

Project Report

On

# A STUDY ON MODULES

*Submitted*

*in partial fulfilment of the requirements for the degree of*

MASTER OF SCIENCE

*in*

MATHEMATICS

*by*

JASMINE JULIAN

(Register No. SM20MAT005)

(2020-2022)

*Under the Supervision of*

DHANALAKSHMI O.M



DEPARTMENT OF MATHEMATICS

ST. TERESA'S COLLEGE (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2022

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

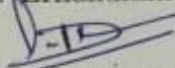


CERTIFICATE


This is to certify that the dissertation entitled, **A STUDY ON MODULES** is a bonafide record of the work done by Ms. **JASMINE JULIAN** under my guidance as partial fulfillment of the award of the degree of **Master of Science in Mathematics** at St. Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Date: 26/05/22

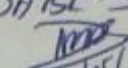
Place: Ernakulam

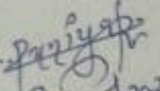
  
**DHANALAKSHMI O.M**  
Assistant Professor,  
Department of Mathematics,  
St. Teresa's College(Autonomous),  
Ernakulam.



  
**Dr. Ursala Paul**  
Assistant Professor & HOD,  
Department of Mathematics,  
St. Teresa's College(Autonomous),  
Ernakulam.

External Examiners

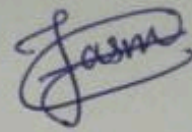
1: **DIVYA..... MARY DAISE S**  
  
26/05/2022

2: **MARY RUNIYA**  
  
26/05/2022



## DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of DHANALAKSMI O.M, Assistant Professor, Department of Mathematics, St. Teresa's College(Autonomous), Ernakulam and has not been included in any other project submitted previously for the award of any degree.



Ernakulam.

JASMINE JULIAN

Date: 26/05/22

SM20MAT005

## ACKNOWLEDGEMENTS

I have to mention several individuals who encouraged me to carry this work and their continuous invaluable knowledgeably guidance throughout the course of this study helped me to complete the work up to this stage in less time.

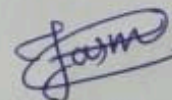
I am very grateful to my project guide DHANALAKSHMI O.M for the immense help during the period of work. I also express my gratitude to thank the almighty for keeping me strong and good during the whole work.

In addition, very energetic and competitive atmosphere of the Department had much to do with this work. I acknowledge with thanks to faculty, teaching and non-teaching staff of the department and Colleagues.

I also very thankful to HOD Dr.URSALA PAUL for their valuable suggestions, critical examination of work during the progress.

Ernakulam.

Date: 26/05/22



JASMINE JULIAN

SM20MAT005

Project Report

On

# A STUDY ON MODULES

*Submitted*

*in partial fulfilment of the requirements for the degree of*

MASTER OF SCIENCE

*in*

MATHEMATICS

*by*

JASMINE JULIAN

(Register No. SM20MAT005)

(2020-2022)

*Under the Supervision of*

DHANALAKSHMI O.M



DEPARTMENT OF MATHEMATICS

ST. TERESA'S COLLEGE (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2022

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM



**CERTIFICATE**

This is to certify that the dissertation entitled, **A STUDY ON MODULES** is a bonafide record of the work done by Ms. **JASMINE JULIAN** under my guidance as partial fulfillment of the award of the degree of **Master of Science in Mathematics** at St. Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Date:

Place: Ernakulam

**DHANALAKSHMI O.M**

Assistant Professor,  
Department of Mathematics,  
St. Teresa's College(Autonomous),  
Ernakulam.

**Dr.Ursala Paul**

Assistant Professor & HOD,  
Department of Mathematics,  
St. Teresa's College(Autonomous),  
Ernakulam.

**External Examiners**

1:.....

2: .....

# DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of **DHANALAKSMI O.M**, Assistant Professor, Department of Mathematics, St. Teresa's College(Autonomous), Ernakulam and has not been included in any other project submitted previously for the award of any degree.

Ernakulam.

**JASMINE JULIAN**

Date:

**SM20MAT005**

## ACKNOWLEDGEMENTS

I have to mention several individuals who encouraged me to carry this work and their continuous invaluable knowledgeably guidance throughout the course of this study helped me to complete the work up to this stage in less time.

I am very grateful to my project guide **DHANALAKSHMI O.M** for the immense help during the period of work. I also express my gratitude to thank the almighty for keeping me strong and good during the whole work.

In addition, very energetic and competitive atmosphere of the Department had much to do with this work. I acknowledge with thanks to faculty, teaching and non-teaching staff of the department and Colleagues.

I also very thankful to HOD **Dr.URSALA PAUL** for their valuable suggestions, critical examination of work during the progress.

Ernakulam.

JASMINE JULIAN

Date:

**SM20MAT005**



# Contents

<i>CERTIFICATE</i> . . . . .	ii
<i>DECLARATION</i> . . . . .	iii
<i>ACKNOWLEDGEMENTS</i> . . . . .	iv
<i>CONTENT</i> . . . . .	v
<i>INTRODUCTION</i> . . . . .	1
<b>1 Preliminaries</b>	<b>3</b>
1.1 Group Theory . . . . .	3
1.2 Ring Theory . . . . .	4
1.3 Homomorphisms . . . . .	6
<b>2 Module</b>	<b>9</b>
2.1 Definition and examples . . . . .	9
<b>3 Submodule and classification of Modules</b>	<b>15</b>
3.1 Submodules . . . . .	15
3.2 Classification of Modules . . . . .	20
3.2.1 Simple Modules . . . . .	20
3.2.2 Free Modules . . . . .	22
3.2.3 Quotient Modules . . . . .	23
3.2.4 Modules over PID's . . . . .	24
3.2.5 Cyclic Modules . . . . .	25
3.2.6 Finitely Generated Modules . . . . .	26
<b>4 Module Homomorphism</b>	<b>27</b>
<b>5 Modules with Chained Conditions</b>	<b>31</b>
5.1 Artinian Modules . . . . .	31

5.2	Noetherian Modules . . . . .	32
6	Applications and Contributions	<b>33</b>
6.1	Applications . . . . .	33
6.2	Contributions in Module Theory . . . . .	34
	<i>REFERENCES</i> . . . . .	36
	<i>CONCLUSION</i> . . . . .	37

# INTRODUCTION

A module is one of the fundamental algebraic structures used in abstract algebra. A module over a ring is a generalization of the notion of vector space over a field, wherein the corresponding scalars are elements of an arbitrary given ring (with identity) and a multiplication (on the left or on the right) is defined between elements of the ring and the elements of the module. In simple words, we can say that it's an abelian group with distributive action of a ring. A module is a generalized form of vector space over the field  $K$ , where  $K$  be replaced by a ring.

The simplest examples of modules (finite abelian groups - they are  $\mathbb{Z}$ -modules) were already known to C.F. Gauss as class groups of binary quadratic forms. The general notion of a module was first encountered in the 1860's till the 1880's in the work of R. Dedekind and L. Kronecker, devoted to arithmetic of algebraic numbers and function fields. At approximately the same time, the research on finite-dimensional associative algebras, in particular, group algebras of finite groups (B. Pierce, F. Frobenius), led to the study of ideals of certain non-commutative rings. At first, the theory of modules was developed primarily as a theory of ideals of a ring. Only later, in the work of E. Noether and W. Krull, it was observed that it was more convenient to formulate and prove many results in terms of arbitrary modules, and not just ideals. Subsequent developments in the theory of modules were connected with the application of methods and ideas of the theory of categories, in particular, methods of Homological algebra.

This dissertation aims in giving an elementary introduction to the module theory. First, we discuss some of the familiar concepts, we been studied, and recollecting all such previous topics under modules, then some of the basic definitions regarding modules, along with some examples and properties. We can see how vector spaces are viewed as modules. The concept of sub-modules is also discuss detaily. Then we move on, about the discussion on module homomorphisms. In the next chapter, it's on classification of modules. The major classifications of

modules I introduce in this dissertation are Free modules, Simple modules, Quotient modules, Modules over PID's, and Cyclic modules. And finally we conclude this study on modules by a discussion of Modules with chain conditions on its rings. It is actually a 6 continuation of the previous chapter, as we have mentioned there about some modules which falls under this category. Modules discussed in his chapter are Artinian modules, Noetherian modules, and Modules of finite length. With the discussion of these aspects of Modules, we will get a deep study on modules through this dissertation.

# Chapter 1

## Preliminaries

---

### Basic Definitions and Concepts

#### 1.1 Group Theory

**Definition 1.1.1.** A Group  $(G,*)$  is a set  $G$ , closed under binary operation  $*$ , such that the following axioms are satisfied.

- 1) For all  $a, b, c \in G$  we have  $(a * b) * c = a * (b * c)$
- 2) There is an element  $e \in G$  such that for all  $x \in G$ ,  
 $e * x = x * e = x$
- 3) Corresponding to each  $a \in G$ , there is an element  $a^{-1}$  in  $G$  such that  $a * a^{-1} = a^{-1} * a = e$

**Definition 1.1.2.** A group  $G$  is abelian, if its binary operation is commutative.

**Theorem 1.1.1.** If  $G$  is a group with binary operation  $*$ , then  $a*b = a*c$  implies  $b = c$  and  $b * a = c * a$  implies  $b = c$  for all  $a, b, c \in G$ .

**Theorem 1.1.2.** If  $G$  is a group with binary operation  $*$  and if  $a$  and  $b$  are any elements of  $G$ , then the linear equations  $a * x = b$ ,  $y * a = b$  have unique solutions  $x$  and  $y$  in  $G$ .

**Definition 1.1.3.** If a subset  $H$  of a group  $G$  is closed under the binary operation of  $G$  and if  $H$  with the induced binary operation from



$G$  is itself a group, then  $H$  is a subgroup of  $G$ .

**Definition 1.1.4.** Let  $G$  be a group and let  $a \in G$ .

If  $G = \{a^n : n \in \mathbb{N}\}$ , then  $G$  is called a Cyclic Group Generated by  $a$ , and is denoted by  $\langle a \rangle$ .

## 1.2 Ring Theory

**Definition 1.2.1.** A ring  $\langle R, +, \cdot \rangle$  is a set  $R$  together with two binary operations  $+$  and  $\cdot$ , which we call addition and multiplication respectively, defined on  $R$  such that the following axioms are satisfied:

- 1)  $\langle R, + \rangle$  is an abelian group.
- 2) Multiplication is associative.
- 3) For all  $a, b, c \in R$ , the left distributive law,  $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$  and the right distributive law  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$  hold.

Some basic properties of a ring follow immediately from the axioms:

- The additive identity is unique.
- The additive inverse of each element is unique.
- The multiplicative identity is unique.
- For any element  $x$  in a ring  $R$ , one has  $x0 = 0 = 0x$  (zero is an absorbing element with respect to multiplication) and  $(-1)x = -x$ .
- If  $0 = 1$  in a ring  $R$  (or more generally,  $0$  is a unit element), then  $R$  has only one element, and is called the zero ring.
- If a ring  $R$  contains the zero ring as a subring, then  $R$  itself is the zero ring.[6]
- The binomial formula holds for any  $x$  and  $y$  satisfying  $xy = yx$ .

**Theorem 1.2.1.** If  $R$  is a ring with additive identity  $0$ , then for any  $a, b \in R$ , we have,

1.  $0a = a0 = 0$
2.  $a(-b) = (-a)b = -(ab)$
3.  $(-a)(-b) = ab$

**Definition 1.2.2.** A ring in which multiplication is commutative is a commutative ring. A ring with a multiplicative identity element is a ring with unity; the multiplicative identity element 1 is called "unity".

**Definition 1.2.3.** An element  $a$  in a ring  $R$  with identity is said to be left invertible, if there exists  $c \in R$  such that  $ca = 1_R$ . The element  $c$  is called left inverse of  $a$ . Similarly, an element  $a$  in a ring  $R$  with identity is said to be right invertible, if there exists  $b \in R$  such that  $ab = 1_R$ . The element  $b$  is called right inverse of  $a$ . An element that is both left and right invertible is said to be a unit.

**Definition 1.2.4.** A commutative ring  $R$  with identity  $1_R \neq 0$  and no zero divisors are called an integral domain. A ring  $D$  with identity  $1_D \neq 0$  in which every nonzero element is a unit is called a division ring. A field is a commutative division ring.

**Remarks 1.2.1 .** 1. Every integral domain and every division ring has atleast two elements (namely 0 and 1)

2. A ring  $R$  with identity is a division ring if and only if the nonzero elements of  $R$  form a group under multiplication.

**Definition 1.2.5.** Let  $R$  be a ring. If there is a least positive integer  $n$  such that  $na = 0$  for all  $a \in R$ , then the least value of  $n$  is the characteristic of  $R$ . If no such  $n$  exists, then  $R$  is said to have characteristic zero.

**Definition 1.2.6.** Let  $R$  be a ring and  $S$  a non empty subset of  $R$  that is closed under the operations of addition and multiplication in  $R$ . If  $S$  is itself a ring under these operations, then  $S$  is called a subring of  $R$ .

**Definition 1.2.7.** A subring  $I$  of a ring  $R$  is a left ideal provided  $r \in R$  and  $x \in I \rightarrow xr \in I$ .  $I$  is an ideal if it is both left and right ideal.

**Definition 1.2.8.** If  $R$  is a commutative ring with unity and  $a \in R$ , the ideal  $\{ra : r \in R\}$  of all multiples of  $a$  is the principal ideal generated by  $a$ , and is denoted by  $\langle a \rangle$ . An ideal  $N$  of  $R$  is a principal ideal if  $N = \langle a \rangle$  for some  $a \in R$ .

**Definition 1.2.9.** An integral domain  $D$  is called a principal ideal domain if every ideal in  $D$  is a principal ideal.

**Definition 1.2.10.** 1. A maximal ideal of a ring  $R$  is an ideal  $M$  different from  $R$  such that there is no proper ideal  $N$  of  $R$  properly containing  $M$ .

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

### 1.3 Homomorphisms

**Definition 1.3.1.** For groups  $\langle G, * \rangle$  and  $\langle H, \oplus \rangle$ , a homomorphism from  $\langle G, * \rangle$  to  $\langle H, \oplus \rangle$  is a map  $\phi : G \rightarrow H$  such that  $\phi(a * b) = \phi(a) \oplus \phi(b)$ . It is simply expressed as  $\phi(ab) = \phi(a)\phi(b)$  with the understanding of the respective operations.

**Definition 1.3.2.** For rings  $R$  and  $R'$ , a map  $\phi : R \rightarrow R'$  is a homomorphism, if the following two conditions are satisfied for all  $a, b \in R$  :

1.  $\phi(a + b) = \phi(a) + \phi(b)$
2.  $\phi(ab) = \phi(a)\phi(b)$

**Definition 1.3.3.** If  $R$  and  $R'$  are rings, and  $\phi : R \rightarrow R'$  is a homomorphism, then the kernel of  $\phi$  denoted by  $\text{Ker}\phi$  is the set of all elements in  $R$  which are mapped to the additive identity of  $R'$  by  $\phi$ . That is,  $\text{Ker}\phi = \{a \in R; \phi(a) = 0'\}$  where  $0'$  is the additive identity of  $R'$ .

**Definition 1.3.4.** An isomorphism  $\phi : R \rightarrow R'$  , where  $R$  and  $R'$  are rings, is a homomorphism that is one to one and onto  $R$ . The rings  $R$  and  $R'$  are isomorphic, if there is an isomorphism of  $R$  onto  $R'$  .

**Definition 1.3.5.** A ring homomorphism  $f : R \rightarrow S$  is called :

1. a monomorphism if  $f$  is one-one
2. an epimorphism if  $f$  is onto
3. an isomorphism if  $f$  is one-one and onto
4. an endomorphism if  $R = S$
5. an automorphism if  $R = S$  and  $f$  is an isomorphism.

**Definition 1.3.6.** Let  $f : R \rightarrow S$  and  $g : S \rightarrow T$  be two homomorphisms. Then, the following are true:

1.  $g \circ f : R \rightarrow T$  is a homomorphism
2.  $g \circ f$  is an isomorphism if both  $g$  and  $f$  are isomorphisms. The converse is not true.

**Definition 1.3.7.** A non-empty set  $X$  with partial order ' $\leq$ ' is called a poset. i.e., ' $\leq$ ' satisfies the following:

1. Reflexivity :  $x \leq x, \forall x \in X$
2. Anti symmetry :  $x \leq y$  and  $y \leq x \Rightarrow x = y$
3. Transitivity :  $x \leq y$  and  $y \leq z \Rightarrow x \leq z$

A subset  $Y$  of  $X$  is called a chain or said to be totally ordered if any two elements of  $Y$  are comparable, i.e., given  $x, y \in Y$  , either  $x \leq y$  or  $y \leq x$ .

**Definition 1.3.8.** A subset  $A$  of  $X$  is said to be bounded above if there is an  $a \in X$  such that  $x \leq a$  for all  $x \in A$ . Such an  $a$  is called an upper bound for  $A$  in  $X$ . It need not belong to  $A$ .

**Definition 1.3.9.** A subset  $A$  of  $X$  is said to have maximal element if there is an  $a \in A$  such that  $a$  not less than  $x$  for all  $x \in A$ ,  $x \neq a$ . A partially ordered set where every totally ordered subset of it is bounded above has an interesting property.



# Chapter 2

## Module

---

### 2.1 Definition and examples

The concept of module over a ring  $R$  is a generalization, be the concept of vector space over a field.

**Definition 2.1.1.** Let  $R$  be any ring. A left  $R$  module  $M$ , is an abelian group  $(M, +)$  together with a map  $R \times M; (a, x) \rightarrow ax$  called scalar multiplication or structure map such that

1.  $a(x + y) = ax + ay, \forall a \in R$  and  $x, y \in M$
2.  $(a + b)x = ax + bx, \forall a, b \in R$ , and  $x \in M$
3.  $(ab)x = a(bx), \forall a, b \in R$  and  $x \in M$

Elements of  $R$  are called scalars. Note that the ring  $R$  can be with or without 1 and commutative or not. For convenience, we adopt the notations  $[0_M]$  and  $[0_R]$  for the identities of group  $M$  and  $R$  respectively

**Definition 2.1.2.** If  $R$  is a ring with unity, a left  $R$  module  $M$  is said to be a unitary left  $R$  module if

$$1 \cdot x = x, \forall x \in M$$

**Definition 2.1.3.** An abelian group  $(M, +)$  is called a right  $R$  module if there is a map from  $M \times R \rightarrow M$ , denoted by  $(x, a) \rightarrow xa$  such that

1.  $(x + y)a = xa + ya, \forall a \in R \text{ and } x, y \in M$
2.  $x(a + b) = xa + xb, \forall a, b \in R \text{ and } x \in M$
3.  $x(ab) = (xa)b, \forall a, b \in R \text{ and } x \in M$

**Proposition 2.1.1.** For an abelian group  $M$ , let  $End_z(M)$  be the ring of all (additive) endomorphisms of  $M$ . Let  $R$  be any ring. Then we have the following:

1.  $M$  is a left  $R$ -module if and only if there exists a homomorphism of rings  $\psi : R \rightarrow End_z M$
2.  $M$  is a right  $R$ -module if and only if there exists an anti-homomorphism of rings  $\psi : R \rightarrow End_z(M)$ , i.e.,  $\psi_0$  is additive and reverses the multiplication.
3.  $M$  is  $R$ -unitary if and only if  $\psi(1_R) = id_M$

**Proof.** (1) Let  $M$  be a left  $R$ -module and  $R \times M \rightarrow M$  be structure map, which we denote by  $(a, x) \rightarrow ax$ .

Now define  $\psi : R \rightarrow End_z M$  by  $a \rightarrow \psi(a) ; M \rightarrow M$  is given by  $x \rightarrow ax$ , i.e.,  $\psi(a)(x) = ax$  for all  $a \in R$  and  $x \in M$ .

**Claim :**  $\psi$  is a homomorphism of rings. Let  $a, b \in R$  and  $x \in M$ .

We have,

$$\begin{aligned}
 \psi(a + b)(x) &= (a + b)x \\
 &= ax + bx \\
 &= \psi(a)(x) + \psi(b)(x) \\
 &= [\psi(a) + \psi(b)](x)
 \end{aligned}$$

This implies that  $\psi(a+b) = \psi(a) + \psi(b)$ .

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

$$\begin{aligned}
 \psi(ab)(x) &= (ab)(x) \\
 &= a(bx) \\
 &= a(\psi(b)(x)) \\
 &= \psi(a)(\psi(b)(x)) \\
 &= (\psi(a) \circ \psi(b))(x)
 \end{aligned}$$

This implies that  $\psi(ab) = \psi(a)\psi(b)$ .

Therefore  $\psi$  is a homomorphism of rings. Conversely, suppose

$\psi : \mathbf{R} \rightarrow \text{End}_z(M)$  is a homomorphism of rings. Now, define the scalar multiplication by,

$$\mathbf{R} \times \mathbf{M} \rightarrow \mathbf{M}; (\mathbf{a}, \mathbf{x}) \rightarrow \mathbf{ax} = (\psi(\mathbf{a}))(\mathbf{x})$$

Claim : This defines the left  $\mathbf{R}$ -module structure on  $\mathbf{M}$ .

Consider any  $\mathbf{a}, \mathbf{b} \in \mathbf{R}$  and  $\mathbf{x}, \mathbf{y} \in \mathbf{M}$ . Since  $\psi(\mathbf{a}) \in \text{End}_z(M)$ ,

we have,

$$\begin{aligned} \mathbf{a}(\mathbf{x} + \mathbf{y}) &= (\psi(\mathbf{a}))(\mathbf{x} + \mathbf{y}) \\ &= \psi(\mathbf{a})(\mathbf{x}) + \psi(\mathbf{a})(\mathbf{y}) \\ &= \mathbf{ax} + \mathbf{ay} \end{aligned}$$

Similarly,

$$\begin{aligned} (\mathbf{a} + \mathbf{b})(\mathbf{x}) &= \psi(\mathbf{a} + \mathbf{b})(\mathbf{x}) \\ &= [\psi(\mathbf{a}) + \psi(\mathbf{b})](\mathbf{x}) \\ &= \psi(\mathbf{a})(\mathbf{x}) + \psi(\mathbf{b})(\mathbf{x}) \\ &= \mathbf{ax} + \mathbf{bx} \\ (\mathbf{ab})(\mathbf{x}) &= \psi(\mathbf{ab})(\mathbf{x}) \\ &= (\psi(\mathbf{a}) \circ \psi(\mathbf{b}))(\mathbf{x}) \\ &= \psi(\mathbf{a})(\psi(\mathbf{b})(\mathbf{x})) \\ &= \psi(\mathbf{a})(\mathbf{bx}) \\ &= \mathbf{a}(\mathbf{bx}) \end{aligned}$$

Thus,  $\mathbf{M}$  is an  $\mathbf{R}$ -module.

(2) Proof of (2) is similar to (1).

(3) Suppose  $\mathbf{M}$  is  $\mathbf{R}$ -unitary and  $\psi : \mathbf{R} \rightarrow \text{End}_z(M)$  is the corresponding homomorphism of rings. We have,

$$\psi(\mathbf{1}) : \mathbf{M} \rightarrow \mathbf{M}, \mathbf{x} \rightarrow \psi(\mathbf{1})(\mathbf{x}) = \mathbf{1} \bullet \mathbf{x} = \mathbf{x}.$$

Hence  $\psi(\mathbf{1}_R) = \text{id}_M$

Conversely, suppose  $\psi(\mathbf{1}_R) = \text{id}_M$ , where,  $\psi: \mathbf{R} \rightarrow \text{End}_z(M)$  is a homomorphism of rings, and the scalar multiplication defined as above.

$$\mathbf{R} \times \mathbf{M} \rightarrow \mathbf{M}(\mathbf{a}, \mathbf{x}) \rightarrow \mathbf{ax} = (\psi(\mathbf{a}))(\mathbf{x})$$

We have,  $\mathbf{1} \bullet \mathbf{x} = (\psi(\mathbf{1})(\mathbf{x})) = \text{id}_M(\mathbf{x}) = \mathbf{x}$ , as required.

Note that, for a ring  $\mathbf{R}$ , the opposite ring  $\mathbf{R}^0$  is the ring with same addition as in  $\mathbf{R}$  and with multiplication reversed. Using the above theorem, we now establish a relation between  $\mathbf{R}$ -modules and

$R^0$  -modules.

**Corollary 2.1.1.**  $M$  is a left  $R$ -module if and only if  $M$  is a right  $R^0$  -module, where,  $R^0$  is the ring opposite to  $R$

**Proof.** We have a homomorphism of rings  $\psi : R \rightarrow \text{End}_z(M)$ . Compose this with the identity map  $i_d : R \rightarrow R^0$ , which is an anti-homomorphism, to get an anti-homomorphism  $R^0 \rightarrow \text{End}_z(M)$ . This means,  $M$  is a right  $R^0$  -module.

Conversely, suppose that we have an anti-homomorphism of rings  $\psi: R^0 \rightarrow \text{End}_z(M)$ .

Compose this with the identity map  $i_d : R \rightarrow R^0$  which is an anti-homomorphism, to get a homomorphism mapping  $R \rightarrow \text{End}_z(M)$ .

Therefore,  $M$  is a left  $R$ -module.

**Remarks 2.1.1.** 1. If  $R$  is commutative, any left  $R$ -module is also a right  $R$ -module. i.e., the notions of left and right modules coincide.

2. If one knows all about all left modules over all possible rings, then one also knows all about all right modules over all rings. In other words, the study of all left modules over all rings is equivalent to the study of all right modules over all rings. This does not mean that the study of all left modules over a particular ring  $R$  is equivalent to the study of all right modules over  $R$ .

Here on wards, we consider only left  $R$ -modules for the theoretical discussion. By an  $R$ -module, we mean a left  $R$ -module unless or otherwise specified,

Now we see examples of Modules.

**Examples of modules**

1. Unitary modules over  $Z$  are simply abelian groups.

For, suppose,  $M$  is an abelian group. We have the natural map

$$\eta : Z \times M \rightarrow M, (n,x) \rightarrow nx$$

$$= \begin{cases} 0, n = 0 \\ x + x + \dots + x, n \text{ times if } n > 0 \\ -x - x - \dots - x, n \text{ times if } n < 0 \end{cases} \quad (2.1)$$

Then,

$$\begin{aligned} n(x + y) &= (x + y) + (x + y) + \dots + (x + y) / (n - \text{times}) \\ &= (x + x + \dots + x) - n - \text{times} + (y + y + \dots + y) - \\ &\quad n - \text{times} \\ &= nx + ny \end{aligned}$$

Similarly,  $(n + m)x = nx + mx$  and  $(nm)x = n(mx)$ .

This makes  $M$  into a unitary  $\mathbb{Z}$ -module.

Conversely, given a unitary  $\mathbb{Z}$ -module  $M$ , given by

$\mathbb{Z} \times M \rightarrow M$ ,  $(n, x) \rightarrow n \cdot x$ , we show that  $n \cdot x = nx$  for all  $n \in \mathbb{Z}$ .

For  $n \geq 0$ , we have,

$$\begin{aligned} n \cdot x &= (1 + 1 + \dots + 1) | n - \text{times} \cdot x \\ &= (1 \cdot x + 1 \cdot x + \dots + 1 \cdot x) | n - \text{times} \\ &= x + x + \dots + x | n - \text{times} \\ &= nx \end{aligned}$$

If  $n \leq 0$ ,  $n \cdot x = (-|n|) \cdot x = |n| \cdot (-x) = nx$ . Thus,  $n \cdot x = nx$  for all  $n \in \mathbb{Z}$  and  $x \in M$ .

**Definition 2.1.4.** Let  $R$  be any ring and,  $M, N$  are (left)  $R$ -modules, then the cartesian product of  $M \times N$  can be made into an  $R$ -module, called the direct product of  $M$  and  $N$  in a natural way.

$$R \times (M \times N) \rightarrow M \times N; (a, (x, y)) \rightarrow (ax, ay)$$

This can be generalised to an arbitrary family of modules. If  $\{M_\alpha\}$  is a family of  $R$ -modules, then  $M = \prod_{\alpha \in I} M_\alpha$  is an  $R$ -module in a natural way:  $R \times M \rightarrow M (a, (x_\alpha)_{\alpha \in I}) \rightarrow (ax_\alpha)_{\alpha \in I}$



**Special cases :**

$$R^2 = \mathbf{R} \times \mathbf{R}$$

$$R^n = \mathbf{R} \times \mathbf{R} \times \dots \times \mathbf{R} \mid \text{ntimes}$$

$$R^\infty = \prod_{i=1}^\infty \mathbf{R}$$

$$R^I = \prod_{\alpha \in I} \mathbf{R}^\alpha, \text{ for all } \alpha \in I$$

## Chapter 3

# Submodule and classification of Modules

---

### 3.1 Submodules

**Definition 3.1.1.** Let  $M$  be an  $R$ -module. A non empty subset  $N$  of  $M$  is called an  $R$ -submodule, or simply a submodule of  $M$  if,

- (1)  $x, y \in N \Rightarrow x + y \in N$  (i.e.,  $(N, +)$  is a subgroup of  $(M, +)$ )
- (2)  $x \in N, a \in R \Rightarrow ax \in N$ . (i.e.,  $N$  is closed under scalar multiplication).

In other words, the restriction of  $N$  to addition and scalar multiplication in  $M$  makes  $N$  into an  $R$ -module in its own right.

**Theorem 3.1.2.** Let  $M$  be a unitary  $R$ -module. Then a non-empty subset  $N$  of  $M$  is a submodule of  $M$  iff for all  $a, b \in R$  and  $x, y \in N$ , then  $ax + by \in N$

**Proof.** Let  $N$  be a submodule of the unitary  $R$ -module  $M$ . Then for  $a, b \in R$  and  $x, y \in N$ ,  $ax \in N$  and  $(-bx) \in N$  and hence  $ax + by = ax - (-(bx)) \in N$ .

Conversely, let  $N$  be a non empty subset of  $M$  such that for all  $a, b \in R$  and  $x, y \in N$ ,  $ax + by \in N$ .

$1_R$  and  $-1_R \in R = 1_Rx + (1_R)y \in N \Rightarrow x + y \in N \Rightarrow (N, +)$  is a subgroup of  $(M, +)$ .

Again  $0_R \in R \Rightarrow ax + 0_Ry = ax \in N \Rightarrow N$  is stable under external law of

composition. Consequently,  $N$  is a submodule of  $M$ .

**Corollary 3.1.3.** Let  $M$  be a unitary  $R$ -module. Then a non empty subset  $N$  of  $M$  is a submodule of  $M$  iff

- (1)  $x, y \in N \Rightarrow x + y \in N$  and
- (2)  $a \in R, x \in N \Rightarrow ax \in N$ .

**Example 3.1.4.** (1) If  $(G, +)$  is an abelian group, then  $G$  is a  $Z$ -module. The submodules of the  $Z$ -module  $G$  are precisely the subgroups of  $G$ . In particular,  $E = \{0, \pm 2, \pm 4, \dots\}$  is a submodule of the  $Z$ -module  $Z$ .

(2) Submodules of a ring are precisely its ideals.

3) Every ring  $R$  may be considered as a left  $R$ -module. Let  $I$  be a submodule of  $R$ . Then  $I \subseteq R$  is such that  $x - y \in I$  and  $rx \in I$ ,  $\forall x, y \in I$  and  $\forall r \in R$ . Consequently,  $I$  is a left ideal of  $R$ .

Conversely, let  $I$  be a left ideal of  $R$ . Then  $I \subseteq R$  is such that  $x - y \in I$  and  $rx \in I$ ,  $\forall x, y \in I$  and  $\forall r \in R$ . Hence  $I$  is a submodule of the left  $R$ -module  $R$ . Thus the submodules of the left  $R$ -module  $R$  are just the left ideals of  $R$ . Thus the submodules of  $R$  are precisely the left ideals of  $R$ .

Likewise, considering  $R$  as a right  $R$ -module, the submodules of  $R$  are precisely the right ideals of  $R$ . In particular, if the ring  $R$  is commutative, then the submodules of  $R$  are precisely the ideals of  $R$ .

**Theorem 3.1.5.** Let  $M$  be an  $R$ -module and  $\{M_i\}_{i \in I}$  be a family of submodules of  $M$ . Then the intersection  $T, \bigcap_{i \in I} M_i$  is again a submodule of  $M$ .

**Proof.** Let  $A = \bigcap_{i \in I} M_i$ .  $0_M \in M_i$  for each  $i \in I$ , since each submodule  $M_i$  is a subgroup of  $M \Rightarrow 0_M \in A \Rightarrow A \neq \phi$ . Again,  $x - y \in M_i$  and  $rx \in M_i$  for each  $i \in I$  and  $\forall x, y \in M_i, \forall r \in R \Rightarrow x - y, rx \in A \Rightarrow A$  is a submodule of  $M$ .

**Remarks 3.1.6.** The union of two modules of an  $R$ -module  $M$  need not in general be submodule of  $M$ , because, union of two subgroups

of a group need not in general be a group. We now cite the following examples.

**Example 3.1.7.** (1) Let  $M_1 = \{0, \pm 2, \pm 4, \pm 6, \dots\}$  and  $M_2 = \{0, \pm 3, \pm 6, \pm 9, \dots\}$ . Then  $M_1$  and  $M_2$  are both submodules of the  $\mathbf{Z}$ -module  $\mathbf{Z}$ . Now  $3 \in M_1 \cup M_2$  and  $2 \in M_1 \cup M_2$ . But,  $3 + 2 = 5 \notin M_1 \cup M_2$ . Hence,  $M_1 \cup M_2$  cannot be a submodule of the  $\mathbf{Z}$ -module  $\mathbf{Z}$ .

(2) Let  $M_1 = \{(x, 0) \in R^2\}$  and  $M_2 = \{(0, y) \in R^2\}$ . Then,  $(1, 0) \in M_1$  and  $(0, 1) \in M_2$ , but,  $(1, 0) + (0, 1) = (1, 1) \notin M_1 \cup M_2 \Rightarrow M_1 \cup M_2$  is not a subgroup of  $R^2 \Rightarrow M_1 \cup M_2$  cannot be a submodule of  $\mathbf{Z}$ -module  $R^2$ .

Let  $M$  be an  $\mathbf{R}$ -module. If  $M_1$  and  $M_2$  are submodules of  $M$ , then  $M_1 \cap M_2$  is the largest submodule of  $M$  contained in both  $M_1$  and  $M_2$ . Because,  $M_1 \cap M_2$  is a submodule of  $M$ , and  $M_1 \cap M_2$  is the largest subset of  $M$  containing both  $M_1$  and  $M_2$ .

**Definition 3.1.8.** Let  $M$  be an  $\mathbf{R}$ -module and  $S$  be a subset of  $M$ . Then the submodule generated or spanned by  $S$ , denoted by  $\langle S_i \rangle$  is defined to be the smallest submodule of  $M$  containing  $S$ , i.e.,  $\langle S_i \rangle$  is a submodule of  $M$  obtained by the intersection of all submodules  $M_i$  of  $M$  containing  $S$ . To determine the elements of  $\langle S \rangle$ , we introduce the concept of linear combinations of elements of  $S$ .

**Definition 3.1.9.** Let  $M$  be an  $\mathbf{R}$ -module and  $S \neq \phi$  be a subset of  $M$ . Then an element  $x \in M$  is said to be a linear combination of elements of  $S$ , iff  $\exists x_1, x_2, \dots, x_n \in S$

and  $r_1, r_2, \dots, r_n \in \mathbf{R}$  such that  $x = \sum_1^n r_i x_i$

We denote the set of all linear combinations of elements of  $S$  by  $C(S)$

**Definition 3.1.10.** Let  $M$  be an  $\mathbf{R}$ -module. A subset  $S$  of  $M$  is said to be linearly dependent over  $\mathbf{R}$  if and only if, there exists distinct elements  $x_1, x_2, x_3, \dots, x_n \in S$  and elements  $r_1, r_2, r_3, \dots, r_n$  (not all zeroes) in  $\mathbf{R}$  such that  $r_1 x_1 + r_2 x_2 + \dots + r_n x_n = 0_M$ . Otherwise,  $S$  is said to be linearly

independent over  $R$ .

**Remarks 3.1.11.** (1)  $0_M$  and any subset  $S$  (of  $M$ ) containing  $0_M$  are linearly dependent over  $R$ .

(2) If  $S$  is linearly dependent over  $R$  and  $T$  is any subset of  $M$  such that  $S \subseteq T$ , then  $T$  is also linearly dependent over  $R$ . i.e., any subset containing a linearly dependent set is also linearly dependent.

(3) If  $S$  is linearly independent over  $R$  and  $T$  is any subset of  $M$  such that  $T \subseteq S$ , then  $T$  is also linearly independent over  $R$ . i.e., any subset contained in a linearly independent set is also linearly independent.

**Definition 3.1.12.** Let  $M$  be an  $R$ -module. A submodule  $N$  ( $\neq M$ ) of  $M$  is said to be maximal iff for a submodule  $P$  of  $M$  such that  $N \subseteq P \subseteq M$ , then  $P = N$  or  $P = M$ . i.e., there is no submodule  $P$  of  $M$  satisfying  $N \subseteq P \subseteq M$ .

**Definition 3.1.13.** A submodule  $N$  ( $\neq \{0_M\}$ ) is said to be minimal iff for a submodule  $P$  of  $M$  such that  $P \subseteq N$ , then  $P = \{0_M\}$  or  $P = N$ . i.e., the only submodules of  $M$  contained in  $N$  are ( $\neq \{0_M\}$ ) and  $N$ .

**Definition 3.1.14.** A module  $M$  ( $\neq \{0_M\}$ ) is said to be simple iff the only submodules of  $M$  are  $\{0_M\}$  and  $M$ .

**Theorem 3.1.15.** Let  $M$  be a unitary  $R$ -module. Then  $M$  is simple iff for every non zero  $x \in M$ ,  $M = Rx = \{rx \mid r \in R\}$ . i.e., iff  $M$  is generated by  $\{x\}$  for every  $x \neq 0$  in  $M$ .

**Proof.** Let  $M$  be a simple unitary  $R$ -module. Then for  $x \neq 0_M$  in  $M$ ,  $x = 1_{Rx} \in Rx \Rightarrow Rx \neq \phi$ . Next, let  $rx, tx \in Rx$ , where  $r, t \in R$ .

Then  $(rx + tx) = (r + t)x \in Rx$  and  $r(tx) \in Rx$ . Consequently,  $Rx$  is a submodule of  $M$ . Since for  $x \neq 0_M$ ,  $x = 1_{Rx} \in Rx$ ,  $Rx \neq 0_M$ . Again,  $M$  being a simple  $R$ -module,  $Rx = M$ .

Conversely, let  $Rx = M$  for every non-zero  $x \in M$ . Suppose  $A \neq 0_M$  is



a submodule of  $M$ . Then,  $\exists$  a non-zero element  $x$  in  $A$  such that  $Rx \subseteq A$ . i.e.,  $M \subseteq A$ . Since  $A \subseteq M$ , it follows that  $A = M$ . Consequently,  $M$  is a simple  $R$ -module.

**Definition 3.1.16.** Suppose  $M$  is an  $R$ -module and  $P, Q$  are  $R$ -submodules of  $M$ . Then the sum of the submodules  $P, Q$  is defined as:

$P + Q = \{x + y \mid x \in P \text{ and } y \in Q\}$  This is an  $R$ -submodule of  $M$  containing  $P$  and  $Q$ . This concept can be generalised for any family

$\{P_\alpha\}_{\alpha \in I}$  of submodules of  $M$ :  $\sum_{(\alpha \in I)} P_\alpha = \{ \sum_{(\alpha \in I)} x_\alpha \mid x_\alpha \in P_\alpha, x_\alpha = 0 \text{ except for finitely many } \alpha\}$  This is a submodule of  $M$  containing each  $P_\alpha, \alpha \in I$ .

**Definition 3.1.17.** Suppose  $M$  and  $N$  are  $R$ -modules. Consider the cartesian product  $P = M \times N$ , which is again an  $R$ -module. We observe that  $P$  contains  $M$  and  $N$  as submodules, namely

$$M = \{(x, 0) \in P \mid x \in M\} \subseteq P \text{ and } N = \{(0, y) \in P \mid y \in N\} \subseteq P.$$

The sum of the submodules  $M$  and  $N$  in  $P$  is called the direct sum of the modules  $M$  and  $N$ . This is denoted by  $M \oplus N$ . We have,

$$\begin{aligned} M \oplus N &= \{(x, 0) + (0, y) \mid x \in M \text{ and } y \in N\} \\ &= \{(x, y) \in P \mid x \in M \text{ and } y \in N\} \end{aligned}$$

This sum is direct in the following sense :

Every element of  $M \oplus N$  can be uniquely written as the sum of an element in  $M$  and an element in  $N$ , or, equivalently,  $P = M + N$ , with  $M \cap N = (0)$

**Proposition 3.1.18.** Suppose  $M$  and  $N$  are submodules of a module  $P$  over  $R$ . Then  $M \cap N = (0)$  if and only if every element  $z \in M + N$  can be written uniquely as  $z = x + y$  with  $x \in M$  and  $y \in N$ .

**Proof.** Suppose  $M \cap N = (0)$ . Let  $z = x + y = x' + y'$ ;  $x, x_0 \in M$  and  $y, y' \in N$ . Then,  $x - x' = y - y' \in M \cap N = (0)$ , which implies  $x = x'$  and  $y = y'$ , showing the uniqueness.

Conversely, suppose that every element of  $M + N$  has a unique decomposition. Let  $z \in M \cap N$ . Now,  $0 = z + (-z) = 0 = 0 + 0 \in M + N, z \in M,$

$-z \in N$ . By uniqueness of decomposition, we get  $z = 0$ . i.e.,  $M \cap N = (0)$

**Definition 3.1.19.** A module  $P$  over  $R$  is called a direct sum of a family of submodules  $\{P_\alpha\}_{\alpha \in I}$  if  $P = \sum_{\alpha \in I} P_\alpha$  and every element  $z \in P$  can be written uniquely as  $z = \sum_{\alpha \in I} x_\alpha$ ,  $x_\alpha \in P_\alpha$ ,  $x_\alpha = 0$  except for finitely many  $\alpha$ 's. We write  $P = \bigoplus_{\alpha \in I} P_\alpha$

## 3.2 Classification of Modules

In this chapter, we shall discuss some significant types of modules over various rings, and give a brief description of their properties.

### 3.2.1 Simple Modules

**Definition 3.2.1.1** A module  $M$  is called a simple module if

1.  $M \neq (0)$ , and
2. the only submodules of  $M$  are  $(0)$  and  $M$

In this section, we discuss about a simple module. A simple module is a module with no non-trivial submodules. We start by defining Maximal and Minimal submodules, explain how they are related to simple modules, and further, examine some properties of simple modules.

**Definition 3.2.1.2** A submodule  $N$  of a module  $M$  is called a maximal submodule if

1.  $N \neq M$ , and,
2.  $N \subseteq P \subseteq M$ ,  $P$  is a submodule of  $M \Rightarrow P = N$  or  $P = M$ , i.e., the only submodules of  $M$  containing  $N$  are  $N$  and  $M$ .

**Definition 3.2.1.3.** A submodule  $N$  of a module  $M$  is called a minimal submodule if

1.  $N \neq (0)$ , and
2.  $P \subseteq N$ ,  $P$  is a submodule of  $M \Rightarrow P = N$  or  $P = (0)$ , i.e., the only

submodules of  $N$  contained in  $N$  are  $(0)$  and  $N$ .

**Lemma 3.2.1.4. (Schur's Lemma) :** Let  $N$  and  $M$  be simple  $R$ -modules. Then, any  $R$ -linear map  $f : M \rightarrow N$  is either  $0$  or an isomorphism. In particular,  $D = \text{End}_R(M)$  is a division ring.

**Proof.** Suppose  $f : M \rightarrow N$  is  $R$ -linear and  $f \neq 0$ , i.e.,  $f(x) \neq 0$  for some  $x_0 \in M$ . We have  $\text{Ker}(f)$  is a submodule of  $M$ . Therefore  $\text{Ker}(f)$  is either  $(0)$  or  $M$  since  $M$  is simple. Since  $f \neq 0$ ,  $\text{Ker}(f) \neq M$ , and hence,  $\text{Ker}(f) = (0)$ , i.e.,  $f$  is one-one. On the other hand, the image  $f(M)$  is a submodule of  $N$ . Therefore  $f(M) = (0)$  or  $N$  (since  $N$  is simple), i.e.,  $f \cong 0$  or  $f$  is onto. But  $f$  not congruent to  $0$ , and so  $f$  is an isomorphism.

To see the last assertion, let  $f : M \rightarrow M$  be  $R$ -linear. Since  $M$  is simple,  $f$  is either zero or an isomorphism which means that  $D = \text{End}_R(M)$  is a division ring.

**Proposition 3.2.1.5.** Let  $R$  be any ring. Then an  $R$ -module  $M$  is simple if and only if  $M \approx R/I$  for some maximal left ideal in  $R$ .

**Proof.** Suppose  $M \approx R/I$  for some maximal left ideal  $I$  in  $R$ . Then we know that  $R/I \neq (0)$  and  $R$ -submodules of  $R/I$  are  $(0)$  and  $R/I$ . Hence  $R/I$  is simple, i.e.,  $M$  is simple.

Conversely, suppose  $M$  is a simple  $R$ -module. We know that  $M \neq (0)$ . Take any  $x_0 \in M$ ,  $x_0 \neq 0$ . Then the submodule  $(x_0)$  generated by  $x_0$  is non-zero and hence is equal to  $M$ , i.e.,  $M$  is a cyclic  $R$ -module. Now look at the map  $f : R \rightarrow M$  given by  $a \rightarrow ax_0$ .

This is  $R$ -linear and surjective. Hence by Epimorphism theorem, we get  $R/\text{Ker}(f)$  is isomorphic to  $M$ , i.e.,  $\text{Ker}(f)$  is maximal left ideal, as required. In the backdrop of the above proposition, the annihilator of any element of a simple module have some interesting properties. We now discuss these properties in detail.

**Corollary 3.2.1.6** The annihilator of any non-zero element of a sim-

ple module is a maximal left ideal and vice-verse.

**Proof.** If  $M$  is simple,  $x_0 \in M$ ,  $x_0 \neq 0$ , and  $f : R \rightarrow M$ ,  $a \rightarrow ax_0$ , then  $\text{Ker}(f) = \{a \in R \mid ax_0 = 0\}$  is the annihilator of  $x_0$  which is a maximal left ideal. Conversely, if  $m$  is a maximal left ideal of  $R$ , then  $m$  is the annihilator of the non-zero element  $x_0 = 1 + m$  of the simple module  $R/m$ , as required.

**Note:** Every simple module is cyclic. And converse need not be true.

**Examples**

1. Any one dimensional vector space is simple.
2. Any minimal submodule of a module is simple.

### 3.2.2 Free Modules

**Definition 3.2.2.1.** An  $R$  module  $M$  is called free module if  $M$  has a basis (A subset  $x$  subset  $M$  is basis if it is spanned by  $x$  and linearly independent and satisfy linear combinations).

**Examples**

1.  $R^n = R^n = R \times R \times \dots \times R$  |  $n$  times is a free  $R$ -module if  $R$  has 1. The set  $B = \{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\}$  is an  $R$ -basis for  $R^n$ , called the standard basis of  $R^n$ .

**Example of a non-free module**

Any finite abelian group is not free as a module over  $Z$ . In fact, any abelian group  $M$ , which has a non-trivial element of finite order cannot be free as a module over  $Z$ . For, suppose  $M$  is free. Say  $B$  is a basis for  $M$  over  $Z$ . Let  $0 \neq x \in M$  be such that  $nx = 0$  for some  $n \in N$ ,

$mx \neq 0$  for  $m < n$  and  $n \geq 2$ . Now we have  $x = n_1b_1 + n_2b_2 + \dots + n_rb_r$  for some  $b_1, b_2, \dots, b_r \in B$  and  $n_1, n_2, \dots, n_r \in Z$

Hence,  $0 = nx = n[n_1b_1 + n_2b_2 + \dots + n_rb_r] = nn_1b_1 + nn_2b_2 + \dots + nn_rb_r \Rightarrow nn_1 = 0$

$nn_2 = 0, \dots, nn_r = 0$  (by linear independence of  $B \Rightarrow n_1 = 0, n_2 = 0, \dots, n_r = 0$  (since  $n \neq 0$ ), i.e.,  $x = 0$ , a contradiction.

**Theorem 3.2.2.2.** A vector space is a free module. i.e., it has a basis.

**Proof.** Let  $V$  be a non-zero vector space over a division ring  $D$ . Let  $F$  be a family of all independent subsets of  $V$ . i.e.,  $F = \{A \subseteq V ; A \text{ is linearly independent over } D\}$

Observe that  $F \neq \emptyset$  because  $F$  contains all non-zero elements of  $V$ . Partially order  $F$  under the set inclusion and apply Zorn's lemma to get a maximal element  $B$  in  $F$ .

**Claim :**  $B$  is a basis for  $V$ . We only have to show that  $B$  spans  $V$ . If not, there exists  $v \in V$  such that  $v$  is not a subset of any finite combination of subsets of  $B$ . Now,  $B \cup \{v\}$  is linearly independent, for

$\alpha v + \alpha_1 b_1 + \dots + \alpha_r b_r = 0 \Rightarrow \alpha \neq 0 \Rightarrow -\alpha^{-1} [\alpha_1 b_1 + \dots + \alpha_r b_r] = -\alpha^{-1} \alpha_1 b_1 + \dots + -\alpha^{-1} \alpha_r b_r \Rightarrow v \in \text{span } B$  which is a contradiction to our assumption.

Hence  $B \cup \{v\}$  is linearly independent. This contradicts the maximality of  $B$ . Hence  $B$  spans  $V$  over  $D$

Notes:

- 1) Zero Module is free with empty sets as basis.
- 2)  $z_6$  is a free  $z_6$  module, but not  $2z_6$ .
- 3)  $Q$  is torsion free as  $z$ -module, since  $Q$  is a field that contains  $Z$  as a submodules.

E.g: For torsion free module, ideal  $(x,y)$  of polynomial ring  $k(x,y)$  over field  $k$ ,  $Q$  is a torsion free.

### 3.2.3 Quotient Modules

In this section, for an  $R$ -module  $M$ , and its submodule  $N$ , we discuss the structure of the quotient group  $M/N$  and discuss some properties of quotient group of modules.

**Definition 3.2.3.1.** Given an  $R$ -module  $M$ , and its submodule  $N$ , the quotient group  $M/N$  has a natural structure of an  $R$ -module as follows:

$\mathbf{R} \times (M/N) \rightarrow M/N; (a, x + N) \rightarrow ax + N, \forall a \in \mathbf{R}, \text{ and } x \in M$

This scalar multiplication is well defined because, if  $x + N = y + N$ , for  $x, y \in M$ ,

we have,  $x - y \in N$  and hence  $ax - ay = a(x - y) \in N$ ,

i.e.,  $ax + N = ay + N$ , as required. It is a simple matter to check that  $M/N$  is an  $\mathbf{R}$ -module, called the quotient of  $M$  modulo  $N$ .

**Proposition 3.2.3.2.** Suppose  $N$  is a submodule of an  $\mathbf{R}$ -module  $M$ . Then the set of submodules of  $M/N$  is naturally bijective with set of all submodules of  $M$  containing  $N$ .

**Proof.** Let  $P$  be a submodule of  $M/N$ . Consider the set

$P_0 = \{x \in M ; x + N \in P\}$ . Since  $x + N = N \in P, \forall x \in N$ , we have,  $N \subseteq P_0$ .

**Claim :**  $P_0$  is a submodule of  $M$ .

Let  $u, v \in P_0$ . Since  $P$  is a submodule, we have

$(u + N) - (v + N) = (u - v) + N \in P$  implies  $u - v \in P_0$ .

Now, let  $x \in P_0$ , i.e.,  $x + N \in P$ . Let  $a \in \mathbf{R}$ . Since  $P$  is a submodule of  $M/N$ , we have  $a(x+N) = ax+N \in P$  implies  $ax \in P_0$ . Hence  $P_0$  is a submodule of  $M$ . It is easy to see that  $P \subseteq P'$ , in  $M/N \Leftrightarrow P_0 \subseteq P_0'$  in  $M$ .

Hence,  $P \neq P_0$  in  $M/N \Leftrightarrow P_0 \neq P_0'$  in  $M$ . Finally, if  $K$  is a submodule in  $M$  containing  $N$ , then  $K^\sim = \{x + N ; x \in K\}$  is a submodule in  $M/N$  and furthermore, we have,  $K_0^\sim = \{x \in M ; x + N \in K^\sim\}$

$= \{x \in M ; x \in K\} = K$

This proves the proposition.

**Notes:** Any quotient  $\mathbf{R}/M$  is a simple module.

### 3.2.4 Modules over PID's

In this section, we shall establish some elementary and standard facts about modules over Principal Ideal Domains (PID's). These are natural generalisations of well-known properties of abelian groups. But abelian groups are modules over  $\mathbf{Z}$  which is a PID.

**Definition 3.2.4.1.** A module is said to be a torsion module if every

element is a torsion element, i.e., annihilated by some non-zero scalar.

**Definition 3.2.4.2.** A module having no non-zero torsion elements is called a torsion free module. (This is equivalent to saying that every non-zero element is linearly independent).

**Definition 3.2.4.3.** The set of all torsion elements of a module  $M$  (over a commutative ring) form a submodule, called the torsion part of the module  $M$ , denoted by  $M_t$ . (It is the largest torsion submodule of  $M$  and saying that  $M$  is torsion free is same as saying that its torsion part  $M_t$  is  $(0)$ )

**Example of a torsion free module which is not free** Let  $R = Z$  and  $M = (Q, +)$  which is obviously torsion free, i.e., it has no elements of finite additive order other than 0. But  $(Q, +)$  is not free because any two elements of  $(Q, +)$  are linearly dependent over  $Z$  and  $(Q, +)$  is not cyclic itself.

**Remarks 3.2.4.4**

1. Torsion modules are nothing but modules of rank 0.
2. Finitely generated torsion modules over  $Z$  are nothing but finite abelian groups.

### 3.2.5 Cyclic Modules

**Definition 3.2.5.1.** Let  $M$  be a right  $R$ -module. A submodule  $V$  of  $M$  (possibly  $V = M$ ) is cyclic if there exists an element  $x \in M$  such that  $V = x_R$ , i.e.,  $V$  is generated by one element, so that  $V = x_R = \{xr ; r \in R\}$ . Any  $y \in V$  such that  $V = y_R$  is a cyclic vector. Some of the examples for cyclic modules are given below .

**Examples 1.** Let  $R = Z$  and let  $M$  be any  $R$ -module (a  $Z$ -module

is just an abelian group). If  $a \in M$ , then  $a_Z$  is the cyclic subgroup of  $M$  generated by  $a$ , denoted by  $\langle a \rangle$ . So,  $M$  is generated as a  $Z$ -module by a set  $A$  which is an abelian group.

### 3.2.6 Finitely Generated Modules

**Definition 3.4.6.1.** A submodule  $N$  of  $M$  is said to be finitely generated if it is generated by some finite subset  $x$  of  $M$ .

Eg:  $R$  module  $N = r[x]$  is not finitely generated.

**Theorem 3.4.6.2.** A finitely generated torsion free module over a PID is free.

**Proof.** Let  $M$  be torsion free, non-zero, and generated by  $X = \{x_1, \dots, x_n\}$ . By reordering if necessary, we may assume that  $B = \{x_1, \dots, x_m\}$  is a maximal linearly independent subset of  $X$ . Let  $F = \text{Span } B$ . Since  $M$  is non-zero and torsion free, we have  $M \geq 1$ . For each  $i$ , there are scalars  $a_i, a_{ij}$ , not all zero such that

$$a_i x_i + \sum_{j=1}^m a_{ij} x_j = 0$$

Since  $B$  is linearly independent, it is clear that  $a_i \neq 0, \forall i$ . Let

$a = a_1 a_2 \dots a_n$  so that  $a \neq 0$ . For,  $a_i x_i \in F$  and so  $a x_i \in F, \forall i$ ,

i.e.,  $aM \subseteq F$ . Now the map  $f : M \rightarrow F; x \rightarrow ax$ , is  $R$ -linear and a monomorphism since  $M$  is torsion free. Hence  $M \approx f(M)$  which is a submodule of the free module  $F$  and so  $f(M)$  is free, i.e.,  $M$  is free, as required.



## Chapter 4

# Module Homomorphism

---

In this section, we study homomorphisms of rings which are similar to that we see in groups. The purpose, concepts, terminologies are similar to that of groups.

**Definition 4.1.** For given  $R$ -modules  $M$  and  $N$ , by an  $R$ -module homomorphism  $f : M \rightarrow N$ , we mean a map that is additive and commutes with scalar multiplication.

i.e.,  $f(x + y) = f(x) + f(y)$ , and  $f(ax) = af(x)$  for all  $x, y \in M$  and  $a \in R$ .

**Definition 4.2.** Given a homomorphism  $f : M \rightarrow N$  of  $R$ -modules  $M$  and  $N$ , the kernel of  $f$  is defined as  $\{x \in M \mid f(x) = 0\}$ , denoted by  $\text{Ker}f$ . It is a submodule of  $M$ .

**Definition 4.3.** A homomorphism  $f : M \rightarrow N$  of  $R$ -modules  $M$  and  $N$  is called

1. a monomorphism if  $f$  is one-one
2. an epimorphism if  $f$  is onto
3. an isomorphism if  $f$  is one-one and onto
4. an endomorphism if  $M = N$
5. an automorphism if  $M=N$  and  $f$  is an isomorphism.

**Definition 4.4.** Let  $f, g : M \rightarrow N$  be  $R$ -linear homomorphisms. Then, define

$$f + g : M \rightarrow N, \text{ by } x \rightarrow f(x) + g(x)$$

Note that  $f + g$  is linear, because,

$$\begin{aligned} (f + g)(x + y) &= f(x + y) + g(x + y) \\ &= f(x) + f(y) + g(x) + g(y) \\ &= (f + g)(x) + (f + g)(y), \end{aligned}$$

$$\begin{aligned} \text{and } (f + g)(ax) &= f(ax) + g(ax) \\ &= af(x) + ag(x) \\ &= a(f + g)(x). \end{aligned}$$

Under this addition,  $Hom_R(M, N)$  is an abelian group with  $0$  map as the identity element and  $f$  defined by  $(f)(x) = (f(x))$  which is linear, as the inverse of  $f$ .

**Theorem 4.5. (Epimorphism Theorem):** Suppose  $f : M \rightarrow N$  is an epimorphism of  $R$ -modules with  $P = \text{Ker } f$ . Then there exists a unique isomorphism  $\tilde{f} : M/P \rightarrow N$  such that  $f = \tilde{f} \circ \eta$ , where  $\eta$  is the natural map given by  $\eta : M \rightarrow M/P, x \rightarrow x + P$ .

i.e., is commutative.

**Proof.** Let  $\tilde{f} : M/P \rightarrow N$  be defined as  $\tilde{f}(x+P) = f(x)$  for all  $x \in M$ .

**Claim 1 :**  $\tilde{f}$  is well defined. Suppose  $x+P = y+P$ , for some  $x, y \in M$ .

This means that  $x-y \in P$ , i.e,  $x-y \in \text{Ker } f$ . Thus  $f(x-y) = 0$  implies  $f(x) = f(y)$  ( $f$  being a homomorphism). i.e.,  $\tilde{f}(x + P) = \tilde{f}(y + P)$ .

Hence the map  $\tilde{f}$  is well defined.

**Claim 2 :**  $\tilde{f}$  is injective.

Suppose that  $\tilde{f}(x + P) = \tilde{f}(y + P)$ . Then we have to show that  $x + P = y + P$ . But we have  $f(x) = f(y)$ . i.e.,  $f(x) - f(y) = 0$ . Since  $f$  is a homomorphism, we get that  $f(x - y) = 0$ . Thus,  $x - y \in \text{Ker } f = P$ . Hence,  $x + P = y + P$  as required.

**Claim 3 :**  $\tilde{f}$  is a homomorphism. For all  $x, y \in M$ , we have

$$\begin{aligned} \tilde{f}((x + P) + (y + P)) &= \tilde{f}(x + y + P) \\ &= f(x + y) \\ &= f(x) + f(y) \end{aligned}$$

$$\begin{aligned}
&= \tilde{f}(x + P) + \tilde{f}(y + P) \\
\text{and, } \tilde{f}((x + P) \bullet (y + P)) &= \tilde{f}(xy + P) \\
&= f(xy) \\
&= f(x).f(y) \\
&= \tilde{f}(x + P) \cdot \tilde{f}(y + P)
\end{aligned}$$

Therefore,  $\tilde{f}$  is an isomorphism and hence a monomorphism.

**Claim 4 :**  $\tilde{f}$  is an isomorphism if and only if  $f$  is an epimorphism. We have,  $f = \tilde{f} \circ \eta$ . If  $\tilde{f}$  is an isomorphism, then  $\tilde{f}$  is an epimorphism. The natural map  $\eta$  is also an epimorphism. Then by claim 3 above,  $f$  is an epimorphism. Similarly,  $f$  is an epimorphism implies that  $\tilde{f}$  is an epimorphism, hence an isomorphism as required.

**Theorem 4.6. (Quotient of a quotient):** Suppose  $P \subseteq N \subseteq M$  are  $R$ -submodules of an  $R$ -module  $M$ . Then, there exists a natural isomorphism  $\tilde{\eta} : (M/P)/(N/P) \rightarrow M/N$ , making commutative

**Proof.** Define  $\tilde{\eta} : (M/P)/(N/P) \rightarrow M/N$  by  $\tilde{\eta}(a+P + N/P) = a+N$ .

**Claim 1 :**  $\tilde{\eta}$  is well defined.

Let  $a, b \in R$  and  $a + P + N/P = b + P + N/P$ . Then,

$$\begin{aligned}
(a + P) - (b + P) \in N/P &\Rightarrow (a - b) + P \in N/P \\
&\Rightarrow a - b \in N \\
&\Rightarrow a + N = b + N
\end{aligned}$$

Then by definition,  $\tilde{\eta}(a + P + N/P) = \tilde{\eta}(b + P + N/P)$ . Hence,  $\tilde{\eta}$  is well defined.

**Claim 2 :**  $\tilde{\eta}$  is a homomorphism of rings.

Let  $a, b \in M$ . Then,

$$\begin{aligned}
\tilde{\eta}((a + P + N/P) + (b + P + N/P)) &= \tilde{\eta}(a + b + P + N/P) \\
&= a + b + N \\
&= (a + N) + (b + N) \\
&= \tilde{\eta}(a + P + N/P) + \tilde{\eta}(b + P + N/P) \\
\text{and, } \tilde{\eta}(a + P + N/P)(b + P + N/P) &= \tilde{\eta}(ab + P + N/P)
\end{aligned}$$

$$\begin{aligned}
&= ab + N \\
&= (a + N).(b + N) \\
&= \tilde{\eta}(a + P + N/P).\tilde{\eta}(b + P + N/P)
\end{aligned}$$

Thus,  $\tilde{\eta}$  is a homomorphism.

**Claim 3 :**  $\tilde{\eta}$  is surjective.

Let  $x \in M/N$ , say  $x = a + N$  for some  $a \in M$ . Now, consider  $\tilde{\eta}(a + P + N/P)$ . We have,  $\tilde{\eta}(a + P + N/P) = a + N = x$ . Therefore,  $\tilde{\eta}$  is surjective.

**Claim 4 :**  $\tilde{\eta}$  is injective.

By definition, we have,

$$\begin{aligned}
\text{Kerf} &= \{a + P + N/P \in (M/P)/(N/P) ; \tilde{\eta}(a + P + N/P) = 0\} \\
&= \{a + P + N/P \in (M/P)/(N/P) ; a + N = N\} \\
&= \{a + P + N/P \in (M/P)/(N/P) ; a \in N\} \\
&= N/P = 0_{\text{in}(M/P)/(N/P)}
\end{aligned}$$

Therefore,  $\tilde{\eta}$  is injective.

Thus  $\tilde{\eta}$  is an isomorphism.

## Chapter 5

# Modules with Chained Conditions

---

In this chapter, we study some important classes of modules. Modules discussed here are Artinian and Noetherian modules.

### 5.1 Artinian Modules

**Definition 5.1.1.** A module  $M$  is called Artinian if descending chain condition (d.c.c) (or equivalently, the minimum condition) holds for  $M$ .

**Remarks 5.1.2.** Minimal submodules exist in a non-zero Artinian module because a minimal submodule is simply a minimal element in the family of all non-zero submodules of  $M$ .

**Examples:**

1. A module which has only finitely many submodules is Artinian. In particular, finite abelian groups are Artinian as modules over  $\mathbb{Z}$ .
2. Finite dimensional vector spaces are Artinian (for reasons of dimension), whereas infinite dimensional ones are not Artinian.

**Theorem 5.1.3.** Submodules and quotient modules of Artinian modules are Artinian.

**Proof.** Let  $M$  be Artinian and  $N$  be a submodule of  $M$ . Any family of submodules of  $N$  is also one in  $M$  and hence the result follows. On the other hand, any descending chain of submodules of  $M/N$  corresponds to one in  $M$  (wherein each member contains  $N$ ) and hence the result.

## 5.2 Noetherian Modules

**Definition 5.2.1.** A module  $M$  is called Noetherian if a.c.c, (or equivalently the maximum condition or the finiteness condition) holds for  $M$ .

**Remarks 5.2.2.** Maximal submodules exist in a non-zero Noetherian module because a maximal submodule is simply a maximal element in the family of all non-zero submodules  $N$  of  $M$ ,  $N \neq M$ .

### Examples

1. A module which has only finitely many submodules is Noetherian. In particular, finite abelian groups are Noetherian as modules over  $\mathbb{Z}$ .
2. Finite dimensional vector spaces are Noetherian (for dimension reasons) whereas infinite dimensional ones are not Noetherian.

**Theorem 5.2.3.** Submodules and quotient modules of Noetherian modules are Noetherian.

**Proof.** Let  $M$  be Noetherian and  $N$  a submodule of  $M$ . Any family of submodules of  $N$  is also one in  $M$  and hence the result follows. On the other hand, any ascending chain of submodules of  $M/N$  corresponds to one in  $M$  (wherein each member contains  $N$ ) and hence the result.

## Chapter 6

# Applications and Contributions

---

### 6.1 Applications

There are some applications of modules we see in our day to day life, in each sectors like mathematics, chemistry, physics, computer science, botony, games etc

1) Every vector space is a module and having no trouble in finding applications of vector spaces in a wide variety of fields.

Note: The constant value  $\pi$  is not a module; since it is not even a vector space. If  $\pi$  was a vector space then we can say that  $\pi$  was a module; since every vector spaces is a module.

2) The study of set of solutions of system of linear differential equation with constant coefficients is facilitated by realization that they form an  $R[D]$ -module

Eg: consider the system of differential equations

$$x' = -x + 6y$$

$$y' = x - 2y$$

thus,

$$x'' + 3x' - 4x = 0$$

$$x'' = -x' + 6y'$$

$$= 3x' - 4x$$

The resulting differential equation with characteristic equation

$$r^2 + 3r - 4 = 0$$

3) Error detecting codes: decoding algorithms of certain codes use Grobner basis of modules over the ring of polynomials

4) Telecommunications engineering: signal constellation design is facilitated by use of modules over an algebraic number field.

5) Modern cryptography: construction of NTRU cryptosystem similarly uses a structure that IIRC is best viewed as a module over ring of modular polynomials.

6) Theoretical physics: representation theory for groups uses module theory.

## 6.2 Contributions in Module Theory

- First course in module theory A by Mike E Keating: It deals with an intro to module theory about linear algebra and ring theory.
- Rings, Modules and total by Friedrich Kasch and Adolf Mader: Ring defined as set  $R$  with two associative operations Addition and Multiplication distinguish between concept and current module.
- On trace for Modules- Howard Bheckwick: Trace is taken to be  $R$ -module homomorphism and basic trace property'
- Kostia Beidar's contributions to module Ring theory by Christian Lamp, Robert Wisbaner 2007: Dealing with works on rings with polynomial identities and condition for rings, and extended Modules later over rings over prime PI-rings.
- Group Action on Fuzzy Modules: Mohammed Yamin Poonam Kumar sharma, Introducing the Fuzzy  $g$ -Modules by defining group action of  $G$  on a fuzzy  $G$ -submodules and so on.
- Fuzzy projective-injective Modules: Mohammed Mehdi Zahedi Rezo Ameri, Equivalent condition for object in category for fuzzy  $R$ - Modules to be injective or projective.



- Fuzzy lattice ordered soft groups:concept of lattice ordered fuzzy soft group is explained.
- Module theory, extending Modules and generalization:Generalisation of CS modules Rings
- Galois module structure of Lubin Tate Model:Extension of Galois extension over the fields.
- Rough G-Modules and their properties:rough theory concept being explained with abstract algebra rough structures.
- Fuzzy lattice ordered G-Modules :Ursula Paul Paul Issac, How study of mathematics reflect in real life. Also fuzzy and rough set theories used to make decision .

## REFERENCES

---

- [1] C.Musili , “Introduction to rings and modules ”, book Second Edition, Narosa Publishing House Private Limited 1994
- [2] I.S Luthar, I.B.S Passi , “Modules (volume 3,) , ” A work on Modules,Volume 3, Narosa Publishing House Private Limited,2000
- [3] Carl Faith, “Algebra: Rings, Modules and categories I” A Journal on Springer Sciences Business Media, 2012
- [4] Hilary , “, Algebra II: Rings and Modules ” Lecture notes, 2016
- [5] Citation I- [ <https://en.m.wikipedia.org/wiki/Module?>] , “Modules, ” Wikipedia on Modules
- [6] Citation II- [ <http://www.ripublication.com/?>] , “Contributions in Modules, ” Research on Contributions on Modules

## CONCLUSION

A study on Module gives the idea of modules as an important algebraic structures. As part of this I explore various aspects of mathematical world and also importance of modules in algebra and preparation on module theory was a great learning experience.