.4.24

A right R-module M_R is called ***Artinian*** of M if M is finitely generated and M satisfies the D.C.C. on submodules.

Definition 2.4.25

Let M be a right R-module and $a \in M$. We denote, the ***right annihilator*** of a as the set

$$\wp_R(a) = \{r \in R: ar = 0\}.$$

Then $\wp_R(a)$ is a right ideal of R.

Definition 2.4.26

Let M be a right R-module and $a \in M$. We denote, the ***left annihilator*** of a as the set

$$\ell_R(a) = \{r \in R: ra = 0\}.$$

Then $\ell_R(a)$ is a left ideal of R.

Note.

01. Let M be a right R-module, $S = End(M_R)$, $I \subset S$, a subset and $X \subset M$, a subset. Then, $\ell_S(X) = \{f \in S: f(x) = 0, \forall x \in S\}$ = left annihilator of X in R, is a left ideal of S.
02. A right ideal I of R is called a right annihilator if we can find a subset $X \subset R$ such that $XI = 0$.

CHAPTER III
SIMPLE AND SEMISIMPLE RINGS AND MODULES

Semisimple rings and modules are characterized by many researchers over commutative rings such as multiplication modules. But for the case of noncommutative rings these structures are not similar. A simple ring is a ring which has no two-sided ideals besides the zero ideal and itself. A non-zero module is simple if it is nonzero and M has no proper non-zero submodules. In particular, a right R-module M is simple if $M \neq 0$ and for any submodule X of M either $X = 0$ or $X = M$. This means that 0 and M are the only submodules of M. A module is semisimple if it is a sum of simple submodules.

3.1 Simple Rings and Modules

Definition 3.1.1

A ring R is said to be a ***simple ring*** if $R \neq 0$ and if R has no proper non-zero ideals. In this case, if a ring R is simple then R has no two-sided ideals other than 0 and R.

A simple ring is a ring which has no two-sided ideals besides the zero ideal and itself. Furthermore, a ring R is a simple commutative ring if and only if R is a field. This is because if R is a commutative ring, then we can pick a non-zero element $x \in R$ for which the set $\{xr : r \in R\}$ is an ideal. Then since R is simple, this ideal is the entire ring and so it contains the identity element 1. Therefore, there is some non-zero element $y \in R$ such that $xy = 1$ implying that R is a field.

For example, each of the rings $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ is a simple ring. A matrix ring $M_n(F)$ over a field F is simple but not a division ring for $n > 1$. Also, every division ring is a simple ring.

Example 3.1.2

The ring $M_2(\mathbb{R})$ is a simple ring but is not a division ring.

Proof: Let I be a non-zero ideal of $M_2(\mathbb{R})$. Then there exists a non-zero element $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in I$. Now at least one of a, b, c, d is non-zero. Because I is an ideal and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in M_2(\mathbb{R})$, we have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 \\ d & 0 \end{bmatrix} \in I,$$

$$\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}=\begin{bmatrix}c & d\\0 & 0\end{bmatrix}\in I \text{ and}$$

$$\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}=\begin{bmatrix}d & 0\\0 & 0\end{bmatrix}\in I.$$

Therefore we find that I contains a matrix $\begin{bmatrix}a & b\\c & d\end{bmatrix}$ such that $a \neq 0$.Now $a^{-1} \in \mathbb{R}$ and $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}a^{-1} & 0\\0 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ca^{-1} & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\in I$. Thus $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}=\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}\in I$.

Finally, $\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\0 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\in I$. Hence, $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}=\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}+\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\in I$.

This implies that $I = M_2(\mathbb{R})$. Also note that $M_2(\mathbb{R})$ is not a division ring.

□

Example 3.1.2 shows that there are simple rings which are not division rings.

Definition 3.1.3

A non-zero right R-module M_R is said to be a ***simple module*** if $M \neq 0$ and M has no proper non-zero submodules. In particular, a right R-module M is called a ***simple right R-module*** if $M \neq 0$ and for any submodule $X \subset_{>} M$, either $X = 0$ or $X = M$. This means that 0 and M are the only submodules of M. For example, an abelian group is simple as a $\mathbb{Z}$-module if and only if it is simple as a group, if and only if it is cyclic of prime order. Also, a vector space is simple if and only if it has dimension 1.

Definition 3.1.4

Let M be a right R-module and let $X \subset_{>} M$. Then the relation xRy is an equivalence relation if and only if $x - y \in X$ and we consider M/R, the quotient set. Denote $M/X \equiv M/R$, where

$$M/X = \{\overline{m} = m + X | m \in M\}$$

On M/X, we define $\overline{m} + \overline{m'} = \overline{m + m'}$ and $\overline{m} \cdot \overline{r} = \overline{mr}\ \forall m, m' \in M, \forall\ r \in R$. Then M/X becomes a right R-module, called a ***factor module*** of M by X.

Lemma 3.1.5

For a submodule $Y \subset_{>} X$, X/Y is simple if and only if Y is a maximal submodule of X.

Theorem 3.1.6

Let M be a right R-module. Then, a submodule $X \subset_{>} M$ is maximal if and only if M/X is simple.

3.2 Semisimple Rings and Modules

Definition 3.2.1

Let M be a right R-module. Then M is called a ***semisimple module*** if every submodule is a direct summand of M. That is, M is semisimple if and only if for any submodule $X \subset M$, there exists a submodule $Y \subset M$ such that $M = X \oplus Y$.

Note. By definition, the module 0 is semisimple (being the direct sum of an empty family of simple submodules). Clearly the direct sum of a family of semisimple modules is semisimple.

Corollary 3.2.3 [2]

Let M be a right R-module. Then, any submodule of a semisimple module is semisimple.

Now we will prove the **Modular Law**:

Lemma 3.2.4

If X, Y, Z are submodules of a right R-module M and if $X \subset Y$ then

$$Y \cap (X + Z) = X + (Y \cap Z)$$

Proof: Write $X + (Y \cap Z) = Y \cap X + Y \cap Z \subset Y \cap (X + Z)$. Take $y = x + z \in Y \cap (A + Z)$ with $y \in Y, x \in X, z \in Z$. Then, $x \in X \subset Y$ implies that $z \in Y \cap Z$. Thus, $Y \cap (X + Z) \subset X + (Y \cap Z)$.

This completes the proof of the modular law.

□

Theorem 3.2.5

Let M be a semisimple module. Then every submodule contains a simple submodule.

Proof: Suppose that M is a semisimple and A its non-zero submodule. Then we can find a non-zero element $a \in A$ such that $0 \neq aR \subset_{>} A$ where the submodule aR is finitely generated.

Therefore, aR contains a maximal submodule B, say. By assumption, $M = B \oplus C$ for some submodule C of M. Using Modular Law 3.2.4, we can write $aR = aR \cap M = aR \cap (B \oplus C) = B \oplus (aR \cap C)$. Then $aR \cap C \cong {}^{aR}/_{B}$ where ${}^{aR}/_{B}$ is simple. This shows that A contains a simple submodule.

□

Theorem 3.2.6

Let M be a right R-module. Then M is semisimple if and only if $M = \sum_{i \in I} M_i$, where each M_i is simple for any $i \in I$.

Proof: Assume that M is semisimple. Let $X = \sum_{i\in I} M_i$, where M_i is a simple submodule of M, for all $i \in I$. Then X is a direct summand of M. This means that $M = X \oplus Y$ for some submodule Y of M. If $Y \neq 0$, let $0 \neq y \in Y$. Then yR is cyclic where $yR \subset_{>} Y \subset_{>} M$ and then yR is finitely generated. So yR contains a maximal submodule A, say. We see that both of yR and A is a direct summand of M.
By the modular law 3.2.4, A is a direct summand of yR. Hence $yR = A \oplus B$ and so $B \cong yR/A$ is simple. Then $B \subset_{>} yR \subset_{>} Y$. Then B is simple but $B \not\subset_{>} X$, a contradiction. Hence $M = X \oplus 0 = X = \sum_{i\in I} M_i$, where each M_i is simple for all $i \in I$.
Conversely, assume that $M = \sum_{i\in I} M_i$, where each M_i is simple for any $i \in I$. Let X be any submodule of M. We must show that X is a submodule of M. If $X = 0$, it is obvious that $M = 0 + M$. So, suppose that $X \neq 0$. Let M_i be a submodule of M for all $i \in I$. Then $M_i \subset_{>} X$ or $M_i \cap X = 0$ for all $i \in I$. If $M_i \cap X \neq 0$ for all $i \in I$. then $0 \neq M_i \cap X \subset_{>} M_i$ for all $i \in I$. Since M_i is simple, $M_i \cap X = M_i$ for all $i \in I$. Then $M_i \subset_{>} X$ for all $i \in I$. Let, $F = \{M_i | M_i \cap X = 0\}$ and $G = \{M_i | M_i \subset_{>} X\}$. Then we have $M = \sum_{i\in I} M_i = \sum_{M_i \in F} M_i \oplus \sum_{M_i \in G} M_i \subseteq X \oplus \sum_{M_i \in F_i} M_i \subseteq M$. Thus, $M = X \oplus \sum_{i\in I} M_i$ and so X is a direct summand of M. Therefore M is semisimple.

□

Definition 3.2.7

A ring R is said to be ***semisimple*** if the right R-module R_R is semisimple.

Theorem 3.2.8

Any right R-module M over a semisimple ring R is semisimple.

Proof: Let M be a right R-module. If m is a non-zero element of M, take the homomorphism $f: R \rightarrow M$, which takes $r \rightarrow mr$. Then mR is a submodule of M isomorphic to $R/Ker\ f$, which is a semisimple right R-module since R is semisimple. Thus mR is semisimple. Since M is a sum of semisimple submodules, M is also semisimple.

□

Theorem 3.2.9

The following statements are equivalent for a right R-module M:

i) Every submodule of M is a sum of simple submodules;

ii) M is a direct sum of simple submodules;

iii) Every submodule of M is a direct summand.

Proposition 3.2.10 [5]

The following properties of a right R-module M are equivalent:

i) M is semisimple;

ii) M is generated by simple modules;

iii) M is a sum of all simple submodules;

iv) M is a direct sum of simple submodules;

v) Every submodule of M is a direct summand.

Proof: (i) implies (ii): Let M be a semisimple right R-module with semisimple decomposition $M = \oplus\ _A T_\alpha$. If $0 \to K \xrightarrow{f} M \xrightarrow{g} N \to 0$ is an exact sequence of right R-modules, then the sequence splits and both K and N are semisimple. Since Imf is a submodule of M. The sequence splits and $N \cong M/Imf \cong \oplus\ _\beta T_\beta$. But also $M = (\oplus\ _{A/B} T_\alpha) \oplus (\oplus\ _\beta T_\beta)$, so that $K \cong Imf \cong\oplus\ _{A/B} T_\alpha$. Every submodule and every factor module of a semisimple module are semisimple. Moreover, every submodule is a direct summand. Also (ii) ⇔ (iii) ⇔ (iv) are all trivial.

Finally, (v) implies (ii). Assume that M satisfies (v). We claim that every non-zero submodule of M has a simple submodule. Indeed, let $x \neq 0$ in M. Thus R_x has a maximal submodule, say H.

By (v), we have $M = H \oplus H'$ for some $H' \subset_{>} M$. Thus by modularity, $R_x = R_x \cap M = H \oplus (R_x \cap H')$ and $R_x \cap H' \cong R_x/H$ is simple, so R_x has a simple submodule.

Let N be the sum of all simple submodules of M. Then, $M = N \oplus N'$, by (v) for some $N' \subset_{>} M$, since $N \cap N' = 0$ has no simple submodule. But as we have just seen, this means $N' = 0$. So $N = M$.

□

Lemma 3.2.11 [3]

Let $M = \sum_{i\in I} X_i$, where each X_i is simple for any $i \in I$. Then

i) For any $A \subset_{>} M$, there exists $J \subseteq I$ such that $M = A \oplus \left(\bigoplus_{i\in J} X_i\right)$

ii) There exists $K \subseteq I$ such that $M =\bigoplus_{i\in K} X_i = \sum_{i\in K} X_i$, $\left[X_i \bigcap_{i\neq j, j\in I} X_j = 0\right]$.

Proof:

i) If $A = M$, choose $J = \phi$. Suppose $A \neq M$. We can find at least one $X_{io} \nsubseteq A$ and then $X_{io} \cap A = 0$. Let $\mathcal{F} = \{J \subseteq I | A \cap\bigoplus_{i\in I} X_i = 0\}$. Then $\mathcal{F} \neq \phi$. Considering the inclusion operation, suppose $J_1 \subseteq \cdots \subseteq J_n \subseteq \cdots$ in $\mathcal{F}$. Let $J = \bigcup_{k=1}^{\infty} J_k \subseteq I$. Then $\bigoplus_{i\in J} X_i = \bigcup_{k=1}^{\infty} \bigoplus_{i\in J_k} X_i$, and so $A \cap \left(\bigcup_{k=1}^{\infty} \bigoplus_{i\in J_k} X_i\right) = \bigcup_{k=1}^{\infty} \left(A \cap\bigoplus_{i\in J_k} X_i\right) = 0$. So $J \in \mathcal{F}$. By Zorn's Lemma, $\mathcal{F}$ contains a maximal element, J(say). We want to show that $A \oplus \left(\bigoplus_{i\in J} X_i\right) = M$. Suppose that $A \oplus$

$\left(\bigoplus_{i\in J} X_i\right) \neq M$. Then there exists $X_{io} \nsubseteq A \oplus \left(\bigoplus_{i\in J} X_i\right)$. So $X_{io} \cap \left(A \oplus \left(\bigoplus_{i\in J} X_i\right)\right) = 0$ and hence $\left[A \oplus \left(\bigoplus_{i\in J} X_i\right)\right] \oplus X_{io} \subset_{>} M$.Then $A \oplus \left(\bigoplus_{i\in J\cup\{X_{io}\}} X_i\right) \subset_{>} M$. Hence $J \subseteq J \cup \{io\} \in \mathcal{F}$, a contradiction.

ii) Since $A = 0 \subset_{>} M$, $M = 0 \oplus \left(\bigoplus_{i\in K} X_i\right) = \bigoplus_{i\in K} X_i$.

□

Theorem 3.2.12 [4]

Let M be a right R-module. Then the following conditions are equivalent:

i) M is semisimple.

ii) $M = \sum_{i\in I} X_i$, where each X_i is simple.

iii) $M = \bigoplus_{j\in I} X_j$, where each X_j is simple.

Proof: i) implies ii): Let $S = \sum_{X_i \subset_{>}^{max} M} X_i \subsetneq_{>} M$. By (i), $S \subset_{>}^{\oplus} M$, i.e., $M = S \oplus A$, for some non-zero submodule, which is a contradiction.

ii) implies iii): Clear by Lemma 3.2.11(ii).

iii) implies i): Clear by Lemma 3.2.11(i).

□

The above theorem follows the following Corollary.

Corollary 3.2.13 [3]

Let $f: M_R \longrightarrow N_R$ be an R-homomorphism.

i) M is semisimple implies that $f[M]$ is semisimple.

ii) M is semisimple and $X \subset_{>} M$ implies that M/X is semisimple.

iii) M is semisimple and $X \subset_{>} M$ implies that M is semisimple.

Theorem 3.2.14 [3]

Let R be a ring. Then if ${}_{R}R$ is a semisimple as a left R-module, then R_R is a semisimple as a right R-module.

Proof: Assume that ${}_{R}R$ is semisimple. Then ${}_{R}R = \sum_{i=1}^{n} Re_i$, where each Re_i is simple, $\forall i \in I$. Since $1 = r_1e_1 + \cdots + r_ne_n$, $e_1 = r_1e_1e_1 + \cdots + r_ne_ne_1 = r_1e_1$, then $1 = e_1 + \cdots + e_n$, where $e_ie_j = 0, \forall i \neq j$ and ${e_i}^2 = e_i, \forall i \in I$. Hence $R = \sum_{i=1}^{n} e_i R$. We need to show each e_iR is simple for any $i \in I$. Take $e \in \{e_1,\ e_2, \dots, e_n\}$. We have Re is simple. Let $a \in eR$ and $a \neq 0$. Obviously, $aR \subseteq eR$. Since ${}_{R}R$ is semisimple, $Ra \subset_{>}^{\oplus} {}_{R}R$. This means that $R = Ra \oplus B$ for some left ideal B.

Define $\varphi\colon Re \longrightarrow Ra, re \to rea = ra$. Then φ is a left R-homomorphism [φ is one-one because $\varphi(Ra)$ is simple and φ is onto because for any $a \in Ra$, $\exists e \in R\colon a = \varphi(e)$]. Consider $\psi\colon R = \varphi(Ra) \longrightarrow {}_{R}R$, $ra + b \longrightarrow \varphi^{-1}(ra) = re$. Then ψ is well-defined and a left R-homomorphism. For each $x \in R$, $x = ra + b$ and $\psi(sx) = \psi(sra + sb) = (sr)e = s(re) = s\psi(x)$ and $\psi(x + y) = \psi(x) + \psi(y)$. Then ψ is a right multiplication, i.e., there exists $e \in R\colon \psi(x) = xe$. Then $\psi(a) = \psi(1a + 0) = 1e = e$ and $\psi(a) = ae$. So $e = ae \in aR$, i.e., $eR \subseteq aR$. Thus $aR = eR$, i.e., eR is simple.

□

Proposition 3.2.15

$\overline{R}_{\overline{R}}$ is semisimple if and only if $\overline{R}_R$ is semisimple.

Proof: Suppose that $\overline{R}_{\overline{R}}$ is semisimple. Then for any submodule $A_{\overline{R}}$ of $\overline{R}_{\overline{R}}$ is a direct summand, i.e., $\overline{R}_{\overline{R}} = A_{\overline{R}} \oplus B_{\overline{R}}$. Then $\overline{R}_R = A_R \oplus B_R$. Since $\overline{R}_{\overline{R}}$ is semisimple, $\overline{R}_{\overline{R}} = \oplus\, I_{\overline{R}}$, $I_{\overline{R}}$ is simple. We need to show that $\overline{R}_R = \oplus\, I_R$, where I can be considered as a right R-module. Then I_R is simple. So $\overline{R}_R = \oplus\, I_R$, I_R is simple, implies that $\overline{R}_R$ is semisimple.

Conversely, suppose that $\overline{R}_R$ is semisimple. Then $\overline{R}_R = \oplus\, I_R$, I_R is simple. We want to show that I_R is a right $\overline{R}$-module. We have $U = I_R \cong R/A$, where $A \subset_{>}^{max} R_R$ and $A = ann(I)$. If $A = ann(U)$, then $A \subset_{>} R_R$, $R \longrightarrow I = uR, r \mapsto ur$. So $I \cong R/ann_R(U), J \subseteq ann_R(U)$. So I can be considered as a right $\overline{R}$-module, i.e., $\overline{R} = \oplus\, I_{\overline{R}}$ is a semisimple right $\overline{R}$-module and $I_{\overline{R}} \cong \overline{R}/\overline{A} \cong (R/J)/(A/J) \cong R/A$.

□

Lemma 3.2.16

Let I be a right ideal of a ring R. Then, $I \subset_{>}^{\oplus} R_R$ if and only if there exists $e \in R$ such that $e^2 = e$ and $I = eR$, i.e., I is generated by an idempotent.

Proof: Assume that $I \subset_{>}^{\oplus} R_R$. Then there exists a right ideal J of R such that $R = I \oplus J$. Then $1 = e + f$ for some $e \in I$ and $f \in J$. So $e = e^2 + ef$ and $e = e^2 + fe$. This implies that $ef = fe$. Since $e - e^2 = fe \in I \cap J = 0$, it follows that $e^2 = e$.

To show that $I = eR$. Clearly, $eR \subseteq I$. Take any $x \in I \subseteq R_R$. Since $1 = e + f$, we have $x = ex + fx$. So $x - ex = fx \in I \cap J = 0$, i.e., $x = ex \in eR$. Hence $x \in eR$, and so we have $I \subseteq eR$. Thus $I = eR$.

Conversely, assume that $I = eR$ for some idempotent e in R. Now, We can see that $R = eR + (1 - e)R$. To show $eR \cap (1 - e)R = 0$, let $x \in eR \cap (1 - e)R$. Then there exists $r, s \in R$ such that $x = er = (1 - e)s$. Then $ex = eer = er = x$ and $ex = e(1 - e)s = 0$. So that $x = 0$ and consequently, $eR \cap (1 - e)R = 0$. Thus $R = eR \oplus (1 - e)R$, i.e., $I \subset_{>}^{\oplus} R_R$. □

3.3 Regular Ring

Definition 3.3.1

A ring R is called a von Neumann regular ring if for any $a \in R$, there exists $x \in R$ such that $a = axa$. For example, in the ring $\mathbb{Z}$, the only regular elements are $0,\ 1$ and -1. Thus, $\mathbb{Z}$ is not a regular ring. Again, let R be a division ring and $x \in R$. If $x = 0$, then $x = xxx$, suppose $x \neq 0$. Then $xx^{-1} = 1$, so $x = xx^{-1}x$. Thus, R is a regular ring.

Lemma 3.3.2 [5]

Every semisimple ring is regular [12]. Conversely, every right noetherian regular ring is semisimple.

Theorem 3.3.3 [5]

For any ring R, the following conditions are equivalent:

i) R is regular;

ii) Every principal right ideal of R is generated by an idempotent;

iii) Every finitely generated right ideal of R is generated by an idempotent.

Proof: (i) implies (ii): Let $I = aR$ be a principal right ideal. Since R is von Neumann regular, there exists $x \in R$ such that $a = axa$. Let $e = ax \in I$. Then $e^2 = axax = (axa)x = ax = e$ and $eR \subset_{>} I$. Since $a = axa = ea$, we have $a \in eR$. Now for any $x \in I$, we have $x = ar$ for some $r \in R$, and since $a = ea$, we have $x = ear \in eR$ and so $I \subset_{>} eR$. Hence $I = eR$ with $e^2 = e$.

(ii) implies (i): Let $a \in R$. Then $aR = eR$ for some idempotent element $e \in R$. So we get $a = er$ and $e = as$ for some $r, s \in R$. Since $a = er$, we have $ea = eer = er = a$. So $a = ea = asa$. Thus R is von Neumann regular.

(iii) implies (ii): Clear.

(iii) implies (i): Clear.

(ii) implies (iii): Let $I = aR + bR$. By (2), $aR = eR$ and $bR = fR$ for some idempotents $e, f \in R$. Then $I = eR + fR$ with $e^2 = e$ and $f^2 = f$. Let $f' = (1-e)f = -ef + f \in I$. We must show that $I = eR \oplus f'R$. Clearly, $eR \subseteq I$ and $f'R \subseteq I$. Then $eR + f'R \subseteq I$.

For each $x \in I$, there exists $r, s \in R$ such that $x = er + fs = er + (1-e)fs + efs = e(r + efs) + (1-e)fs \in eR + f'R$. Thus $I \subseteq eR + f'R$. Let $x \in eR \cap (1-e)fR$. Then there exist $r, s \in R$ such that $x = er = (1-e)fs$. Then $ex = eer = er = x$ and $ex = e(1-e)fs = 0$. This implies that $x = 0$. Hence $I = eR \oplus f'R$.

By (ii), there is an idempotent $g \in R$ such that $f'R = gR$. Then $I = eR \oplus gR$. Thus $I = aR + bR = eR \oplus gR$ with $e^2 = e$ and $g^2 = g$. Since $g = f't$ for some $t \in R$, we have $g = (1-e)ft$ and $eg = e(1-e)ft = 0$. Put $h = e + g - ge$. Then $h^2 = (e+g-ge)(e+g-ge) = e(e+g-ge) + g(e+g-ge) - ge(e+g-ge) = ee + eg - ege + ge + gg - gge - gee - geg + gege =$
$e + g - ge = h$

Thus h is an idempotent and $h = e + g - ge = e + g(1-e) \in eR + gR = I$. This means that $hR \subseteq I$. Since $h = e + g - ge$, we have $he = e + ge - ge = e$ and $hg = eg + g - geg = g$. Then $e \in hR$ and $g \in hR$. Thus $eR \subseteq hR$ and $gR \subseteq hR$. Hence $I = eR + gR \subseteq hR \subseteq I$. So $I = hR$ is principal with $h^2 = h$. Therefore, $I = aR + bR$ is generated by an idempotent.

In general, $I = a_1R + a_2R + a_3R + \cdots + a_nR$.

□

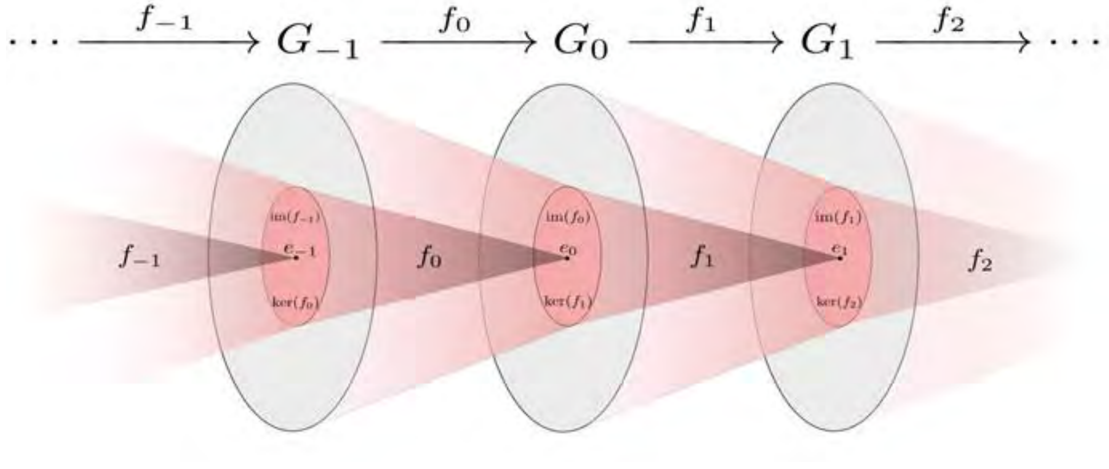
3.4 Injective and Projective Modules

Definition 3.4.1

A ***sequence*** is a function whose domain is the set of positive integers, that is, a sequence in a set is a function $f\colon \mathbb{N} \to S$ where $\mathbb{N}$ is the set of natural numbers and is written as $(f_i), i = 1,2,3, \dots$ or $(f_1, f_2, f_3, \dots)$, where $f_i = f(i)$.

Definition 3.4.2

Let $\{G_i : i \in I\}$ be a collection of right R-modules. For each $i \in I$, let $f_i\colon G_i \longrightarrow G_{i+1}$ be an R-homomorphism. Then a sequence $G_1 \overset{f_1}{\to} G_2 \overset{f_2}{\to} \dots \xrightarrow{f_{n-1}} G_n \overset{f_n}{\to} G_{n+1} \xrightarrow{f_{n+1}} \dots$ is called an ***exact sequence*** at G_n if $Im(f_{n-1}) = kerf_n$. Then the sequence is called an exact sequence if it is exact at each G_n.



$\cdots \xrightarrow{f_{-1}} G_{-1} \xrightarrow{f_0} G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \cdots$
f_{-1}
im(f_{-1})
e_{-1}
ker(f_0)
f_0
im(f_0)
e_0
ker(f_1)
f_1
im(f_1)
e_1
ker(f_2)
f_2

Definition 3.4.3

An exact sequence of special form $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is called a ***short exact sequence***. Here, the exactness means that α is injective, β is surjective and $Im(\alpha) = \ker \beta$.

Definition 3.4.4

A short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is called ***split exact*** if $Im(f) \subset_{>}^{\oplus} B$, (i.e., there exists $B' \subset_{>} B: B = Im(f) \oplus B'$).

For example, let A, C be right R-modules, then $\{0\} \to A \to A \oplus C \to C \to \{0\}$ is a short exact sequence.

If C is a submodule of D, then the sequence $0 \to C \xrightarrow{i} D \xrightarrow{\nu} D/C \to 0$ is exact, where i is the inclusion map and ν is the canonical epimorphism.

Definition 3.4.5

For a pair of sets A and B, a map $f: A \to B$ is called ***injective*** if and only if it has a left inverse, which means that there is a map $f': B \to A$ such that $f' \circ f = 1_A$, the identity map of A.

Dually, for a pair of sets C and D, a map $g: C \to D$ is called ***surjective*** if and only if it has a right inverse. This means that there exists a map $g': D \to C$ such that $g \circ g' = 1_D$, the identity map of D.

We now extend this notion to modules. Let $f: A \to B$ be an R-homomorphism of right R-modules A and B. If there exists an R-homomorphism $f': B \to A$ such that $f' \circ f = 1_A$, then f is a ***monomorphism***.

Note. Suppose that $f: A \to B$ is a monomorphism of right R-modules. Then there does not always exists an R-homomorphism $f': B \to A$such that $f' \circ f = 1_A$. If B is semisimple, then there exists f' for all right R-modules A. For all right R-modules B, if such homomorphism f' exists, then we call A an ***injective module***.

Definition 3.4.6

Let X and Y are right R-modules. In the categorical viewpoint, a right R-module M is said to be ***injective*** (or R-injective) if for any monomorphism $f: M \to X$ and any R-homomorphism $g: M \to Y$, then there exists an R-homomorphism $h: X \to Y$ such that $h \circ f = g$, i.e. such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & X \arrow[dl, "h"] \\
& Y &
\end{tikzcd}$$

Diagram: 01

If the above condition is true only for a special module B, then M is called a B-injective module. Thus, a right R-module M is said to be injective if and only if it is B-injective for any right R-module B. A right R-module B is called quasi-injective if B is B-injective.

Definition 3.4.7

A right R-module M is said to be ***projective*** (or R-projective) if for any epimorphism $g: B \to C$ and any homomorphism $\psi: M \to C$, there exists a homomorphism $\bar{\psi}: M \to B$ such that $g \circ \bar{\psi} = \psi$.

$$\begin{tikzcd}
& M \arrow[d, "\psi"] \arrow[dl, dotted, "\bar{\psi}"'] & \\
B \arrow[r, "g"'] & C \arrow[r] & 0
\end{tikzcd}$$

Diagram: 02

Consider an R-homomorphism $g: C \to D$ of right R-modules. If there is an R-homomorphism $g': D \to C$ such that $gog' = 1$, then g is an epimorphism. In general, such a homomorphism does not always exist. If it exists for all modules C, then D is a free module. When it exists for any module C, we call D a projective module.

Definition 3.4.8

A right R-module M is called a ***quasi-projective modul***e if for any epimorphism $g: M \to X$ and any homomorphism $\psi: N \to X$, there exists a homomorphism $\bar{\psi}: N \to M$, such that $g\bar{\psi} = \psi$.

$$\begin{tikzcd}
& N \arrow[dl, dotted, "\overline{\psi}"'] \arrow[d, "\psi"] & \\
M \arrow[r, "g"'] & X \arrow[r] & 0
\end{tikzcd}$$

Diagram: 03

The right R-module M is a ***projective module*** if for any $g: Y \to X$ and any homomorphism $\psi: M \to X$, there exists a homomorphism $\bar{\psi}: M \to Y$ such that $g\bar{\psi} = \psi$.

$$\begin{tikzcd}
& M \arrow[dl, dotted, "\overline{\psi}"'] \arrow[d, "\psi"] & \\
Y \arrow[r, "g"'] & X \arrow[r] & 0
\end{tikzcd}$$

Diagram: 04

If it satisfies for only one Y, we say that M is Y -projective. But if it satisfies for all Y, we say that M is projective. For $N \in Mod\text{-}R$, M_R is N-projective.

$$\begin{tikzcd}
& M \arrow[dl, dotted, "\overline{\psi}"'] \arrow[d, "\psi"] & \\
N \arrow[r, "g"'] & X \arrow[r] & 0
\end{tikzcd}$$

Diagram: 05

If M is M-projective, we say that M is quasi-projective. If M is N-projective for all $N \in Mod\text{-}R$, we say that M is projective. Clearly, a ring R is always projective.

Lemma 3.4.9

Every semisimple module is a quasi-projective module.

Proof: Let M be semisimple module. Consider the following diagram:

$$\begin{tikzcd}
& Y \arrow[d, "\varphi"] \arrow[dl, dotted, "\bar{\varphi}"'] & \\
M \arrow[r, "g"'] & X \arrow[r] & 0
\end{tikzcd}$$

Diagram: 06

Since $Ker(g) \subset_{>} M$, there exists $Y \subset_{>} M$ such that $M = Ker\ (g) \oplus Y$ and then $X \cong M/Ker(g) \cong Y$. Hence the above exact sequence splits and there is a $g' : X \to M$ such that $gg' = 1_X$. Put $\bar{\varphi} = \ g'\varphi$. Then $g\bar{\varphi} = gg'\varphi = 1_X\varphi = \varphi$. Thus M is quasi-projective.

□

Definition 3.4.10

Let R, S be two rings and let M be an abelian group. Then the abelian group M is called an ***RS-bi-module*** if M is a left R-module, right S-module, and if for any $r \in R, m \in M, s \in S$, we have $r(ms) = (rm)s$. We denote it by $\ _RM_S$.

Semisimple rings and modules are characterized by many researchers over commutative rings such as multiplication modules. But for the case of noncommutative rings these structures are not similar.

3.5 Structure of Endomorphism Rings

Let M_R, N_R be two right R-modules. Then a map $f: M \to N$ is called an R-homomorphism if for any $x, y \in M$ and any $r \in R, f(x + y) = f(x) + f(y)$ and $f(xr) = f(x)r$

i) Let $S = End_R(M)$ be the set of all R-homomorphisms from M_R to M_R. Prove that with the two operations $+$ and $\circ$, for any $f, g \in S$ and for any $x \in M$: $(f\ + g)(x) = f(x) + g(x)$ and $(f \circ g)(x) = f(g(x))$. Then S becomes an associative ring with identity. Finally, M becomes an S-R-bimodule.

ii) Prove that A is a summand of M if and only if there is an idempotent $f^2 = f \in S$ such that $A = f(M)$.

iii) A submodule A of M is called fully invariant if for any $f \in S = End_R(M)$, we have $f(A) \subset A$. Prove that an abelian subgroup X of M_R is a bi-submodule of ${}_SM_R$ if and only if X is a fully invariant submodule of M_R. M_R is called a duo module if every submodule is fully invariant. A ring R is called right duo (resp. left duo) if every right (resp. left) ideal is two-sided.

iv) Prove that $End(R_R) \cong R$ and $End\ _R(R) \cong R$.

A map $f: R \to S$ is called a ring homomorphism if for any $x, y \in R, f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$. The map f is an isomorphism if it is one-one and onto.

<u>Proof of (i):</u> Denote, $Hom_R(M, N) = \{f: M \longrightarrow N \,|\, f$ is an R-Homomorphism$\}$. We must prove that, $Hom_R(M, N)$ is an abelian group with the binary operation addition. Then for any $f, g \in Hom_R(M, N)$, $(f+g)(x) = f(x) + g(x)$. So addition is well-defined. Now for any $f, g \in Hom_R(M, N)$.

Consider the map $: Hom_R(M, N) \times Hom_R(M, N) \longrightarrow Hom_R(M, N)$, $(f, g) \longmapsto f + g$, $(f+g)(x) = f(x) + g(x)$. Then the map φ is well defined because for any $(f, g) \in Hom_R(M, N) \times Hom_R(M, N)$, we have only one $f(x)$ and only one $g(x)$ and $+$ is the addition on N, so $(f+g)(x)$ is defined. Therefore, $(f, g) \longmapsto (f+g)$is defined.

Also, $(f, g) = (p, q)$

$$\Rightarrow f = p, g = q \Rightarrow f(x) = p(x) \text{ and } g(x) = q(x)\ \forall x \in M$$
$$\Rightarrow (f+g)(x) = (p+q)(x)$$
$$\Rightarrow f + g = p + q$$

So, the map φ is well defined. Moreover, $f + g$ is an R-homomorphism.

For any $x, y \in M$ and $r \in R$, we have

$(f+g)(x+y) = f(x+y) + g(x+y)$ [By definition]

$= (f(x) + f(y)) + (g(x) + g(y))$ [Because f, g are R-homomorphisms]

$= (f(x) + g(x)) + (f(y) + g(y))$ [Because $+$ is commutative in N]

$= (f+g)(x) + (f+g)(y)$ [By definition]

Also, $(f+g)(xr) = f(xr) + g(xr)$ [By definition]

$= f(x)r + g(x)r$ [Because f, g are R-homomorphisms]

$= (f(x) + g(x))r$ [Because N is right R-module]

$= ((f+g)(x))r$ [By definition]

So, $f + g \in Hom_R(M, N)$.

Take any $f + g \in Hom_R(M, N)$. Then for any $x \in M$,

$(f + g)(x) = f(x) + g(x)$ [By definition]

$= g(x) + f(x)$ [Because N is an abelian]

$= (g + f)(x)$ [By definition]

Thus $f + g = g + f$.

The addition on $Hom_R(M, N)$ is associative. In fact, let $f, g, h \in Hom_R(M, N)$. Then for any $x \in M$,

$((f + g) + h)(x) = (f + g)(x) + h(x)$ [By definition]

$= (f(x) + g(x)) + h(x)$ [By definition]

$= f(x) + (g(x) + h(x))$ [Because N is an abelian group]

$= f(x) + (g + h)(x)$ [By definition]

$= (f + (g + h))(x)$ [By definition]

Thus, $(f + g) + h = f + (g + h)$.

Define $O: M \to N$ by $O(x) = 0$ for any $x \in M$. We can see that O is an R-homomorphism. For any $(f + O)(x) = f(x) + O(x) = f(x) + 0 = f(x)$. Thus, $f + O = O + f = f$. So, O is the zero element of $Hom_R(M, N)$. Let $f \in Hom_R(M, N)$. Define, $-f$ as follows: For any $x \in M$, $(-f)(x) = -f(x)$. Then $-f \in Hom_R(M, N)$. We have $(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = O(x)$, for any $x \in M$. Hence, $f + (-f) = 0$. This shows that $Hom_R(M, N)$ is an abelian group.

Let $S = End_R(M) = Hom_R(M, M)$ and $f, g \in S$. Then for any $x \in M$, $(f + g)(x) = f(x) + g(x)$ and $(f \circ g)(x) = f\big(g(x)\big)$. We must prove that, S is an associative ring with identity.

a) We can see that $Hom_R(M, M)$ is an abelian group. Take any $f, g \in S$, we have $f \circ g \in S$.

b) For any $, g, h \in S$, $(f \circ g) \circ h = f \circ (g \circ h)$, $f \circ (g + h) = f \circ g + f \circ h$,$(g + h) \circ f = g \circ f + h \circ f$.

c) Finally, we must prove that if $1: M \to M$ then $1_M \in S$ and for any $f \in S$, $f \circ 1 = 1 \circ f = f$. Since f, g maps from M to M, so is $f \circ g$ and $\forall x, y \in M$, $\forall r \in R$, we have

$(f \circ g)(x + y) = f\big(g(x + y)\big)$ [By definition]

$= f\big(g(x) + g(y)\big)$ [By definition]

$= f\big(g(x)\big) + f\big(g(y)\big) = (f \circ g)(x) + (f \circ g)(y)$

And $(f \circ g)(xr) = f\big(g(xr)\big) = f(g(x)r) = [(f \circ g)(x)]r$

Hence $f \circ g \in S$. In fact, let $f, g, h \in S$.

Then for any $x \in M$, we have

$$((f \circ g) \circ h)(x) = (f \circ g)\big(h(x)\big) = f\left(g\big(h(x)\big)\right) = f\big((g \circ h)(x)\big) = (f \circ (g \circ h))(x)$$

Hence $(f \circ g) \circ h = f \circ (g \circ h)$.

Again for any $x \in M$, we have

$$(f \circ (g + h))(x) = f((g + h)(x)) = f(g(x) + h(x)) = f\big(g(x)\big) + f(h(x))$$
$$= (f \circ g)(x) + (f \circ h)(x)$$

Hence $f \circ (g + h) = f \circ g + f \circ h$.

Similarly, for any $x \in M$, we have

$$((g + h) \circ f)(x) = (g + h)(f(x)) = g\big(f(x)\big) + h\big(f(x)\big)$$
$$= (g \circ f)(x) + (h \circ f)(x)$$

Hence $(g + h) \circ f = g \circ f + h \circ f$.

Let $1: M \rightarrow M$ then $1_M \in S$ and for any $f \in S$. We have

$f \circ 1_M = 1_M \circ f = f$,

$1_M(x + y) = (x + y) = 1_M(x) + 1_M(y)$ and

$1_M(xr) = xr = 1_M(x)r$

Hence $1_M \in S$. Also $(f \circ 1_M)(x) = f(1_M(x))$.

which implies that $f \circ 1_M = f$ and $(f \circ 1_M)(x) = 1_M f(x) = f(x)$ implies that $1_M \circ f = f$.

Hence this ring S is not commutative in general.

Last part

We finally show that M is an S-R-bimodule. Let M_R be a right R-module. We first show that M is a left S-module.

Define $\psi: M \times S \rightarrow M$ by $\psi(m\alpha) = \ \alpha(m)$. Then for any $\alpha, \beta \in S$ and for any $m, m' \in M$, we have $\alpha \cdot (m + m') = \alpha(m + m') = \alpha(m) + \alpha(m') = \alpha m + \alpha m'$, because $\alpha \in S$.

Also, $(\alpha + \beta) \cdot m = (\alpha + \beta)(m) = \alpha(m) + \beta(m) = \alpha \cdot m + \beta \cdot m$ and $1_M \cdot m = 1_M(m) = m$ (unitary). Now $\forall \alpha \in S, \forall m \in M, \forall r \in R$, we have $\alpha(mr) = (\alpha \cdot m)r = \alpha(m)r$.

Proof of (ii): Suppose that A is a summand of M. Then $M = A \oplus B$ for some submodule $B \subset M$. Consider $\pi_A: M \rightarrow A$, $\pi_A(m) = a$ where $m = a + b$. Then π_A is an R-homomorphism. Let $\iota_A: A \rightarrow M$, be defined by $\iota_A(a) = a$, the embedding. Consider, the map $M \overset{\pi_A}{\rightarrow} A \overset{\iota_A}{\rightarrow} M$.Put $f = \iota_A \circ \pi_A$. Then $f: M \rightarrow M$. Therefore $f(M) = \iota_A \pi_A(M) = \iota_A(A) = A$.

We now show that $f^2 = f$. Take any $m \in M$. Then $m = a + b$, by hypothesis, where $a \in A, b \in B$. Also, we have $f(m) = a$. So $f^2(m) = f(f(m)) = f(a) = a = f\ (m)$, because $a = a + 0$. Thus $f^2 = f$.

Conversely, let $f^2 = f \in S$ and $A = f(M)$. We must show that A is a summand of M. We first show that $M = f(M) + (1 - f)(M)$. We always have, $f(M) \subset_{>} M$ and $(1 - f)(M) \subset_{>} M$, so $f(M) + (1 - f)(M) \subset_{>} M$. Take any $m \in M$, then $m = f(m) + (1 - f)(m) \in f(M) + (1 - f)(M)$. This shows that $M \subset_{>} f(M) + (1 - f)(M)$. Hence $M = f(M) + (1 - f)(M)$. Take any $y \in f(M) \cap (1 - f)(M)$. Then $y = f(m) = (1 - f)(n)$ and so $f(y) = f^2(m) = f(1 - f)(n) = f(m) = f\big((1 - f)(n)\big) = f\big(1(n) - f(n)\big) = f(n) - f^2(n) = f(n) - f(n) = 0$. Thus $M = f(M) \oplus (1 - f)(M)$.

<u>Proof of (iii):</u> If $A \subset_{>} M_R$, then $A \in Mod\text{-}R$. If A is a left S-module, then for any $f \in S$, and for any a ∈ A, we must have $f \cdot a \in S$. This means that $f(A) \subset A$ (not all submodules of M are left S-modules). If M is a left R-module and $S = End_R(M)$, then M is an R-S-bimodule. For any $\alpha \in S$ and any $m \in A$, we have $m\alpha \equiv \alpha(m)$. ${}_RM$ is a duo module if every submodule is fully invariant.

<u>Proof of (iv):</u> If $f: R_R \to R_R$ is an R-homomorphism, then f is a left multiplication and conversely. Let $f: R_R \to R_R$. Then for any $x \in R$, we have $f(x) = f(1 \cdot x) = f(1)x$. Put $a = f(1)$. Then $f(x) = ax$. Conversely, let $f(x) = sx, s \in R$ be the left multiplication. We can check that f is an R-homomorphism of R_R. Similarly, $f\colon {}_RR \to {}_RR$ is an R-homomorphism if and only if f is a right multiplication. Now consider $\varphi: End(R_R) \to R, f \longmapsto \varphi(f) = f(1)$. Then φ is an isomorphism and φ is well-defined. So $\varphi(f + g) = (f + g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g)$ and $\varphi(f \circ g) = (f \circ g)(1) = f\big(g(1)\big) = f\big(1 \cdot g(1)\big) = f(1) \cdot g(1) = \varphi(f) \circ \varphi(g)$. So φ is a ring homomorphism. Let $\varphi(f) = \varphi(g) \Rightarrow f(1) = g(1) \Rightarrow f(x) = f(1x) = f(1)x$ and $g(x) = g(1x) = g(1)x$. This shows that $f = g$. So φ is one-to-one. Take any $a \in R$. Define $f: R_R \to R_R$ by $f(r) = ar$. Then $f \in End(R_R)$ and $\varphi(f) = f(1) = a$. So φ is onto. Thus, $End(R_R) \cong R$.

□

Extension 3.5.1

Let M be a right R-module and $S = End_R(M)$ be its endomorphism ring. Then, for a right ideal J of I in S, I/J is simple if and only if J is a maximal right ideal of I in S.

Definition 3.5.2

A right R-module M is called a ***regular module*** if $S = End_R(M)$ is a von Neumann regular ring.

Theorem 3.5.3 [5]

The endomorphism ring of a semisimple module is regular.

Proof: Let M be a semisimple right R-module. We want to show that $End_R(M)$ is regular. Let $\alpha: M \to M$. Since $Ker(\alpha)$, $Im(\alpha) \subset_{>} M$, there exist $K, N \subset_{>} M$ such that $M = Ker(\alpha) \oplus N$ and $M = Im(\alpha) \oplus N$. We have,

$$Im(\alpha) \cong M/Ker(\alpha) \cong K$$

Then there exists $\beta: K \to Im(\alpha)$ such that $\beta\big(\alpha(m)\big) = m + Ker(\alpha)$, $m \in M$. β extends $\xi: Im(\alpha) + N \to M, u + n \mapsto \beta(u) = \xi(u + n)$. To show that $\alpha\xi\alpha = \alpha$. Let $m \in M$. Then

$$\alpha\xi\alpha(m) = \alpha\left(\xi\big(\alpha(m)\big)\right) = \alpha\left(\beta\big(\alpha(m)\big)\right) = \alpha(m + Ker(\alpha)) - \alpha\big(m + \alpha^{-1}(0)\big) - \alpha(m)$$

Thus $\alpha\xi\alpha - \alpha$, i.e., $End_R(M)$ is regular.

□

Theorem 3.5.4

If M is a semisimple module, then $S = End_R(M)$ is a skew-field.

Theorem 3.5.5

If M is a regular module, then for any $\alpha \in S$, $\alpha(M)$ is a direct summand of M. Conversely, if for any $\alpha \in S$, $\alpha(M)$ is a direct summand of M and M is quasi-projective, then M is regular.

Proof: Assume that M is a regular module. Then $S = End_R(M)$ is a regular ring. Let $\alpha \in S$. Then $\alpha S = eS$ with $e^2 = e$. This means that $\alpha = eu$ and $e = \alpha t$ for some $u, t \in S$. Then $\alpha(M) = eu(M) \subseteq e(M)$ and $e(M) = \alpha t(M) \subseteq \alpha(M)$, implying that $\alpha(M) = e(M)$. Then for any $m \in M$, $m = e(m) + (1 - e)(m)$. Hence $M = e(M) + (1 - e)(M)$.

Now, let $x \in e(M) \cap (1 - e)(M)$. Then $x = e(m_1) = (1 - e)(m_2)$ for some $m_1, m_2 \in M$. Then $e(x) = e(e(m_1)) = e(1 - e)(m_2) = 0 = x$. Hence $x = 0$. So $e(M) \cap (1 - e)(M) = 0$. Thus $M = e(M) \oplus (1 - e)(M)$.

$$\begin{tikzcd}
 & M \arrow[dl, dotted, "\xi"'] \arrow[d, "e"] & \\
M \arrow[r, "\alpha"'] & \alpha(M) \arrow[r] & 0
\end{tikzcd}$$

Diagram: 07

Conversely, assume that for any $\alpha \in S$, $\alpha(M) \subset_{>}^{\oplus} M$ and M is quasi-projective. We must show that M is regular. Let $\alpha \in S$ and let $e = e_{\alpha(M)} \in S$. Then $e^2 = e \in S$. Since $e(\alpha(M)) = \alpha(M)$, we have for any $m \in M$, $e(\alpha(m)) = \alpha(m)$ which implies that $e\alpha = \alpha$. Then $\alpha \in eS$ and so $\alpha S \subseteq eS$. Since M is quasi-projective, there exists $\xi \colon M \to M$ such that $\alpha\xi = e$. Then $e \in \alpha S$ and so $eS \subseteq \alpha S$, i.e., $\alpha S = eS$, where $e^2 = e \in S$.

□

CONCLUSION

Ring theory has been contributed by the works of inventors and their followers for the long history of evolution. Since the investigation on commutative and general setting of algebraic structures and representation theory of groups, the pioneers like Wedderburn, Artin, Noether, Hilbert, Dedekind, Frobenius had offered the framework for the later development of pure research in abstract ring theory. The Wedderburn-Artin theorem is the cornerstone of noncommutative ring theory. In this thesis, we have concerned mainly with some non-commutative rings. An example of this is $M_n(F)$, a set of matrices over a field F. Another example is the set of upper triangular matrices. More generally, for any ring R, the set $M_n(R)$ of matrices with entries in R is a ring.

A field F is simple which can be viewed as a module over itself. The module $M_n(F)$ is semisimple. For a division ring, the module $M_n(F)$ is not simple as a left or a right module. A vector space is the direct sum of one-dimensional subspaces. Each subspace consists of scalar multiples of a basis vector. A one-dimensional subspace is simple in the sense that it does not have a nontrivial proper subspace. Thus any vector space is a direct sum of simple subspaces. There is a close connection between modules and vector spaces. For studying vector spaces in linear algebra, simple and semisimple modules play a vital role.

The structure of an ideal (a submodule) is the backbone of a ring (a module). In ring theory, ideals play a basic role. Ideals serve to understand the inner structure of rings which contribute many important constructions that include kernels of ring homomorphisms, constructing quotient rings, constructing rings of quotients, even the powerful tools of radicals must be constructed with specific sets of ideals.

A semisimple module is the sum of simple submodules. Considering the modular law, in Theorem 3.2.5, we have proved that every submodule of a semisimple module contains a simple submodule. In Theorem 3.2.8, we have proved that a module over a semisimple ring is again semisimple. Following the direction of Wedderburn-Artin theorem, some characterizations of semisimple modules over associative rings are provided in Proposition 3.2.10. Every semisimple ring is a regular ring. The theory of semisimplicity of regular rings has always carried out on the basis of finite-dimensionality. In Theorem 3.3.3, we have studied some characterizations of von Neumann regular rings. Following the direction of Wedderburn-Artin theorem, in Lemma 3.4.9, we have showed that every semisimple module is a quasi-projective module.

Establishing the structure of endomorphism rings, in Theorem 3.5.3, we have proved that the endomorphism ring of a semisimple module is regular. This has served the first step for studying modules over endomorphism rings. This structure has important significance for studying vector space transformations.

Semisimple rings and modules have been characterized by many researchers over commutative rings such as multiplication modules. But for the case of noncommutative rings, these structures are not very much similar. Finally, in Theorem 3.5.5, we have provided the module-theoretic version of von Neumann regular rings.

Future Scope

From this research, it is expected that there will be a development of analyzing the application of Wedderburn-Artin theorem to chain conditions, to vector spaces, to coding theory, to cryptography and many other fields in science and engineering. Future research may be conducted on the properties of semisimple rings and modules, i.e. on radical, socle and singular submodules. Wedderburn-Artin theorem characterizes injective and projective modules. It gives properties of Noetherian and Artinian rings and modules. It is well-known that not every Artinian module is Noetherian. Examples include the Prüfer group. So there are scopes to analyze semisimple Noetherian and Artinian rings and modules.

REFERENCES

[1] J.H.V. Lint, Introduction to Coding Theory, Springer-Verlag, New York, 1982.

[2] K.R. Goodearl and R.B. Warfield, An Introduction to Noncommutative Noetherian Rings, Cambridge University Press, 2004.

[3] F. Kasch, Modules and Rings, London Mathematical Society Monograph, No. 17, Academic Press, London-New York-Paris, 1982.

[4] F.W. Anderson and K.R. Fuller, Rings and Categories of Modules, Graduate Texts in Mathematics, No. 13, Springer-Verlag, New York-Heidelberg-Berlin, 1922.

[5] B. Stenström, Rings of Quotients, Springer-Verlag, Berlin-Heidelberg-New York, 1975.

[6] S. Asgari, A. Haghany and Y. Tolooei, t-semisimple modules and t-semisimple rings, Communications in Algebra, Vol. 41, No. 5, pp. 1882-1902, 2013.

[7] G. Lee, S.T. Rizvi and C. Roman, Modules whose endomorphism rings are von-Neuman regular, Communications in Algebra, Vol. 41, No. 11, pp. 4066-4088, 2013.

[8] N. Agayev, C. Celik and T. Ozen, On a generalization of semisimple modules, Proceedings of Indian Academy of Sciences, Vol. 128, No. 20, 2018.

[9] N.V. Sanh, N.A. Vu, K.F.U. Ahmed, S. Asawasamrit and L.P. Thao, Primeness in module category, Asian-European Journal of Mathematics, Vol. 3, No. 1, pp. 145-154, 2010.

[10] E. Artin, Zur theorie der hypercomplexen Zahlen, Abh. Math. Sem. Univ. Hamburg, Vol. 5, pp. 251-260, 1927.

[11] J.H.M. Wedderburn, On hypercomplete numbers, Proceedings of London Mathematical Society, Vol. 6, pp. 77-117, 1908.

[12] C. Faith, Algebra II: Ring Theory, Springer-Verlag, Berlin-Heidelberg-New York, 1976.

[13] T. Y. Lam, A First Course in Noncommutative Rings, Graduate Texts in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, Vol. 131, 1991.

[14] T. Y. Lam, Exercises in Modules and Rings, Springer-Verlag, New York, 2000.

[15] K. R. Goorearl, Ring theory: Nonsingular Rings and Modules, Chapman & Hall/CRC Pure and Applied Mathematics, Marcel Dekker Inc., New York, 1976.

[16] R. Wisbauer, Foundations of Module and Ring Theory, Gordon and Breach, Tokyo, 1991.

[17] I. M. A. Hadi, F. D. Shyaa, Strongly t-semisimple modules and strongly t-semisimple rings, International Journal of Pure and Applied Mathematics, Vol. 115, No. 1, pp. 27-41, 2017.

[18] N. V. Dung, J. L. Garcia, Preinjective modules over pure semisimple rings, Journal of Pure and Applied Algebra, Vol. 212, pp. 1207-1221, No. 5, 2008.

[19] N. V. Dung, J. L. Garcia, Endofinite modules and pure semisimple rings, Journal of Algebra, Vol. 289, No. 2, pp. 574-593, 2005.

[20] A. Mozaffarikhah, E. Momtahan, A. R. Olfati and S. Safaeeyan, p-semisimple modules and type submodules, Journal of Algebra and Its Applications, Vol. 19, No. 4, 2020.

[21] D. Bennis, K. Hu, and F. Wang, On 2-SG-semisimple rings, Rocky Mountain Journal of Mathematics, Vol. 45, No. 4 , pp. 1093-1100, 2015.

[22] X. J. Guo and K. P. Shum, Baer semisimple modules and Baer rings, Algebra and Discrete Mathematics, No. 2, pp. 42-49, 2008.

[23] I. M. A. Hadi, F. D. Shyaa, Fi-Semisimple, Fi-t-semisimple and strongly Fi-t-semisimple modules, Al-Qadisiyah Journal of Pure Science, Vol. 24, No. 1, pp. 37-44, 2019.

[24] Y. Hirano, H. Tsutsui, A Generalization of semisimple Artinian Rings, Journal of Algebra and Its Applications, Vol. 4, No. 3, pp. 231-235, 2005.

[25] M. Boulagouaz, L. Oukhtite, σ-semisimple rings, Contributions to Algebra and Geometry Volume 42, No. 2, pp. 385-393, 2001.

[26] H. Q. Dinh, D. V. Huynh, A decomposition theorem for $\wp*$-semisimple rings, Journal of Pure and Applied Algebra, Vol. 186, No. 2, pp. 139-149, 2004.

[27] K. Engin, B. N. Turkmen, E. Turkmen, A note on generalizations of semisimple modules, Commentationes Mathematicae Universitatis Carolinae, Vol. 60, No. 3, pp. 305-312, 2019.

[28] M. M. Abed and A. G. Ahmad, Semisimple (simple) module and length property, AIP Conference Proceedings, Vol. 1571, No. 1, 2013.

[29] A. W. Chatters and C. R. Hajarnavis, Rings with Chain Conditions, Pitman Advanced Publishing Program, 1980.

[30] J. C. McConnell and J. C. Robson, Noncommutative Noetherian Rings, Graduate Studies in Mathematics 30, American Mathematical Society, Providence, Rhode Island, 2001.

[31] J. Jenkins and P. F. Smith, On the prime radical of a module over a commutative ring, Communications in Algebra, Vol. 20, pp. 3593–3602, 1992.

[32] T. Y. Lam, Lectures on modules and rings, Graduate Texts in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, No.189, 1999.

[33] R. L. McCasland and M. E. Moore, Prime submodules, Communications in Algebra, Vol. 20, pp. 1803-1817, 1992.

[34] R. L. McCasland and P. F. Smith, Prime submodules of Noetherian modules, Rocky Mountain J. Math., Vol. 23, pp. 1041–1062, 1993.

[35] M. Behboodi, E. Bigdeli, Prime virtually semisimple modules and rings, Communications in Algebra, Vol. 47, No. 10, pp. 3995-4008, 2019.

[36] M. Behboodi, A. Daneshvar and M. R. Vedadi, Virtually semisimple modules and a generalization of the Wedderburn-Artin theorem, Communications in Algebra, Vol. 46, No. 6, pp. 2384-2395, 2018.

[37] M. Behboodi, A. Daneshvar and M. R. Vedadi, Structure of virtually semisimple modules over commutative rings, Communications in Algebra, Vol. 48, No. 7, pp. 2872-2882, 2020.