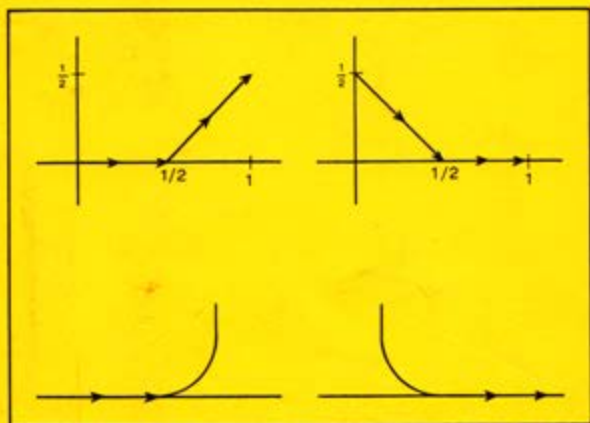


Introduction to

Rings and Modules

Second Revised Edition



C Musili



Narosa

Introduction to
RINGS AND MODULES
Second Revised Edition

Introduction to
RINGS AND MODULES
Second Revised Edition

C. Musili



Narosa Publishing House
New Delhi ● Madras ● Bombay ● Calcutta

C. Musili

Professor of Mathematics

School of Mathematics & Computer/ Information Sciences

University of Hyderabad

Hyderabad, India

Copyright © 1992, 1994, Narosa Publishing House Pvt. Ltd.

Second Revised Edition 1994

Third Reprint 2003

Fourth Reprint 2006

Fifth Reprint 2009

NAROSA PUBLISHING HOUSE PVT. LTD.

22 Delhi Medical Association Road, Daryaganj, New Delhi 110 002

35-36 Greams Road, Thousand Lights, Chennai 600 006

306 Shiv Centre, Sector 17, Vashi, Navi Mumbai 400 703

2F-2G Shivam Chambers, 53 Syed Amir Ali Avenue, Kolkata 700 019

www.narosa.com

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission of the publisher.

All export rights for this book vest exclusively with Narosa Publishing House Pvt. Ltd.
Unauthorised export is a violation of terms of sale and is subject to legal action.

ISBN 978-81-7319-037-7

Published by N.K. Mehra for Narosa Publishing House Pvt. Ltd.,
22 Delhi Medical Association Road, Daryaganj, New Delhi 110 002

Printed in India

To My
Wife and Children
for their
fortitude and support

Preface

This book¹ is a revised and slightly expanded version of *Class Notes* of a course of lectures on Algebra I gave to the M.Sc.(senior) students of the University of Hyderabad in the winter semester of 1987. The present contents constituted two thirds of that course (the remaining being Galois theory). The main text does not depend on the exercises in a serious way and therefore it is completely self-contained. Proofs are given in detail retaining the full flavour of class room exposition. All this facilitates easy self study even by an average student.

In this exposition, we give an elementary introduction to two topics “Rings” and “Modules”. The prerequisites are a little of Group Theory and Linear Algebra, kept to a minimum. As the title indicates, there are two parts, namely, Part I (Rings) and Part II (Modules). Part I contains four chapters covering the very basic aspects of Rings, Ideals, Homomorphisms of Rings and Factorisation in commutative integral domains. Part II consists of the remaining two chapters on Modules and Artinian & Noetherian modules and rings. A glance at the table of contents gives a fairly good idea of the organisation of the material. Dependence of the chapters is progressively linear.

Emphasis in the course was laid on two aspects: (1) developing the concepts with adequate examples and counter-examples drawn from topics such as Analysis (Real, Complex or Functional), Topology, etc., that the students were already (or in the process of being) exposed to and (2) (most crucial) making the student participation *total*.

The student participation was two-fold: In turns (without the exception of a single student), (1) working out exercises and sorting out True/False statements on the board in a 15–30 minute session after *each* lecture hour and (2) giving seminar expositions (hourly once a week) on pre-assigned topics. A good test of understanding of the material lies in one’s ability to explain to others and to correctly sort out the True/False statements with proper justification.

Most of the seminar topics covered in the course are incorporated as additional exercises (with adequate hints), mixed with the class room ones. The seminar topics were chosen with the main aim of instilling confidence in a student that he/she is potentially capable of self study and secondly to open up new topics for further study by those interested. It is also to

¹Written on $\text{\LaTeX}$

make the interested students realise that the amount of Algebra that needs to be absorbed is *enormous* irrespective of what the future specialisations are going to be. To name a few, these topics include: (1) Euclidean division rings (1.1.21), (2) Structure theorem for Boolean rings (1.7.3), (3) Lie rings (1.13.31) and Derivations (3.6.25), (4) Zariski topology on $\text{Spec}(R)$ (2.9.39), (5) Localisations (3.6.17), (6) Classification of primes in the ring of Gaussian integers $\mathbb{Z}[i]$ (4.7.10), etc., (7) Modules over P.I.D's (5.10.37), (8) Semi-simple modules and rings (5.10.19), (9) Group rings (5.10.38) and Maschke's theorem (6.8.22), (10) Asymmetric Artinian and Noetherian rings (6.8.15) and so on. The labelling for cross references is self explanatory. For instance, (5.7.3) refers to Chapter 5, section 7 and item 3. End of a proof is signalled by $\diamond$ and of a section by $\blacksquare$.

The course was rather intensive and very tightly packed for a semester. On the average with 5 contact hours a week (including problem sessions and seminars), I have tried this material, in the above fashion, several times in this University and elsewhere (the first couple of times being at the University of California at Los Angeles (Course No. 110A), in 1974–76), with varying degrees of success.

The *Class Notes* were prepared by Ms. Navneet Arora, one of the students of the course mentioned above. It was typed by Ms. Jayshree. The typed text was used to prepare the revised and expanded current version on a Personal Computer with an active and indispensable involvement of my student P.L.N. Varma. In fact, he initiated me into the $\text{\LaTeX}$ way of preparing Mathematical documents on a PC. My special thanks are due to Navneet, Jayshree and Varma for their respective roles in this venture.

Thanks are also due to my colleagues: S.K. Ray, G.L. Reddy, M. Sitaramayya, R. Tandon for their patient reading (in parts) and critical comments for an improved form of the text and K. Viswanath for useful suggestions. I am grateful to M.S. Raghunathan, of the Tata Institute of Fundamental Research, Bombay, for his valuable advice. Finally, I record my appreciation to the academic adviser of the Narosa Publishing House based on whose comments some slight improvements were made in the text besides providing hints for a few more exercises.

While every care is taken in proof reading, the so called printer's devil (henceforward the *author's devil*) may appear here and there but hopefully be inconsequential.

Hyderabad,
November 1991.

C. Musili

Preface to the Second Edition

I am pleased to say that this exposition has been indeed liked by both students and teachers. It has also reached the international market as distributed by Toppan and Camlot.

When the copies of the first printing were sold out in India, instead of merely reprinting it, we thought it more appropriate to effect the needed changes and bring out a paper back so that it would be within the reach of the student community. I am happy to say that the Narosa Publishing House readily responded with characteristic zeal.

Apart from *casting out the author's devil* (hopefully once and for all), I have made a lot of changes for better or worse but nevertheless gained about 40 pages (mainly by cutting down the previously lavish spacing between sections, etc.).

The sections in which mathematical changes are made (very minor additions as indicated against each) are the following.

• (1.2.2) Note (p.13); (1.7.3) Remarks 2 and 3 (p.20); (1.9.3) Example (p.22); Notation (p.69); (3.1.8) Examples (pp.69 and 70); (4.3.7) More Examples of Euclidean and Principal Ideal Domains and a Theorem without proof (pp. 98 and 99); (5.7.6) insufficient hypothesis supplemented (p.134); (6.2.3) (p.155); (6.5.6) Hilbert Basis Theorem—proof recast to make it independent of §6.2 and Exs.(6.8.25) & (6.8.26) (p.183)•

I take this opportunity to express my gratitude to all the students and teachers for their appreciative and encouraging comments.

Hyderabad,
May 1994.

C. Musili

Contents

Preface	vii
Glossary of Notation	xv

Part I : RINGS

Chapter 1 : Rings	3
-------------------	---

1.1 Terminology	3
1.2 Rings of Continuous Functions	10
1.3 Matrix Rings	14
1.4 Polynomial Rings	16
1.5 Power Series Rings	17
1.6 Laurent Rings	18
1.7 Boolean Rings	19
1.8 Some Special Rings	20
1.9 Direct Products	22
1.10 Several Variables	23
1.11 Opposite Rings	24
1.12 Characteristic of a Ring	24
1.13 Exercises	26
1.14 True/False Statements	31

Chapter 2 : Ideals	33
--------------------	----

2.1 Definitions	33
2.2 Maximal Ideals	34
2.3 Generators	39
2.4 Basic Properties of Ideals	41
2.5 Algebra of Ideals	48
2.6 Quotient Rings	51
2.7 Ideals in Quotient Rings	53
2.8 Local Rings	57
2.9 Exercises	60
2.10 True/False Statements	65

Chapter 3 : Homomorphisms of Rings 67

3.1 Definitions and Basic Properties	67
3.2 Fundamental Theorems	70
3.3 Endomorphism Rings	75
3.4 Field of fractions	77
3.5 Prime fields	82
3.6 Exercises	83
3.7 True/False Statements	87

Chapter 4 : Factorisation in Domains 89

4.1 Division in Domains	89
4.2 Euclidean Domains	92
4.3 Principal Ideal Domains	96
4.4 Factorisation Domains	99
4.5 Unique Factorisation Domains	101
4.6 Eisenstein's Criterion	106
4.7 Exercises	108
4.8 True/False Statements	111

Part II : MODULES

Chapter 5 : Modules 115

5.1 Definitions and Examples	115
5.2 Direct Sums	121
5.3 Free Modules	122
5.4 Vector Spaces	124
5.5 Some Pathologies	126
5.6 Quotient Modules	132
5.7 Homomorphisms	133
5.8 Simple Modules	137
5.9 Modules over P I D's	139
5.10 Exercises	144
5.11 True/False Statements	149

Chapter 6 : Modules with Chain Conditions	151
6.1 Artinian Modules	151
6.2 Noetherian Modules	154
6.3 Modules of Finite Length	158
6.4 Artinian Rings	163
6.5 Noetherian Rings	164
6.6 Radicals	170
6.6n Nil Radical	171
6.6j Jacobson Radical	172
6.7 Radical of an Artinian Ring	176
6.8 Exercises	180
6.9 True/False Statements	183
Answers to True/False Statements	185
Index	187

Glossary of Notation

a.c.c	ascending chain condition 154
$a \mid b$	a divides b or a is a factor of b 89
$\text{Ann}_R(x)$	Annihilator of an element x 44, 132
$\text{Ann}_R(M)$	Annihilator of a module M 132

$c(f)$	$= c(f(X))$ Content of a polynomial $f(X)$ 103
$\mathbb{C}, \mathbb{C}$	Complex numbers 4
$\mathbb{C}\{z\}$	Complex entire functions 22, 122
$\mathcal{C}(X, \mathbb{R})$	Real valued continuous functions on X 10
$\mathcal{C}([0, 1], \mathbb{R})$	Real valued continuous functions on $[0, 1]$ 12, 29
$\mathcal{C}^n([0, 1], \mathbb{R})$	Continuously n times diferentiable functions 12
$\mathcal{C}^\infty([0, 1], \mathbb{R})$	Real valued smooth functions on $[0, 1]$ 12
$\mathcal{C}^\infty(\mathbb{R})$	Real valued smooth functions on $\mathbb{R}$ 29
$\text{Char } R$	Characteristic of a ring R 24

d.c.c	descending chain condition 151
$\text{Der}(R)$	Derivations of a ring R 86
$\text{Der}_R(S)$	R -derivations of S 87
∂/∂_X	Partial derivative w.r.t X 87
$\dim_D(V)$	Dimension of a vector space V 125

E_{ij}	Matrix whose $(i, j)^{\text{th}}$ entry is 1 and 0's elsewhere 14
$\text{End}_D(V)$	D -linear endomorphisms of a vector space V 75, 167
$\text{End}_{\mathbb{Z}}(G)$	Endomorphisms of an abelian group G 75, 116
$\text{End}_R(M)$	R -linear endomorphisms of a module M 134, 180

FD	Factorisation domain 99
$\mathbb{F}_q$	Finite field of q elements 108

gcd	greatest common divisor 91
------------	----------------------------

$\text{Hom}_{\text{rings}}(R, S)$	Homomorphisms of rings 85
$\text{Hom}_R(M, N)$	R -linear homomorphisms of modules 134
$\mathbb{H}_{\mathbb{Q}}$	$= \mathbb{Q}[i, j, k]$ = Rational quaternions 9
$\mathbb{H}_{\mathbb{R}}$	$= \mathbb{R}[i, j, k]$ = Real quaternions 8
$I + J$	Sum of ideals I and J 48
IJ	Product of ideals I and J 49
I^n	n^{th} power of an ideal I 50
$\sqrt{I}$	Square root (or radical) of an ideal I 60
$\text{Im}(f)$	Image of a map f 69
$J(R)$	Jacobson radical of a ring R 172, 175
$J_l(R)$	left Jacobson radical of a ring R 173
$J_r(R)$	right Jacobson radical of a ring R 175
$K(X)$	$= Q(K[X])$ = Field of frac. of $K[X]$ for a field K 80
$K((X))$	$= Q(K[[X]])$ = $\dots$ of $K[[X]]$ for a field K 81
$\text{Ker}(f)$	Kernel of a homomorphism f 68, 133
lcm	least common multiple 92
$\ell_R(M)$	Length of an R -module M 162
$L(R)$	Lie ring associated to a ring R 29
λ_α	homothety defined by α 137, 147
$\text{Maps}(X, R)$	Set of R -valued maps defined on X 69
$\text{Maps}_0(X, R)$	Set of R -valued maps with finite support 70
M_t	Torsion part of a module M over a PID 141
$M_n(R)$	$n \times n$ matrices over R 14
$M + N$	Sum of submodules M and N of a module 120
$M \oplus N$	Direct sum of modules M and N 121
M/N	Quotient of M modulo a submodule N 132
μ_n	Complex n^{th} roots of unity 157
μ_{p^*}	$= \cup_{n=1}^{\infty} \mu_{p^n}$ 157

- $\mathbb{N}, \mathbb{N}$ Positive integers 4
 $N(R)$ Nil radical of a ring R 171
 $\text{ord}(f(X))$ order of a power series $f(X)$ 18, 95
 PID Principal Ideal Domain 41, 96
 PIR Principal Ideal Ring 41
 $\text{Pol}(R)$ R -valued polynomial functions on a ring R 31
 $\mathcal{P}(X)$ Boolean ring of subsets of a set X 19
 $\sum_{\alpha \in I} P_{\alpha}$ Sum of a family of submodules 120
 $\prod_{\alpha \in I} P_{\alpha}$ Direct product of a family of modules 121
 $\oplus_{\alpha \in I} P_{\alpha}$ Direct sum of a family of modules 121
 $\mathbb{Q}, \mathbb{Q}$ Rational numbers 4, 9
 $\mathbb{Q}[i]$ Gaussian numbers 21
 $\mathbb{Q}[i, j, k] = \mathbb{H}_{\mathbb{Q}}$ Rational quaternions 9, 21
 $\mathbb{Q}^{(p)}$ p -adic integers 22
 $\mathbb{Q}^{(p_1, \dots, p_n)}$ for prime numbers p_j 's 59
 $Q(R)$ Field of fractions of a com. int. domain R 79
 $Q(K[X]) = K(X) = \dots$ of $K[X]$ for a field K 80
 $Q(K[[X]]) = K((X)) = \dots$ of $K[[X]]$ for a field K 81
 $\text{rank}_R(M)$ Rank of a module over a PID 142
 $\mathbb{R}, \mathbb{R}$ Real numbers 4, 8
 $\mathbb{R}[i] = \mathbb{C}$ Complex numbers 4, 21
 $\mathbb{R}[i, j, k] = \mathbb{H}_{\mathbb{R}}$ Real quaternions 8
 $\mathbb{R}\{x\}$ Real analytic functions 29
 $R \times S$ Direct product of R and S 22
 R^{op} $= R^0$ = Ring opposite to R 24
 $R[G]$ Group ring of a group G over R 148

$R[X]$	Polynomials over R in the variable X	16
$R[X_1, \dots, X_n]$	... in several variables	23
$R[[X]]$	Formal power series over R in X	17
$R[[X_1, \dots, X_n]]$	... in several variables	23
$R[X, X^{-1}]$	Laurent polynomials over R in X	18
$R[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$	... in several variables	24
$R < X >$	Laurent series over R in X	18
$R < X_1, \dots, X_n >$	... in several variables	24
R/I	Quotient ring modulo a 2-sided ideal I	52
R/I	Quotient module modulo an ideal I	132
R_P	Localisation of R at a prime ideal P	85
$\text{Seq}(R)$	Set of sequences in R	31, 70
$\text{Spec}(R)$	Prime ideals of a commutative ring R	63
UFD	Unique factorisation domain	101
$\mathcal{U}(R)$	Group of units of a ring R	5, 93
$V(I)$	$= \text{Spec}(R/I) =$ Prime ideals of R containing I	63
(x)	Principal 2-sided ideal generated by x	41
$(x)_\ell$	Principal left ideal generated by x	40
$(x)_r$	Principal right ideal generated by x	40
χ_x	Characteristic function of $\{x\}$	147
$\mathbb{Z}, \mathbb{Z}$	Integers	4, 75
$\mathbb{Z}^+$	Non-negative integers	13
$\mathbb{Z}_n$	Integers modulo n	20
	$= \mathbb{Z}/n\mathbb{Z} =$ Quotient of $\mathbb{Z}$ modulo $n\mathbb{Z}$	55
$\mathbb{Z}_{(p)}$	Localisation of $\mathbb{Z}$ at $p\mathbb{Z}$	85
$\mathbb{Z}[\sqrt{d}]$	for an integer d	21
$\mathbb{Z}[i]$	Gaussian integers	21
$\mathbb{Z}[i, j, k]$	Integral quaternions	21, 29
$Z(L)$	Centre of a Lie ring L	30
$Z(R)$	Centre of a ring R	6
*****	*****	

Part I

RINGS

Chapter 1

Rings

In what follows, some very basic knowledge of Group Theory and a little of Linear Algebra (vector spaces and matrices over fields such as real numbers, complex numbers, etc.) are assumed. We begin with the fundamentals of Ring Theory. While Group Theory involves the study of only one binary operation, Ring Theory involves two binary operations with some interrelations. We formally define what a ring is and give some examples interspersed with a few elementary properties of rings. The examples we give are what one usually comes across in various contexts (such as Algebra [Abstract, Linear, Differential]; Analysis [Real, Complex, Functional]; Topology; Modules; etc.) and they serve to illustrate or counter-illustrate different aspects of rings that we propose to study in this exposition.

1.1 Terminology

1.1.1 Ring: A non-empty set R together with two binary operations $(+)$ and $(\cdot)$, called *addition* and *multiplication* respectively, is called a *ring* if it has the following three properties.

- (i) $(R, +)$ is an abelian group,
- (ii) $(R, \cdot)$ is a semi-group and
- (iii) Distributive laws hold.

To spell out these conditions, we have the following.

(i) Abelian Group

(a) $a, b \in R \Rightarrow a + b \in R$.

(b) $a, b, c \in R \Rightarrow (a + b) + c = a + (b + c)$.

(c) $\exists 0_R \in R$ such that $a + 0_R = a = 0_R + a$, $\forall a \in R$.

(Such an 0_R is unique and is called the *additive identity* or the *zero element*. This 0_R is denoted simply by 0 since no confusion is likely.)

(d) $\forall a \in R$, $\exists b \in R$ such that $a + b = 0 = b + a$. (Such a b is unique and is denoted by $-a$. It is called the *additive inverse* of a .)

(e) $\forall a, b \in R$, $a + b = b + a$.

(ii) Semi-group

(f) $a, b \in R \Rightarrow a \cdot b \in R$.

(g) $a, b, c \in R \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iii) Distributive laws

(h) $\forall a, b, c \in R$, $\begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c, \\ (a + b) \cdot c = a \cdot c + b \cdot c. \end{cases}$

1.1.2 Examples: 1. The sets of integers ($\mathbb{Z}$), rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$) and complex numbers ($\mathbb{C}$) with usual addition and multiplication are rings.

2. Let $n \in \mathbb{N}$. The set of all $n \times n$ matrices over $\mathbb{R}$ is a ring with respect to usual addition and multiplication of matrices.

1.1.3 Proposition: *The following properties hold in any ring R .*

1. $0 \cdot a = 0 = a \cdot 0$, $\forall a \in R$.

2. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, $\forall a, b \in R$.

3. $n(ab) = (na)b = a(nb)$, $\forall a, b \in R$ and $n \in \mathbb{Z}$.

4. $(mn)a = m(na) = n(ma)$, $\forall n, m \in \mathbb{Z}$ and $a \in R$, where

$$na = \begin{cases} a + a + \cdots + a & (n \text{ terms}) & \text{if } n \geq 0, \\ -(a + a + \cdots + a) & (-n \text{ terms}) & \text{otherwise.} \end{cases}$$

Proof: Easy verification. ◇

1.1.4 Unity element: If the semi-group $(R, \cdot)$ has an identity, it is unique and is denoted by 1_R or simply 1 and is called the *identity element* or the *unity* of R .

1.1.5 Commutative ring: A ring R is said to be *commutative* if the semi-group $(R, \cdot)$ is commutative, i.e., $a \cdot b = b \cdot a$, $\forall a, b \in R$.

1.1.6 Units: Let R be a ring with 1. An element $u \in R$ is said to be a *unit* or *invertible* if there exists $v \in R$ such that $uv = vu = 1$. Such a v is unique, called the *multiplicative inverse* of u and is denoted by u^{-1} .

Notation: The set of units in R is denoted by $\mathcal{U}(R)$.

Examples: The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are commutative with 1. Every non-zero element of $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ is invertible and the inverse of $a \neq 0$ is $1/a$. However, the only units in $\mathbb{Z}$ are ± 1 .

1.1.7 Remarks: 1. If u and v are units in R , so is uv and $(uv)^{-1} = v^{-1}u^{-1}$. It follows that $\mathcal{U}(R)$ is a group under multiplication with 1 as its identity, called the *group of units* of R .

2. The element '0' is never a unit unless $0 = 1$. (Note that $0 = 1$ if and only if $R = \{0\}$.)

3. Sum of two units need not be a unit. For example, 1 and -1 are units in $\mathbb{Z}$ but $1 + (-1) = 0$ is not a unit.

1.1.8 Zero-divisors: An element $a \in R$ is said to be a *left zero-divisor* if there exists $b \neq 0$ such that $a \cdot b = 0$. Similarly a is a *right zero-divisor* if there is a $c \neq 0$ such that $c \cdot a = 0$. An element $a \in R$ is said to be a *zero-divisor* if a is either a left zero-divisor or a right zero-divisor.

1.1.9 Remark: In any ring R with atleast two elements, 0 is a zero-divisor, called the *trivial zero-divisor*.

1.1.10 Nilpotent element: An element $a \in R$ is said to be *nilpotent* if there is a positive integer n ($= n(a)$ depending on a) such that $a^n = 0$, where a^n stands for $a \cdot a \cdots a$ (n factors). (In any ring R , 0 is a nilpotent element, called the *trivial nilpotent element*.)

1.1.11 Idempotent element: An element $a \in R$ is said to be an *idempotent* if $a^2 = a$. (In any ring R , 0 and 1 (if 1 exists) are idempotents called the *trivial idempotents*.)

Two idempotents $a, b \in R$ are said to be *orthogonal* (to each other) if $ab = 0 = ba$. For example, if R has unity and a is an idempotent, then $1 - a$ is also an idempotent and a and $1 - a$ are orthogonal.

1.1.12 Remarks: 1. The ring $R = \{0\}$ is called the *zero ring*. Hence a non-zero ring R means R has atleast two elements.

2. The element 0 is the only element which is both nilpotent and idempotent in any ring R .

3. Let $(G, +)$ be any abelian group. By defining $ab = 0$, for all $a, b \in G$, we see that $(G, +, \cdot)$ is a ring. This ring is called a *trivial ring* and this multiplication is called the *trivial multiplication*. Thus the class of all trivial rings is exactly the class of all abelian groups.

1.1.13 Subring: Let R be a ring. A non-empty subset S of R is called a *subring* of R if $(S, +)$ is a subgroup of $(R, +)$ and $(S, \cdot)$ is a subsemi-group of $(R, \cdot)$. Or, equivalently, the restrictions of the operations $(+)$ and $(\cdot)$ on R to S make $(S, +, \cdot)$ a ring in its own right. It is obvious that a subring of a subring of a ring R is a subring of R .

Examples: 1. The subsets $\{0\}$ and R are subrings of any ring R and are called the *trivial subrings* of R .

2. The subset $Z(R) = \{a \in R \mid ax = xa, \forall x \in R\}$ which is obviously a subring of R , is called the *centre* of R . Any subring of $Z(R)$ is called a *central subring* of R .

3. The subsets $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ are all subrings of $\mathbb{C}$.

1.1.14 Some pathologies: If S is a subring of a ring R , then we have the following possibilities.

1. S may be commutative but not R .

The set S of all $n \times n$ diagonal matrices is a commutative subring of the ring R of all $n \times n$ matrices over $\mathbb{Z}$, $n \geq 2$.

2. S may not have unity even if R has.

The set S of all even integers is a subring without unity of the ring R of all integers.

3. S may have unity even if R does not have.

For an example, see (1.9.2) below.

4. *S and R may both have unities but they may not be the same.*

Let R be the 2×2 real matrices, i.e., $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$

and let $S = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} \mid x \in \mathbb{R} \right\}$. Then $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $1_S = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$.

5. *An element $a \in S$ may be a zero-divisor in R but not in S .*

Let $S = \{0\}$ and $R = \mathbb{Z}$; 0 is a zero divisor in R but not in S .

6. *Even when the unities of R and S are equal, an element $a \in S$ may be a unit in R but not in S .*

Let $R = \mathbb{R}$ and $S = \mathbb{Z}$; then $1_R = 1_S = 1$. We know that $2 \in R$ is a unit in $\mathbb{R}$ but not a unit in $\mathbb{Z}$.

7. *If the unities in R and S exist and are distinct, then an element $a \in S$ may be a unit in S but not in R .*

Let R and S be as in 4 above. For $x \neq 0$, $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$ is a unit in S , but not in R . (It is a singular matrix in R .)

1.1.15 Integral domain: A non-zero ring R is called an *integral domain* if there are no non-trivial zero-divisors in R .

The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are examples of integral domains.

We note that it is *not* necessary to assume that an integral domain should be commutative or must have unity, as some authors assume. What is essential is that it should have at least 2 elements besides being free from non-trivial zero-divisors.

1.1.16 Division ring: A ring R in which the set R^* of non-zero elements is a group with respect to the multiplication in R is called a *division ring* or a *skew-field*. Equivalently, R is a division ring if every non-zero element of R has a *multiplicative inverse* in R .

The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are some examples of division rings. See (1.1.18) or (1.1.19) below, for examples of non-commutative division rings.

1.1.17 Field: A commutative division ring R is called a *field*. Or, equivalently, if the set of non-zero elements of R is an abelian group

with respect to the multiplication in R .
The rings $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are examples of fields.

1.1.18 Remarks: 1. *Every field is a division ring and every division ring is an integral domain. But not conversely.*

To see that every division ring is an integral domain, let R be a division ring. Note that $R \neq \{0\}$. Let R have zero divisors, i.e., $\exists a, b (\neq 0) \in R$ such that $a \cdot b = 0$. Since R is a division ring and $a \neq 0$, a has its inverse a^{-1} in R and we have

$$a^{-1}(ab) = a^{-1}(0) = 0, \text{ i.e., } b = a^{-1}(ab) = 0$$

which is a contradiction.

The ring of integers $\mathbb{Z}$ is an integral domain but not a field since the only invertible elements in $\mathbb{Z}$ are ± 1 .

A division ring need not be a field. For example, consider $R = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \mid u, v \in \mathbb{C} \right\}$. Here 'bar' denotes the complex conjugation. Clearly R is a ring with respect to matrix addition and multiplication. Every non-zero element $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ has an inverse $\frac{1}{(u\bar{u}+v\bar{v})} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix}$. Hence R is a division ring but not a field because matrix multiplication is not commutative for these matrices.

2. *Multiplicative cancellation of non-zero elements holds in an integral domain R , i.e., if $a \neq 0$, then $ax = ay$ or $xa = ya \Rightarrow x = y$.*

Let $a (\neq 0) \in R$ and $ax = ay$ for any $x, y \in R$. Then $ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x - y) = 0$. Since $a \neq 0$ and R is an integral domain, we have $x - y = 0 \Rightarrow x = y$. Similarly $xa = ya \Rightarrow x = y$ for $a \neq 0$.

3. *The only idempotents in an integral domain with 1 are 0 and 1.*

Let $a \in R$ be an idempotent. Then we have $a - a^2 = 0$, i.e., $a(1 - a) = 0$. Since R is an integral domain, we should have either $a = 0$ or $1 - a = 0$, i.e., $a = 0$ or $a = 1$, as required.

1.1.19 Real quaternions: Let $\mathbb{H}_{\mathbb{R}} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4$ be the 4-dimensional real vector space. Elements of $\mathbb{H}_{\mathbb{R}}$ are called *real quaternions*. In $\mathbb{H}_{\mathbb{R}}$, define addition and multiplication as follows.

Addition : *Addition is coordinatewise.*

Multiplication: Let $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$ and $k = (0, 0, 0, 1)$ be the unit vectors in $\mathbb{R}^4$ along the coordinate axes. Then every element $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ is uniquely written as $x_1 + x_2i + x_3j + x_4k$ with $x_i \in \mathbb{R}$. Let $v = a + bi + cj + dk$, $w = x + yi + zj + tk$ where $a, b, c, d, x, y, z, t \in \mathbb{R}$. Then the product $v \cdot w$ is defined as follows.

$$\begin{aligned} v \cdot w &= (a + bi + cj + dk) \cdot (x + yi + zj + tk) \\ &= (ax - by - cz - dt) + (ay + bx + ct - dz)i \\ &\quad + (az + cx + dy - bt)j + (at + dx + bz - cy)k \end{aligned}$$

Multiplication table for i, j, k :

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

With respect to this addition and multiplication, the real quaternions form a ring which is not commutative because $ij = k = -ji$.

This $\mathbb{H}_{\mathbb{R}}$ is a division ring because the vector $1 = (1, 0, 0, 0)$ is the unity element and given $v = (x_1, x_2, x_3, x_4) \neq 0$, we have $\sum_{i=1}^4 x_i^2 \neq 0$ and hence we find that the inverse of v is

$$v^{-1} = \left[1 / \left(\sum_{i=1}^4 x_i^2 \right) \right] (x_1, -x_2, -x_3, -x_4) \in \mathbb{H}_{\mathbb{R}}.$$

1.1.20 Remarks: 1. The above construction is valid for any subfield K of $\mathbb{R}$. Then what we get is called the division ring $\mathbb{H}_K$ of quaternions over K . In particular, when $K = \mathbb{Q}$, $\mathbb{H}_{\mathbb{Q}} = \mathbb{Q}[i, j, k]$ is called *rational quaternions* and when $K = \mathbb{R}$, $\mathbb{H}_{\mathbb{R}} = \mathbb{R}[i, j, k]$ is called the *real quaternions*, etc.

2. Given $v = (x_1, x_2, x_3, x_4) \in \mathbb{R}^4$, the vector $\bar{v} = (x_1, -x_2, -x_3, -x_4)$ is called the *conjugate* of v . We have

$$\begin{aligned} v\bar{v} &= (x_1, x_2, x_3, x_4)(x_1, -x_2, -x_3, -x_4) = (x_1^2 + x_2^2 + x_3^2 + x_4^2, 0, 0, 0) \\ &= \left(\sum_{i=1}^4 x_i^2 \right) (1, 0, 0, 0) = \left(\sum_{i=1}^4 x_i^2 \right) 1_{\mathbb{H}_{\mathbb{R}}}. \end{aligned}$$

Thus $v^{-1} = \bar{v} / (x_1^2 + x_2^2 + x_3^2 + x_4^2)$. The scalar $\sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$ is called the *norm* of the quaternion $v = (x_1, x_2, x_3, x_4)$.

3. The division ring of rational quaternions is a subdivision ring of the real quaternions. In fact, $\mathbb{H}_{\mathbf{Q}} \subseteq \mathbb{H}_K$ for any subfield K of $\mathbb{R}$.

4. See (1.8.5) below, for integral quaternions.

1.1.21 Remarks: It is a natural question to ask if one can define a multiplication $(\cdot)$ on $(\mathbb{R}^n, +)$ so that $(\mathbb{R}^n, +, \cdot)$ is a division ring for a positive integer ' n ', where $+$ stands for the usual addition of vectors. We know the following.

1. For $n = 1$, $\mathbb{R}$ is a field under the usual addition and multiplication of real numbers.

2. For $n = 2$, $\mathbb{C} = \mathbb{R}^2$ is a field under the usual addition and multiplication of complex numbers.

3. For $n = 4$, $\mathbb{H}_{\mathbb{R}} = \mathbb{R}^4$ is a division ring under the usual addition and multiplication of real quaternions (as above).

However, it is a well-known (non-trivial) *classical theorem* that for $n \neq 1, 2$ or 4 , it is not possible to define multiplication on $(\mathbb{R}^n, +)$ to make $(\mathbb{R}^n, +, \cdot)$ into a division ring. Furthermore, for $n = 1, 2$ or 4 , the only possible multiplications are the familiar ones as in (1), (2) and (3) above. Finally, for $n = 8$, $(\mathbb{R}^8, +)$ can be made into a non-associative non-commutative division ring, called the ring of *Cayley numbers*. (See "The four and eight square problem and division algebras" by C.W. Curtis in "STUDIES IN MODERN ALGEBRA" (edited by A.A. Albert), Vol. 2, Studies in Mathematics, Published by the Mathematical Association of America, Prentice Hall, Englewood Cliffs, (1963).) ■

1.2 Rings of Continuous Functions

An exposure to a first course in Elementary Topology is assumed in this section. Others can skip this section except for the Examples 4 and 5 of (1.2.2) below.

1.2.1 Definition: Let X be a topological space and $R = C(X, \mathbb{R})$, the set of real valued continuous maps on X . Then R is a commutative ring with unity under the pointwise addition and multiplication of

maps. This is called the ring of *continuous functions* on X .

We have $f, g \in \mathcal{C}(X, \mathbb{R}) \Rightarrow (f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in X$.

The *additive identity* is the constant map 0_R , taking the value zero everywhere. The *unity element* is the constant map (1_R) taking the value 1 everywhere.

This ring is commutative, i.e., $f(x)g(x) = g(x)f(x)$, $\forall x \in X$ and $f, g \in R$ because $f(x)$ and $g(x)$ are real numbers and multiplication in $\mathbb{R}$ is commutative.

The map $-f : X \rightarrow \mathbb{R}$, $x \mapsto -f(x)$, is the additive inverse of $f \in R$.

In general, R is not an integral domain.

1.2.2 Examples: 1. Let X be an indiscrete space. The only continuous maps are constant maps from $X \rightarrow \mathbb{R}$ and hence the ring R can be identified with the field $\mathbb{R}$.

2. Let X be a discrete space with at least two elements. In this case we know that every map from X to $\mathbb{R}$ is continuous. Consider any $x_0 \in X$ and let $Y = X - \{x_0\} (\neq \emptyset)$. Define $f, g : X \rightarrow \mathbb{R}$ as

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{if } x \neq x_0 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 0 & \text{if } x = x_0 \\ 1 & \text{if } x \neq x_0 \end{cases}$$

Both f and g are non-zero continuous maps. But their product fg is the constant map zero. Thus R has non-trivial zero divisors and therefore it is not an integral domain.

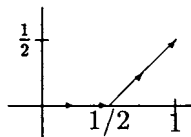
3. Let X be a disconnected space, say $X = A \cup_{\text{disj}} B$ where A and B are non-trivial open subsets of X . Then consider the functions $f, g : X \rightarrow \mathbb{R}$ defined as follows.

$$f(x) = \begin{cases} 0 & \text{if } x \in A \\ 1 & \text{if } x \in B \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in B \end{cases}$$

It is clear that $f|_A : A \rightarrow \mathbb{R}$ and $f|_B : B \rightarrow \mathbb{R}$ are continuous. It is easy to check that f is continuous. Similarly $g : X \rightarrow \mathbb{R}$ is also continuous. Now, we have $fg \equiv 0$ with $f \not\equiv 0$ and $g \not\equiv 0$. Thus R is not an integral domain.

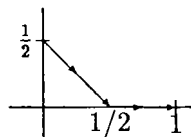
4. Let $R = C([0, 1], \mathbb{R}) = \{f : [0, 1] \rightarrow \mathbb{R} \mid f \text{ continuous}\}$. This is not an integral domain even though $X = [0, 1]$ is a connected space. For, let $f, g : [0, 1] \rightarrow \mathbb{R}$ be defined as follows.

$$f(x) = \begin{cases} 0 & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2} & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Graph of f

and

$$g(x) = \begin{cases} \frac{1}{2} - x & 0 \leq x \leq \frac{1}{2} \\ 0 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Graph of g

Both f and g are continuous and $fg \equiv 0$ but $f \not\equiv 0$ and $g \not\equiv 0$.

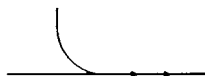
5. Let $R = C([0, 1], \mathbb{R})$ and $S_1 = C^1([0, 1], \mathbb{R})$ be the ring of all continuously differentiable functions. Then S_1 is a subring of R with $1_S = 1_R = 1$. We know that R is not an integral domain. The subring S_1 is also not an integral domain. For, define $f, g : [0, 1] \rightarrow \mathbb{R}$ as follows.

$$f(x) = \begin{cases} 0 & 0 \leq x \leq \frac{1}{2} \\ (x - \frac{1}{2})^2 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Graph of f

and

$$g(x) = \begin{cases} (\frac{1}{2} - x)^2 & 0 \leq x \leq \frac{1}{2} \\ 0 & \frac{1}{2} \leq x \leq 1 \end{cases}$$

Graph of g

We find that both f and g are continuously differentiable and $fg \equiv 0$ but $f \not\equiv 0$ and $g \not\equiv 0$.

Note: 1. Let $\mathbb{Z}^+$ be the set of all non-negative integers. For each $n \in \mathbb{Z}^+$, let $S_n = C^n([0, 1], \mathbb{R})$ be the ring of all continuously n -times differentiable functions where $S_0 = C([0, 1], \mathbb{R})$. It is obvious that S_n is a subring of S_{n-1} . It can be seen that S_n is *not* an integral domain (for all n).

2. Recall that an infinitely differentiable function is also called a *smooth* function. The set of all smooth functions is obviously a ring and it is simply $C^\infty([0, 1], \mathbb{R}) = \bigcap_{n=0}^\infty S_n$. We have a strictly descending chain of rings *none* of which is an integral domain, namely,

$$R = S_0 \supset S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} \supset \cdots \supset C^\infty([0, 1], \mathbb{R}).$$

Nevertheless, see Ex.(1.13.24) below, for an example of a subring of $C^\infty([0, 1], \mathbb{R})$ which is an integral domain. (It is not the obvious field of all constant functions.)

1.2.3 Proposition: *Let $R = C(X, \mathbb{R})$. Then we have the following.*

1. *R has no non-trivial nilpotent elements and*

2. *R has no non-trivial idempotents if and only if X is connected.*

Proof: Suppose $f \in R$ is nilpotent. Then there is an $n \geq 1$ such that $f^n \equiv 0$. This means $[f(x)]^n = 0$, $\forall x \in X$ and hence $f(x) = 0$, $\forall x \in X$, i.e., $f \equiv 0$, as required.

Suppose $g \in R$ is an idempotent. Then $g(x)^2 = g(x)$ and so $g(x) = 0$ or $g(x) = 1$, $\forall x \in X$, i.e., $g(X) \subseteq \{0, 1\}$. It is clear that g is non-trivial if and only if $g(X) = \{0, 1\}$.

If X is not connected, then R has a non-trivial idempotent by Example (1.2.2)(3) above. On the other hand, if X is connected, then the continuous image $g(X)$ of X is a connected subset of $\mathbb{R}$. But it is well-known that the only connected subsets of $\mathbb{R}$ are intervals and so $g(X) \neq \{0, 1\}$, i.e., $g(X) = \{0\}$ or $g(X) = \{1\}$ which means that g is a trivial idempotent, as required. ■

1.3 Matrix Rings

1.3.1 Ring of matrices: Let R be any ring and $n \geq 1$ be an integer. Let $S = M_n(R) = \{(a_{ij}) | a_{ij} \in R, 1 \leq i, j \leq n\}$ be the set of all $n \times n$ matrices with entries in R where

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}.$$

Exactly the same way as for the matrices over $\mathbb{R}$, we define addition and multiplication in S as

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \quad \text{and} \quad (a_{ij}) \cdot (b_{ij}) = (c_{ij})$$

where $c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}$, $\forall i, j, 1 \leq i, j \leq n$. It is easy to verify that S is a ring. This is called the *matrix ring of order n* over R .

This ring has 1 if and only if R has 1. If R has 1, then

$$1 = 1_S = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

called the $n \times n$ identity matrix and is denoted by $I_{n \times n}$ or simply I_n .

If a matrix (a_{ij}) is such that $a_{ij} = 0$, $\forall i \neq j$, we call it a *diagonal* matrix and write it as $\text{diag}(a_{11}, \dots, a_{nn})$. If a diagonal matrix is such that all of its diagonal entries are equal, say equal to a , then we call it a *scalar* matrix defined by a . We have $\text{diag}(a, \dots, a) = aI_n$ if R has 1 and $I_n = \text{diag}(1, \dots, 1)$.

1.3.2 Remark: If R is non-commutative, S is not commutative because if $ab \neq ba$ for some $a, b \in R$, then we have

$$\begin{aligned} \text{diag}(a, \dots, a) \cdot \text{diag}(b, \dots, b) &= \text{diag}(ab, \dots, ab) \\ &\neq \text{diag}(ba, \dots, ba) = \text{diag}(b, \dots, b) \cdot \text{diag}(a, \dots, a). \end{aligned}$$

In case R has 1, the above calculations take the simple form that

$$(aI_n) \cdot (bI_n) = abI_n \neq baI_n = (bI_n) \cdot (aI_n).$$

Notation: For $a \in R$, aE_{ij} stands for the matrix with a at the $(i, j)^{\text{th}}$ place and zeros elsewhere, $1 \leq i, j \leq n$. In case R has 1, aE_{ij} is nothing but $a \cdot E_{ij}$, where E_{ij} is the matrix with 1 at the $(i, j)^{\text{th}}$ place and zeros elsewhere. Note that we have

$$aE_{ij} bE_{kl} = \begin{cases} abE_{il} & \text{if } j = k, \\ 0 & \text{otherwise,} \end{cases} \quad \forall a, b \in R.$$

1.3.3 Remark: Even if R is commutative, S need not be commutative (unless R is a trivial ring (1.1.12)).

Let $a, b \in R$ be such that $ab \neq 0$. Now consider the matrix $A = aE_{12}$, and $B = bE_{11}$. Then $AB = aE_{12}bE_{11} = abE_{12}E_{11} = 0$ whereas

$$BA = bE_{11}aE_{12} = baE_{11}E_{12} = baE_{12} = abE_{12} \neq 0.$$

1.3.4 Remark: Given $A = (a_{ij}) \in M_n(R)$, A can be written *uniquely* as $A = \sum_{i,j=1}^n a_{ij}E_{ij}$. If $B = \sum_{k,l=1}^n b_{kl}E_{kl}$, then

$$AB = \sum_{i,j,k,l=1}^n (a_{ij}b_{kl})(E_{ij}E_{kl}) = \sum_{i,l=1}^n \left(\sum_{k=1}^n a_{ik}b_{kl} \right) E_{il} = \sum_{i,l=1}^n (AB)_{il} E_{il}.$$

1.3.5 Proposition: If R is commutative with 1, then $A \in M_n(R)$ is a unit if and only if its determinant, $\det(A)$ is a unit in R .

Proof: Suppose that $A \in M_n(R)$ is a unit. Then there is a non-zero $B \in M_n(R)$ such that $AB = BA = I_n$. Taking determinants we get that $\det(AB) = \det(BA) = \det(I_n) = 1$. But $\det(AB) = \det(A)\det(B)$. Hence $\det(A)$ is a unit in R .

Conversely, suppose that $A \in M_n(R)$ is such that $\det(A)$ is a unit in R . Then recall that we have $A(\text{adj}A) = (\text{adj}A)A = \det(A)I_n$ where $\text{adj}(A)$ is the *adjoint* of the matrix A , i.e., the transpose of the matrix (A_{ij}) of the *cofactors* of A . (Recall that the cofactor A_{ij} is $(-1)^{i+j}$ times the determinant of the submatrix of A obtained by deleting the i^{th} row and j^{th} column, $1 \leq i, j \leq n$.) Since $\det(A)$ is a unit in R , we see that $A^{-1} = (\det A)^{-1}(\text{adj}A)$, as required. $\diamond$

1.3.6 Remarks: 1. If R is a field, then $A \in M_n(R)$ is a unit if and only if $\det(A) \neq 0$ in R .

2. Determinant of a matrix $A \in M_n(R)$ is not defined if R is not commutative. Consequently, in this case, there is no natural criterion for characterising units in $M_n(R)$.

3. The ring $M_n(R)$ has non-trivial zero-divisors, nilpotent and idempotent elements for $n \geq 2$ even if R has none of them. (It is easy to construct examples.) $\blacksquare$

1.4 Polynomial Rings

1.4.1 Ring of polynomials: Let R be a ring. Let X be an *indeterminate* or a *variable* over R . (See Exs.(1.13.39) and (1.13.40) below, for a way to interpret the variable X .)

Let $R[X]$ be the set of all *formal polynomial expressions* in X with coefficients in R , i.e.,

$$R[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_rX^r \mid a_i \in R, r \in \mathbb{Z}^+\}.$$

Convention: $X^0 = 1 \in R$, if R has 1.

Equality in $R[X]$: Let $p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_rX^r$ and $q(X) = b_0 + b_1X + b_2X^2 + \cdots + b_sX^s$ be in $R[X]$. Then $p(X) = q(X)$ if and only if $r = s$ and $a_i = b_i$, $\forall i$, $0 \leq i \leq r$. In particular, $a_0 + a_1X + a_2X^2 + \cdots + a_rX^r = 0$ if and only if $a_i = 0$, $\forall i$.

Addition and multiplication in $R[X]$: Let $p(X)$ and $q(X)$ be as above. (We may assume $r \leq s$.) Define

$$\begin{aligned} p(X) + q(X) &= (a_0 + a_1X + a_2X^2 + \cdots + a_rX^r) + (b_0 + b_1X + b_2X^2 + \cdots + b_sX^s) \\ &= (a_0 + b_0) + (a_1 + b_1)X^1 + (a_2 + b_2)X^2 + \cdots + (a_r + b_r)X^r \\ &\quad + b_{r+1}X^{r+1} + \cdots + b_sX^s \quad \text{and} \end{aligned}$$

$$\begin{aligned} p(X)q(X) &= (a_0 + a_1X + a_2X^2 + \cdots + a_rX^r)(b_0 + b_1X + b_2X^2 + \cdots + b_sX^s) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 \\ &\quad + \cdots + (a_0b_i + a_1b_{i-1} + \cdots + a_ib_0)X^i + \cdots + (a_rb_s)X^{r+s}. \end{aligned}$$

It can be checked easily that the set $R[X]$ is a ring under the above operations. Elements of this ring are called *polynomials* in the variable X with coefficients in R .

1.4.2 Definitions: If $p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_rX^r \neq 0$, we may assume that $a_r \neq 0$. Then a_r is called the *leading coefficient* of $p(X)$ and r is called the *degree* of $p(X)$. The term a_0 is called the *constant term* of $p(X)$. A polynomial whose constant term is zero is called a polynomial *without* constant term. If R has 1, a non-zero polynomial whose leading coefficient is 1 is called a *monic polynomial*.

Note: 1. No degree is assigned to the zero polynomial.

2. The constant 1 is the unique monic polynomial of degree zero. The set of all monic polynomials of degree one is $\{a_0 + X \mid a_0 \in R\}$ which is bijective with R as a set. Likewise, the set of all monic polynomials of degree two is bijective with $R \times R$ as a set and so on.

1.4.3 Definitions: Elements of R are called *constants*. Polynomials of *degree zero* are precisely the non-zero constants. Polynomials of degree 1, 2, 3, 4, 5, ... are called *linear, quadratic, cubic, biquadratic, quintic, ...* etc. ■

1.5 Power Series Rings

1.5.1 Ring of power series: Given a ring R , let $R[[X]]$ be the formal power series with coefficients in R , i.e.,

$$R[[X]] = \{a_0 + a_1X + a_2X^2 + \dots \mid a_i \in R\}.$$

Equality of power series: Let $p(X) = a_0 + a_1X + a_2X^2 + \dots$ and $q(X) = b_0 + b_1X + b_2X^2 + \dots$ be in $R[[X]]$. Then $p(X) = q(X)$ if and only if $a_r = b_r$, $\forall r \in \mathbb{Z}^+$.

Addition and Multiplication of power series: Let $p(X)$ and $q(X)$ be as above. Then we define

$$\begin{aligned} p(X) + q(X) &= (a_0 + a_1X + a_2X^2 + \dots) + (b_0 + b_1X + b_2X^2 + \dots) \\ &= (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + \dots \quad \text{and} \end{aligned}$$

$$\begin{aligned} p(X)q(X) &= (a_0 + a_1X + a_2X^2 + \dots)(b_0 + b_1X + b_2X^2 + \dots) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \dots \\ &\quad + (a_0b_i + a_1b_{i-1} + \dots + a_ib_0)X^i + \dots \end{aligned}$$

Under these operations $R[[X]]$ is a ring, called the ring of (*formal*) *power series* over R in the variable X .

1.5.2 Definitions: The term a_0 of $a_0 + a_1X + a_2X^2 + \dots$, is called the *constant term* of the power series. If a power series is of the form $f(X) = a_nX^n + a_{n+1}X^{n+1} + \dots$ with $a_n \neq 0$, $n \geq 0$, (i.e., $a_i = 0$ for

$0 \leq i \leq n-1$), then n is called the *order* of the power series and is denoted by $\text{ord}(f(X))$. ■

1.6 Laurent Rings

1.6.1 Laurent polynomials: Given a ring R , a formal expression of the form $a_{-n}X^{-n} + a_{-n+1}X^{-n+1} + \cdots + a_{-1}X^{-1} + a_0 + a_1X + \cdots + a_mX^m$, where $a_i \in R$ and $n, m \in \mathbb{Z}^+$, is called a *Laurent polynomial* in the variable X with coefficients in R .

The set of all Laurent polynomials is denoted by $R[X, X^{-1}]$ or $R[X^{\pm 1}]$.

1.6.2 Laurent series: Given a ring R , a formal expression of the form $a_{-n}X^{-n} + a_{-n+1}X^{-n+1} + \cdots + a_{-1}X^{-1} + a_0 + a_1X + \cdots$, where $a_i \in R$ and $n \in \mathbb{Z}^+$ is called a *Laurent series* in the variable X with coefficients in R . In this expression $a_{-n}X^{-n} + a_{-n+1}X^{-n+1} + \cdots + a_{-1}X^{-1}$ is called the *principal part* and $a_0 + a_1X + \cdots$ is called the *power series part*. The set of all Laurent series is denoted by $R < X >$. We have

$R < X > = \{a_{-n}X^{-n} + \cdots + a_{-1}X^{-1} + a_0 + a_1X + \cdots \mid a_i \in R, n \in \mathbb{Z}^+\}$. Equality, addition and multiplication for the Laurent series follow the same rule as for the power series. For example, product of two Laurent series is given by

$$\left(\sum_{\substack{n=-m \\ m \geq 0 \text{ fixed}}}^{\infty} a_n X^n \right) \left(\sum_{\substack{r=-l \\ l \geq 0 \text{ fixed}}}^{\infty} b_r X^r \right) = \sum_{s=-(m+l)}^{\infty} c_s X^s.$$

where

$$c_s = \sum_{\substack{n+r=s \\ n, r}} a_n b_r.$$

Note that c_s is a finite sum of elements in R for all s . It is clear that $R[X^{\pm 1}]$ is a subring of $R < X >$. In fact, we have a strictly ascending sequence of subrings, namely, $R \subset R[X] \subset R[X^{\pm 1}] \subset R < X >$ and $R \subset R[X] \subset R[[X]] \subset R < X >$.

Properties of $R[X]$, $R[X^{\pm 1}]$, $R[[X]]$, $R < X >$ relative to R

1.6.3 Theorem: *Let R be an integral domain with 1.*

1. *A polynomial $p(X) = a_0 + a_1X + a_2X^2 + \cdots + a_rX^r$ is a unit in $R[X]$ $\iff a_0$ is a unit in R and $r = 0$. (See also Ex.(1.13.19) and (2.7.6) below.)*
2. *A Laurent polynomial $f(X)$ is a unit in $R[X^{\pm 1}]$ $\iff f(X) = aX^r$ for some unit $a \in R$ and $r \in \mathbb{Z}$.*
3. *A power series $a_0 + a_1X + \cdots$ is a unit in $R[[X]]$ $\iff a_0$ is a unit in R .*
4. *A Laurent series $a_{-n}X^{-n} + \cdots + a_{-1}X^{-1} + a_0 + a_1X + \cdots$ with $a_{-n} \neq 0$, is a unit in $R < X >$ $\iff a_{-n}$ is a unit in R .*

Proof: Easy verification. ◇

1.6.4 Remarks: For convenience, let S stand for one of the four rings $R[X]$, $R[X^{\pm 1}]$, $R[[X]]$ or $R < X >$. Then we have

1. R is commutative $\iff S$ is commutative,
2. R has unity $\iff S$ has unity and the unities are the same,
3. R is an integral domain $\iff S$ is so and
4. R is a division ring $\iff R < X >$ is a division ring. (This is a corollary to Theorem (1.6.3) above.)

Caution: *The rings $R[X]$, $R[X^{\pm 1}]$ and $R[[X]]$ are never division rings or fields whatever be R .* ■

1.7 Boolean Rings

1.7.1 Boolean ring: A ring R in which every element is an idempotent is called a *Boolean ring*.

1.7.2 Example: Let X be any non-empty set and $\mathcal{P}(X)$ be the *power set* of X , i.e., set of all subsets of X . Define addition and multiplication on $\mathcal{P}(X)$ as follows.

Addition is the *symmetric difference* of sets, namely,

$$A + B = A \triangle B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A).$$

Multiplication is the *intersection* of sets, i.e., $AB = A \cap B$.

Under these operations, $\mathcal{P}(X)$ is a commutative ring with unity and it is a Boolean ring.

1.7.3 Remarks: 1. $\wedge$ subring of a Boolean ring is obviously Boolean. It is of interest to know that essentially $\mathcal{P}(X)$ is the *only* Boolean ring, i.e., the *Universal Boolean ring*, in the sense that
“Every Boolean ring is a subring of $\mathcal{P}(X)$ for some X .”

This is called the *structure theorem for Boolean rings*.

(See “THEORY OF RINGS” by N. H. McCoy, Chelsea, New York (1973).)

2. See (1.9.3) below, for an apparently different looking example of a Boolean ring. See also (3.1.8) below.

3. A Boolean ring need not have unity. For example, if X is an *infinite* set, then the subring of $\mathcal{P}(X)$ consisting of all *finite* subsets of X has no unity. ■

1.8 Some Special Rings

1.8.1 Integers modulo n : For a fixed positive integer n , let $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, be the set of remainders of integers modulo n . Under the addition and multiplication modulo n , $\mathbb{Z}_n$ is a ring, called the ring of *integers modulo n* .

It is obvious that $\mathbb{Z}_n$ is a finite commutative ring with unity ($= \bar{1}$) having exactly n elements. The additive group $(\mathbb{Z}_n, +)$ is a cyclic group of order n generated by $\bar{1}$. Now we have the following.

1.8.2 Theorem: 1. $\mathbb{Z}_n = (0) \Leftrightarrow n = 1$. (Assume therefore $n \geq 2$.)

2. $\bar{x} \in \mathbb{Z}_n$ is a unit $\Leftrightarrow \bar{x}$ is not a zero-divisor $\Leftrightarrow x$ is coprime to n . Consequently, the set of units in $\mathbb{Z}_n$ is a group of order $\varphi(n)$ where φ is the Euler's totient function, i.e., $\varphi(n)$ is the number of positive integers less than n and coprime to n .

3. $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow n$ is a prime $\Leftrightarrow \mathbb{Z}_n$ is a field.

4. $\mathbb{Z}_n$ has no non-trivial nilpotent elements $\Leftrightarrow n$ is square free.

5. Non-units in $\mathbb{Z}_n$ form an additive subgroup of $(\mathbb{Z}_n, +) \Leftrightarrow n$ is a power of a prime.

6. If n is a prime, then $x^n = x, \forall x \in \mathbb{Z}_n$.

Proof: Easy verification. See also (2.7.4)–(2.7.6) below. $\diamond$

1.8.3 Gaussian integers: Consider the subset of $\mathbb{C}$ given by $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ where $i \in \mathbb{C}$ is such that $i^2 = -1$.

This is the set of integral points in the Euclidean plane, i.e., the set of points whose both coordinates are integers. It is easy to see that $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ called the ring of *Gaussian integers* where addition and multiplication are given by

$$\begin{aligned}(a + ib) + (c + id) &= (a + c) + i(b + d) \text{ and} \\ (a + ib) \cdot (c + id) &= (ac - bd) + i(ad + bc).\end{aligned}$$

The unity of $\mathbb{Z}[i]$ is the same as that of $\mathbb{C}$. The group of units in $\mathbb{Z}[i]$ is the cyclic group $\{\pm 1, \pm i\}$ of order 4.

1.8.4 Gaussian numbers: Consider the subset of $\mathbb{C}$ given by $\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$. It can be seen easily that $\mathbb{Q}[i]$ is a subfield of $\mathbb{C}$ called the field of *Gaussian numbers*.

We have $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{Q}[i] \subset \mathbb{R}[i] = \mathbb{C}$, a sequence of subrings of $\mathbb{C}$ where the first two are not fields whereas the last two are fields.

1.8.5 Integral quaternions: The set given by

$$\mathbb{Z}[i, j, k] = \{a + ib + jc + kd \mid a, b, c, d \in \mathbb{Z}\}$$

is a subring of $\mathbb{Q}[i, j, k] \subseteq \mathbb{H}_{\mathbb{Q}}$, called the ring of *integral quaternions*. (See (1.1.20) above, for other types of quaternions.) Units in $\mathbb{Z}[i, j, k]$ is given by $\mathcal{U}(\mathbb{Z}[i, j, k]) = \{\pm 1, \pm i, \pm j, \pm k\}$ which is the quaternion group of order 8 whose multiplication table is as in (1.1.19) above.

1.8.6 A class of subrings of $\mathbb{C}$: Let

$$\mathbb{Z}[\sqrt{-2}] = \mathbb{Z}[i\sqrt{2}] = \{a + i\sqrt{2}b \mid a, b \in \mathbb{Z}\}.$$

This is a subring of $\mathbb{C}$. More generally, for an integer d such that $\sqrt{|d|}$ is not an integer, let

$$\mathbb{Z}[\sqrt{d}] = \begin{cases} \{a + i\sqrt{|d|}b \mid a, b \in \mathbb{Z}\} & \text{if } d < 0, \\ \{a + \sqrt{d}b \mid a, b \in \mathbb{Z}\} & \text{if } d > 0. \end{cases}$$

This is a subring of $\mathbb{C}$. It is a subring of $\mathbb{R}$ if and only if $d > 0$.

1.8.7 p -adic integers: Let p be a positive prime number. Define

$$\mathbb{Q}^p = \{\frac{a}{b} \in \mathbb{Q} \mid b \neq 0, a, b \in \mathbb{Z}, p \nmid b\}.$$

This is a subring of $\mathbb{Q}$, called the ring of *p-adic integers*.

1.8.8 Complex entire functions: (For those who have studied a little of complex analytic functions in one variable). Let

$$\mathbb{C}\{z\} = \{\sum_{i=0}^{\infty} a_i z^i \mid a_i \in \mathbb{C}, \sum_{i=0}^{\infty} a_i z^i \text{ is convergent, } \forall z \in \mathbb{C}\}.$$

Since the addition and multiplication in $\mathbb{C}\{z\}$ are the same as for formal power series, this is a subring of $\mathbb{C}[[z]]$, called the ring of *Complex entire functions*. ■

1.9 Direct Products

1.9.1 Direct product: Let R and S be two rings. Let $T = R \times S$ be the Cartesian product of R and S . Define addition and multiplication on T coordinatewise, i.e.,

$$(a, x) + (b, y) = (a + b, x + y) \quad \text{and} \quad (a, x)(b, y) = (ab, xy).$$

Under these operations, T is a ring called the *direct product* or the *Cartesian product* of R and S .

1.9.2 Remarks: It is easy to check the following.

1. T is a ring with 1 if and only if both R and S are with 1 and $1_T = (1_R, 1_S)$.
2. T is commutative if and only if both R and S are commutative.
3. Even if R and S are fields, T is not even an integral domain.

More generally, if $\{R_\alpha\}_{\alpha \in I}$ is a non-void family of rings, then the direct product $T = \prod_{\alpha \in I} R_\alpha$ is a ring under coordinatewise addition and multiplication.

Note: In case $R_\alpha = R$, $\forall \alpha \in I$, we write $T = \prod_I R$ or $T = R^{|I|}$. If I is finite, then $T = \prod_I R = R^n = \underbrace{R \times \cdots \times R}_{n \text{ copies}}$ where $n = |I|$ is the

cardinality of I . (See (3.1.8) below.)

1.9.3 Example: If I is any non-empty set (finite or not), then $R = \prod_I \mathbb{Z}_2$ is obviously a Boolean ring with 1. (See (3.1.8) below for the relation between R and the Universal Boolean ring $\mathcal{P}(I)$ as defined in (1.7.3) above.) ■

1.10 Several Variables

1.10.1 Polynomial rings in several variables: Let R be a ring and Y be an indeterminate over $R[X]$. Then $(R[X])[Y]$ is the ring of all polynomials in Y with coefficients in $R[X]$, namely,

$$\begin{aligned}
 (R[X])[Y] &= \{a_0(X) + a_1(X)Y + a_2(X)Y^2 + \cdots + \\
 &\quad \cdots + a_s(X)Y^s \mid a_i(X) \in R[X], 0 \leq i \leq s, s \in \mathbb{Z}^+\} \\
 &= \{(a_{00} + a_{01}X + \cdots + a_{0t_0}X^{t_0}) + (a_{10} + a_{11}X + \cdots \\
 &\quad + a_{1t_1}X^{t_1})Y + \cdots + (a_{s0} + a_{s1}X + \cdots + a_{st_s}X^{t_s})Y^{t_s} \mid \\
 &\quad a_{ij} \in R, 0 \leq i \leq s, 0 \leq j \leq t_i\} \\
 &= \{a_{00} + (a_{01}X + a_{10}Y) + (a_{02}X^2 + a_{11}XY + a_{20}Y^2) + \\
 &\quad + \cdots \mid a_{ij} \in R\} \\
 &= \left\{ \sum_{n \geq 0} \sum_{\substack{i+j=n \\ i, j \geq 0}} a_{ij} X^i Y^j \mid a_{ij} \in R \right\} = \{f(X, Y)\}.
 \end{aligned}$$

Thus $(R[X])[Y]$ is the ring of all polynomials in two “independent” variables X and Y with coefficients in R and is denoted by $R[X, Y]$. We notice that $R[X, Y] = (R[X])[Y] = (R[Y])[X] = R[Y, X]$.

If $X_1, X_2, \dots, X_n$ are finitely many independent indeterminates, we have the polynomial ring in n variables $R[X_1, X_2, \dots, X_n]$.

1.10.2 Remark: Given a non-void family $\{X_i\}_{i \in I}$ of indeterminates, we can construct the polynomial ring $R[\{X_i\}_{i \in I}]$ in a natural way. An element in this ring is seen to be a polynomial in some *finitely many variables* from the family $\{X_i\}_{i \in I}$.

1.10.3 Power series ring in several variables: Exactly as above, we can construct the power series rings in two variables X and Y over a given ring R , which by definition is $(R[[X]])[[Y]]$ and is denoted by $R[[X, Y]]$. We have $R[[X, Y]] = \{\sum_{i+j=0, i, j \geq 0} a_{ij} X^i Y^j \mid a_{ij} \in R\}$. Again if $X_1, X_2, \dots, X_n$ are finitely many indeterminates, we have the power series ring in n variables $R[[X_1, X_2, \dots, X_n]]$.

Note: It is clear that $R \subseteq R[X_1, X_2, \dots, X_n] \subseteq R[[X_1, X_2, \dots, X_n]]$.

1.10.4 Laurent rings: Laurent polynomial and power series in

several variables over a ring R are defined in a similar way and are respectively denoted by $R[X_1^{\pm 1}, \dots, X_n^{\pm 1}]$ and $R \langle X_1, \dots, X_n \rangle$. ■

1.11 Opposite Rings

1.11.1 Opposite ring: Given a ring R , let R^0 , or R^{op} (read as R -opposite), be the same set R . Define addition (+) and multiplication (*) on R^0 as $a + b = a + b$ and $a * b = b \cdot a$, $\forall a, b \in R$.

Under these operations, R^0 is a ring called the *ring opposite* to R or the *opposite ring* of R . It is clear that $(R^0)^0 = R$.

1.11.2 Remarks: 1. $R = R^0$ if and only if R is commutative.

2. R has unity if and only if R^0 has unity. In fact the unity of R is the same as that of R^0 , i.e., $1_R = 1_{R^0}$. ■

1.12 Characteristic of a Ring

1.12.1 Definition: Given a ring R (commutative or not, with or without unity), by the *characteristic* of R , denoted by $\text{Char}(R)$, we mean the least positive integer n such that $na = 0$ for all $a \in R$ if such an n exists; otherwise, it is defined to be 0.

1.12.2 Remarks: 1. $\text{Char}(R) = 1 \iff R = (0)$.

2. $\text{Char}(R) = 0$ if and only if given any positive integer n , there is an $a = a(n)$ (depending on n) such that $na \neq 0$.

3. $\text{Char}(R) = n \neq 0 \iff nx = 0, \forall x \in R$ and for any positive integer $m < n$, there is an $a \in R$ such that $ma \neq 0$.

1.12.3 Proposition: *If a ring R has 1, then we have*

1. $\text{Char}(R) = 0$ if and only if the additive order of 1 in the abelian group $(R, +)$ is infinite.

2. $\text{Char}(R) = n \neq 0$ if and only if the additive order of 1 in $(R, +)$ is finite and is equal to n .

Proof: We note that for any positive integer n , we have $na = 0, \forall a \in R$ if and only if $n1 = n \cdot 1 = 0$. Now the result follows just from the definitions of “ $\text{Char}(R)$ ” and of the “order of 1” in the abelian group $(R, +)$. ◇

1.12.4 Theorem: Let R be a ring with 1. Let $P = \{n1 \mid n \in \mathbb{Z}\}$ be the smallest subring of R containing 1, called the prime subring of R . Then we have the following.

1. $\text{Char}(R) = 0$ if and only if P is infinite.
2. $\text{Char}(R) = n \neq 0$ if and only if P is finite and has exactly n elements, or equivalently, n is the additive order of 1.

Proof: Easy consequence of definitions. $\diamond$

1.12.5 Corollary: The characteristic of an integral domain (in particular, of a division ring or a field) is either 0 or a prime number.

Proof: Let R be an integral domain. Suppose $\text{Char}(R) = n \neq 0$. Note then that $n \geq 2$. Let, if possible, n be not a prime, say $n = rs$ with $r, s < n$. By definition of $\text{Char}(R)$, there are elements $a, b \in R$ such that $ra \neq 0$ and $sb \neq 0$ and so $(ra)(sb) \neq 0$ (since R is a domain). But then, we have $0 = nab = rsab = (ra)(sb) \neq 0$ which is a contradiction. Hence n must be a prime, as required. (In case R has 1, we can take $a = b = 1$ to serve the purpose.) $\diamond$

1.12.6 Remark: Let S be a subring of a ring R . Then $\text{Char}(S) \leq \text{Char}(R)$ and equality holds if both R and S have the same unity. (However, if S has unity but different from that of R , then equality may or may not hold.)

1.12.7 Examples:

1. $\text{Char}(\mathbb{Z}) = \text{Char}(\mathbb{Q}) = \text{Char}(\mathbb{R}) = \text{Char}(\mathbb{C}) = \text{Char}(\mathbb{H}) = 0$.
2. $\text{Char}(M_n(R)) = \text{Char}(R)$.
3. $\text{Char}(R) = \text{Char}(R[X]) = \text{Char}(R[[X]]) = \text{Char}(R \langle X \rangle)$.
4. $\text{Char}(\mathbb{Z}_n) = n$.

1.12.8 Remarks: 1. If R and S are rings, then

$$\text{Char}(R \times S) = \begin{cases} 0 & \text{if } \text{Char}(R) \text{ or } \text{Char}(S) \text{ is } 0, \\ \ell & \text{otherwise.} \end{cases}$$

where $\ell = \text{lcm}(\text{Char}(R), \text{Char}(S))$.

2. If R is a ring with trivial multiplication (1.1.12), then

$$\text{Char}(R) = \begin{cases} 0 & \text{if the additive orders of elements of} \\ & (R, +) \text{ are unbounded,} \\ n & \text{if } n \text{ is the maximum of the additive} \\ & \text{orders of elements of } (R, +). \end{cases}$$

1.12.9 Proposition: *Suppose R is a ring with 1 such that the non-units in R form a subgroup of $(R, +)$, then $\text{Char}(R)$ is either 0 or else a power of a prime.*

Proof: Suppose $\text{Char}(R) = n \neq 0$ and n has two distinct prime divisors, say p and q . Now $p \cdot 1 \neq 0$ and $q \cdot 1 \neq 0$ and both are zero-divisors since $0 = n \cdot 1 = (mpq) \cdot 1 = 0$ for some $m \in \mathbb{N}$, where $n = mpq$. Note that $m \cdot 1 \neq 0$. Thus $p \cdot 1$ and $q \cdot 1$ being non-units, any integral linear combination of them is also a non-unit by assumption. But now we have $pa + qb = 1$ for some $a, b \in \mathbb{Z}$ since p and q are coprime and hence $1 = a(p \cdot 1) + b(q \cdot 1)$ is a non-unit in R which is absurd. This shows that n must be a power of a prime. ■

1.13 Exercises

Unless otherwise stated explicitly, a ring is not necessarily commutative nor has unity.

1. Given a ring R , let $S = \mathbb{Z} \times R$. Show that S is a ring with unity under the coordinatewise addition but the multiplication being $(m, x)(n, y) = (mn, my + nx + xy)$. Identifying R with the subset $\{(0, x) \mid x \in R\}$ of S , verify that R is a subring of S . Thus any ring R can be realised as a subring of a ring S with unity. (Note that if R has 1, $1_R \neq 1_S$.)
2. Show that the intersection of any family of subrings of a ring is a subring.
3. Show that the union of two subrings of a ring is a subring if and only if one of them contains the other as a subset. Give examples of two subrings of $\mathbb{Z}$ whose union is not a subring.
4. Give examples of two zero-divisors in the matrix ring $M_2(\mathbb{Z})$ whose sum is not a zero-divisor. Do the same in $M_n(\mathbb{Z})$, $n \geq 2$.
5. For any ring $R \neq (0)$, show that the variable X is not a zero-divisor in $R[X]$. Do the same in $R[[X]]$ and $R \langle X \rangle$.

6. Suppose R is a commutative ring such that $R[X]$ has a non-trivial zero-divisor $f(X)$. Show that $af(X) = 0$ for some non-zero element $a \in R$. Is the commutativity of R essential?
7. Give an example of a non-trivial commutative ring in which every element is of square 0.
8. Let $R = M_n(\mathbb{Z})$ and N be the subset of all *strictly upper triangular* matrices, i.e., matrices with zeros along and below the main diagonal. Show that
 - N is a subring of R ,
 - N is non-commutative if $n \geq 3$ and
 - $x^n = 0, \forall x \in N$.
9. In any ring R , show that ab is nilpotent if and only if ba is nilpotent. Can one say the same for zero-divisors?
10. Let $R = M_2(\mathbb{Z})$. Give examples of matrices in R having the following properties.
 - $A \in R$ is such that A is a zero-divisor but not nilpotent and
 - $A, B \in R$ are such that both A and B are nilpotent but $A + B$ is not nilpotent. Verify that for such a pair $AB \neq mBA, \forall m \in \mathbb{Z}$.
11. Let a and b be two commuting elements in a ring R , i.e., $ab = ba$. For any positive integer n , prove the binomial expansion that

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i.$$

Hence or otherwise, show that the set of all nilpotent elements in a commutative ring is a subring.

12. Let R be a commutative ring whose characteristic is a prime p . Then show that $(a + b)^p = a^p + b^p$ for all a, b in R . Hence deduce that

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

for all a and b in R and $n \in \mathbb{N}$. Show that this result need not be true if the characteristic is *not* a prime. (Hint: $p \mid \binom{p}{i}$ since p is a prime.)

13. Let $f(X) \in \mathbb{Z}_n[[X]]$ be a non-zero power series all of whose coefficients are nilpotent. Show that $f(X)$ is nilpotent. See Ex.(6.8.9) below, for a similar problem. (Hint: Such an $f(X)$ can be written as a sum

of finitely many suitable nilpotent elements in $\mathbf{Z}_n[[X]]$, by collecting terms with the same coefficient.)

14. Let R be a non-zero ring with 1 and $S = R[[X]]$. Show that S is an uncountable set. In fact, show that S contains uncountably many non-units and at least as many units. (Hint: The set of all sequences formed from a two point set $\{0, 1\}$ is uncountable.)
15. Verify that the linear polynomial $\bar{8}X$ as well as the quadratic polynomial $\bar{8}X^2$ in $\mathbf{Z}_{16}[X]$ has 8 roots (or zeros) in $\mathbf{Z}_{16}$. How is that the number of roots is far larger than the degree of the polynomial? (See Ex.(4.7.6) below.) What does Ex.8 above, say about the set of zeros in $M_n(\mathbf{Z})$ of the polynomial $X^n \in M_n(\mathbf{Z})[X]$?
16. Show that the set of real quaternions which are zeros of $X^2 + 1 \in \mathbf{H}_{\mathbf{R}}[X]$ is uncountable, in fact, it is bijective with the set of points of the unit sphere in $\mathbf{R}^3$.
17. Let R be a Boolean ring with unity. Show that
 - $x = -x$, $\forall x \in R$, i.e., R is of characteristic 2,
 - R is commutative,
 - 0 is the only nilpotent element,
 - 1 is the only unit and
 - R is an integral domain $\iff R = \mathbf{Z}_2$, the field of 2 elements.
 Give an example of a commutative ring with 1 of characteristic 2 which is not a Boolean ring.
18. Let R be a ring with 1. If $x \in R$ is nilpotent, show that $1 + x$ is a unit in R . Can one replace “nilpotent” by “zero-divisor”?
19. Let R be commutative with 1. Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ in $R[X]$ be such that a_0 is a unit and $a_1, \dots, a_n$ are all nilpotent in R . Show that $f(X)$ is a unit in $R[X]$. (See (2.7.6) below, for the converse.)
20. Show that an element in a finite ring with 1 is a unit if it is not a zero-divisor.
(Hint: Look at the set of positive powers of such an element.)
21. Let R be a non-zero ring such that the equation $ax = b$ has a solution in R for all $a, b \in R$ with $a \neq 0$. Show that R must have unity and it is a division ring.

22. Let R be a finite integral domain. Show that R must have unity and that R is a division ring.
23. Let $\mathcal{C}([0, 1], \mathbb{R})$ be the ring of all real-valued continuous functions on the interval $[0, 1]$. Determine its nilpotents and units.
Do the same for $\mathcal{C}^\infty(\mathbb{R})$, the ring of all *smooth* (i.e., infinitely differentiable) functions on the real line. Is this an integral domain?
24. Let $\mathbb{R}\{x\}$ be the ring of all power series with real coefficients each of whose radius of convergence is infinite. Show that this is an integral domain and is a subring of $\mathcal{C}^\infty(\mathbb{R})$, called the ring of *real analytic functions*. (Hints: Term by term differentiation is valid for a convergent power series and it is also the Taylor series at the origin for its sum.)
25. Show that the ring of complex entire functions $\mathbb{C}\{z\}$ (1.8.8) is an integral domain. Determine its units. Is it a field? (See also (3.4.7) below.) (Hint: The zeros of a non-zero entire function are isolated.)
26. Let $R = \mathbb{Z}[i, j, k]$ be the ring of integral quaternions (1.8.5). Show that the units in R is a group of order 8.
27. Show that $R = \mathbb{Z}[\sqrt{-2}]$ has no units other than ± 1 whereas $S = \mathbb{Z}[\sqrt{2}]$ has infinitely many units. Is S a field?
28. Show that the centre of a division ring is a field. Determine the centres of the real and integral quaternions.
29. Let R be a ring and $Z = Z(R)$ be its centre. Show that
 - $Z[X]$ is the centre of $R[X]$ but
 - $M_n(Z)$ is *never* the centre of $M_n(R)$ if $n \geq 2$.
 Determine the centre of $M_n(R)$ for all $n \in \mathbb{N}$.
30. Let $R = \mathbb{Z}[\sqrt{5}]$. For $x = m + n\sqrt{5}$, let $N(x) = |m^2 - 5n^2|$. Then
 - $N(xy) = N(x)N(y)$ for all $x, y \in R$,
 - x is a unit if and only if $N(x) = 1$ and
 - x is a non-zero, non-unit in $R \Rightarrow N(x) \geq 4$.
31. Let R be a ring. For $a, b \in R$, let $[a, b] = ab - ba$, called the *commutator* or the *Lie product* of a and b . Show that $L(R) = (R, +, [,])$ is a *Lie ring* in the following sense.
 - $(L(R), +)$ is an abelian group,
 - $[a, a] = 0, \forall a \in L(R)$,
 - $[a + b, c] = [a, c] + [b, c], \forall a, b, c \in L(R)$

i.e., distributive laws hold and

- $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0, \forall a, b, c \in L(R),$
i.e., *Jacobi identity* holds.

- Define the *characteristic* of a Lie ring L in an obvious way. Show that $[a, b] = -[b, a], \forall a, b \in L$, i.e., L is *anti-commutative*. Is this property equivalent to saying that $[a, a] = 0, \forall a \in L$ if $\text{Char}(L) \neq 2$?
- Give an example of a ring R such that the Lie product $[a, b]$ is *not* associative in the Lie ring $L(R)$ associated to R . (Thus a Lie ring is *not* a ring in the *strict* sense of the word. All the same, it is a *non-associative* (and anti-commutative) ring. It is obvious that a Lie ring $L \neq (0)$ cannot have a multiplicative identity.)
- Define a *Lie subring* of a Lie ring in an obvious way. Show that a subring S of a ring R is a Lie subring of $L(R)$ but not conversely.
- The *centre* of a Lie ring L is defined as

$$Z(L) = \{a \in L \mid [a, b] = 0, \forall b \in L\}.$$

A Lie ring L is said to be *abelian* if the Lie multiplication is *trivial*, i.e., $L = Z(L)$. If $L = L(R) = (R, +, [,])$, show that $Z(R) = Z(L)$, hence R is commutative $\iff L$ is abelian.
- Show that a ring R is commutative if $x^3 = x$ for all $x \in R$.
 (Hints: (i) $(x+x)^3 = 2x \Rightarrow 6x = 0$ and $(x^2-x)^3 = x^2-x \Rightarrow 3x^2 = 3x$, (ii) $(3x)^2 = 3x, (3x)(3y) = (3y)(3x)$ and $3xy = 3yx$ and (iii) $(x \pm y)^3 = x \pm y \Rightarrow 2xy = 2yx$.)
- List all examples of rings R appearing in the text or related ones such that $x^3 = x$ for all $x \in R$. Anything found other than $\mathbb{Z}_3$ or its Cartesian powers?
- Show that a ring R is commutative if one of the following conditions is satisfied, namely,
 - $\forall x \in R, x^n = x$ for some fixed positive integer n or
 - $\forall x \in R, \exists n(x) \in \mathbb{N}$ such that $x^{n(x)} = x$ or
 - $\forall x \in R, x^n - x$ is in the centre of R for some fixed positive integer n or
 - $\forall x \in R, \exists n(x) \in \mathbb{N}$ such that $x^{n(x)} - x$ is in the centre of R .

Remark: Results of the type 38 above, are only of theoretical importance since one does not usually come across examples satisfying such apparently

strong conditions occurring therein. *However, their proofs are by no means easy, in fact, often call for a bunch of ingenious and tricky calculations.* The interested reader may chase some papers of Herstein and Jacobson in the 1950's towards a progressively more and more general and involved results such as the above. (See "NON COMMUTATIVE RINGS" by I. N. Herstein, Carus Mathematical Monograph No. 15, The Mathematical Association of America, Washington, D.C. (1968).)

39. Let R be a ring. Let $\text{Seq}(R)$ denote the set of all sequences $\{a_n\}_{n=0}^{\infty}$ with values in R . Define *addition* and *multiplication* in $\text{Seq}(R)$ by

- **Addition:** $\{a_n\} + \{b_n\} = \{a_n + b_n\}$, $\forall n \in \mathbb{Z}^+$ and
- **Multiplication:** $\{a_n\}\{b_n\} = \{c_n\}$ where $c_n = \sum_{i=0}^n a_i b_{n-i}$, $\forall n \in \mathbb{Z}^+$.

Show that $\text{Seq}(R)$ is a ring with $1 = \{1, 0, 0, 0, \dots, 0, \dots\} \iff R$ has 1. Suppose R has 1. Let $X = \{0, 1, 0, \dots, 0, \dots\}$. Show that

$$X^n = \underbrace{\{0, \dots, 0, 1, 0, \dots\}}_{n \text{ terms}}, \forall n \in \mathbb{Z}^+$$

and consequently, every element $\{a_n\}_{n=0}^{\infty}$ in $\text{Seq}(R)$ can be formally expressed as the power series $\sum_{n=0}^{\infty} a_n X^n$ and the ring $\text{Seq}(R)$ can be naturally identified with the power series ring $R[[X]]$.

40. Let $\text{Pol}(R)$ be the subset of $\text{Seq}(R)$ consisting of all sequences each of whose terms are 0 except for finitely many. Show that $\text{Pol}(R)$ is a subring of $\text{Seq}(R)$ and it is simply the polynomial ring $R[X]$ in the identification of $\text{Seq}(R)$ with $R[[X]]$, as above. ■

1.14 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counter-example if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be.

1. Everything mentioned in this chapter is already known to me.
2. Units in the ring $\mathbb{Z}$ are precisely ± 1 .
3. Units in the ring $M_2(\mathbb{Z})$ are precisely $\pm \text{Id}$.
4. In the ring $\mathbb{Z}[\sqrt{2}]$, $7 - 5\sqrt{2}$ is a unit.
5. The ring $\mathbb{Z}_{10}[X]$ is an integral domain.
6. In a ring with 1, sum of two units is a unit.

7. In the ring $\mathbb{Z}_{2k}$, $\bar{k}$ is an idempotent if k is odd.
8. For $p, n \in \mathbb{N}$ with p a prime, every zero-divisor in $\mathbb{Z}_{p^n}$ is nilpotent.
9. In the ring $\mathbb{Z}_{85}$, every zero-divisor is nilpotent.
10. A ring has no non-trivial nilpotent elements if it has no non-trivial elements of square zero.
11. In the ring $\mathbb{Z}[X]$, $1 - X^3$ is a unit.
12. In the ring $\mathbb{Z}_4[X]$, $\bar{1} - \bar{2}X + \bar{3}X^2$ is a unit.
13. The ring $\mathbb{R} \langle X \rangle$ is a field.
14. The ring $\mathbb{Z}_2[[X]]$ contains uncountably many units as well as uncountably many non-units.
15. In the ring of real valued continuous functions on $\mathbb{R}$, $\log(x)$ is the inverse of $\exp(x)$.
16. The element $1 + i\sqrt{3}$ is a unit in $\mathbb{Z}[i\sqrt{3}]$.
17. The element $\bar{5} + \bar{6}X + \bar{12}X^2$ is a unit in the ring $\mathbb{Z}_{24}[X]$.
18. In the ring of complex entire functions $\cosh z$ is a unit.
19. For a ring R with 1, units in $R =$ units in $R[X]$.
20. The ring $\mathbb{Q}[i]$, is a field.
21. The ring $\mathbb{Q}[\sqrt{2}] \langle X \rangle$ is not a field.
22. In $M_n(\mathbb{Z}_m)$, every element is a zero-divisor or a unit, $\forall m, n \in \mathbb{N}$.
23. A Lie ring (1.13.31) is a ring.
24. An abelian Lie ring is a trivial ring.
25. Every Lie subring of $L(R) = (R, +, [,])$ is a subring of R .
26. A commutative ring R gives rise to an abelian Lie ring $L(R)$.
27. I have worked out all the exercises in this chapter. ■

Chapter 2

Ideals

In this chapter, we study one of the most important aspects of rings, namely, the so called “ideals”. Some of these (i.e., the 2-sided ideals) correspond to the “normal” subgroups in the study of groups. Almost all properties of the 2-sided ideals have their parallels for normal subgroups.

2.1 Definitions

2.1.1 Left ideal: Let R be a ring. A subset I of R is called a *left ideal* of R if

1. I is a subgroup of $(R, +)$, i.e., $a, b \in I \Rightarrow a - b \in I$ and
2. I is closed for arbitrary multiplication on the left by elements in R , i.e., $a \in I$ and $x \in R \Rightarrow xa \in I$.

2.1.2 Right ideal: A subset I of R is called a *right ideal* of R if

1. $a, b \in I \Rightarrow a - b \in I$ and
2. $a \in I$ and $x \in R \Rightarrow ax \in I$.

2.1.3 Two sided ideal: A subset I of R which is both a left ideal and a right ideal is called a *two sided ideal*, i.e.,

1. $a, b \in I \Rightarrow a - b \in I$ and
2. $a \in I$ and $x \in R \Rightarrow$ both $ax \in I$ and $xa \in I$.

2.1.4 Remarks: 1. A subset I is a left/right/2-sided ideal in R implies I is a subring of R . The converse is not true.

For example, the subring of integers is not an ideal in the ring of rational numbers.

2. If R is commutative, the notions of left, right and 2-sided ideals all coincide.

3. If $I \subseteq R$, then I is a left ideal in R if and only if I is a right ideal in R^0 where R^0 is the opposite ring of R (1.11.1).

2.1.5 Examples: 1. R is an ideal in R and is called the *unit ideal*. Note that If R has 1, then R is the only ideal (left/right/2-sided) of R containing 1.

2. (0) is also an ideal in R and is called the *zero ideal*.

The ideals (0) and R are called the *trivial ideals* of R .

3. For a fixed integer n , $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.

4. The sets $I_1 = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R \right\}$ and $I_2 = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in R \right\}$ are respectively right and left ideals of $M_2(R)$ for any ring R . ■

2.2 Maximal Ideals

2.2.1 Maximal left ideal: A left ideal I in R is said to be a *maximal left ideal* in R if

1. $I \neq R$ and
2. for a left ideal J of R , $I \subseteq J \subseteq R \Rightarrow J = I$ or $J = R$, i.e., there are no left ideals strictly in between I and R .

2.2.2 Minimal left ideal: A left ideal I in R is said to be a *minimal left ideal* in R if

1. $I \neq (0)$ and
2. for a left ideal J of R , $(0) \subseteq J \subseteq I \Rightarrow J = (0)$ or $J = I$, i.e., there are no left ideals strictly in between (0) and I .

Remark: *Maximal* (resp. *minimal*) *right/2-sided ideals* are defined in exactly the same way as above.

2.2.3 Maximal subring: A subring S of R is said to be a *maximal subring* of R if

1. $S \neq R$ and
2. for any subring T of R , $S \subseteq T \subseteq R \Rightarrow T = S$ or $T = R$, i.e., there are no subrings strictly in between S and R .

2.2.4 Zorn's Lemma: *A partially ordered non-empty set in which every chain is bounded above (resp. below) has a maximal (resp. minimal) element.*

This is taken as an *axiom* and is very crucial for several proofs below. We shall just explain the terms used.

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

- *Reflexivity:* $x \leq x$, $\forall x \in X$,
- *Anti-Symmetry:* $x \leq y$ and $y \leq x \Rightarrow x = y$ and
- *Transitivity:* $x \leq y$ and $y \leq z \Rightarrow x \leq z$.

A subset Y of X is called a *chain* or *totally ordered* if any two elements of Y are comparable, i.e., given $x, y \in Y$, either $x \leq y$ or $y \leq x$. In particular, given finitely many elements $y_1, \dots, y_n$ in Y , there is a permutation σ of $1, \dots, n$ such that $y_{\sigma(1)} \leq \dots \leq y_{\sigma(n)}$.

A subset A of X is said to be *bounded above* (resp. *below*) if there is an $\alpha \in X$ such that $a \leq \alpha$ (resp. $\alpha \leq a$) for all $a \in A$. Such an α is called an *upper* (resp. a *lower*) *bound* for A . It need not belong to A .

A subset A of X is said to have a *maximal* (resp. *minimal*) *element* if there is an $a \in A$ such that $a \not\leq x$ (resp. $x \not\leq a$) for all $x \in A$, $x \neq a$. Note that a *maximal* (resp. *minimal*) *element* need not exist or it need not be an *upper* (resp. a *lower*) *bound* when exists or it need not be unique.

Zorn's lemma guarantees the existence of maximal left/right/ 2-sided ideals in a ring R with 1, as shown below. (See (2.2.6) and (2.2.7) below, for what happens if R has no unity or if maximal is replaced by minimal.)

2.2.5 Theorem: *If R is a ring with 1 and I is a (left/right/2-sided) ideal in R such that $I \neq R$, then there is a maximal ideal M of the same kind as I such that $I \subseteq M$.*

Proof: The argument being identical for all cases of (left/ right/ 2-sided) ideals, we shall prove it for left ideals for example.

Let $I \neq R$ be a left ideal in R . Consider the family $\mathcal{F} = \mathcal{F}_I$ of all left ideals in R containing I except the unit ideal R , i.e.,

$$\mathcal{F} = \mathcal{F}_I = \{J, \text{ left ideal in } R, J \supseteq I, J \neq R\}.$$

The theorem is *equivalent* to showing that $\mathcal{F}$ has a maximal element with set inclusion as the partial order (i.e., if $J_1, J_2 \in \mathcal{F}$ then say $J_1 \leq J_2$ if $J_1 \subseteq J_2$). Since $I \in \mathcal{F}$, $\mathcal{F} \neq \emptyset$. To apply Zorn's lemma to the family $\mathcal{F}$, we have to verify that every totally ordered subset $\mathcal{T}$ of $\mathcal{F}$ has an upper bound in $\mathcal{F}$. Given such a $\mathcal{T}$, let $T_0 = \cup_{T \in \mathcal{T}} T$. We will show that $T_0 \in \mathcal{F}$ (so that T_0 is obviously an upper bound for $\mathcal{T}$). We have $T_0 \supseteq I$.

(i) T_0 is a left ideal of R .

For, $x, y \in T_0 \implies x \in T_1$ and $y \in T_2$ for some $T_1, T_2 \in \mathcal{T}$. Since $\mathcal{T}$ is totally ordered, we have $T_1 \subseteq T_2$ or $T_2 \subseteq T_1$, say $T_1 \subseteq T_2$. Hence $x, y \in T_2$. But T_2 is a left ideal, hence $x - y \in T_2$ and so $x - y \in T_0$, i.e., T_0 is an additive subgroup of R . Let $x \in T_0$ and $r \in R$. Since $x \in T_0$, we have $x \in T$ for some $T \in \mathcal{T}$. Since T is a left ideal we have $rx \in T$, hence $rx \in T_0$. Thus T_0 is a left ideal.

(ii) $T_0 \neq R$.

For, if $T_0 = R$ then $1 \in T_0$. Hence $1 \in T$ for some $T \in \mathcal{T}$. But then $T = R$ which is a contradiction.

Now by Zorn's lemma, $\mathcal{F}$ has a maximal element, say M . Since $M \in \mathcal{F}$, we have $M \neq R$, $M \supseteq I$ and M is a left ideal.

(iii) M is a maximal left ideal of R .

For, suppose J is a left ideal such that $M \subseteq J \subseteq R$. If $J \neq R$ then $J \in \mathcal{F}$. By maximality of M in $\mathcal{F}$, we get that $M = J$, as required. $\diamond$

2.2.6 Example to show that the above theorem is not true if R has no unity (even if R is commutative).

Let $(G, +)$ be an abelian group and make it into a ring with *trivial multiplication* $(*)$, i.e., $a * b = 0$ for all $a, b \in G$. Note that all subgroups of $(G, +)$ are ideals in $(G, +, *)$. Therefore, a maximal ideal in $(G, +, *)$ is simply a maximal subgroup of $(G, +)$. Now choose $G = (\mathbb{Q}, +)$. We show that $(\mathbb{Q}, +)$ has no maximal subgroups, hence the ring $(\mathbb{Q}, +, *)$ which is without 1, has no maximal ideals.

$(\mathbb{Q}, +)$ has no maximal subgroups.

For, suppose it has a maximal subgroup $H (\neq \mathbb{Q})$, i.e., there is an $r/s \in \mathbb{Q}$ such that $r/s \notin H$. Since H is a maximal subgroup of $\mathbb{Q}$, we have $H \neq \{0\}$. Take $0 \neq m_0/n_0 \in H$. If $m/n \in H$, then $n \cdot m/n = m \in H$. Thus we have $m_0 \in H$. Since H is maximal, $r/s \notin H$ and $H \subset H + (r/s) \subset \mathbb{Q}$, we get that $H + (r/s) = \mathbb{Q}$. Therefore for each rational $x/y \in \mathbb{Q}$, we have

$$x/y = h + t \cdot r/s \text{ for some } h \in H \text{ and } t \in \mathbb{Z}.$$

In particular, $r/(sm_0s) = h_1 + t_1 \cdot r/s$ for some $h_1 \in H$ and $t_1 \in \mathbb{Z}$. Now $h_1 \in H \Rightarrow m_0sh_1 \in H$ and $m_0 \in H \Rightarrow t_1rm_0 \in H$ and hence

$$r/s = m_0h_1s + m_0t_1s(r/s) = m_0h_1s + m_0t_1r \in H$$

which is a contradiction.

2.2.7 Remark: Theorem (2.2.5) above need not be true for minimal (left/right/2-sided) ideals of R even if R is commutative with 1, i.e., if I is a non-zero (left/right/2-sided) ideal in R , then, in general, there need not be a minimal ideal J in R such that $J \subseteq I$. For example, let $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$. We know that any ideal $J \subseteq 2\mathbb{Z}$ is of the form $J = 2k\mathbb{Z}$ for some $k \in \mathbb{N}$. We note that J cannot be minimal in $\mathbb{Z}$ whatever be k because $J = 2k\mathbb{Z} \supseteq 4k\mathbb{Z} \neq (0)$ and $4k\mathbb{Z} \neq 2k\mathbb{Z}$.

2.2.8 Prime ideal: Let R be a commutative ring. An ideal I of R is said to be a *prime ideal* if

1. $I \neq R$ and
2. $x, y \in R, xy \in I \Rightarrow$ either $x \in I$ or $y \in I$.

Note: The definition of a prime ideal in a non-commutative ring is given in Ex.(2.9.22) below. (The obvious guess one makes from the commutative case is not the right thing to do!)

It is clear that saying R is a commutative integral domain is the same as saying that $R \neq (0)$ and (0) is a prime ideal in R . Secondly, we find that any nilpotent element in R is in all prime ideals of R , i.e., if

$$N = \{a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N}\} \text{ and } N' = \bigcap_P P$$

where the intersection is taken over all prime ideals of R , then $N \subseteq N'$. Now we have the following.

2.2.9 Theorem: The set of all nilpotent elements in a commutative

ring R with 1 is the intersection of all prime ideals, i.e., $N = N'$.

Proof: It is a simple matter (Ex.(2.9.3) below) to see that N is an ideal of R since R is commutative. Since $N \subseteq N'$, we have only to show that $N' \subseteq N$ or equivalently, we will show that *a is not nilpotent if and only if a does not belong to some prime ideal of R* . Now $a \notin N$ implies $a^n \neq 0$ for all $n \in \mathbb{N}$.

Let $A = \{1, a, a^2, a^3, \dots\}$. We have $0 \notin A$ and $a^m, a^n \in A \Rightarrow a^{m+n} \in A$. Let $\mathcal{F}$ be the family of all ideals in R disjoint from A , i.e.,

$$\mathcal{F} = \{I \mid I \text{ an ideal in } R, I \cap A = \emptyset\}.$$

The theorem is *equivalent* to showing that $\mathcal{F}$ contains a prime ideal of R . We shall first show that $\mathcal{F}$ has a maximal element (under set inclusion as the partial order) and then show that any such element is a prime ideal.

We have $\mathcal{F} \neq \emptyset$ since $(0) \in \mathcal{F}$. Let $\mathcal{T}$ be a totally ordered subset of $\mathcal{F}$. Let $T_0 = \bigcup_{J \in \mathcal{T}} J$. If we show that $T_0 \in \mathcal{F}$ then T_0 is obviously an upper bound for $\mathcal{T}$.

(i) T_0 is an ideal of R .

The verification is the same as in (i) of proof of (2.2.5) above.

(ii) $T_0 \cap A = \emptyset$, i.e., $T_0 \in \mathcal{F}$.

For, $T_0 \cap A = \bigcup_{J \in \mathcal{T}} (J \cap A) = \emptyset$ (since $J \cap A = \emptyset, \forall J$).

Now by Zorn's lemma $\mathcal{F}$ has a maximal element say P , i.e., P is an ideal in R maximal for the property that $P \cap A = \emptyset$.

(iii) P is a prime ideal of R .

For, suppose $xy \in P$ but $x \notin P$ and $y \notin P$. Let $J_1 = Rx + P$ and $J_2 = Ry + P$ so that both J_1 and J_2 ideals in R strictly larger than P , hence $A \cap J_1 \neq \emptyset$ and $A \cap J_2 \neq \emptyset$. Take $s \in J_1 \cap A$ and $t \in J_2 \cap A$. Then $s = a^m$ and $t = a^n$ for some m and $n \in \mathbb{Z}^+$. Because $s \in J_1$, s can be written as $s = rx + k$ for some $r \in R$ and $k \in P$. Similarly, $t = zy + l$ for some $z \in R$ and $l \in P$. Since $xy, k, l \in P$, we have

$$st = (rx + k)(zy + l) = (rxyz + rxl + kzy + kl) \in P,$$

i.e., $st \in A \cap P = \emptyset$ which is a contradiction, as required. ■

2.3 Generators for Subrings and Ideals

Let X be a subset of a ring R .

2.3.1 Subgroup generated by X in $(R, +)$: The smallest subgroup of $(R, +)$ containing X is called the *subgroup generated by X* in $(R, +)$, or equivalently, subgroup generated by X in $(R, +) = \cap S$ where the intersection is taken over all subgroups S of R containing X . This intersection is over a non-empty family because $(R, +)$ is a member. This can also be seen to be equal to the set

$$\{\sum^{\text{finite}} n_i x_i \mid n_i \in \mathbb{Z}, x_i \in X\},$$

i.e., finite sums and differences of elements of X . In particular,

1. if $X = \emptyset$, the subgroup generated by $\emptyset$ is (0) .
2. if $X = \{x\}$, a singleton, the subgroup generated by X is simply the cyclic subgroup generated by x and it is $\{nx \mid n \in \mathbb{Z}\}$.

2.3.2 Subring generated by X in $(R, +, \cdot)$: The *subring generated by X* in $(R, +, \cdot)$ is defined as the smallest subring of R containing X , or equivalently, the intersection of all subrings of R , each containing X . This intersection is non-empty because $(R, +, \cdot)$ is a subring containing X . It can be seen to be equal to finite sums and differences of finite products in X , i.e., subring generated by X in R is

$$\left\{ \sum_{\substack{J \\ n_J \in \mathbb{Z}}}^{\text{finite}} n_J \left(\prod_{\substack{\{(x_1, \dots, x_r)\} \subseteq J \subseteq X^r \\ r \geq 0}}^{\text{finite}} (x_1 \cdots x_r) \right) \right\}$$

In particular,

1. If $X = \emptyset$, subring generated by $\emptyset$ is (0) .
2. If $X = \{x\}$, the subring generated by x is of the form $\{\sum_{i \geq 0}^{\text{finite}} m_i x^i, m_i \in \mathbb{Z}\}$, i.e., polynomial expressions in x without constant term with integer coefficients.

2.3.3 Left ideal generated by X : The *left ideal generated by X* is the smallest left ideal in R containing X , or equivalently, it can be defined as the intersection of all the left ideals in R containing X

which can be seen to be equal to

$$\left\{ \sum_{\substack{n_i \in \mathbb{Z} \\ x_i \in X}}^{\text{finite}} n_i x_i + \sum_{\substack{r_j \in R \\ y_j \in X}}^{\text{finite}} r_j y_j \right\}$$

In particular,

1. If $X = \emptyset$, the left ideal generated by $\emptyset$ is (0) .
2. If $X = \{x\}$, the left ideal generated by x is $\{nx + rx \mid n \in \mathbb{Z}, r \in R\}$, ($= \{sx \mid s \in R\}$, if $1 \in R$). This is denoted by $(x)_l$ (left ideal generated by x).

2.3.4 Principal left ideal: A left ideal I in R is called a *principal left ideal* if I is generated by one element, i.e., $I = (x)_l$ for some $x \in I$.

2.3.5 Right ideal generated by X : The *right ideal generated by X* is the smallest right ideal in R containing X , or equivalently, it can be defined as the intersection of all the right ideals in R containing X which can be seen to be equal to

$$\left\{ \sum_{\substack{n_i \in \mathbb{Z} \\ x_i \in X}}^{\text{finite}} n_i x_i + \sum_{\substack{r_j \in R \\ y_j \in X}}^{\text{finite}} y_j r_j \right\}$$

In particular,

1. If $X = \emptyset$, the right ideal generated by $\emptyset$ is (0) .
2. If $X = \{x\}$, the right ideal generated by x is $\{nx + xr \mid n \in \mathbb{Z}, r \in R\}$, ($= \{xs \mid s \in R\}$, if $1 \in R$). This is denoted by $(x)_r$ (right ideal generated by x) and is called the *principal right ideal* generated by x .

2.3.6 Two-sided ideal generated by X : The *2-sided ideal generated by X* is defined as the smallest 2-sided ideal in R containing X , or equivalently, intersection of all the 2-sided ideals in R containing X . This can be seen to be equal to

$$\left\{ \sum_{\substack{n_i \in \mathbb{Z} \\ x_i \in X}}^{\text{finite}} n_i x_i + \sum_{\substack{r_j \in R \\ y_j \in X}}^{\text{finite}} r_j y_j + \sum_{\substack{s_k \in R \\ z_k \in X}}^{\text{finite}} z_k s_k + \sum_{\substack{t_\ell \in X \\ a_\ell, b_\ell \in R}}^{\text{finite}} a_\ell t_\ell b_\ell \right\}$$

In particular,

1. If $X = \emptyset$, the 2-sided ideal generated by $\emptyset$ is (0) .
2. If $X = \{x\}$, the 2-sided ideal generated by $x = \{nx + rx + xs + axb \mid n \in \mathbb{Z}, r, s, a, b \in R\}$, i.e., $= \{\sum^{\text{finite}} a_i x b_i \mid a_i, b_i \in R\}$ if R has unity. This 2-sided ideal generated by $\{x\}$ is denoted by (x) and is called the *principal 2-sided ideal* generated by x .

2.3.7 Principal ideal ring: A ring is called a *principal ideal ring* ($P \mid R$) if R is commutative and every ideal of R is principal.

2.3.8 Principal ideal domain: A principal ideal ring which is an integral domain is called a *principal ideal domain* ($P \mid D$).

2.3.9 Finitely generated ideal: An ideal (left/right/2-sided) is said to be *finitely generated* if there is a finite subset $X = \{x_1, \dots, x_n\}$ of I such that the ideal generated by X is I (i.e., every element of I can be expressed as a (left/right/2-sided) R -linear combinations of $x_1, \dots, x_n$). ■

2.4 Basic Properties of Ideals

2.4.1 Proposition: Suppose R is a ring with 1. Let I be a left ideal. Then the following are equivalent.

1. $I = R$.
2. $1 \in I$.
3. I contains a unit.
4. I contains an element which has a left inverse.

Proof: (1) $\Leftrightarrow$ (2): Suppose $I = R$. Then since $1 \in R$, we have $1 \in I$. Now suppose $1 \in I$. Then for all $x \in R$, $x = x \cdot 1 \in I$. (Since I is a left ideal and $1 \in I$.) Therefore $R \subseteq I$ and I being an ideal in R , $I \subseteq R$. Hence $I = R$.

(2) $\Leftrightarrow$ (3): If $1 \in I$, I contains a unit (obviously). Suppose I contains a unit u , then $1 = u^{-1} u \in I$.

(3) $\Leftrightarrow$ (4): Suppose I contains a unit. Then I contains an element which has a left inverse (trivial). Suppose I contains an element a

which has a left inverse, say b . Then $1 = b \cdot a \in I$. $\diamond$

2.4.2 Corollary: *Suppose R is a ring with 1. Let I be a principal left ideal generated by x , i.e., $I = (x)_l$. Then $(x)_l = R$ if and only if x has a left inverse.*

2.4.3 Remark: Suppose R has 1 and I is a right ideal of R . Then $I = R$ if and only if $1 \in I$ or if and only if I contains a unit or if and only if I contains an element which has a right inverse.

2.4.4 Corollary: *If $I = (x)_r$ and R contains 1, then $(x)_r = R$ if and only if x has a right inverse.*

2.4.5 Proposition: *Suppose R contains 1 and I is a 2-sided ideal of R . Then $I = R \iff 1 \in I \iff I$ contains a unit $\iff I$ contains an element which has a left inverse or a right inverse.* $\diamond$

However, if $(x) = R$, then x need not have left inverse or right inverse. (But in case x has a left inverse or right inverse we have $(x) = R$. In other words, only the implication $(\Leftarrow)$ of (2.4.4) is true for principal 2-sided ideals.) For instance, look at the following.

Example: Let $R = M_2(\mathbb{R})$ and $x = E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. It is obvious that x has no left or right inverse. Now we show that $(x) = R$, for which it suffices to show that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in (x)$. But $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_{11} + E_{22} = E_{11} + E_{21} \cdot E_{11} \cdot E_{12} = x + E_{21} \cdot x \cdot E_{12} \in (x)$. Therefore, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in (x)$. Hence $(x) = R$.

2.4.6 Theorem: *Let R be a ring with 1. Then R is a division ring $\xLeftrightarrow{(1)} (0)$ and R are the only left ideals in $R \xLeftrightarrow{(2)} (0)$ and R are the only right ideals in R .*

Proof: (1). Suppose R is a division ring. Let I be any ideal in R . If $I \neq (0)$ then I contains a non-zero element, say ' a '. Since $1 = a^{-1}a \in I$, we have $I = R$.

Conversely, suppose (0) and R are the only left ideals in R . Let $a \in R$, $a \neq 0$. Look at $I = Ra$, the left ideal generated by a , i.e.,

$I = \{xa \mid x \in R\}$. By hypothesis $I = R \implies 1 \in R = Ra$, i.e., $1 = xa$, for some $x \in R$, i.e., ' a ' has a left inverse in R . Note that, this $x \neq 0$. By the same argument as above with x in place of a , we get that x has a left inverse, say ' z ', i.e., $zx = 1$. Thus x has a left inverse z and a right inverse a . This gives $z = a$, i.e., $ax = 1 = xa$. Therefore, a is a unit and hence R is a division ring.

(2): Similar to (1). ◇

2.4.7 Corollary: *If R is a commutative ring with 1 then R is a field if and only if R has no ideals other than (0) and R .*

2.4.8 Remark: If R is a division ring it is obvious that R cannot have 2-sided ideals other than (0) and R . But the converse is not true, i.e., if R is such that it has no 2-sided ideals other than (0) and R then it need not imply that R is a division ring.

Example: Let $R = M_2(\mathbb{R})$. This is not a division ring. But R has no 2-sided ideals other than (0) and R . For, consider a 2-sided ideal I in R where $I \neq (0)$. Take any $x \in I$, $x \neq 0$. Say $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$, i.e., one of a or b or c or d is non-zero. Say $b \neq 0$. We have $(x) \subseteq I$.

Now $x = aE_{11} + bE_{12} + cE_{21} + dE_{22} \implies xE_{21} = aE_{11}E_{21} + bE_{12}E_{21} + cE_{21}E_{21} + dE_{22}E_{21} = 0 + bE_{11} + 0 + dE_{21}$. Therefore $xE_{21} = bE_{11} + dE_{21}$.

Since $b \neq 0$, we have $b^{-1}E_{11}xE_{21} = b^{-1}E_{11}bE_{11} + b^{-1}E_{11}dE_{21} = b^{-1}bE_{11} = E_{11}$ which implies $E_{11} = b^{-1}E_{11}xE_{21} \in (x)$. Therefore (x) contains the ideal generated by E_{11} . But by the Example in (2.4.5) above, we have $(E_{11}) = R$. Therefore $R = (E_{11}) \subseteq (x) \subseteq I$, i.e., $R = I$. (This is a special case of (2.4.11) below.)

2.4.9 Theorem: *Let R be a non-zero ring in which the multiplication is non-trivial. Then R is a division ring if and only if R has no left ideals other than (0) and R , (i.e., R contains a pair x, y such that $xy \neq 0$). Then if R has no left (resp. right) ideals other than (0) and R , R has 1 and R is a division ring.*

Proof: In view of (2.4.6) above, it is enough to prove that R has 1.

(a) Existence of an idempotent:

By hypothesis, there are $x, y \in R$ such that $xy \neq 0$. Consider $Ry = \{zy \mid z \in R\}$ the set of all left multiples of y . Since $xy \neq 0$ and $xy \in Ry$, $Ry \neq (0)$. Clearly Ry is a left ideal in R . Hence by hypothesis, we have $Ry = R$. Since $y \in R = Ry$, we have $y = ey$ for some $e \in R$. Then $y = ey = e^2y = \cdots \Rightarrow (e^2 - e)y = 0$. $(*)$

Consider the left annihilators of y , i.e., $L(\text{Ann}(y)) = \{z \in R \mid zy = 0\}$. It is easy to show that $L(\text{Ann}(y))$ is a left ideal in R . Further, $xy \neq 0$ implies $x \notin L(\text{Ann}(y))$. Hence $L(\text{Ann}(y)) \neq R$. By hypothesis, we have $L(\text{Ann}(y)) = (0)$. From $(*)$, we know that $(e^2 - e)y = 0$. Hence $e^2 - e \in L(\text{Ann}(y)) = (0)$ which implies $e^2 - e = 0$, i.e., $e^2 = e$. Hence e is an idempotent.

(b) e is a right identity of R , i.e., $ae = a, \forall a \in R$.

Consider $I = \{(ae - a) \mid a \in R\}$. Since $0 = 0 \cdot e - 0 \in I$, $I \neq \emptyset$.

(i) I is a left ideal.

For, let $(ae - a)$ and $(be - b) \in I$, $a, b \in R$. Then $(ae - a) - (be - b) = ae - be - a + b = (a - b)e - (a - b) \in I$ and $r(ae - a) = (ra)e - (ra) \in I$, for all $r \in R$ and for all $ae - a \in I$.

(ii) $I = (0)$.

It is enough to show that $I \subseteq L(\text{Ann}(y))$. Consider any $ae - a \in I$. Then we have $(ae - a)y = aey - ay = ay - ay = 0$ (since $ey = y$). Therefore, $(ae - a) \in L(\text{Ann}(y)) = (0)$ which implies $I = (0)$, i.e., $ae = a, \forall a \in R$. Hence e is a right identity in R .

(c) e is a left identity of R , i.e., $ea = a, \forall a \in R$.

Consider $J = \{(ea - a) \mid a \in R\}$. We have $J \neq \emptyset$ (because $0 = e \cdot 0 - 0$). This J is a left ideal. In fact, we have $(ea - a) - (eb - b) = e(a - b) - (a - b) \in J, \forall a, b \in R$ and $r(ea - a) = rea - ra = ra - ra = 0 \in J, \forall r \in R$. Now $J = (0)$ or R (by hypothesis).

Suppose $J = R$. Then $y \in J$ which implies $y = ea - a$, for some $a \in R$. But then $xy = x(ea - a) = (xe)a - xa = xa - xa = 0$, i.e., $xy = 0$ a contradiction. Hence $J \neq R$ which gives $J = (0)$, i.e., $ea = a, \forall a \in R$. Therefore e is left identity in R .

Thus e is both a left and a right identity of R , as required. $\diamond$

2.4.10 Theorem: Let R be a ring with 1 and $S = M_n(R)$, $n \geq 1$. Then we have the following.

1. For a left ideal I in R , $M_n(I)$ is a left ideal in S .
2. For a right ideal I' in R , $M_n(I')$ is a right ideal in S .
3. For a 2-sided ideal J of R , $M_n(J)$ is a 2-sided ideal of S .

The converse is true only for 2-sided ideals, i.e., every two sided ideal K in S is of the form $K = M_n(J)$ for some 2-sided ideal J in R . Furthermore, the three mappings,

$$\begin{aligned}\varphi_\ell &: \{\text{left ideals in } R\} &\longrightarrow \{\text{left ideals in } S\} \\ \varphi_r &: \{\text{right ideals in } R\} &\longrightarrow \{\text{right ideals in } S\} \\ \varphi &: \{2\text{-sided ideals in } R\} &\longrightarrow \{2\text{-sided ideals in } S\}\end{aligned}$$

defined by $K \mapsto M_n(K)$ are all injective and inclusion preserving with φ bijective (while φ_ℓ and φ_r need not be onto). (If R is without 1, even φ need not be onto (see (2.4.14) below)).

Proof: (a): The proof being identical for (1) (2) and (3), we start with I an ideal (left/right/2-sided) in R and prove that $M_n(I)$ is an ideal in S of the same kind as I . Since $0 \in I$, $0 \in M_n(I)$ and hence $M_n(I)$ is non-empty.

Let $A = (a_{ij})$ and $B = (b_{ij}) \in M_n(I)$, (i.e., $a_{ij}, b_{ij} \in I$, $\forall i, j$). Then $A - B = (a_{ij} - b_{ij}) \in M_n(I)$ (since $a_{ij} - b_{ij} \in I$, $\forall i, j$). Let $X = (x_{ij}) \in S$. Then $(XA)_{ij} = \sum_{k=1}^n x_{ik}a_{kj}$. Since I is a left ideal, we get that $XA \in M_n(I)$, i.e., $M_n(I)$ is a left ideal in S . Similar proof holds for $M_n(I)$ being right or 2-sided ideal in S . Thus $M_n(I)$ is an ideal in S of the same kind as I in R .

(b): (i) The maps φ , φ_ℓ and φ_r are obviously *inclusion preserving*.

(ii) φ , φ_ℓ and φ_r are *injective*.

For, let $I \neq I'$. Let, if possible, $M_n(I) = M_n(I')$. For $a \in I$, we have $aE_{11} \in M_n(I)$. Since $M_n(I) = M_n(I')$, we get that $aE_{11} \in M_n(I')$. This implies that $a \in I'$, i.e., $I \subseteq I'$. Similarly $I' \subseteq I$ and hence $I = I'$ which is a contradiction.

(c): φ is *bijective*.

We have only to prove the *surjectivity* of φ . Let K be a 2-sided ideal in S . We shall find a 2-sided ideal J in R such that $K = M_n(J)$. In

fact, take J to be the set of all $(1, 1)^{th}$ entries of all matrices in K .

Claim 1: J is a 2-sided ideal in R .

Since $0 \in J$, $J \neq \emptyset$. Let $a, b \in J$. Then there exist $A, B \in K$ such that $a = A_{11}$ and $b = B_{11}$. But then $a - b = (A - B)_{11}$ and $A - B \in K$. Thus $a - b \in J$. Furthermore, let $a \in J$ and $r \in R$. Then there is an $A \in K$ such that $a = A_{11}$. Since $rE_{11}A, ArE_{11} \in K$, we get that $ra = (rE_{11}A)_{11}$ and $ar = (ArE_{11})_{11}$, i.e., $ra, ar \in J$, as required.

Claim 2: (i) $M_n(J) \subseteq K$ and (ii) $M_n(J) \supseteq K$ (hence equal).

(i) Let $A = (a_{ij}) \in M_n(J)$ so that there are matrices $N^{(ij)} \in K$ such that $N^{(ij)} = a_{ij}E_{11} + \dots$, i.e., $(N^{(ij)})_{11} = a_{ij}$, $\forall i, j$. We shall show that $A = \sum_{i,j=1}^n E_{i1}N^{(ij)}E_{1j}$ which is in K because $N^{(ij)} \in K$ and K is a 2-sided ideal. We have

$$\begin{aligned} \sum_{i,j=1}^n E_{i1}N^{(ij)}E_{1j} &= \sum_{i,j=1}^n E_{i1} \left(\sum_{k,l=1}^n (N^{(ij)})_{kl} E_{kl} \right) E_{1j} \\ &= \sum_{i,j=1}^n \sum_{k,l=1}^n (N^{(ij)})_{kl} E_{i1} E_{kl} E_{1j} \\ &= \sum_{i,j=1}^n \sum_{l=1}^n (N^{(ij)})_{1l} E_{i1} E_{1j} \\ &= \sum_{i,j=1}^n (N^{(ij)})_{11} E_{ij} = \sum_{i,j=1}^n a_{ij} E_{ij} = A. \end{aligned}$$

(ii) Let $A = (a_{ij}) \in K$. To show that $a_{ij} \in J$, we have to find a matrix $N^{(ij)}$ whose $(1, 1)^{th}$ entry is a_{ij} . Since K is a 2-sided ideal, $N^{(ij)} = E_{li}AE_{j1} \in K$. But we have

$$\begin{aligned} N^{(ij)} &= E_{li}AE_{j1} = E_{li} \left(\sum_{k,l=1}^n a_{kl} E_{kl} \right) E_{j1} \\ &= \sum_{k,l=1}^n a_{kl} E_{li} E_{kl} E_{j1} = \sum_{k=1}^n a_{kj} E_{li} E_{k1} \\ &= a_{ij} E_{11} = (N^{(ij)})_{11} E_{11}, \text{ as required. } \diamond \end{aligned}$$

2.4.11 Corollaries: 1. The ring $M_n(\mathbb{Z})$ has infinitely many 2-sided ideals because $\mathbb{Z}$ has infinitely many ideals.

2. If R is a division ring then $M_n(R)$ has no 2-sided ideals other than (0) and R . In particular, for any non-zero matrix $A \in M_n(R)$, the principal 2-sided ideal generated by A is the unit ideal $(A) = M_n(R)$.

2.4.12 Simple ring: A non-zero ring R is said to be a *simple ring* if R has no 2-sided ideals other than (0) and R .

Examples: 1. Division rings are simple.

2. Matrix rings over division rings are simple.

3. More generally, if R is a simple ring with 1, then $M_n(R)$ is a simple ring (by Theorem (2.4.10) above).

(Note that a simple ring need not have unity. See (3.3.4) below.)

2.4.13 Remark: The maps φ_l and φ_r in Theorem (2.4.10) above, need not be surjective.

Examples: 1. Let $R = \mathbb{Q}$ and $S = M_n(\mathbb{Q})$, $n \geq 2$. Now $\mathbb{Q}$ has no ideals other than (0) and $\mathbb{Q}$, but $M_n(\mathbb{Q})$ has proper left ideals, namely,

$$J_k = \left\{ \begin{pmatrix} 0 & 0 & \cdots & a_{1k} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_{2k} & 0 & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & a_{rk} & 0 & \cdots & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & a_{nk} & 0 & \cdots & 0 \end{pmatrix} \mid a_{ik} \in \mathbb{Q} \right\}$$

it is trivial to check that J_k 's are left ideals ($1 \leq k \leq n$). In fact these are *minimal left ideals*.

To show that the J_i 's are minimal left ideals in $M_n(\mathbb{Q})$, take a left ideal J in $M_n(\mathbb{Q})$ such that $J \subseteq J_k$. Assume that $(0) \neq J$. Then there is an $A \in J$, $A \neq 0$. Let

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_{1k} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & a_{2k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{nk} & 0 & \cdots & 0 \end{pmatrix}$$

where $a_{ik} \in \mathbb{Q}$, with at least one $a_{ik} \neq 0$. Let $B = a_{ik}^{-1} E_{ii} \in M_n(\mathbb{Q})$. We have $BA = E_{ik} \in (A)_l \subseteq J$ (since J is a left ideal). But $E_{ik} =$

$\sum_{j=1}^n E_{ij}E_{jk}$. Thus $E_{1k} = E_{1i}E_{ik} \in (A)_\ell$. Similarly, $E_{2k} = E_{2i}E_{ik}, \dots$, $E_{nk} = E_{ni}E_{ik}$ are all in $(A)_\ell$. But every element of J_k is a $\mathbb{Q}$ -linear combination of $E_{1k}, \dots, E_{nk}$ and so $J_k \subseteq (A)_\ell \subseteq J \subseteq J_k$. Hence $J = J_k$, as required.

?. A similar proof shows that the following are *minimal right ideals*, namely,

$$K_j = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 \end{pmatrix} \mid a_{ji} \in \mathbb{Q} \right\}$$

2.4.14 Remark: If R is *without* unity, the map φ in Theorem (2.4.10) above, need not be onto.

Example: Take $R = 2\mathbb{Z}$ and $S = M_2(2\mathbb{Z})$. Consider the 2-sided ideal J in S , namely,

$$J = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in 2\mathbb{Z} \text{ with } a \in 4\mathbb{Z} \right\}.$$

Since $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \notin J$, we have $J \neq S$. If at all φ is onto, it is easy to

see that $J = M_2(4\mathbb{Z})$, but $\begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix} \in J$ while $\begin{pmatrix} 4 & 2 \\ 0 & 0 \end{pmatrix} \notin M_2(4\mathbb{Z})$.

In other words, J is a 2-sided ideal strictly in between $M_2(4\mathbb{Z})$ and $M_2(2\mathbb{Z})$ but there are no ideals between $4\mathbb{Z}$ and $2\mathbb{Z}$ in $\mathbb{Z}$. ■

2.5 Algebra of Ideals

Let R be a ring and I and J be ideals in R of the same kind, i.e., left/right/2-sided.

2.5.1 Addition of ideals: Addition of ideals I and J is defined as

$$I + J = \{x + y \mid x \in I, y \in J\} \subseteq R.$$

2.5.2 Proposition: 1. *Sum of two ideals of the same kind is again an ideal of the same kind.*

2. *Addition of ideals is commutative and associative.*

Proof: (1) Let I and J be left ideals in R and suppose $z_1, z_2 \in I + J$. Then $z_1 = x_1 + y_1$ and $z_2 = x_2 + y_2$ for some $x_1, x_2 \in I$ and $y_1, y_2 \in J$. Then $z_1 - z_2 = x_1 + y_1 - x_2 - y_2 = x_1 - x_2 + y_1 - y_2 \in I + J$, since $x_1 - x_2 \in I$, $y_1 - y_2 \in J$. Again suppose $z \in I + J$ and $r \in R$. Then $z = x + y$, for some $x \in I$, $y \in J$. We have $rz = r(x + y) = rx + ry \in I + J$ (since rx and ry are in I and J respectively). Thus $I + J$ is a left ideal in R . Similar proof holds for right/2-sided ideals.

(2) is obvious. ◇

Note that we have (i) $R + I = R$, (ii) $I + (0) = I$ and (iii) $I = -I = \{-x \mid x \in I\}$.

2.5.3 Multiplication of ideals: Define multiplication of *two subsets* I and J of R as

$IJ = \{x_1y_1 + x_2y_2 + \cdots + x_ny_n \mid x_i \in I, y_i \in J, 1 \leq i \leq n, n \in \mathbb{N}\}$, i.e., finite sums of products of pairs of elements one from I and the other from J . (It is the additive subgroup generated by the products xy with $x \in I$ and $y \in J$.)

Caution: The notation IJ in the context of Rings is quite different from its counter part in Groups.

2.5.4 Proposition: 1. *Product of two ideals of the same kind is again an ideal of the same kind.*

2. Product of ideals is associative but need not be commutative.

Proof: Let I and J be left ideals in R . Let $z_1, z_2 \in IJ$. Say

$$z_1 = \sum_{i=1}^m x_i y_i \text{ and } z_2 = \sum_{j=1}^n a_j b_j \text{ with } x_i, a_j \in I \text{ and } y_i, b_j \in J.$$

Then we have

$$z_1 - z_2 = \sum_{i=1}^m x_i y_i - \sum_{j=1}^n a_j b_j = \sum_{i=1}^m x_i y_i + \sum_{j=1}^n (-a_j) b_j \in IJ.$$

If $z = \sum_{i=1}^r x_i y_i \in IJ$ and $t \in R$, then we have

$$\begin{aligned} tz &= t(x_1y_1 + x_2y_2 + \cdots + x_r y_r) \\ &= (tx_1)y_1 + (tx_2)y_2 + \cdots + (tx_r y_r) \in IJ. \end{aligned}$$

Thus IJ is a left ideal of R . A similar proof holds for right/2-sided ideals. It is quite easy to prove that product of ideals is associative. ◇

2.5.5 Remarks: From the definitions and verification above, we

note the following.

1. IJ is a left ideal if I is a left ideal and J any subset of R .
 2. IJ is a right ideal if I is any subset of R and J is a right ideal.
 3. IJ is a 2-sided ideal if I is a left ideal and J is a right ideal.
- Furthermore, if R has 1, then $IR = I = RI$. However, if R is without 1, then $IR \subseteq I$ and $RI \subseteq I$ (equality need not hold).
4. The set of all additive subgroups of $(R, +)$ is a commutative *semi-group* with identity under addition but not a group.
 5. The set of all left/right/2-sided ideals is a *sub-semigroup* with identity under addition but not a group.
 6. The set of all left/right/2-sided ideals in R is a *semigroup* with identity (namely, R), under multiplication (provided R has 1) but not a group.

2.5.6 Power of an ideal: Given an ideal I of R , we define

$$I^2 = I \cdot I = \left\{ \sum_{i=1}^{\text{finite}} x_i y_i \mid x_i, y_i \in I \right\},$$

$$I^3 = I \cdot I \cdot I = I \cdot I^2 = I^2 \cdot I = \left\{ \sum_{i=1}^{\text{finite}} x_i y_i z_i \mid x_i, y_i, z_i \in I \right\},$$

$$I^n = I \cdot I^{n-1} = I^{n-1} \cdot I, \text{ etc.}$$

2.5.7 Nilpotent ideals: An ideal I of a ring R is said to be *nilpotent* if $I^n = (0)$ for some $n \geq 1$.

2.5.8 Remark: If I is nilpotent say $I^n = (0)$, then it follows that $x_1 \cdot x_2 \cdots x_n = 0$, $\forall x_i \in I$, $1 \leq i \leq n$. In particular, $x^n = 0$, $\forall x \in I$.

2.5.9 Nil ideal: An ideal I in a ring R is called a *nil ideal* if every element of I is nilpotent.

2.5.10 Remark: Every nilpotent ideal is a nil ideal but the converse is not true.

Example: Let $R = \prod_{n=1}^{\infty} \mathbb{Z}_{2^n}$. Let I be the ideal of all nilpotent elements in R . Obviously I is a nil-ideal. But I is not nilpotent, because if $I^n = (0)$ for some n , then $x^n = 0$ for all $x \in I$. Now take

$x_n = (0, 0, \dots, 0, \bar{2}, 0, 0, \dots)$, with $\bar{2}$ at the $(n+1)^{\text{th}}$ place. We see that $x_n^{n+1} = 0$ but $x_n^n \neq 0$.

2.5.11 Proposition: *Let R be a commutative ring. Then a nil ideal I is nilpotent if I is finitely generated.*

Proof: Suppose I is a finitely generated nil ideal, say generated by $X = \{x_1, x_2, \dots, x_r\}$. Since all the x_i 's are nilpotent, say, $x_i^{n_i} = 0$, $n_i \geq 1$, $i = 1, 2, \dots, r$. If $n = \max_{1 \leq i \leq r} n_i$, we have $x_i^n = 0$ for all i , $1 \leq i \leq r$. Since I is generated by X , elements of I are of the form, $\sum_{i=1}^r n_i x_i + \sum_{i=1}^r a_i x_i$ for some $n_i \in \mathbb{Z}$ and $a_i \in R$. Since R is commutative and x_i 's are all nilpotent, any linear combination of these x_i 's is also nilpotent. Thus we get, for example,

$$\left(\sum_{i=1}^r n_i x_i + \sum_{i=1}^r a_i x_i \right)^{2rn} = 0$$

for all $a_i \in R$ and $n_i \in \mathbb{Z}$, i.e., $x^{2rn} = 0$, for all $x \in I$. But I^n is generated by $\{x_{i_1} x_{i_2} \cdots x_{i_m} \mid 1 \leq i_1, i_2, \dots, i_m \leq r, i_j \text{'s not necessarily distinct}\}$, i.e., generated by $\{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \mid n_i \geq 0, \sum_{i=1}^r n_i = m\}$.

Claim: $I^{rn} = (0)$.

Since I^{rn} is generated by $\{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \mid n_i \geq 0, \sum_{i=1}^r n_i = rn\}$, we find that $n_{i_0} \geq n$ for at least one i_0 , $1 \leq i_0 \leq r$, i.e., $x_1^{n_1} \cdots x_{i_0-1}^{n_{i_0-1}} \cdot x_{i_0}^{n_{i_0}} \cdot x_{i_0+1}^{n_{i_0+1}} \cdots x_r^{n_r} = \cdots x_{i_0-1}^{n_{i_0-1}} \cdot 0 \cdot x_{i_0+1}^{n_{i_0+1}} \cdots = 0$, i.e., $I^{rn} = (0)$, as required. ■

2.6 Quotient Rings

2.6.1 Definition: Let R be a ring and I be a subgroup of $(R, +)$. We know that R/I , the set of additive cosets of I , is an abelian group under usual addition of cosets, i.e., $(a + I) + (b + I) = a + b + I$, for all $a, b \in R$. In this group, the identity is the trivial coset I and the inverse of $a + I$ is $-a + I$, $\forall a \in R$.

2.6.2 Theorem: *The natural multiplication of cosets of I , namely, $(a + I)(b + I) = ab + I$, make R/I into a ring if and only if I is a*

2-sided ideal. For a 2-sided ideal I , R/I is called the quotient ring or residue ring of R modulo I .

Proof: Suppose $(R/I, +, \cdot)$ is a ring. Since I is already a subgroup of $(R, +)$, we have to show that I is closed for multiplication on left and right by any element of R . We have $a + I = I$, $\forall a \in I$ and I is the zero element in R/I . Therefore, $(r + I)I = I(r + I) = I$, $\forall r \in R$. Now for $a \in I$, we have

$(r + I)(a + I) = (r + I)I = I(r + I) = (a + I)(r + I)$, i.e., $(ra + I) = I = (ar + I)$. This implies that $ra \in I$ and $ar \in I$. Hence I is a 2-sided ideal.

Conversely, suppose that I is a 2-sided ideal in R . First of all, let us check that the coset multiplication $(a + I)(b + I) = ab + I$, $\forall a, b \in R$, is well-defined, i.e., if $a + I = a' + I$ and $b + I = b' + I$, then we should show that $ab + I = a'b' + I$. We have $a - a' \in I$ and $b - b' \in I$. Hence

$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$
(since I is a 2-sided ideal and $a - a', b - b' \in I$). Hence $ab + I = a'b' + I$, as required.

Claim: $(R/I, +, \cdot)$ is a ring.

Obviously $(R/I, +)$ is an abelian group. Secondly,

1. *Multiplicative semi-group:* For $a, b, c \in R$, we have

$$\begin{aligned} (a + I)(b + I) &= ab + I \in R/I \text{ and} \\ (a + I)[(b + I)(c + I)] &= (a + I)[bc + I] = a(bc) + I \\ &= abc + I = (ab)c + I = (ab + I)(c + I) \\ &= [(a + I)(b + I)](c + I). \end{aligned}$$

2. *Distributive laws:* Let $a, b, x \in R$. Then we have

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

Similarly, $(x + I)[(a + I) + (b + I)] = (x + I)(a + I) + (x + I)(b + I)$. Therefore, $(R/I, +, \cdot)$ is a ring. $\diamond$

2.6.3 Remarks: 1. $R/I = R$ if and only if $I = (0)$ and $R/I = (0)$ if and only if $I = R$.

2. R/I is commutative if R is commutative (but not conversely).
3. R/I is a ring with 1 if R is with 1 (but not conversely).
4. If $a \in R$ is a unit, then $a + I$ is a unit in R/I (but not conversely).
5. Nilpotency and idempotency of an element $a \in R$ implies the same for $a + I$ in R/I (but not conversely). In fact, notice that
 - $a + I$ is nilpotent in $R/I \iff a^n \in I$ for some $n \in \mathbb{N}$.
 - $a + I$ is an idempotent in $R/I \iff a^2 - a \in I$.
6. However, note that a is a zero divisor in R *need not imply* that $a + I$ is a zero-divisor in R/I .

2.6.4 Examples of Quotient rings: 1. The ring $\mathbb{Z}_n$, of integers modulo n (1.8.1), is the quotient ring of $\mathbb{Z}$ modulo the ideal $(n) = n\mathbb{Z}$, i.e., $\mathbb{Z}_n = \mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$.

2. Let $S = R[X]$ and suppose $I = (X)$, the ideal generated by X . Then we have $S/I = R[X]/(X) = R$.

For, if $a(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in R[X]$, then $a(X) + (X) = a_0 + (X) \in R[X]/(X)$, i.e., the constant term of $a(X)$ determines the residue class $a(X) + (X)$. Furthermore, we see that the addition and multiplication of residue classes $a(X) + (X)$ and $b(X) + (X)$ are exactly that of the constant terms of $a(X)$ and $b(X)$, i.e., we have

$$(a(X) + (X)) + (b(X) + (X)) = a_0 + b_0 + (X) \text{ and} \\ (a(X) + (X))(b(X) + (X)) = a_0b_0 + (X).$$

3. If $S = R[[X]]$ and $I = (X)$, then (again by the same proof as above) we have $S/I = R[[X]]/(X) = R$.

Note that $R < X > / (X) = (0)$ since X is a unit in $R < X >$, i.e., $(X) = R < X >$. ■

2.7 Ideals in Quotient Rings

2.7.1 Theorem: Let I be a 2-sided ideal in R and $S = R/I$, the quotient ring of R modulo I . Then we have the following.

1. The set of all subgroups of $(R/I, +)$ is naturally bijective with the set of all subgroups of R each containing I .
2. The set of all subrings of R/I is naturally bijective with the set of subrings of R each containing I .
3. The set of all left/right/2-sided ideals of R/I is naturally bijective

with the set of left/right/2-sided ideals of R each containing I .

Proof: Let J be a subgroup of $(R/I, +)$. Consider $J_0 = \{a \in R \mid a + I \in J\}$. Since $a + I = I \in J$, $\forall a \in I$, we get that $I \subseteq J_0$. Let $a, b \in J_0$. Then $a + I$ and $b + I$ are in J . Since J is a subgroup of $(R/I, +)$, we have $(a + I) - (b + I) = (a - b) + I \in J$. This shows that $a - b \in J_0$. Therefore, J_0 is a subgroup of $(R, +)$.

The verification that J_0 is a subring/left ideal/right ideal/2-sided ideal of R if J is so in R/I is exactly the same as above.

It is trivial to see that if $J \subseteq J'$ in R/I if and only if $J_0 \subseteq J'_0$ in R .

If K is a subgroup/subring/ideal in R containing I , then $\widehat{K} = \{a + I \mid a \in K\}$ is a subgroup/subring/ideal in R/I and $(\widehat{K})_0 = K$. $\diamond$

2.7.2 Theorem: Let R be a commutative ring with 1 and I be an ideal in R . Then we have the following. 1. R/I is an integral domain if and only if I is a prime ideal in R .

2. R/I is a field if and only if I is a maximal ideal in R .

If I is maximal, R/I is called the *residue field* of R at I .

Proof: (1) Suppose I is an ideal of R such that R/I is an integral domain. To prove that I is a prime ideal, let $a, b \in R$ be such that $ab \in I$. We have to show that $a \in I$ or $b \in I$. Since $ab \in I$, we have $(a + I)(b + I) = ab + I = I$, i.e., $(a + I)(b + I) = 0$ in R/I . But R/I is an integral domain. Therefore, either $a + I = I$ or $b + I = I$, i.e., $a \in I$ or $b \in I$, as required.

Conversely, let I be a prime ideal in R . Let $a + I, b + I$ be non-zero elements of R/I . Then $a + I \neq I$ and $b + I \neq I$, i.e., $a \notin I$ and $b \notin I$. Let, if possible, $(a + I)(b + I) = I$. Then $ab + I = I \Rightarrow ab \in I$, a contradiction to the assumption that I is a prime ideal.

(2) We shall prove this part in two apparently different ways.

Method I: Suppose R/I is a field. Therefore R/I contains at least two elements. Hence $R/I \neq (0)$. This implies $I \neq R$. Suppose J is an ideal such that $I \subseteq J \subseteq R$. If $J \neq I$, then there is an a in $J - I$. Then $a + I \neq I$, i.e., $a + I \neq 0$ in R/I . Thus $a + I$ is invertible in R/I .

Hence there is a $b \in R$ such that $(a + I)(b + I) = ab + I = 1 + I$. This implies $ab - 1 \in I \subseteq J$ and hence $ab - 1 \in J$. Since J is an ideal and $ab \in J$, we get that $ab - (ab - 1) = 1 \in J$. Hence $J = R$, as required.

Conversely, let I be a maximal ideal in R . Since $I \neq R$, we have $R/I \neq (0)$. Take any non-zero element $a + I \in R/I$. Since I is maximal, we get that $I + (a) = R$. Hence $1 \in I + (a)$ which implies $1 = x + ya$ for some $x \in I$ and $y \in R$. Therefore $1 + I = x + ya + I = (x + I) + (ya + I) = ya + I$ (since $x + I = I$). Then $1 + I = ya + I = (y + I)(a + I)$ which implies $y + I$ is the inverse of $a + I$ in R/I . Hence R/I is a field.

Method II: Let R/I be a field. Then $I \neq R$ and R/I has no ideals other than (0) and R/I . By (2.7.1) above, we get that the only ideals in R containing I are I and R , i.e., I is a maximal ideal in R .

Conversely, let I be a maximal ideal in R . Since $I \neq R$, we have $R/I \neq (0)$. Since I is maximal, the only ideals in R containing I are I and R . Then by Theorem (2.7.1) above, the only ideals in R/I are (0) and R/I . Thus R/I is a commutative ring with 1 such that $R/I \neq (0)$ and it has no ideals other than (0) and R/I . Hence R/I is a field by Corollary (2.4.7) above. $\diamond$

2.7.3 Corollary: *A maximal ideal (in a commutative ring) is a prime ideal but not conversely.*

Proof: I a maximal ideal in $R \Rightarrow R/I$ is a field $\Rightarrow R/I$ is an integral domain $\Rightarrow I$ is a prime ideal, as required. $\diamond$

• In $\mathbb{Z}$, (0) is a prime ideal but not maximal.

The following facts about the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ are stated without proof in (1.8.2) above.

2.7.4 Corollary: *For $2 \leq n \in \mathbb{N}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is a field $\iff \mathbb{Z}/n\mathbb{Z}$ is an integral domain $\iff n$ is a prime number.*

The first implication is obvious since a field is an integral domain and secondly a finite commutative integral domain is a field.

We now prove that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is a prime. Let $\mathbb{Z}/n\mathbb{Z}$ be an integral domain and if possible, assume that n is not a prime. Say, $n = n_1 n_2$ with $1 < n_1, n_2 < n$. For $m \in \mathbb{Z}$, let $\overline{m} = m + n\mathbb{Z}$. Then $\overline{n_1} \overline{n_2} = \overline{n_1 n_2} = \overline{n} = 0$ with $\overline{n_1} \neq 0$ and $\overline{n_2} \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. This is a contradiction.

Conversely, suppose that n is a prime. Consider any $x \neq 0 \in \mathbb{Z}/n\mathbb{Z}$. We may assume $x \neq 1$, i.e., we can choose $a \in \mathbb{Z}$ such that $2 \leq a \leq n-1$ with $\overline{a} = x$. This shows that $(a, n) = 1$ (since n is prime). Then there exist r and $m \in \mathbb{Z}$ such that $ar + nm = 1$. This implies that $ra \equiv 1 \pmod{n}$. Hence $\overline{r} \overline{a} = 1$ in $\mathbb{Z}/n\mathbb{Z}$ i.e., $\overline{a}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Hence $\mathbb{Z}/n\mathbb{Z}$ is a field. $\diamond$

2.7.5 Proposition: *For $n \geq 2$, the ring $\mathbb{Z}/n\mathbb{Z}$ has no non-trivial nilpotent elements if and only if n is square free.*

Proof: Suppose $\mathbb{Z}/n\mathbb{Z}$ has no non-trivial nilpotent elements. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the *prime decomposition* of n , i.e., p_i 's are distinct primes and $a_i \in \mathbb{N}$. Recall that " n is square free" means that it is a product of distinct primes, i.e., $a_1 = a_2 = \cdots = a_r = 1$.

Let, if possible, n be not square free, say $a_1 \geq 2$. Consider $m = p_1 p_2^{a_2} \cdots p_r^{a_r}$ so that $m < n$, i.e., $\overline{m} \neq 0$ in $\mathbb{Z}/n\mathbb{Z}$. But $m^{a_1} = (p_1 p_2^{a_2} \cdots p_r^{a_r})^{a_1}$ which is a multiple of n . Thus $\overline{m}^{a_1} = 0$ in $\mathbb{Z}/n\mathbb{Z}$, i.e., $\overline{m}$ is non-trivial and nilpotent, a contradiction.

Conversely, suppose n is square free and $\mathbb{Z}/n\mathbb{Z}$ has non-trivial nilpotent elements, say $\overline{a^r} = 0$ in $\mathbb{Z}/n\mathbb{Z}$ and $\overline{a} \neq 0$. Thus n divides a^r but not a . Writing $n = p_1 p_2 \cdots p_s$ as the product of distinct primes, we get that each p_i divides $(n$ and hence divides) a^r which implies that p_i divides a . But then it follows that their product $p_1 p_2 \cdots p_s = n$ divides a which is a contradiction. $\diamond$

2.7.6 Theorem: *Suppose R is a commutative ring with 1. Then $a(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_r X^r \in R[X]$ is a unit in $R[X]$ if and only if a_0 is a unit in R and $a_1, a_2, \dots, a_r$ are all nilpotent in R .*

Proof: Suppose $a(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_r X^r$ is such that a_0 is a unit in R and $a_1, a_2, \dots, a_r$ are all nilpotent in R . Since R is

commutative, we get that $a_1X, a_2X^2, \dots, a_rX^r$ are all nilpotent and hence also their sum, i.e., $z = a_1X + a_2X^2 + \dots + a_rX^r$ is nilpotent (Ex. (1.13.11) above). Now $a_0^{-1}z$ is nilpotent and so $1 + a_0^{-1}z$ is a unit (by Ex.(1.13.18) above). Thus $a(X) = a_0 + z = a_0(1 + a_0^{-1}z)$ which is a product of two units in $R[X]$ is a unit.

Conversely, suppose $a(X) = a_0 + a_1X + a_2X^2 + \dots + a_rX^r$ is a unit in $R[X]$. It follows immediately that a_0 must be a unit in R . Now take any prime ideal P in R . For $a \in R$, let $\bar{a} = a + P$ in R/P . Look at the natural map

$$f_P : R[X] \rightarrow (R/P)[X], b(X) = b_0 + \dots + b_sX^s \mapsto \bar{b}_0 + \dots + \bar{b}_sX^s.$$

This f_P preserves addition and multiplication (such a map is called a homomorphism of rings, see § 3.1 below). Secondly, it takes the unity of $R[X]$ to that of $(R/P)[X]$ and hence it takes units to units. In particular, $f_P(a(X)) = \bar{a}_0 + \bar{a}_1X + \dots + \bar{a}_rX^r$ is a unit in $(R/P)[X]$. Since P is a prime ideal, R/P is an integral domain and hence $(R/P)[X]$ is an integral domain. Now $\bar{a}_0 + \bar{a}_1X + \dots + \bar{a}_rX^r$ is a unit in $(R/P)[X]$ means (by Theorem (1.6.3) above) that $\bar{a}_0$ is a unit in R/P and $\bar{a}_1 = \bar{a}_2 = \dots = \bar{a}_r = 0$, i.e., $a_1, a_2, \dots, a_r \in P$. This shows that $a_1, a_2, \dots, a_r$ belong to the intersection of all prime ideals in R which is nothing but the set of all nilpotent elements in R (by (2.2.9) above). Thus $a_1, a_2, \dots, a_r$ are all nilpotent in R , as required. ■

2.8 Local Rings

2.8.1 Proposition: *Let R be a ring with 1. Then the set M_R of all non-units in R is precisely the union of all proper left/right ideals of R which in turn is also equal to the union of all maximal left/right ideals of R .*

Proof: By (2.4.1) - (2.4.5) above, it follows that M_R contains all proper ideals. On the other hand, if $x \in R$ is a non-unit, then x has either no left inverse or no right inverse which means that either the principal left ideal $(x)_l$ or the right ideal $(x)_r$ is a proper ideal. The second part is immediate since every proper left/right ideal is contained in a maximal left/right ideal by Zorn's lemma (2.2.4). ◇

2.8.2 Local ring: A ring R with 1 is called a *local ring* if the set

of all non-units in R is an ideal.

2.8.3 Proposition: *A ring R with 1 is a local ring if and only if it has a unique maximal ideal, maximal simultaneously as a left/right/2-sided ideal.*

Proof: Suppose R is local with M_R its ideal of non-units. By (2.8.1) M_R contains all maximal left/right/ 2-sided ideals and hence M_R maximal simultaneously as a left/right/2-sided ideal. Conversely, if R has a unique maximal ideal, then it must be precisely the set of all non-units in R , as required. $\diamond$

2.8.4 Corollary: *If R is a local ring with M_R its ideal of non-units, then the quotient R/M_R is a division ring.*

For, since M_R is maximal as a left ideal, the quotient ring R/M_R has no proper left ideals (by (2.7.1) above) and hence is a division ring (by (2.4.6) above). $\diamond$

2.8.5 Examples of local rings: 1. All division rings (and in particular fields) are local rings. The set of non-units is (0) and it is the maximal ideal.

2. For any division ring D , $D[[X_1, X_2, \dots, X_n]]$ is a local ring. Recall that an element of $D[[X_1, X_2, \dots, X_n]]$ is a unit if and only if its constant term is a unit in D , i.e., its constant term is non-zero in D . Hence the set of all non-units in $D[[X_1, X_2, \dots, X_n]]$ is the set of all formal power series in $X_1, X_2, \dots, X_n$, whose constant term is zero, i.e., $\{(a_1X_1 + a_2X_2 + \dots + a_nX_n) + \text{higher degree terms}\}$, the ideal generated by $X_1, X_2, \dots, X_n$.

3. $\mathbb{Q}^p = \{a/b \in \mathbb{Q} \mid a, b \in \mathbb{Z}, (a, b) = 1 \text{ and } p \nmid b\}$, the ring of p -adic integers (1.8.7), is a local ring for any prime number p .

2.8.6 Examples of non-local rings: 1. The ring of integers $\mathbb{Z}$ is not local since its set of non-units is $\mathbb{Z} - \{\pm 1\}$ which is not even a subgroup of $\mathbb{Z}$.

2. The polynomial ring $K[X]$ over a field K is not local. The set of non-units in $K[X]$ is $K[X] - K^*$, i.e., the set of all non-constant polynomials together with 0 which is not a subgroup of $(K[X], +)$.

3. The matrix ring $M_n(R)$ (over a ring R with 1) is not local (i) if

R is not local or (ii) $n \geq 2$ when R is local.

For, the first case is obvious and in the second case we have non-units $E_{11}, E_{22}, \dots, E_{nn}$ whose sum $E_{11} + E_{22} + \dots + E_{nn} = 1$ is a unit.

2.8.7 Theorem: *The characteristic of a local ring is either 0 or a power of a prime.*

Proof: Let R be a local ring (with 1). Suppose $\text{char } R = n \neq 0$. Let, if possible, n be divisible by two distinct primes p and q . We know that $1 = mp + nq$ for some $m, n \in \mathbb{Z}$. Since $p \cdot 1$ and $q \cdot 1$ are (non-zero) zero-divisors in R , both are non-units and hence are elements of the maximal ideal M of R . But then $1 = (mp + nq) \cdot 1 = m(p \cdot 1) + n(q \cdot 1) \in M$ which is a contradiction. $\diamond$

2.8.8 Proposition: *For $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is a local ring if and only if n is a power of a prime.*

Proof: Let $\mathbb{Z}/n\mathbb{Z}$ be local. Then $n = \text{Char } \mathbb{Z}/n\mathbb{Z}$ is a power of a prime. Conversely, let $n = p^r$ be a power of a prime p and $r \geq 1$. Notice that the set of non-units of $\mathbb{Z}/p^r\mathbb{Z}$ is simply all integral multiples of $\bar{p}$ which obviously is an ideal, as required. $\diamond$

2.8.9 Semi-local ring: A commutative ring with 1 is called a *semi-local ring* if it has only finitely many maximal ideals.

2.8.10 Example of a semi-local ring: Let $p_1, \dots, p_n$ be distinct prime numbers in $\mathbb{Z}$. Let

$$\mathbb{Q}^{(p_1, \dots, p_n)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid (a, b) = 1 = (p_i, b), \forall i, 1 \leq i \leq n \right\}.$$

It is easy to see that this is a subring of $\mathbb{Q}$ whose only maximal ideals are (p_i) , $1 \leq i \leq n$ and hence semi-local (and non-local if $n \geq 2$). ■

2.9 Exercises

Unless otherwise specified, an ideal means a left/right/2-sided ideal. When two or more ideals are referred to, all of them are supposed to be ideals of the same type.

1. Do Exs.(1.13.2) and (1.13.3) for ideals instead of subrings.
2. Give an example of a ring in which an ideal of an ideal is not an ideal.
3. In a commutative ring, show that the set of all nilpotent elements is an ideal. (Hint: Use Ex.(1.13.11) above.)
4. Let a, b be a pair of orthogonal idempotents in a ring R . Show that the principal left/right/ ideals generated by a and b are such that

$$(a)_l \cap (b)_l = (0) = (a)_r \cap (b)_r.$$
 However, give examples so that the principal 2-sided ideals are such that $(a) \cap (b) \neq (0)$.
5. Is the set of all zero-divisors in a Boolean ring containing atleast 3 elements an ideal?
6. Show that every prime ideal of a Boolean ring is maximal.
7. Let X be a non-empty set and $\mathcal{P}(X)$ be the Boolean ring of all subsets of X . Show that
 - any finitely generated ideal of $\mathcal{P}(X)$ is principal,
 - any principal ideal of $\mathcal{P}(X)$ is of the form $\mathcal{P}(Y)$ for some $Y \subseteq X$,
 - $\mathcal{P}(X)$ is a principal ideal ring (PIR) if and only if X is finite,
 - any minimal ideal is of the form $\mathcal{P}(\{x\})$ for some $x \in X$ and
 - $\forall x \in X, \mathcal{P}(X - \{x\})$ is a maximal ideal but not conversely unless X is finite.
8. Show that the additive group $(\mathbb{Q}, +)$ has no maximal subgroups but the ring $(\mathbb{Q}, +, \cdot)$ has maximal subrings. (Hint: Try $\mathbb{Q}^p$ (1.8.7).)
9. Show that the semi-local ring $\mathbb{Q}^{(p_1, \dots, p_n)}$ of (2.8.10) is the intersection (in $\mathbb{Q}$) of the local rings $\mathbb{Q}^{p_i}$, $1 \leq i \leq n$.
10. For an ideal I in a commutative ring R , let $\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$, called the *radical* or the *square root* of I . Show that
 - $\sqrt{I}$ is an ideal of R containing I , in particular, the set of all nilpotent elements is an ideal,

- $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$ (but not conversely, $\sqrt{I} = \sqrt{J}$ but I and J may be incomparable),
 - $\sqrt{\sqrt{I}} = \sqrt{I}$ and
 - $R/\sqrt{I}$ has no non-trivial nilpotent elements.
11. Show that $\sqrt{I}$ is the intersection of all prime ideals containing I . What does this mean for $I = (0)$? (See (2.2.9) above.)
 12. For a positive integer m , show that $\sqrt{(m)} = (n)$ in $\mathbb{Z}$ where n is the product of all the distinct prime divisors of m . For example, $\sqrt{(9)} = \sqrt{(27)} = \sqrt{(3)}$ and $\sqrt{(30)} = \sqrt{(60)} = \sqrt{(90)} = \sqrt{(300)}$, etc. Deduce that m is *square free* if and only if $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ has no non-trivial nilpotent elements. (See (2.7.5) above.)
 13. Let $R = \mathcal{C}([0,1], \mathbb{R})$. For $x \in [0,1]$, let $M_x = \{f \in R \mid f(x) = 0\}$. Then show that M_x is a maximal ideal in R and every maximal ideal of R is of this form. (Hint: Use compactness of the interval $[0,1]$.) Show that the result is not true if we replace $[0,1]$ by $(0,1)$. (Hint: Look at the ideal I generated by the set of all functions each of which vanishes outside a compact subset of $(0,1)$ and apply Zorn's lemma to get a maximal ideal containing I .) What happens in the case when $[0,1]$ is replaced by $\mathbb{R}$?
 14. Let $\mathbb{C}\{z\}$ be the ring of Complex entire functions (1.8.8). For $\lambda \in \mathbb{C}$, let M_λ be the set of all entire functions which have a zero at λ . Show that M_λ is a maximal ideal in $\mathbb{C}\{z\}$. Is every maximal ideal of $\mathbb{C}\{z\}$ of this form for some λ ? (Try a maximal ideal containing all entire functions each of which has zeros at all but finitely many integers.)
 15. Show that a prime ideal in a finite commutative ring with 1 is maximal.
 16. Show that for a commutative ring R , the principal ideal (X) is prime in $R[X]$ if and only if R is an integral domain.
 17. Show that for any prime ideal P of a commutative R , the ideal $P[X]$ is prime in $R[X]$. However, show that a prime ideal in $R[X]$ need not be of this form. Secondly, show that $P[X]$ is never maximal in $R[X]$ even if P is maximal in R .
 18. Show that the intersection of two prime ideals is prime if and only if one of them is contained in the other.

19. Show that the principal ideal $(1 + i)$ in $\mathbb{Z}[i]$ is maximal. (Hint: $m + in \equiv (m - n) \pmod{1 + i}$, $\forall m, n \in \mathbb{Z}$ and $2 \equiv 0 \pmod{1 + i}$.) (See (4.7.10)–(4.7.16), for some more exercises of this kind.)
20. Let S be a subring of a commutative ring R having the same unity as R . Show that $P \cap S$ is a prime ideal of S for every prime ideal P of R . However, give an example to show that $M \cap S$ need not be maximal in S if M is maximal in R . What happens if $1_S \neq 1_R$?
21. Show that an ideal P in a commutative ring R is prime $\iff$ for any pair of ideals I and J with $IJ \subseteq P \Rightarrow I \subseteq P$ or $J \subseteq P$. This property of prime ideals in commutative rings allows a generalisation to the non-commutative rings as follows.
22. Let P be a 2-sided ideal in a ring R with unity. Show that the following are equivalent.
- If $a, b \in R$ are such that $aRb \subseteq P$, then $a \in P$ or $b \in P$.
 - If $a, b \in R$ are such that $RaRb$ (resp. $aRbR$) $\subseteq P$, then $a \in P$ or $b \in P$.
 - If I and J are left (resp. right) ideals in R such that $IJ \subseteq P$, then either $I \subseteq P$ or $J \subseteq P$.
- A 2-sided ideal P of a ring R is called a *prime ideal* if $P \neq R$ and it satisfies any one (and hence all) of the above properties.
23. Show that a maximal 2-sided ideal is a prime ideal in any ring. In particular, (0) is a prime ideal in $M_n(D)$ for any division ring D and $n \in \mathbb{N}$. (Prove this from first principles without using that (0) is a maximal 2-sided ideal but perhaps using the fact that the left annihilator of a non-zero left ideal is (0) in $M_n(D)$.)
- Caution:** The above example shows that unlike in the commutative case, saying that R is an integral domain is *not* the same as saying that (0) is a prime ideal in R . The following gives the exact equivalence.
24. Show that a ring R is an integral domain if and only if $R \neq (0)$, R has no non-trivial nilpotent elements and (0) is a prime ideal in R .
25. If I and J are ideals in a ring R with 1 which are *coprime* or *comaximal*, i.e., $I + J = R$, show that I^m and J^n are coprime for all $m, n \in \mathbb{N}$. (Hint: If $K = I^m + J^n \neq R$, apply Zorn's lemma.)
26. Prove the associativity and distributive laws for ideals, i.e., for all ideals I, J and K , we have $I(JK) = (IJ)K$, $I(J + K) = IJ + IK$ and $(I + J)K = IK + JK$.

27. Show that a quotient of a principal ideal ring ($P \mid R$) is one such.
28. Show that the ideal I_2 consisting of all polynomials in $\mathbb{Z}[X]$ with constant term even is a non-principal maximal ideal. Do the same with “even” replaced by “multiples” of a fixed prime number p in $\mathbb{Z}$. If I_p is this ideal, show that $\mathbb{Z}[X]/I_p = \mathbb{Z}/p\mathbb{Z} (= \mathbb{Z}_p)$.
29. Show that $K[X]$ and $K[[X]]$ are P I D's for any field K . (Hint: Pick an element of least degree (resp. order (1.5.2)) in any non-zero ideal.)
30. Show that $K[X, Y]$ or $K[[X, Y]]$ is *not* a P I D. (Hint: Look at the ideal generated by X and Y .)
31. Show that $\mathbb{Q}^P$ (1.8.7) is a P I D as well as a local ring (2.8.2).
32. Show that $R[[X]]$ is a local ring if and only if R is so. But show that $R[X]$ is not local whatever be R .
33. Show that a ring R with 1 is local if and only if for every $x \in R$, either x or $1 - x$ is a unit in R . Deduce that the only idempotents in a local ring are 0 and 1.
34. Show that a quotient of a local ring by a 2-sided ideal is local.
35. Let M be a maximal ideal in a commutative ring R with 1. Show that R/M^n is a local ring for any positive integer n . Is a similar result true for a maximal 2-sided ideal in a non-commutative ring?
36. If an ideal is contained in the union of two others, show that it must be contained in one of them. What happens if the union is of three or more ideals?
37. If an ideal is contained in the union of finitely many *prime* ideals, show that it must be contained in one of them.
(Hints: $I \subseteq \bigcup_{i=1}^n P_i$, $I \not\subseteq P_i$, $\forall i \Rightarrow \exists x_i \in I$ with $x_i \notin P_j$, $\forall j \neq i$; let $y_i = \prod_{j \neq i} x_j$ and look at $y = \sum_{i=1}^n y_i$.)
38. Let R be a commutative ring with 1 and $\text{Spec}(R)$ be the set of all prime ideals of R , called the *prime spectrum* of R . For an ideal I in R , let $V(I) = \{P \in \text{Spec}(R) \mid I \subseteq P\}$. Show that
 - $\text{Spec}(R) \neq \emptyset$ and $V(I) = \text{Spec}(R/I)$,
 - $V(I) = V(\sqrt{I})$,
 - $V(I) = \emptyset \Leftrightarrow I = R$,

- $V(I) = \text{Spec}(R) \Leftrightarrow I$ is a nil ideal,
 - $V(I) \subseteq V(J) \Leftrightarrow \sqrt{I} \supseteq J$ and
 - $V(I) = V(J) \Leftrightarrow \sqrt{I} = \sqrt{J}$ (but I and J may be even incomparable).
39. Show that the family of subsets $\{V(I) \mid I \text{ an ideal in } R\}$ of $\text{Spec}(R)$ satisfies the axioms of closed sets and hence defines a topology, called the *Zariski topology* on $\text{Spec}(R)$.
40. Show that $\text{Spec}(\mathbb{Z}) = \{(0), (2), (3), (5), \dots, (p), \dots\}$ and that the Zariski topology on $\text{Spec}(\mathbb{Z})$ has the following properties.
- It is a T_0 space but not T_1 ,
 - (0) is the only non-closed point,
 - closed sets are precisely the finite subsets not containing (0) or the whole space,
 - (0) is a *generic point*, i.e., $\{(0)\}$ is *dense* in $\text{Spec}(\mathbb{Z})$ and
 - the intersection of two non-empty open sets is non-empty.
41. Show that the Zariski topology on $\text{Spec}(R)$ is compact and that it is connected if and only if R has no non-trivial idempotents.
42. If R is a commutative local ring with 1, show that $\text{Spec}(R)$ contains only one closed point and that point is in the closure of every non-empty subset. Hence deduce that $\text{Spec}(R)$ is connected.
43. Show that the characteristic of a simple ring is either 0 or a prime. (Hint: If $\text{Char } R = n \neq 0$, take a prime divisor p of n and look at the ideal $\{x \in R \mid px = 0\}$.)
44. Define an ideal in a Lie ring L (1.13.31) and show that a 2-sided ideal in any ring R is an ideal in the associated Lie ring $L(R)$. Is the converse true? Are left/right ideals in R also ideals in $L(R)$?
45. Show that the centre $Z(L)$ of a Lie ring L is an ideal in L . Give an example of a ring R whose centre $Z(R)$ is not an ideal in R . ■

2.10 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counter-example if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be.

1. In $\mathcal{C}([0, 1], \mathbb{R})$, the set of all differentiable functions is an ideal.
2. A non-zero element a in a ring R with 1 is a unit if the principal 2-sided ideal $(a) = R$.
3. The ring $M_n(\mathbb{Z})$ has infinitely many maximal 2-sided ideals.
4. The ring $M_n(\mathbb{Z})$ has infinitely many minimal 2-sided ideals.
5. If R has 1, union of all maximal left ideals is the set of all non-units.
6. The maximal ideal of $\mathbb{Q}[[X, Y]]$ is a principal ideal.
7. The ring $\mathbb{Q}[[X, Y]]$ is local.
8. The ring $\mathbb{Z}$ contains minimal ideals.
9. The ring $M_2(\mathbb{Q})$ has no minimal left ideals.
10. The 2-sided ideal generated by $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ in $M_2(\mathbb{Z})$ is the unit ideal.
11. In the ring $\mathbb{Z}$, $\sqrt{(256)} = (16)$ and $\sqrt{(16)} = (4)$.
12. In a commutative ring with 1, an ideal is maximal if R/I is a field.
13. In the ring $\mathbb{Z}$, $\sqrt{(50)} = (10)$.
14. The ring $M_n(\mathbb{Q})$ is local if and only if $n = 1$.
15. m and n in $\mathbb{N}$ are coprime if the ideals (m) and (n) are coprime.
16. The principal ideal (2) in $\mathbb{Z}[i]$ is a prime ideal.
17. The ideal (0) is maximal in $\mathbb{Q}[i]$.
18. The ideal (0) is maximal in $\mathbb{Z}[i]$.
19. R local with its maximal ideal $M_R \Rightarrow R/M_R$ is a division ring.
20. In the ring $\mathcal{C}([0, 1], \mathbb{R})$, the ideal (0) is prime.
21. Quotient of a local ring is local.
22. Every left ideal in a ring R is an ideal in the Lie ring $L(R)$.
23. Every ideal in the Lie ring $L(R)$ is a 2-sided ideal in the ring R .
24. Centre of a Lie ring L is an ideal in L .
25. Centre of a ring R is a 2-sided ideal in R . ■

Chapter 3

Homomorphisms of Rings

In this chapter, we study homomorphisms of rings which are natural extensions from that of groups. The purpose, concepts, terminology, properties, even proofs, etc., are exactly as in the case of groups (with a few specialities on either side here and there).

3.1 Definitions and Basic Properties

3.1.1 Homomorphism: A mapping $f : R \rightarrow S$ of rings R and S is called a *homomorphism* (of rings) if, for all $x, y \in R$, we have

1. $f(x + y) = f(x) + f(y)$ and
2. $f(xy) = f(x)f(y)$.

Remark: If f is a homomorphism, it is easy to check that $f(0) = 0$, $f(-x) = -f(x)$, but not necessarily $f(1_R) = 1_S$. In case $f(1_R) = 1_S$, then f is said to be *unitary*.

Example: Consider $f : R \rightarrow R \times S$ given by $x \mapsto (x, 0)$. This is a homomorphism, but $f(1_R) = (1_R, 0) \neq (1_R, 1_S)$, the unity of $R \times S$. However, if R and S are division rings and $f \neq 0$, then $f(1_R) = 1_S$. Since $f : R^* \rightarrow S^*$ is then a homomorphism of multiplicative groups R^* and S^* and hence $f(1_R) = 1_S$ (where $R^* = R - \{0\}$, etc.)

3.1.2 Kernel of a homomorphism: The *kernel of a homomorphism* $f : R \rightarrow S$ is defined to be the set $\{x \in R \mid f(x) = 0\}$ and is

denoted by $\text{Ker}(f)$, i.e., $\text{Ker}(f) = \{x \in R \mid f(x) = 0\}$.

3.1.3 Types of homomorphisms: A homomorphism $f : R \rightarrow S$ of rings R and S is called

- a *monomorphism*, if f is injective,
- an *epimorphism*, if f is surjective,
- an *isomorphism*, if f is bijective,
- an *endomorphism*, if $R = S$ and
- an *automorphism*, if $R = S$ and f is an isomorphism.

3.1.4 Composition of homomorphisms: Let $f : R \rightarrow S$ and $g : S \rightarrow T$ be homomorphisms. Then we have the following.

1. $g \circ f : R \rightarrow T$ is a homomorphism.
2. $g \circ f : R \rightarrow T$ is a monomorphism if f and g are monomorphisms. The converse is *not* true. However, if $g \circ f$ is a monomorphism, then f is a monomorphism (while g need not be).
3. $g \circ f : R \rightarrow T$ is an epimorphism if both g and f are epimorphisms. The converse is *not* true. However, if $g \circ f$ is an epimorphism, then g is an epimorphism (while f need not be).
4. $g \circ f$ is an isomorphism if both g and f are isomorphisms. The converse is *not* true. However, if $g \circ f$ is an isomorphism, then f is a monomorphism and g is an epimorphism.

3.1.5 Theorem: *Let I be an ideal in a ring R . Then I is a 2-sided ideal in R if and only if I is the kernel of some homomorphism $f : R \rightarrow S$ for a suitable ring S .*

Proof: Suppose I is a 2-sided ideal of R . Then take $S = R/I$, and $f : R \rightarrow R/I$ be the natural quotient map $x \mapsto x + I$. Let $x, y \in R$. Then we have

- $f(x + y) = (x + y) + I = (x + I) + (y + I) = f(x) + f(y)$ and
- $f(xy) = (xy) + I = (x + I)(y + I) = f(x)f(y)$.

Thus f is a homomorphism of rings. Now we have

- $\text{Ker}(f) = \{x \in R \mid f(x) = 0\} = \{x \in R \mid x + I = 0 \text{ in } R/I\}$
 $= \{x \in R \mid x \in I\} = I$, as required.

Conversely, suppose R and S are rings and $f : R \rightarrow S$ is a homomorphism of rings. Let $I = \text{Ker}(f)$. To show that I is a 2-sided ideal in

R , take $x, y \in I$. Then we have $f(x) = 0 = f(y)$. Since f is a homomorphism, we have $f(x - y) = f(x) - f(y) = 0$. Therefore $x - y \in I$. Secondly, if $r \in R$ and $x \in I$, then we have $f(rx) = f(r)f(x) = f(r)0 = 0$, i.e., $rx \in I$. Similarly, $xr \in I$, as required. $\diamond$

3.1.6 Theorem: *A homomorphism $f : R \rightarrow S$ is a monomorphism if and only if $\text{Ker}(f) = (0)$.*

Proof: Suppose $f : R \rightarrow S$ is a monomorphism. Let $x \in \text{Ker}(f)$. Then $f(x) = 0 = f(0)$. But f being a monomorphism, we have $x = 0$. Hence $\text{Ker}(f) = (0)$. Conversely, suppose $\text{Ker}(f) = (0)$ and $x, y \in R$ such that $f(x) = f(y)$. Then we have $f(x - y) = f(x) - f(y) = 0$. This means that $x - y \in \text{Ker}(f) = (0)$ which shows that $x - y = 0$. Hence $x = y$, i.e., f is a monomorphism. $\diamond$

3.1.7 Remarks: 1. Suppose $f : R \rightarrow S$ and $g : S \rightarrow T$ are homomorphisms of rings. Then $\text{Ker}(g \circ f) \supseteq \text{Ker}(f)$ (equality need not hold). If $g \circ f$ is a monomorphism, then f is a monomorphism.

2. Similarly, we have $\text{Im}(g \circ f) \subseteq g(\text{Im}(f))$ (equality need not hold). If $g \circ f$ is an epimorphism, then g is an epimorphism.

3. Any homomorphism $f : R \rightarrow S$ from a *simple ring* R (2.4.12) (to any ring S) is either identically zero or a monomorphism (because $\text{Ker}(f)$ is a 2-sided ideal in R).

Notation: If a ring R is isomorphic to another S by means of an isomorphism $\varphi : R \rightarrow S$, then we write $R \xrightarrow{\varphi} S$ or $R \xrightarrow{\sim} S$ or $R \xrightarrow{\cong} S$ or simply $R \approx S$.

3.1.8 Examples: 1. Let X be a non-empty set and $\text{Maps}(X, R)$ be the set of all R -valued set maps defined on X for any ring R . Under pointwise addition and multiplication of maps (1.2.1), $\text{Maps}(X, R)$ is a ring (with 1 if and only if R has 1 and it is commutative if and only if R is so). The natural map $\varphi : \text{Maps}(X, R) \rightarrow \prod_X R$, $\varphi(f) = (f(x))_{x \in X}$, is an isomorphism of rings.

2. The natural map $\psi : \mathcal{P}(X) \rightarrow \text{Maps}(X, \mathbb{Z}_2)$ defined by

$$A \mapsto \psi(A), \text{ where } \psi(A)(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A, \end{cases} \quad (\forall A \subseteq X)$$

is the *characteristic function* of the set A , is an isomorphism and consequently, $\varphi \circ \psi: \mathcal{P}(X) \rightarrow \prod_X \mathbb{Z}_2$ is an isomorphism of the Boolean rings (see (1.7.2) and (1.9.3) above).

3. If $X = \mathbb{Z}^+$ is a *countably infinite* set, then we have natural isomorphisms of rings, namely,

$$\left(\prod_{n=0}^{\infty} R \right) \xrightarrow{\varphi^{-1}} \text{Maps}(\mathbb{Z}^+, R) \approx \text{Seq}(R) \approx R[[T]].$$

(See Ex.(1.13.39) above, for the ring $\text{Seq}(R)$.) Under this isomorphism, the polynomial subring $R[X]$ of $R[[X]]$ corresponds to the subring $\text{Maps}_0(\mathbb{Z}^+, R)$ of $\text{Maps}(\mathbb{Z}^+, R)$ consisting of all maps $f: \mathbb{Z}^+ \rightarrow R$ of *finite support*, i.e., $f(n) = 0$ for all but finitely many $n \in \mathbb{Z}^+$. ■

3.2 Fundamental Theorems of Homomorphisms

3.2.1 The Epimorphism Theorem: *Let $f: R \rightarrow S$ be a homomorphism of rings with $I = \text{Ker}(f)$. Then there exists a unique monomorphism $\tilde{f}: R/I \rightarrow S$ such that the diagram*

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ \eta \searrow & & \nearrow \tilde{f} \\ & R/I & \end{array}$$

commutes, i.e., $f = \tilde{f} \circ \eta$, where η is the natural map from R to R/I . Moreover, $\tilde{f}$ is an isomorphism if and only if f is an epimorphism.

Proof: Let $\tilde{f}: R/I \rightarrow S$ be defined by $\tilde{f}(x + I) = f(x)$, $\forall x \in R$.

Step 1. $\tilde{f}$ is well-defined.

For, let $x + I = y + I$ for some $x, y \in R$. This means that $x - y \in I$, i.e., $x - y \in \text{Ker}(f)$. Thus $f(x - y) = 0$, i.e., $f(x) = f(y)$ (f being a homomorphism), hence $\tilde{f}(x + I) = \tilde{f}(y + I)$, as required.

Step 2. $\widetilde{f}$ is injective.

For, let $\widetilde{f}(x + I) = \widetilde{f}(y + I)$. Then we have to show that $x + I = y + I$. 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 $x - y \in \text{Ker}(f) = I$. Hence $x + I = y + I$, as required.

Step 3. $\widetilde{f}$ is a homomorphism.

For all $x, y \in R$ we have

- $\widetilde{f}((x + I) + (y + I)) = \widetilde{f}(x + y + I) = f(x + y) = f(x) + f(y) = \widetilde{f}(x + I) + \widetilde{f}(y + I)$ and
- $\widetilde{f}((x + I)(y + I)) = \widetilde{f}(xy + I) = f(xy) = f(x)f(y) = \widetilde{f}(x + I)\widetilde{f}(y + I)$, as required.

Step 4. $\widetilde{f}$ is an isomorphism if and only if f is an epimorphism.

For, we have $f = \widetilde{f} \circ \eta$. If $\widetilde{f}$ is an isomorphism, then $\widetilde{f}$ is an epimorphism. The natural map η is also an epimorphism. Then by Step 3, f is an epimorphism. Similarly f an epimorphism implies that $\widetilde{f}$ is an epimorphism, hence an isomorphism. $\diamond$

3.2.2 Theorem: (Quotient of a quotient) If $I \subseteq J$ are both 2-sided ideals in R , then $(R/I)/(J/I)$ is naturally isomorphic to R/J .

Proof: Consider the following diagram

$$\begin{array}{ccc}
 & R & \\
 \eta_I \swarrow & & \searrow \eta_J \\
 R/I & \xrightarrow{\eta_{IJ}} & R/J \\
 \eta_{R/J} \searrow & & \nearrow \widetilde{\eta} = \widetilde{\eta}_{IJ} \\
 & (R/I)/(J/I) &
 \end{array}$$

Define $\widetilde{\eta} : (R/I)/(J/I) \rightarrow R/J$ by $\widetilde{\eta}(a + I + J/I) = a + J$.

Step 1. $\widetilde{\eta}$ is well-defined.

For, let $a, b \in R$ be such that $a + I + J/I = b + I + J/I$. Then

- $(a + I) - (b + I) \in J/I \implies (a - b) + I \in J/I \implies a - b \in J \implies a + J = b + J$, i.e., $\widetilde{\eta}(a + I + J/I) = \widetilde{\eta}(b + I + J/I)$, as required.

Step 2. $\tilde{\eta}$ is a homomorphism of rings.

For, let $a, b \in R$. Then we have

- $\tilde{\eta}((a + I + J/I) + (b + I + J/I)) = \tilde{\eta}(a + b + I + J/I) = a + b + J = (a + J) + (b + J) = \tilde{\eta}(a + I + J/I) + \tilde{\eta}(b + I + J/I)$ and
- $\tilde{\eta}((a + I + J/I)(b + I + J/I)) = \tilde{\eta}(ab + I + J/I) = ab + J = (a + J)(b + J) = \tilde{\eta}(a + I + J/I)\tilde{\eta}(b + I + J/I)$, as required.

Step 3. $\tilde{\eta}$ is surjective.

For, let $x \in R/J$, say $x = a + J$ for some $a \in R$. Now we have $\tilde{\eta}(a + I + J/I) = a + J = x$, as required.

Step 4. $\tilde{\eta}$ is injective.

For, by definition, we have

$$\begin{aligned} \text{Ker}(\tilde{\eta}) &= \{a + I + J/I \in (R/I)/(J/I) \mid \tilde{\eta}(a + I + J/I) = 0\} \\ &= \{a + I + J/I \in (R/I)/(J/I) \mid a + J = J\} \\ &= \{a + I + J/I \in (R/I)/(J/I) \mid a \in J\} \\ &= J/I = 0 \text{ in } (R/I)/(J/I), \text{ as required.} \quad \diamond \end{aligned}$$

This theorem can also be stated as follows.

3.2.3 Theorem: Suppose I and J are 2-sided ideals in a ring R . Then the natural map $\eta_{IJ} : R/I \rightarrow R/J$, defined by $a + I \mapsto a + J$ is well-defined if and only if $I \subseteq J$. Moreover, η_{IJ} is an epimorphism whose kernel is J/I . Hence $(R/I)/(J/I)$ is isomorphic to R/J .

Proof: Step 1. Suppose $\eta_{IJ} : R/I \rightarrow R/J$ is defined by $a + I \mapsto a + J$ for all $a \in R$. Assume that η_{IJ} is well-defined. In particular, for $x \in I$ we have $x + I = 0 + I$, hence $\eta_{IJ}(x + I) = \eta_{IJ}(0 + I) = \eta_{IJ}(I)$, i.e., $x + J = 0 + J$, or $x \in J$. Therefore, $I \subseteq J$. Conversely, suppose $I \subseteq J$ and $a + I = b + I$ for some $a, b \in R$. Then $a - b \in I \subseteq J$, i.e., $a + J = b + J$ and hence we have $\eta_{IJ}(a + I) = \eta_{IJ}(b + I)$. Therefore, η_{IJ} is well-defined.

Step 2. η_{IJ} is a homomorphism of rings.

For, let $a, b \in R$. Then we have

- $\eta_{IJ}((a + I) + (b + I)) = \eta_{IJ}(a + b + I) = a + b + J = (a + J) + (b + J) = \eta_{IJ}(a + I) + \eta_{IJ}(b + I)$. Similarly,

- $\eta_{IJ}((a+I)(b+I)) = \eta_{IJ}(ab+I) = ab+J = (a+J)(b+J) = \eta_{IJ}(a+I)\eta_{IJ}(b+I)$, as required.

Step 3. η_{IJ} is surjective.

Consider an $x \in R/J$. Then $x = a+J$ for some $a \in R$. But $a+I \in R/I$ and $\eta_{IJ}(a+I) = a+J = x$, as required.

Step 4. η_{IJ} is injective.

For, we have

$$\begin{aligned} \text{Ker}(\eta_{IJ}) &= \{a+I \in R/I \mid \eta_{IJ}(a+I) = 0\} \\ &= \{a+I \in R/I \mid a+J = J\} \\ &= \{a+I \in R/I \mid a \in J\} = J/I, \text{ as required.} \end{aligned}$$

Now by (3.2.1) above, we get that $(R/I)/(J/I) \approx R/J$. $\diamond$

3.2.4 Corollary: If $m, n \in \mathbb{Z}$, then the natural map $\eta: \mathbb{Z}/m\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, sending $a+m\mathbb{Z} \mapsto a+n\mathbb{Z}$, is well-defined if and only if (i) $m\mathbb{Z} \subseteq n\mathbb{Z}$, or, if and only if (ii) m is a multiple of n . This map is a surjective homomorphism of rings with kernel being $n\mathbb{Z}/m\mathbb{Z} = \{kn+m\mathbb{Z} \mid k \in \mathbb{Z}\}$.

3.2.5 Corollary: Let $f: R \rightarrow S$ be a homomorphism of rings. Then we have the following.

1. $\text{Ker}(f)$ is a prime ideal if S is an integral domain.
2. $\text{Ker}(f)$ is a maximal ideal if f is surjective and S is a field.

3.2.6 Theorem: If I is a 2-sided ideal of R , then $I[X]$ is a 2-sided ideal of $R[X]$ and the quotient ring $R[X]/I[X]$ is naturally isomorphic to $(R/I)[X]$.

Proof: Let I be a 2-sided ideal in R . Then it is easy to check that

$$I[X] = \{a_0 + a_1X + a_2X^2 + \cdots + a_rX^r \mid a_i \in I\}$$

is a 2-sided ideal in $R[X]$. Now look at the natural map $f: R[X] \rightarrow (R/I)[X]$, defined by $a(X) = a_0 + a_1X + a_2X^2 + \cdots + a_rX^r \mapsto \bar{a}_0 + \bar{a}_1X + \bar{a}_2X^2 + \cdots + \bar{a}_rX^r$ (where $\bar{a} = a+I$, $\forall a \in R$). It can easily be checked that this is an epimorphism and $\text{Ker}(f) = I[X]$ because

$$\text{Ker}(f) = \{a(X) \in R[X] \mid \bar{a}_0 + \bar{a}_1X + \bar{a}_2X^2 + \cdots + \bar{a}_rX^r = \bar{0}\}$$

$$\begin{aligned}
&= \{a(X) \in R[X] \mid \bar{a}_0 = 0, \bar{a}_1 = 0, \dots, \bar{a}_r = 0\} \\
&= \{a_0 + a_1X + a_2X^2 + \dots + a_rX^r \mid a_i \in I\} = I[X].
\end{aligned}$$

Then by (3.2.1) above, we have $R[X]/I[X] \approx (R/I)[X]$. $\diamond$

3.2.7 Remark: In a similar way as above, we can show that the rings $R[[X]]/I[[X]]$ and $(R/I)[[X]]$ are isomorphic.

3.2.8 Corollary: *The ideal $I[X]$ (resp. $I[[X]]$) is a prime ideal in $R[X]$ (resp. $R[[X]]$) if and only if I is a prime ideal in R .*

3.2.9 Remarks: Let $f: R \rightarrow S$ be a homomorphism of rings. Then we have the following.

1. *Image of an additive subgroup of R is an additive subgroup of S , i.e., if A is a subgroup of $(R, +)$, then $f(A)$ is a subgroup of $(S, +)$.*

2. *Image of an ideal (left/right/2-sided) of R need not be an ideal in S unless f is an epimorphism.*

For, suppose f is an epimorphism and I is an ideal in R . Then, by (1), $f(I)$ is a subgroup of $(S, +)$. Let $a \in f(I)$ and $x \in S$, say $a = f(z)$ for some $z \in I$. Since f is onto, there is a $y \in R$ such that $f(y) = x \in S$. Now $xa = f(y)f(z) = f(yz) \in f(I)$ (since $yz \in I$). Hence $f(I)$ is an ideal in S . (The inclusion map $i: \mathbb{Z} \hookrightarrow \mathbb{Q}$ is not surjective and $i(2\mathbb{Z}) = 2\mathbb{Z}$ is not an ideal in $\mathbb{Q}$.)

3. *Inverse image of a subgroup of $(S, +)$ is a subgroup of $(R, +)$ and inverse image of an ideal in S is an ideal in R .*

For, let I be an ideal in S and $f^{-1}(I) = \{x \in R \mid f(x) \in I\}$. Let $x, y \in f^{-1}(I)$. Then $f(x), f(y) \in I$ and moreover $f(x) - f(y) = f(x - y) \in I$ (since I is a subgroup of $(S, +)$ and f is a homomorphism). This implies that $x - y \in f^{-1}(I)$. Therefore, $f^{-1}(I)$ is a subgroup of $(R, +)$. Let $r \in R$ and $x \in f^{-1}(I)$. Then, f being a homomorphism, $f(rx) = f(r)f(x)$ and $f(r)f(x) \in I$ because $f(r) \in S$, $f(x) \in I$, i.e., $rx \in f^{-1}(I)$. Hence $f^{-1}(I)$ is an ideal in R .

4. *Inverse image of a prime ideal is a prime ideal in R if both R and S are commutative.*

For, let P be a prime ideal in S , (i.e., $x, y \in S$, $xy \in P$ implies $x \in P$ or $y \in P$). By (3), $f^{-1}(P)$ is an ideal in R . Let $ab \in f^{-1}(P)$,

i.e., $f(ab) \in P$. Since P is a prime ideal, $f(a)f(b) \in P$ implies either $f(a) \in P$ or $f(b) \in P$, i.e., either $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$. Therefore, $f^{-1}(P)$ is a prime ideal in R .

5. Inverse image of a maximal ideal in S need not be a maximal ideal in R unless f is surjective.

For, let M be a maximal ideal in S . By (3), $f^{-1}(M)$ is an ideal in R containing $\text{Ker}(f)$. Since $R/\text{Ker}(f)$ is isomorphic to S (because f is surjective) and $f^{-1}(M)$ is an ideal containing $\text{Ker}(f)$, we know that $f^{-1}(M)$ is maximal in R if and only if M is maximal in S . Furthermore, we have $(R/\text{Ker}(f))/f^{-1}(M) \xrightarrow{\sim} S/M$. Hence, if M is maximal, then S/M is a field, i.e., $(R/\text{Ker}(f))/(f^{-1}(M)/\text{Ker}(f)) = R/f^{-1}(M)$ is a field, or, $f^{-1}(M)$ is a maximal ideal in R . (Consider the inclusion $i: \mathbb{Z} \hookrightarrow \mathbb{Q}$. We know that (0) is a maximal ideal in $\mathbb{Q}$ but $i^{-1}((0)) = (0)$ is not maximal in $\mathbb{Z}$.)

6. Homomorphic image of a PIR is a PIR (2.3.7).

For, let $f: R \rightarrow S$ be a homomorphism of rings with R a PIR. First we show that R is a PIR implies that R/I is a PIR for all ideals I in R . Let J be any ideal in R/I , then we shall show that J is a principal ideal. We know that there is a unique ideal J_0 in R , $J_0 \supseteq I$ with $J_0/I = J$. Since J_0 is an ideal in R we have $J_0 = (a)$ for some $a \in J_0$. Now we have $J_0/I = (a + I)$. We have $a + I \in J_0/I$ (since $a \in J_0$). On the other hand, let $x \in J_0/I$. This means that $x = x_0 + I$ for some $x_0 \in J_0 = (a)$, i.e., $x_0 = na + ra$ for some $n \in \mathbb{Z}$ and $r \in R$. Hence $x_0 + I = (na + I) + (ra + I) = n(a + I) + (r + I)(a + I) \in (a + I)$, i.e., $x_0 \in (a + I)$ implies that $J_0/I \subseteq (a + I)$. Hence $J_0/I = (a + I)$. This is true, in particular, for the ideal $I = \text{Ker}(f)$. Now by (3.2.1) above, we have $f(R) \approx R/I$ which is a PIR, as required. ■

3.3 Endomorphism Rings

One of the most important classes of rings is the following.

3.3.1 Endomorphism ring of an abelian group: Let G be an abelian group, written additively. Let $\text{End}_{\mathbb{Z}}G$ be the set of all group homomorphisms of G into itself, i.e.,

- $\text{End}_{\mathbb{Z}}G = \{f : G \rightarrow G \mid f(x+y) = f(x) + f(y), \forall x, y \in G\}$.

$\text{End}_{\mathbb{Z}}G$ is a ring under pointwise addition and composition of maps, i.e., if $f, g \in \text{End}_{\mathbb{Z}}G$, then $f+g$ and $f \circ g$ are defined by

- $f+g : G \rightarrow G, x \mapsto f(x) + g(x), \forall x \in G$ and
- $f \circ g : G \rightarrow G, x \mapsto f(g(x)), \forall x \in G$.

Then it follows that $f+g$ and $f \circ g$ are both homomorphisms (since G is abelian) and we check that $(\text{End}_{\mathbb{Z}}G, +, \circ)$ is a ring with $1 = \text{Id}_G$, called the *endomorphism ring* of G . In general $\text{End}_{\mathbb{Z}}G$ is not commutative. Units of $\text{End}_{\mathbb{Z}}G$ are precisely the group of all automorphisms of G .

3.3.2 Endomorphism ring of a vector space: Let K be a field and V be a vector space over K . Let $\text{End}_K(V)$ be the set of all K -linear endomorphisms of V , i.e.,

- $\text{End}_K(V) = \{f : V \rightarrow V \mid f(x+y) = f(x) + f(y) \text{ and } f(\alpha x) = \alpha f(x), \forall x, y \in V, \alpha \in K\}$.

Then $\text{End}_K(V) \subseteq \text{End}_{\mathbb{Z}}(V)$ (V as an abelian group). Since the sum $f+g$ and the composition $f \circ g$ of K -linear maps, f, g of V are again K -linear maps, we get that $\text{End}_K(V)$ is a subring of $\text{End}_{\mathbb{Z}}(V)$, having the same unity as that of $\text{End}_{\mathbb{Z}}(V)$, called the endomorphism ring of the vector space V .

3.3.3 Theorem: *The ring $\text{End}_K(V)$ is a simple ring (2.4.12) if and only if V is a finite dimensional vector space over the field K .*

Proof: Step 1. *If $\text{End}_K(V)$ is a simple ring, then V is finite dimensional over K .*

For, let, if possible, V be infinite dimensional over K . Let I be the set of all K -linear endomorphisms of V of *finite rank*, i.e., $I = \{f \in \text{End}_K(V) \mid \dim_K f(V) < \infty\}$. We note that $0 \in I$ and $1 \notin I$ so that $(0) \subseteq I \neq \text{End}_K(V)$.

Claim: *I is a proper 2-sided ideal of $\text{End}_K(V)$.* (This contradicts the hypothesis.)

(a): $I \neq (0)$. Let B be a K -basis of V . Consider any vector $v_0 \in B$. We have $v_0 \neq 0$. Define $f : B \rightarrow V$ such that $f(b) = v_0$, i.e., $f(b) = v_0$ for all $b \in B$. This extends uniquely to a K -linear map denoted again by $f : V \rightarrow V$. Now $f(V) = Kv_0$ which is a one dimensional

subspace of V . Thus $f \neq 0$ and $f \in I$.

(b): I is a 2-sided ideal of $\text{End}_K(V)$.

Let $f, g \in I$. Then $\dim_K(f(V))$ and $\dim_K(g(V))$ are finite. Now $(f - g)(V) \subseteq f(V) + g(V)$ which is finite dimensional over K . Hence $\dim_K((f - g)(V))$ is finite, i.e., $f - g \in I$.

Let $f \in I$ and $r \in \text{End}_K(V)$. We have $(r \circ f)(V) = r(f(V))$. This is finite dimensional (since $f(V)$ is finite dimensional). Hence $r \circ f \in I$. Similarly, $(f \circ r)(V) = f(r(V)) \subseteq f(V)$ is also finite dimensional. Thus $f \circ r \in I$. This proves the claim.

Step 2. *If V is finite dimensional, then $\text{End}_K(V)$ is a simple ring.*

For, let $\dim_K(V) = n < \infty$. Take any basis $B = \{v_1, \dots, v_n\}$ for V over K . With respect to the basis B of V , we recall that any K -linear map $f : V \rightarrow V$ can be identified with an $n \times n$ matrix over K as follows. For each i ($1 \leq i \leq n$), write

$$f(v_i) = \sum_{j=1}^n \alpha_{ji} v_j \text{ with } \alpha_{ji} \in K, 1 \leq i, j \leq n \text{ and } \lambda_f = (\alpha_{ij}).$$

Thus we have a map $\lambda : \text{End}_K(V) \rightarrow M_n(K)$, $f \mapsto \lambda_f$. It is obvious that λ is additive, surjective and $\text{Ker}(f) = (0)$. It is a routine checking that $\lambda_{f \circ g} = \lambda_f \cdot \lambda_g$, i.e., λ is an isomorphism of rings. Since $M_n(K)$ is a simple ring by (2.4.11) above, it follows that $\text{End}_K(V)$ is a simple ring, as required. ■

3.4 Field of Fractions

3.4.1 An equivalence relation: Given a commutative integral domain R with 1, consider the set $X = R \times R^*$ ($R^* = R - \{0\}$). Define a relation on X by saying that $(a, x) \sim (b, y)$ if $ay = bx$, for all $(a, x), (b, y)$ in X .

Claim: ' $\sim$ ' is an equivalence relation on X .

- *Reflexivity*: Clearly $(a, x) \sim (a, x)$, $\forall (a, x) \in X$.
- *Symmetry*: Now $(a, x) \sim (b, y)$, i.e., $ay = bx$, i.e., $bx = ay$ implies that $(b, y) \sim (a, x)$.

• *Transitivity:* $(a, x) \sim (b, y)$ and $(b, y) \sim (c, z) \implies (a, x) \sim (c, z)$.
 (We have $(a, x) \sim (b, y)$ implies that $ay = bx$ and $(b, y) \sim (c, z)$ implies that $bz = cy$. But $a(bz) = a(cy)$ implies that $a(zb) = (bx)c = b(xc) = (xc)b$ (since R is a commutative domain). Hence $az = xc$ which implies that $(a, x) \sim (c, z)$, as required.)

3.4.2 Addition and multiplication of fractions: Let $Q(R)$ be the set of all equivalence classes in X . For $(a, x) \in X$, we denote the equivalence class through (a, x) by the symbol $\frac{a}{x}$ or a/x , called the *fraction* associated to (a, x) . We have

$$\bullet (a, x) \sim (b, y) \iff ay = bx \iff a/x = b/y.$$

We make $Q(R)$ into a ring by defining,

$$\text{addition: } (a/x) + (b/y) = (ay + bx)/xy \text{ and}$$

$$\text{multiplication: } (a/x) \cdot (b/y) = ab/xy.$$

These binary operations on $Q(R)$ are well-defined because if $a/x = a'/x'$ and $b/y = b'/y'$, then we have to show that $(a/x) + (b/y) = (a'/x') + (b'/y')$ and $(a/x) \cdot (b/y) = (a'/x') \cdot (b'/y')$ i.e.,

$$\frac{ay + bx}{xy} = \frac{a'y' + b'x'}{x'y'} \quad \text{and} \quad \frac{ab}{xy} = \frac{a'b'}{x'y'}.$$

This follows easily since $ax' = a'x$ and $by' = b'y$.

3.4.3 Theorem: $(Q(R), +, \cdot)$ is a field containing R as a subring.

Proof: Step 1. $(Q(R), +, \cdot)$ is a field.

- $(Q(R), +)$ is an abelian group whose additive identity is

$$0_{Q(R)} = 0/1 = 0/x, \quad \forall x \in R^*$$

and the additive inverse of a/x is given by

$$-(a/x) = (-a)/x = a/(-x), \quad \forall x \in R^*.$$

- $(Q(R), \cdot)$ is a commutative semigroup with identity

$$1_{Q(R)} = 1/1 = x/x, \quad \forall x \in R^*.$$

- Distributive laws hold, i.e., $\forall a, b, c \in R, x, y, z \in R^*$, we have

$$\frac{a}{x} \left(\frac{b}{y} + \frac{c}{z} \right) = \frac{a}{x} \cdot \frac{b}{y} + \frac{a}{x} \cdot \frac{c}{z} \quad \text{and} \quad \left(\frac{a}{x} + \frac{b}{y} \right) \frac{c}{z} = \frac{a}{x} \cdot \frac{c}{z} + \frac{b}{y} \cdot \frac{c}{z}.$$

Consider any non-zero element α in $Q(R)$, i.e., $\alpha = a/x$, for some

$a, x \in R^*$. Now $x/a \in Q(R)$ and we have

$$\frac{a}{x} \cdot \frac{x}{a} = \frac{ax}{xa} = \frac{1}{1} = \frac{x}{a} \cdot \frac{a}{x} = 1_{Q(R)}.$$

Step 2. R is a subring of $Q(R)$.

Let $R' = \{a/1 \in Q(R)\}$. We note that R' is a subring of $Q(R)$ with $1_{R'} = 1_{Q(R)}$. Let $f: R \rightarrow R'$ be the map given by $a \mapsto a/1$. Then we have the following.

- f is a homomorphism of rings because

$$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b) \quad \text{and}$$

$$f(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b).$$

• f is an isomorphism of rings because if $x \in R'$, then $x = (a/1)$ and hence $f(a) = x$, i.e., f is onto and

$$\begin{aligned} \text{Ker}(f) &= \{a \in R \mid \frac{a}{1} = 0 \text{ in } R'\} = \{a \in R \mid \frac{a}{1} = \frac{0}{1}\} \\ &= \{a \in R \mid a = 0\} = (0). \end{aligned}$$

We identify R with R' and hence treat R as a subring of $Q(R)$. $\diamond$

3.4.4 Theorem: *For any commutative integral domain R with 1, $Q(R)$ is the smallest field containing R as a subring, having the same identity as R , smallest in the sense that if K is a field containing R as a subring, then $K \supseteq Q(R)$ as a subfield. This $Q(R)$ is unique upto isomorphism, called the field of fractions of R .*

Proof: Step 1. Suppose K is a field containing R as a subring. Then we show that $Q(R)$ is a subfield of K . Define the map $f: Q(R) \rightarrow K$ by $a/x \mapsto ax^{-1}$. This f is well-defined. For, suppose $a/x = b/y$. Then $ay = bx \implies ayy^{-1}x^{-1} = bxy^{-1}x^{-1}$ (since $x \neq 0, y \neq 0, x^{-1}, y^{-1} \in K$). Then $ax^{-1} = bxy^{-1}x^{-1}$, i.e., $ax^{-1} = by^{-1}$.

Step 2. f is a homomorphism.

For, let $a/x, b/y \in Q(R)$. We have

$$\begin{aligned} f\left(\frac{a}{x} + \frac{b}{y}\right) &= f\left(\frac{ay + bx}{xy}\right) \stackrel{\text{def}}{=} (ay + bx)(xy)^{-1} = (ay + bx)y^{-1}x^{-1} \\ &= ayy^{-1}x^{-1} + bxy^{-1}x^{-1} = ax^{-1} + by^{-1} = f\left(\frac{a}{x}\right) + f\left(\frac{b}{y}\right). \end{aligned}$$

Similarly,

$$f\left(\frac{a}{x} \cdot \frac{b}{y}\right) = f\left(\frac{ab}{xy}\right) \stackrel{\text{def}}{=} (ab)(xy)^{-1} = ax^{-1}by^{-1} = f\left(\frac{a}{x}\right) \cdot f\left(\frac{b}{y}\right).$$

Step 3. f is a monomorphism.

$$\begin{aligned} \text{Ker}(f) &= \left\{ \frac{a}{x} \in Q(R) \mid ax^{-1} = 0 \text{ in } K \right\} \\ &= \left\{ \frac{a}{x} \in Q(R) \mid ax^{-1} = 0x^{-1} \text{ in } K \right\} \\ &= \left\{ \frac{a}{x} \in Q(R) \mid a = 0 \text{ in } K \right\} = \left\{ \frac{0}{x} \right\} = (0). \end{aligned}$$

Under this monomorphism, we identify $Q(R)$ with its image, again denoted by $Q(R) = \{ax^{-1} \mid a, x \in R, x \neq 0\}$ which is a subfield of K . We have $R \subseteq Q(R) \subseteq K$, as required. $\diamond$

3.4.5 Corollary: $Q(K) = K$ for all fields K .

3.4.6 Remark: Theorem (3.4.4) above, holds even if R has no unity. Proof is the same, except identifying R as a subset of $Q(R)$. We achieve this by identifying R with the subset $\{(ax)/x \in Q(R)\}$ for a fixed $x \in R^*$ and we find that $1_{Q(R)} = x/x = y/y$, for all $x, y \in R^*$.

Note: For non-commutative integral domains, the analogous notion of “division ring of (left/right) fractions” is more complicated and their existence is proved only for a subclass, the so called “(left/right) Ore domains”. (See “NON COMMUTATIVE RINGS” by I. N. Herstein, Carus Mathematical Monograph No. 15, The Mathematical Association of America, Washington, D.C. (1968).)

3.4.7 Examples of fields of fractions:

1. We have $\mathbb{Q} = Q(\mathbb{Z}) = Q(2\mathbb{Z}) = Q(n\mathbb{Z})$, for all $n \in \mathbb{N}$.
2. We have $Q(\mathbb{Q}) = \mathbb{Q}$, $Q(\mathbb{R}) = \mathbb{R}$, $Q(\mathbb{C}) = \mathbb{C}$, etc.
3. The field of fractions of the ring of complex entire functions is the field of meromorphic functions.
4. For a field K , $Q(K[X])$ is denoted by $K(X)$, called the field of *rational functions* in one variable X over K . More generally, the field $Q(K[X_1, \dots, X_n])$ is denoted by $K(X_1, \dots, X_n)$ and is called the field

of *rational functions* in n variables over K .

5. For a commutative domain R , we have $Q(R[X]) = Q(R)(X)$.

For, on the one hand, we have

$$Q(R[X]) = \left\{ \frac{a_0 + a_1X + \cdots + a_rX^r}{b_0 + b_1X + \cdots + b_sX^s} \mid a_i, b_j \in R; b_j \neq 0 \text{ for some } j \right\}.$$

On the other hand, we have

$$\begin{aligned} Q(R)(X) &= \left\{ \frac{\alpha_0 + \alpha_1X + \cdots + \alpha_nX^n}{\beta_0 + \beta_1X + \cdots + \beta_mX^m} \mid \alpha_i, \beta_j \in Q(R), \right. \\ &\quad \left. \beta_j \neq 0 \text{ for some } j \right\} \\ &= \left\{ \frac{(a_0/b_0) + (a_1/b_1)X + \cdots + (a_n/b_n)X^n}{(c_0/d_0) + (c_1/d_1)X + \cdots + (c_m/d_m)X^m} \mid \right. \\ &\quad \left. \alpha_i = a_i/b_i, \beta_j = c_j/d_j, a_i, c_j \in R \text{ and } b_i, d_j \in R^* \right\} \\ &= Q(R[X]) \text{ (by clearing the denominators).} \end{aligned}$$

6. Power Series: Let K be a field. Then we have

$$Q(K[[X]]) = \left\{ \frac{a_0 + a_1X + \cdots}{b_0 + b_1X + \cdots} \mid a_i, b_j \in K, b_\ell \neq 0, \text{ for some } \ell \right\}.$$

We denote this field by $K((X))$.

Claim: We have $Q(K[[X]]) = K((X)) = K \langle X \rangle$ (1.6.2).

For, if $b_0 \neq 0$, recall that $b_0 + b_1X + \cdots$ is a unit in $K[[X]]$ (1.6.3), hence we have

$$\frac{a_0 + a_1X + \cdots}{b_0 + b_1X + \cdots} = (a_0 + a_1X + \cdots)(b_0 + b_1X + \cdots)^{-1} \in K[[X]].$$

We may assume that the denominator is a non-unit in $K[[X]]$. Let ℓ be the order of $b_0 + b_1X + \cdots$. By definition of order (1.5.2), we have $\ell \geq 1$ and $b_0 = b_1 = \cdots = b_{\ell-1} = 0$ but $b_\ell \neq 0$. Consequently,

$$\begin{aligned} \frac{a_0 + a_1X + \cdots}{b_0 + b_1X + \cdots} &= \frac{a_0 + a_1X + \cdots}{b_\ell X^\ell + b_{\ell+1}X^{\ell+1} + \cdots} = \frac{a_0 + a_1X + \cdots}{X^\ell(b_\ell + b_{\ell+1}X + \cdots)} \\ &= \frac{(a_0 + a_1X + \cdots)(b_\ell + b_{\ell+1}X + \cdots)^{-1}}{X^\ell}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} K((X)) &= \left\{ \frac{a_0 + a_1X + \cdots}{X^\ell} \mid a_i \in K, \ell \in \mathbb{Z}^+ \right\} \\ &= \{a_0X^{-\ell} + a_1X^{-\ell+1} + \cdots + a_{\ell-1}X^{-1} + a_\ell + a_{\ell+1}X + \cdots\} \\ &= K < X > . \end{aligned}$$

7. We have $Q(R[[X]]) \subseteq Q(Q(R)[[X]]) = Q(R) < X > .$

8. We have $Q(R[X_1, X_2, \dots, X_n]) = Q(Q(R)[X_1, X_2, \dots, X_n])$
 $= Q(R)(X_1, X_2, \dots, X_n),$
 whereas $Q(R[[X_1, X_2, \dots, X_n]]) \subseteq Q(Q(R)[[X_1, X_2, \dots, X_n]])$
 $= Q(R) < X_1, X_2, \dots, X_n > .$

9. We have $Q(\mathbb{Z}[i]) = Q(\mathbb{Q}[i]) = \mathbb{Q}[i].$

For, we have $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$. Observe that $\mathbb{Q}[i]$ is a field, because $(r + is)^{-1} = r/(r^2 + s^2) - i(s/(r^2 + s^2)), r, s \in \mathbb{Q}, r + is \neq 0$. Hence the field of fractions of $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$, i.e., $Q(\mathbb{Z}[i]) \subseteq \mathbb{Q}[i]$. Take any $x \in \mathbb{Q}[i]$, $x = r + is$ for some $r, s \in \mathbb{Q}$, i.e., $x = a/b + ip/q$, $a, b, p, q \in \mathbb{Z}, b, q \neq 0 = (qa + ipb)/(bq) \in Q(\mathbb{Z}[i])$.

Similarly, we have $Q(\mathbb{Z}[\sqrt{2}]) = Q(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}]$. More generally, $Q(\mathbb{Z}[\sqrt{d}]) = Q(\mathbb{Q}[\sqrt{d}]) = \mathbb{Q}[\sqrt{d}], \forall d \in \mathbb{Z}$.

10. **p -adic integers:** We have $Q(\mathbb{Q}^p) = \mathbb{Q}$ because $\mathbb{Z} \subseteq \mathbb{Q}^p \subseteq \mathbb{Q} = Q(\mathbb{Z})$. Hence $Q(\mathbb{Z}) \subseteq Q(\mathbb{Q}^p) \subseteq Q(\mathbb{Q}) = \mathbb{Q}$, i.e., $\mathbb{Q} \subseteq Q(\mathbb{Q}^p) \subseteq \mathbb{Q}$, as required. ■

3.5 Prime Fields

3.5.1 Theorem: Any division ring D (in particular, a field) contains either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ as the smallest subfield contained in the centre (called central subfield) of D according as the characteristic of D is 0 or a prime p .

Proof: We know that D contains $P = \{n \cdot 1 \mid n \in \mathbb{Z}\}$, the subring generated by 1. It is the smallest central subring of D and $P \approx \mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ according as P is infinite or not, i.e., according as the characteristic of D is 0 or p (by (1.12.4) above). If $K = \text{Centre of } D$, then K is a field containing $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ according as $\text{Char } D =$

($\text{Char } K = 0$ or p . But then K contains the field of fractions of $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$, (i.e., $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$), as required. $\diamond$

3.5.2 Prime field: The smallest (central) subfield of a division ring D is called the *prime field* of D (and it is $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ according as $\text{Char } D = 0$ or p).

3.5.3 Remark: For any ring R with 1, R contains $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ as the smallest central subring containing 1 according as $\text{Char } R$ is zero or n and it is called the *prime subring* of R . In particular,

- if R is an integral domain with 1, then R contains $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$ as its prime subring according as $\text{Char } R$ is zero or a prime p and
- if R is a commutative integral domain with 1, then $Q(R)$ contains $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ as its prime field according as $\text{Char } R$ is zero or p .

3.5.4 Remark: If D and D' are division rings such that there is a non-zero homomorphism of rings $f : D \rightarrow D'$, then $\text{Char } D = \text{Char } D'$ and f is identity on the prime field of D . (This is trivial because $f(1) = 1$ and hence f is identity on $\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z}$, etc.) $\blacksquare$

3.6 Exercises

Homomorphism means a homomorphism of rings, unitary or not.

1. Give an example to show that an epimorphic image of a prime (resp. maximal) ideal need not be one such.
2. Give examples of homomorphisms of rings $f : R \rightarrow S$ and $g : S \rightarrow T$ such that
 - $g \circ f$ is a monomorphism but g is not,
 - $g \circ f$ is an epimorphism but f is not and
 - $g \circ f$ is an isomorphism but neither f nor g is.
3. Show that a homomorphic image of a local ring (resp. PID) is one such. Is it also true of a PID?
4. Show that an ideal in a ring R is 2-sided if and only if it is the kernel of a suitable homomorphism of rings from R to an appropriate ring.

5. Let R be a ring with 1 and S a subring of R containing 1. Let I be a 2-sided ideal in R . Show that
 - $S + I$ is a subring of R and I is a 2-sided ideal in $S + I$,
 - $S \cap I$ is a 2-sided ideal in S and
 - the natural map $f : (S + I)/I \rightarrow S/(S \cap I)$ sending $x + I$ to $x + (S \cap I)$, for all x in S , is an isomorphism of rings.
6. (**Chinese Remainder Theorem**): Let R be a commutative ring with 1 and I and J be ideals coprime to each other (i.e., $I + J = R$). Show that (i) $I \cap J = IJ$ and (ii) the natural map $f : R/IJ \rightarrow (R/I) \times (R/J)$, sending $x + IJ$ to $(x + I, x + J)$, $\forall x \in R$, is an isomorphism of rings. Generalising the above to finitely many pairwise coprime ideals, deduce that the natural map as above,

$$\mathbb{Z}/(n) \rightarrow \mathbb{Z}/(p_1^{n_1}) \times \cdots \times \mathbb{Z}/(p_r^{n_r})$$
 is an isomorphism of rings where $n = p_1^{n_1} \cdots p_r^{n_r}$ is the prime decomposition of an integer $n \geq 2$ into distinct primes $p_1, \dots, p_r$ and $n_i \geq 1$.
7. Show that a non-zero endomorphism of the field of real numbers is the identity. (Hints: Such a map is identity on $\mathbb{Q}$, preserves positive numbers as well as the ordering on all real numbers.)
 Show that a similar assertion is not true for the field of complex numbers $\mathbb{C}$ or the division ring of real quaternions $\mathbb{H}_{\mathbb{R}}$.
8. Let K be a field of positive characteristic p . Let $F : K \rightarrow K$ be the map $x \mapsto x^p$ for all $x \in K$, called the *Frobenius* of K . Show that F is a monomorphism but not an isomorphism, in general. (Hint: Use Ex.(1.13.12) and look at the case of $K = \mathbb{Z}_p(X)$, the field of rational functions(3.4.7) over the field of p elements.)
9. A field K is said to be *perfect* if either its characteristic is 0 or else its Frobenius is surjective. Show that any finite field is perfect.
10. Given a ring R and an $n \in \mathbb{N}$, show that there is a natural isomorphism of $M_n(R)[X]$ onto $M_n(R[X])$. Do the same for power series too.
11. Given any ring R and a positive integer n , show that the map *transpose* : $M_n(R^0) \rightarrow (M_n(R))^0$, sending a matrix to its transpose, is an isomorphism (where R^0 is the ring opposite to R (1.11.1)).
12. Let $f : R \rightarrow S$ be a homomorphism of rings. Show that the induced map $M_n(f) : M_n(R) \rightarrow M_n(S)$, sending (a_{ij}) to $(f(a_{ij}))$, is a homo-

morphism of rings for all $n \in \mathbb{N}$ and that $M_n(f)$ is a monomorphism (resp. epimorphism) if and only if f is so.

Do the same for polynomial (resp. power series, resp. Laurent series) rings in place of matrix rings.

13. Let $\text{Hom}_{\text{rings}}(R, S)$ be the set of all homomorphisms of rings. Show that $\text{Hom}_{\text{rings}}(R, S) = \{0\}$ if either $\text{Char } R \neq 0$ but $\text{Char } S = 0$ or $\text{Char } R \neq 0$ and $\text{Char } S \neq 0$ but $\text{Char } S$ does not divide $\text{Char } R$. In particular, we have the following.
 - $\text{Hom}_{\text{rings}}(\mathbb{Z}_n, \mathbb{Z}) = \{0\}$, $\forall n \in \mathbb{N}$,
 - $\text{Hom}_{\text{rings}}(\mathbb{Z}_n, \mathbb{Z}_m) = \{0\}$, $\forall m, n \in \mathbb{N}$, $(m, n) = 1$. But
 - $\text{Hom}_{\text{rings}}(\mathbb{Z}, \mathbb{Z}_n) = \mathbb{Z}_n$, $\forall n \in \mathbb{N}$, etc.
14. Show that $\text{Hom}_{\text{rings}}(\mathbb{Z}[X_1, \dots, X_n], S) = S^n$ for any ring S and $n \in \mathbb{N}$.
15. Let $f: R \rightarrow S$ be a monomorphism of commutative domains. Let $Q(R)$ and $Q(S)$ be the fields of fractions of R and S respectively. Show that the induced map $Q(f): Q(R) \rightarrow Q(S)$, a/x to $f(a)/f(x)$, $\forall a \in R$ and $x \in R^*$, is well-defined and is a monomorphism. Furthermore, show that $Q(f)$ is an isomorphism if and only if f is so.
16. Show that the field of fractions of $\mathbb{Z}[\sqrt{d}]$ is $\mathbb{Q}[\sqrt{d}]$.
17. Let R be a commutative domain with 1, P a prime ideal in R and $R_P = \{a/x \in Q(R) \mid a, x \in R, x \notin P\}$, called the *localisation* of R at P . Show that
 - R_P is a subring of $Q(R)$ containing R ,
 - $Q(R) = Q(R_P)$ and
 - R_P is a local ring whose maximal ideal is PR_P .
 Moreover, show that the residue field of R_P is isomorphic to $Q(R/P)$. In particular, $R_{(0)} = Q(R)$.
18. If Q is a prime ideal of R , show that $QR_P = R_P \iff Q \not\subseteq P$. In case, $Q \subseteq P$, show that QR_P is a prime ideal of R_P and conversely, every prime ideal of R_P is of this form for some prime ideal $Q \subseteq P$. Furthermore, show that $R_Q = (R_P)_{QR_P}$.
19. For the case when $R = \mathbb{Z}$ and $P = (p)$, p a prime in $\mathbb{Z}$, show that
 - $\mathbb{Z}_{(p)} = \mathbb{Q}^p$ with $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{Z}_p (= \mathbb{Z}/p\mathbb{Z})$ and
 - there are exactly two prime ideals in $\mathbb{Z}_{(p)}$, namely, (0) and $p\mathbb{Z}_{(p)}$.
 Note the important difference between $\mathbb{Z}_{(p)}$ and $\mathbb{Z}_p$.

20. Let R be a commutative integral domain with 1. Let $\mathcal{P}$ (resp. $\mathcal{M}$) be the set of all prime (resp. maximal) ideals in R . Then show that

$$\bigcap_{P \in \mathcal{P}} R_P = R = \bigcap_{M \in \mathcal{M}} R_M$$

where the intersections are taken in $Q(R)$. (Hint: If $y = a_M/b_M \in R_M$, the ideal generated by the denominators $b_M, M \in \mathcal{M}$ of y is R . Writing $1 = \sum_{M \in \mathcal{M}}^{\text{finite}} x_M b_M, x_M \in R$, the result follows.)

21. Let R and S be local rings with their maximal ideals M_R and M_S respectively. A homomorphism $f : R \rightarrow S$ of rings is said to be *local* if f takes non-units to non-units, i.e., $f(M_R) \subseteq M_S$. Show that a local homomorphism f of local rings induces a monomorphism $\bar{f} : R/M_R \rightarrow S/M_S$ of their residue fields. Give an example of a homomorphism between local rings which is *not* local.
22. Let $f : R \rightarrow S$ be a unitary homomorphism of commutative rings with 1. Let $a_f : \text{Spec}(S) \rightarrow \text{Spec}(R)$ be the induced map defined by $Q \mapsto f^{-1}(Q)$. Show that a_f is continuous with respect to the Zariski topologies (2.9.39).
23. Let $f : R \rightarrow S$ be a unitary homomorphism of commutative domains with 1. For $Q \in \text{Spec}(S)$, let $P = f^{-1}(Q) \in \text{Spec}(R)$. Show that the induced map $f_Q : R_P \rightarrow S_Q, a/x \mapsto f(a)/f(x)$, is a local homomorphism of local rings.
24. Define a homomorphism between Lie rings (1.13.31) in an obvious way. Given a homomorphism $f : R \rightarrow S$ of rings R and S , show that $f : L(R) \rightarrow L(S)$ is also a homomorphism of the associated Lie rings. Is the converse true?
25. Let R be a ring. By a *derivation* of R , we mean an additive homomorphism $\partial \in \text{End}_{\mathbb{Z}}(R)$ such that $\partial(ab) = \partial(a)b + a\partial(b)$ for all $a, b \in R$. Let $\text{Der}(R)$ be the set of all derivations of R . Show that
- $\partial(1) = 0$ for all $\partial \in \text{Der}(R)$ if R has 1,
 - sum of two derivations is a derivation and hence $\text{Der}(R)$ is an abelian group,
 - composition of two derivations need *not* be a derivation but the *commutator* of two derivations, namely, $[\partial_1, \partial_2] = \partial_1 \circ \partial_2 - \partial_2 \circ \partial_1$ is a derivation and hence
 - $(\text{Der}(R), +, [,])$ is a Lie ring.

In case R is commutative, show that $a\partial$ is a derivation for all $a \in R$ and $\partial \in \text{Der}(R)$.

26. Let R be a subring of a ring S . Let $\text{Der}_R(S)$ be the set of all R -derivations of S , i.e.,

$$\text{Der}_R(S) = \{\partial \in \text{Der}(S) \mid \partial(a) = 0, \forall a \in R\}.$$

Show that $\text{Der}_R(S)$ is a Lie subring of $\text{Der}(S)$ and that if S has 1, then $\text{Der}(S) = \text{Der}_{\mathbb{Z}}(S)$.

27. Let R be a commutative ring with 1 and $S = R[X_1, \dots, X_n]$. Show that $\partial_i = \partial/\partial X_i$, the formal partial derivative with respect to X_i , is an R -derivation of S , $1 \leq i \leq n$. Furthermore, show that $\text{Der}_R(S)$ is an abelian Lie ring. In fact, show that

- $[\partial_i, \partial_j] = 0$, $\forall i, j$ and
- every R -derivation of S can be written uniquely as an S -linear combination of the ∂_i 's, $1 \leq i \leq n$.

28. Let $R = \mathcal{C}^\infty(\mathbb{R})$ be the ring of all smooth functions on $\mathbb{R}$ (1.13.23). Show that the usual derivative d/dx is an $\mathbb{R}$ -derivation of R and that every element of $\text{Der}_{\mathbb{R}}(R)$ is of the form fd/dx for a unique $f \in R$, i.e., $\text{Der}_{\mathbb{R}}(R) = R[d/dx]$ (which is isomorphic to the polynomial ring in one variable d/dx over R). ■

3.7 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counterexample if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be.

1. Homomorphic image of a unit (resp. an idempotent, resp. a nilpotent) element is one such.
2. Homomorphic image of an ideal is an ideal.
3. Epimorphic image of a maximal ideal is maximal.
4. Inverse image of a prime ideal is a prime ideal.
5. Inverse image of a maximal ideal is a maximal ideal.
6. Inverse image, by an epimorphism, of a maximal ideal is maximal.
7. The kernel of an epimorphism is a maximal ideal.

8. A non-zero homomorphism from a simple ring is a monomorphism.
9. A non-zero homomorphism between simple rings is an isomorphism.
10. An epimorphism between simple rings is an isomorphism.
11. The ring $\mathbf{Q}^p$ (1.8.7) is a local ring where p is a prime.
12. The quaternion norm is a homomorphism of the ring $\mathbf{H}_{\mathbf{R}}$ into $\mathbf{R}$.
13. If m and n are both sums of 4 squares of integers, their product mn is also a sum of 4 squares of integers.
14. If I is a maximal 2-sided ideal in a ring R , then R/I is simple.
15. If I is a maximal 2-sided ideal in R , then non-units go to non-units under the natural map $R \rightarrow R/I$.
16. For positive integers m and n , $\mathbf{Z}/(m)$ is a quotient of $\mathbf{Z}/(mn)$.
17. In $\mathbf{Z}[X]$, the ideal (X) is a prime ideal but not maximal.
18. Under a unitary homomorphism of rings, inverse image of a prime ideal is a prime ideal.
19. Homomorphic image of an integral domain is a domain.
20. Homomorphic image of a PID is a PIR.
21. Identity is the only automorphism of the field $\mathbf{R}$.
22. Identity is the only automorphism of the field $\mathbf{C}$.
23. Any field is the field of fractions of a commutative domain.
24. Any field contains $\mathbf{Q}$ or $\mathbf{Z}_p$ as a subfield for some prime p .
25. Any field containing $\mathbf{Z}[i]$ as a subring contains $\mathbf{Q}[i]$ as a subfield.
26. Any division ring containing the integral quaternions $\mathbf{Z}[i, j, k]$ contains the rational quaternions $\mathbf{Q}[i, j, k]$.
27. A homomorphism of $M_n(\mathbf{R})$ into any ring is 0 or a monomorphism.
28. A homomorphism of $M_n(\mathbf{Z})$ into any ring is 0 or a monomorphism.
29. A matrix ring over a simple ring is a simple ring.
30. A homomorphism of rings R and S is also one of the associated Lie rings $L(R)$ and $L(S)$ (1.13.31).
31. The converse of the above statement is true.
32. A homomorphism of an abelian Lie ring into any other is nothing but an additive homomorphism. ■

Chapter 4

Factorisation in Domains

In this chapter, we extend the concepts of “division”, “division algorithm”, “prime”, “factorisation”, etc., from the ring of integers $\mathbb{Z}$ to an arbitrary commutative integral domain R with 1. Wherever possible in arbitrary rings, we shall formulate and investigate the validity of an extension of the “Fundamental Theorem of Arithmetic”, i.e., unique factorisation of integers.

4.1 Division in Domains

Let R be a commutative integral domain with 1 and $R^* = R - \{0\}$.

4.1.1 Definition: Let $a, b \in R$, $a \neq 0$. We say that a *divides* b or a is a *divisor* (or *factor*) of b and written $a \mid b$ if there exists $c \in R$ such that $b = ac$.

4.1.2 Remark: Let $a, b \in R$, $a \neq 0$. Then $a \mid b$ if and only if $(b) \subseteq (a)$. (For, suppose $a \mid b$. There is a $c \in R$ such that $b = ac$. Hence $b \in (a)$ which implies that $(b) \subseteq (a)$. Conversely, suppose $(b) \subseteq (a)$. Then $b \in (a)$, i.e., $b = ac$ for some $c \in R$, as required.)

4.1.3 Associates: Two elements a and b in R^* are said to be *associates* of each other if $a \mid b$ and $b \mid a$.

4.1.4 Proposition: Let $a, b \in R^*$. Then a and b are associates of each other $\iff a = ub$ for some unit $u \in R \iff (a) = (b)$.

Proof: Suppose a and b are associates of each other, i.e., $a \mid b$ and $b \mid a$. Then $a = bc$ and $b = ad$ for some c and d in R . Hence $a = adc$ which gives $1 = dc$ (since $a \neq 0$ and R is a domain). Thus c is a unit, as required. Conversely, suppose $a = ub$ for some unit $u \in R$. Then $b \mid a$. But $b = u^{-1}a$ and hence $a \mid b$, as required.

On the other hand, suppose a and b are associates of each other, say, $a = ub$ for some unit in R . Then $a \in (b)$ hence $(a) \subseteq (b)$. Similarly, we get that $(b) \subseteq (a)$ hence $(a) = (b)$, as required. Conversely, if $(a) = (b)$, then by (4.1.2) above, we get that $a \mid b$ and $b \mid a$, as required. $\diamond$

4.1.5 Remark: “Being associates” is an equivalence relation on R^* . (This is trivial to verify.) For $a \in R^*$, the equivalence class through a is $\{ua \in R \mid u \text{ a unit in } R\}$, i.e., the equivalence classes are simply the *orbits* in R^* for the natural action by multiplication of the group $\mathcal{U}(R)$ of units in R .

4.1.6 Irreducible element: A non-zero non-unit $a \in R$ is said to be *irreducible* if $a = bc$, then either b or c is a unit, i.e., a cannot be written as a product of two non-units or equivalently, the only divisors of a are its associates or units.

4.1.7 Prime element: A non-zero non-unit $a \in R$ is said to be a *prime* if $a \mid bc$, ($b, c \in R$), then either $a \mid b$ or $a \mid c$.

Note: In $\mathbb{Z}$, ± 1 , being units, are neither irreducible nor primes. The primes are however the familiar ones, namely, $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \dots$

4.1.8 Proposition: *A prime is irreducible but not conversely.*

Proof: Let p be a prime in R . Suppose $p = ab$. Then obviously $p \mid ab$, hence $p \mid a$ or $p \mid b$, say $p \mid a$. Then $a = pc$ for some $c \in R$. Now we have $p = ab = pcb$, hence $1 = cb$ by cancelling (the non-zero) p . Thus b is a unit in R , hence p is irreducible, as required. $\diamond$

To see that the converse need not be true, look at the following.

Example: Let $R = \mathbb{Z}[i\sqrt{3}]$. Notice that the only units in R are ± 1 . Now we show that the element $1 + i\sqrt{3}$ is irreducible but not a prime.

Let $1 + i\sqrt{3} = (a + i\sqrt{3}b)(c + i\sqrt{3}d)$. Now taking norms, i.e., square of the modulus, we get that $4 = (a^2 + 3b^2)(c^2 + 3d^2)$ hence $a^2 + 3b^2 = 1, 2$ or 4 . It is trivial to see that $a^2 + 3b^2 \neq 2$ and so $a^2 + 3b^2 = 1$ or $c^2 + 3d^2 = 1$. In either case, we get $a = \pm 1$ and $b = 0$ or $c = \pm 1$ and $d = 0$. Hence $1 + i\sqrt{3}$ is irreducible. On the other hand, we have $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ but $(1 + i\sqrt{3})$ does not divide 2, as can be easily seen, hence $1 + i\sqrt{3}$ is not a prime, as required.

4.1.9 Theorem: *Let a be a non-zero non-unit in a commutative integral domain R . Then we have the following.*

1. *The element a is irreducible in R if and only if the ideal (a) is maximal among all principal ideals other than R , i.e., there is no principal ideal in R , other than R , properly containing (a) .*
2. *The element a is prime in R if and only if the ideal (a) is a non-zero prime ideal in R .*

Proof: 1. Suppose a is irreducible. Say, $(a) \subseteq (b) \neq R$ for some $b \in R$. Now $a \in (b)$, hence $a = bc$ for some $c \in R$. Since a is irreducible, either b or c is a unit in R . Since $(b) \neq R$, b cannot be a unit, hence c must be a unit. But then, $b = c^{-1}a \in (a)$, i.e., $(b) \subset (a)$, hence $(a) = (b)$, as required. Conversely, suppose (a) is maximal among all principal ideals other than R . Assume that $a = bc$ and that b is not a unit. Then $(a) \subset (c)$ and $(a) \neq (c)$. This contradicts the maximality of (a) unless $(c) = R$ which means c is a unit, as required.

2. Suppose a is a prime in R . Since a is a non-unit, $(a) \neq R$. Assume that $xy \in (a)$. Hence $xy = ab$ for some $b \in R$. Now $a \mid ab$, i.e., $a \mid xy$, hence either $a \mid x$ or $a \mid y$, say $a \mid x$, i.e., $x = ac$ for some $c \in R$, hence $x \in (a)$, showing that (a) is a prime ideal in R and obviously it is non-zero as $a \neq 0$. Conversely, suppose (a) is a non-zero prime ideal in R . Since $(a) \neq R$, a is not a unit. If $a \mid xy$, then $xy \in (a)$, hence either $x \in (a)$ or $y \in (a)$ as (a) is a prime ideal. Say, $x \in (a)$ which means $a \mid x$, showing that a is a prime in R . $\diamond$

4.1.10 Greatest common divisor (gcd): Given $a, b \in R^*$, an element $d \in R^*$ is called a *greatest common divisor* of a and b if

1. $d \mid a$ and $d \mid b$, i.e., d is a common divisor of a and b and

2. $c \mid a$ and $c \mid b \Rightarrow c \mid d$, i.e., d is greatest among the common divisors of a and b .

4.1.11 Least common multiple (lcm): Given $a, b \in R^*$, an element $\ell \in R^*$ is called a *least common multiple* of a and b if

1. $a \mid \ell$ and $b \mid \ell$, i.e., ℓ is a common multiple of a and b and
2. $a \mid m$ and $b \mid m \Rightarrow \ell \mid m$, i.e., ℓ is least among all the common multiples of a and b .

4.1.12 Remark: In general, gcd or lcm need not exist.

For example, look at the ring $R = \mathbb{Z}[i\sqrt{5}]$ and first notice that its units are only ± 1 . Take $x = 2(1 + i\sqrt{5})$ and $y = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ and suppose $d = \gcd(x, y)$ exists. We have $x = da$ and $y = db$ for some $a, b \in R^*$. For $\alpha = m + i\sqrt{5}n \in R$, let $N(\alpha) = m^2 + 5n^2$ (which is a positive integer if $\alpha \neq 0$). Now we have $N(x) = N(d)N(a)$ and $N(y) = N(d)N(b)$, i.e., $4 \cdot 6 = N(d)N(a)$ and $6 \cdot 6 = N(d)N(b)$ which means that $N(d) \mid 24$ and $N(d) \mid 36$. On the other hand, since $2 \mid x$ and $2 \mid y$, $2 \mid d$, i.e., $d = 2d'$ and so $N(d) = 4N(d')$ which means $4 \mid N(d)$. Similarly, since $1 + i\sqrt{5}$ is a common divisor of x and y , we get $6 \mid N(d)$ and hence $12 \mid N(d)$. Therefore it follows that $N(d) = 12$. But it is easy to see that $N(\alpha) \neq 12$ for any $\alpha \in R$ proving that $d \notin R$ which is a contradiction. Similarly, one can show that lcm of x and y does not exist since if it exists, it has to be an element $\ell \in R$ such that $N(\ell)$ is either 72 or 144 which is not possible.

4.1.13 Remark: Given $a, b \in R^*$, if gcd (resp. lcm) of a and b exists, then it is easy to see that it is unique upto associates and is denoted by $\gcd(a, b)$ (resp. $\text{lcm}(a, b)$).

4.1.14 Coprime elements: If the gcd of two elements a, b exists and is equal to 1, i.e., units are the only common divisors of a and b , we say that a and b are *coprime* to each other. ■

4.2 Euclidean Domains

4.2.1 Euclidean domain: A commutative integral domain R (with or without unity) is called a *Euclidean domain* if there is a map $d: R^* \rightarrow \mathbb{Z}^+$ such that

1. $\forall a, b \in R^*, a \mid b \Rightarrow d(a) \leq d(b)$ or equivalently, $d(x) \leq d(xy)$ and
2. $\forall a \in R$ and $b \in R^*, \exists q, r \in R$ (depending on a and b) such that $a = qb + r$ with either $r = 0$ or else $d(r) < d(b)$.

The map d is called the *algorithm map* and the property (2) is called the *division algorithm*. As usual, the elements b, a, q and r in the equation $b = qa + r$ are respectively called the *dividend*, *divisor*, *quotient* and *remainder*.

4.2.2 Proposition: *A Euclidean domain R has unity and whose group of units is given by $\mathcal{U}(R) = \{a \in R^* \mid d(a) = d(1)\}$.*

Proof: By our definition of an integral domain, we have $R^* \neq \emptyset$. Now look at the image $d(R^*) \subseteq \mathbb{Z}^+$, i.e., $d(R^*)$ is a non-empty subset of $\mathbb{Z}^+$ and hence has a least element (by the well-ordering principle). Let $\ell \in d(R^*)$ be the least in $d(R^*)$, say $\ell = d(e)$ for some $e \in R^*$. We have $d(e) \leq d(a)$, $\forall a \in R^*$.

Claim: *R has unity.*

First, we observe that $e \mid a$, $\forall a \in R$. (For, since $e \neq 0$, by the division algorithm, $\exists q, r \in R$ such that $a = qe + r$ with either $r = 0$ or else $d(r) < d(e)$. Since $d(e) \leq d(x)$, $\forall x \in R^*$, we get that r has to be zero. Thus $a = qe$, as required.

In particular, $e \mid e$, say $e = q_0 e$ for some $q_0 \in R^*$. Now we shall show that this q_0 is the unity of R . Given $x \in R$, we have $xq_0 e = xe$ (since $q_0 e = e$). Hence we get $(xq_0 - x)e = 0$ which implies $xq_0 - x = 0$ (since $e \neq 0$). Thus $q_0 = 1$ is the unity of R .

To characterise the units in R , first note that $d(1) = d(e)$ because $d(1) \leq d(1e) = d(e)$ and $d(e)$ is the least in $d(R^*)$. Now suppose x is a unit in R . We have $d(x) \leq d(xx^{-1}) = d(1)$ hence $d(x) = d(1)$. On the other hand, suppose $x \in R^*$ is such that $d(x) = d(1)$. Then, using division algorithm, $\exists q, r \in R$ such that $1 = qx + r$ with either $r = 0$ or else $d(r) < d(x) = d(1)$. But the latter is not possible and hence $r = 0$ which means x is a unit in R , as required. $\diamond$

4.2.3 Examples of Euclidean domains:

0. *Any field K is Euclidean.*

The algorithm map is the *constant* map $d : K^* \longrightarrow \mathbb{Z}^+$, i.e., $d(x) = 1, \forall x \in K^*$. The division algorithm is the trivial property that $x = (xa^{-1})a + 0, \forall x \in K$ and $\forall a \in K^*$.

1. The ring of integers $\mathbb{Z}$ is Euclidean.

The algorithm map is the *absolute value* $d : \mathbb{Z}^* \longrightarrow \mathbb{Z}^+$, i.e., $d(n) = |n|, \forall n \in \mathbb{Z}^*$. The division algorithm is the *usual division of integers*, i.e., given $n \in \mathbb{Z}$ and $a \in \mathbb{Z}^*$, first write

$|n| = q|a| + r$ with $0 \leq r < |a|$, for unique $q, r \in \mathbb{Z}$.

Now we see that $n = q'a + r'$ where $q' = \pm q$ and $r' = \pm r$. (In fact, we can also choose q' in such a that $0 \leq r' < |a|$ even if both n and a are negative.)

2. The ring $\mathbb{Z}[i]$ of Gaussian integers is Euclidean.

The algorithm map d is the *square of the modulus*, i.e., $d : \mathbb{Z}[i]^* \longrightarrow \mathbb{Z}^+$, given by

$$d(m + in) = |m + in|^2 = (m + in)(\overline{m + in}) = m^2 + n^2, \forall m, n \in \mathbb{Z}.$$

The division algorithm is the property that given $x \in \mathbb{Z}[i]$ and $a \in \mathbb{Z}[i]^*$, to find $q, r \in \mathbb{Z}[i]$ such that

$$x = qa + r \text{ with either } r = 0 \text{ or else } |r|^2 = r\bar{r} < a\bar{a} = |a|^2.$$

To prove the division algorithm, we proceed as follows. Consider the complex number $z = x/a$. Then z falls in (or is a vertex of) a unit square with integral vertices, say $(m, n), (m+1, n), (m+1, n+1)$ and $(m, n+1)$ for some $m, n \in \mathbb{Z}$. Now we can choose a vertex q of this square such that $|z - q| < 1$. Let $r = x - qa$ so that $x = qa + r$. If $r \neq 0$, we have

$$\frac{r\bar{r}}{a\bar{a}} = \frac{|r|^2}{|a|^2} = \left| \frac{r}{a} \right|^2 = \left| \frac{x}{a} - q \right|^2 = |z - q|^2 < 1.$$

Thus we have $d(r) = r\bar{r} < a\bar{a} = d(a)$, as required.

3. $R = K[X]$, the polynomial ring in one variable over a field K is Euclidean.

The algorithm map is the *degree map* $d : K[X]^* \longrightarrow \mathbb{Z}^+$, namely, $d(f(X)) = \text{degree of } f(X)$ for a non-zero polynomial $f(X)$. The division algorithm is the *usual division of polynomials*.

To prove the division algorithm, we recall the division process for

polynomials. Let $f(X) \in K[X]$ and $a(X) \in K[X]^*$. If $f(X) = 0$ or $\text{degree } f(X) < \text{degree } a(X)$, then we write $f(X) = 0 \cdot a(X) + f(X)$. Assume that $f(X) \neq 0$ and $m = \text{degree } f(X) > n = \text{degree } a(X)$. Let $f(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$ and $a(X) = a_0 + a_1 X + \cdots + a_n X^n$ with $\alpha_i, a_j \in K$ and $\alpha_m \neq 0, a_n \neq 0$. Let $g(X) = f(X) - (\alpha_m a_n^{-1} X^{m-n} a(X))$. It is clear that $\text{degree } g(X) < m = \text{degree } f(X)$ and hence, by induction on m , we can find $q(X), r(X) \in K[X]$ such that $g(X) = q(X)a(X) + r(X)$ with either $r(X) = 0$ or else $\text{degree } r(X) < \text{degree } a(X)$. Now substituting for $g(X)$, we get that $f(X) = (q(X) + \alpha_m a_n^{-1} X^{m-n})a(X) + r(X)$, as required.

4. $R = K[[X]]$, the formal power series ring in one variable over a field K is Euclidean.

The algorithm map is the *order* of a non-zero power series and the division algorithm is the *usual division* of power series.

Recall that given a non-zero power series $f(X) \in R$ there exist unique unit u in R and non-negative integer n such that $f(X) = uX^n$. This n is called the *order* of $f(X)$ and is denoted by $\text{ord}(f(X))$. Now given $f(X) \in R$ and $a(X) \in R^*$, if $f(X) = 0$ or $\text{ord}(f(X)) < \text{ord}(a(X))$, we have $f(X) = 0 \cdot a(X) + f(X)$. Assume that $f(X) \neq 0$ and $\text{ord}(f(X)) = m > n = \text{ord}(a(X))$. Let u, v be units in R such that $f(X) = uX^m$ and $a(X) = vX^n$. We have $f(X) = (uv^{-1}X^{m-n})vX^n = q(X)a(X) + 0$. Thus we get $f(X) = q(X)a(X) + r(X)$ such that either the quotient $q(X) = 0$ or the remainder $r(X) = 0$ for all $f(X) \in R$. In particular, given $f(X), g(X) \in R^*$, either $f(X) \mid g(X)$ or $g(X) \mid f(X)$.

4.2.4 Remarks: 1. See (4.3.7) below, for some more examples of Euclidean domains.

2. If $R = S[X]$ where S is *not* a field, then R is *not* Euclidean even though the degree map is an algorithm map. What fails is the division algorithm.

• For instance, it is easy to check that the division algorithm does not hold for $f(X) = X$ and $a(X) = \alpha X$ for a non-zero non-unit $\alpha \in S$.

• In fact, it is trivial to see (from the proof of the division algorithm for $K[X]$, K a field) that given $f(X) \in S[X]$ and $a(X) \in S[X]^*$, the division algorithm holds for $f(X)$ with $a(X)$ as the divisor if and only

if the leading coefficient of $a(X)$ is a unit in S .

• We shall see in (4.3.4) below, that $S[X]$ *cannot* be Euclidean for any algorithm map whatsoever if S is not a field.

Caution: Neither $\mathbb{Z}[X]$ nor $\mathbb{Z}[[X]]$ is Euclidean though $\mathbb{Z}$ is. ■

4.3 Principal Ideal Domains

Recall that a commutative integral domain R is called a *principal ideal domain* (PID) if every ideal of R is principal, i.e., generated by one element.

4.3.1 Theorem: Every Euclidean domain is a PID (with 1).

Proof: Let R be a Euclidean domain with the algorithm map d . By (4.2.2) above, R has 1. Let I be an ideal in R . If $I = (0)$, it is principal. Assume that $I \neq (0)$. Now $I^* \neq \emptyset$ hence $d(I^*)$ is a non-empty subset of $\mathbb{Z}^+$ and so $d(I^*)$ has a least element, say $d(a)$ for some $a \in I^*$.

Claim: $I = (a)$.

To see this, first note that $(a) \subset I$ since $a \in I$. To prove that $I \subset (a)$, take any $x \in I$. By division algorithm, $\exists q, r \in R$ such that $x = qa + r$ with either $r = 0$ or else $d(r) < d(a)$. Since $r = (x - qa) \in I$ and $d(a)$ is least in $d(I^*)$, it is not possible that $d(r) < d(a)$ and so $r = 0$, i.e., $x = qa \in (a)$, as required. ◇

4.3.2 Remarks: 1. For any non-zero ideal I in a Euclidean domain R , $I = (a)$ for any element $a \in I^*$ such that $d(a)$ is least in $d(I^*)$, in particular, any two such elements are associates of each other.

2. Applying (1) for the unit ideal R , we get that

$$\begin{aligned} \mathcal{U}(R) &= \text{the set of units in } R \\ &= \text{the set of generators of the ideal } R \\ &= \{u \in R^* \mid d(u) = d(1)\} \text{ (since } d(1) \text{ is least in } d(R^*) \text{)}. \end{aligned}$$

3. The ring of *even integers* $R = 2\mathbb{Z}$ is a *trivial example* of a PID which is not Euclidean since it has no unity.

(See (4.3.7) below, for some non-trivial examples.)

4.3.3 Theorem: *Let R be a PID (with 1). Then we have the following.*

1. *Every irreducible element is a prime in R .*
2. *Every non-zero prime ideal is maximal in R .*

Proof: 1. Let a be an irreducible element in R . We have to show that the ideal (a) is prime in R . In fact, we shall show that (a) is a maximal ideal. Since a is a non-unit, we have $(a) \neq R$ and hence, by Zorn's lemma, there exists a maximal ideal M such that $(a) \subseteq M$. Since R is a PID, $M = (p)$ for some prime p in R . Thus $(a) \subseteq (p)$. But then by (4.1.9) (i) above, $(a) = (p)$ and hence a is an associate of p which means that a is a prime, as required.

2. Let P be non-zero prime ideal in R . Since R is a PID, $P = (p)$ for some prime p . We have already shown above that (p) is a maximal ideal. This proves the result. $\diamond$

4.3.4 Theorem: *For a commutative integral domain R with unity, the following are equivalent.*

1. *R is a field.*
2. *$R[X]$ is Euclidean.*
3. *$R[X]$ is a PID.*

Proof: We have already seen that $(1) \Rightarrow (2) \Rightarrow (3)$. We have only to show that $(3) \Rightarrow (1)$. Since X is a prime in $R[X]$, the ideal (X) is a non-zero prime ideal in $R[X]$ and hence maximal which implies that $R[X]/(X) \simeq R$ is a field, as required. $\diamond$

Caution: *Neither $\mathbb{Z}[X]$ nor $R[X, Y]$ is a PID (even if R is a field).* This can be seen in several ways. For example, neither $\mathbb{Z}$ nor $R[X]$ is a field. Another way is to show that the ideals $(2, X)$ and (X, Y) are not principal in $\mathbb{Z}[X]$ and $R[X, Y]$ respectively.

• In a PID, “gcd” and “lcm” exist and are characterised as follows. (See Ex.(6.8.25) below, for a characterisation of PID's in terms of the existence of gcd and one of its properties such as the following. See also (4.5.7) below.)

4.3.5 Theorem: *Let R be a PID with 1 and $a, b \in R^*$. Then we have*

1. $d = \gcd(a, b) \iff (d) = (a) + (b)$, (in particular, a, b are coprime to each other if and only if $\exists x, y \in R$ such that $1 = ax + by$) and
 2. $\ell = \text{lcm}(a, b) \iff (\ell) = (a) \cap (b)$.

Proof: 1. Let $d = \gcd(a, b)$. Since $d \mid a$, $(d) \supseteq (a)$. Likewise $(d) \supseteq (b)$. Hence $(d) \supseteq (a) + (b)$. Since R is a PID, $(a) + (b) = (c)$ for some $c \in R$. Since $a \in (c)$ and $b \in (c)$, $c \mid a$ and $c \mid b$. Hence $c \mid d$, i.e., $d \in (c)$. Thus $(d) \subseteq (c) \subseteq (d)$, proving that $(d) = (c) = (a) + (b)$, as required. Conversely, if $(d) = (a) + (b)$, then as before we see that d is a common divisor of a and b . If c is a common divisor of a and b , then $a \in (c)$, $b \in (c)$, so $(a) + (b) \subseteq (c)$, i.e., $(d) \subseteq (c)$ which means that $c \mid d$, proving that d is the greatest common divisor of a and b , as required.

2. If $\ell = \text{lcm}(a, b)$, $\ell \in (a)$ and $\ell \in (b)$ hence $\ell \in (a) \cap (b)$, i.e., $(\ell) \subseteq (a) \cap (b)$. Since R is a PID, $(a) \cap (b) = (m)$ for some $m \in R$. It is clear that $a \mid m$ and $b \mid m$. Hence $\ell \mid m$, i.e., $m \in (\ell)$ and so $(m) \subseteq (\ell) \subseteq (m)$, i.e., $(\ell) = (m) = (a) \cap (b)$, as required. The converse is quite easy. $\diamond$

4.3.6 Remark: If R is a Euclidean domain, then the gcd d of a pair of elements $a, b \in R^*$ can be found by the following well-known procedure. To start with, write

$$a = q_1 b + r_1 \text{ with } r_1 = 0 \text{ or else } d(r_1) < d(b).$$

If $r_1 = 0$, then $d = \gcd(a, b) = b$. If $r_1 \neq 0$, then write

$$b = q_2 r_1 + r_2 \text{ with } r_2 = 0 \text{ or else } d(r_2) < d(r_1).$$

If $r_2 = 0$, then $d = r_1$. Proceeding thus we get that

$$\begin{array}{lll} a & = & q_1 b + r_1, & r_1 \neq 0, & d(r_1) < d(b), \\ b & = & q_2 r_1 + r_2, & r_2 \neq 0, & d(r_2) < d(r_1), \\ r_1 & = & q_3 r_2 + r_3, & r_3 \neq 0, & d(r_3) < d(r_2), \\ \vdots & & \vdots & & \vdots \\ r_{n-2} & = & q_n r_{n-1} + r_n, & r_n \neq 0, & d(r_n) < d(r_{n-1}) \text{ but} \\ r_{n-1} & = & q_{n+1} r_n + 0 & (\text{for some } n) & \implies \gcd(a, b) = r_n. \end{array}$$

4.3.7 More Examples of Euclidean/Principal Ideal Domains: The following are some well-known facts from “Algebraic Number Theory” whose proofs are non-trivial and beyond the scope of this

book. See ALGEBRAIC NUMBER THEORY by E. Weiss, McGraw-Hill Book Company (1963), Chapter 6, pp. 241–244.)

Let m be a non-zero *square free* integer (positive or negative) or $m = -1$. Let

$$R(m) = \begin{cases} \mathbb{Z}[\sqrt{m}], & \text{if } m \equiv 2 \text{ or } 3 \pmod{4}, \\ \mathbb{Z}[(1 + \sqrt{m})/2], & \text{if } m \equiv 1 \pmod{4}. \end{cases}$$

Note that $R(m) \supset \mathbb{Z}[\sqrt{m}]$ but *not equal* if $m \equiv 1 \pmod{4}$. For example, $R(-19) \neq \mathbb{Z}[\sqrt{-19}]$. Now we have the following.

Theorem: 1. $R(m)$ is Euclidean $\iff m = -1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ or 73 .

2. Let $m > 0$. Then $R(-m)$ is a PID $\iff m = 1, 2, 3, 7, 11, 19, 43, 67$ or 163 .

In particular, $R(-19) = \mathbb{Z}[(1 + \sqrt{-19})/2]$ is an example of a PID with 1 which is not Euclidean.

Caution: Perhaps *confusing* $R(-19)$ with $\mathbb{Z}[\sqrt{-19}]$, in some books $\mathbb{Z}[\sqrt{-19}]$ is stated as an example of a PID which is not Euclidean. This is quite *incorrect* since $\mathbb{Z}[\sqrt{-19}]$ is *not* a PID *either* as noted in (4.5.6) below.

Note: It is not known but conjectured (i.e., *expected*) that $R(m)$ is a PID for infinitely many positive square free integers m . ■

4.4 Factorisation Domains

4.4.1 Definition: A commutative integral domain R (with 1) is called a *factorisation domain* (FD) if every non-zero element x in R can be written as a unit times a finite product of irreducible elements.

4.4.2 Theorem: Every PID is a factorisation domain.

Proof: Let R be a PID. Let Ω be the set of all elements $x \in R^*$ such that x *cannot* be written as a product of irreducible elements in R . We want to show that $\Omega = \emptyset$. Let, if possible, $\Omega \neq \emptyset$. Now consider the non-empty family of principal ideals $\mathcal{F} = \{(x) \subseteq R \mid x \in \Omega\}$. This is a partially ordered set under set inclusion.

Claim: *The family $\mathcal{F}$ has a maximal element.*

To prove this, we apply Zorn's lemma to $\mathcal{F}$. Take any chain $\mathcal{T}$ in $\mathcal{F}$. Look at $T_0 = \bigcup_{T \in \mathcal{T}} T$ which is an ideal in R since $\mathcal{T}$ is a chain of ideals. Since R is a PID, we find that $T_0 = (a)$ for some $a \in R$. Now $a \in T_0 \Rightarrow a \in T'$ for some $T' \in \mathcal{T}$ and hence we get that $T' \subseteq T_0 \subseteq T'$, i.e., $T_0 = T' \in \mathcal{T}$ is an upper bound for $\mathcal{T}$, as required. Let then $(a) \in \mathcal{F}$ be a maximal element.

This element a cannot be a unit or irreducible in R since $a \in \Omega$. Hence there exist non-units $b, c \in R$ such that $a = bc$. Since b and c are both non-units, we get that $(a) \subset (b), (a) \neq (b)$ and similarly $(a) \subset (c), (a) \neq (c)$. Thus $b, c \notin \Omega$ since (a) is maximal in $\{(x) \mid x \in \Omega\}$. This means both b and c can be factored into irreducibles and hence their product (which is a) can be factored into irreducibles implying that $a \notin \Omega$, a contradiction. Hence $\Omega = \emptyset$, as required. $\diamond$

4.4.3 Proposition: *If d is a positive integer, then the ring $\mathbb{Z}[i\sqrt{d}]$ is a factorisation domain.*

Proof: For any element $x = m + i\sqrt{d}n$, ($m, n \in \mathbb{Z}$), we consider $N(x) = m^2 + dn^2$ and notice that $N(xy) = N(x)N(y)$, $\forall x, y \in R$. Furthermore, we find that the only units in R are the solutions of $N(u) = 1$, namely, $\{\pm 1\}$ or $\{\pm 1, \pm i\}$ according as $d > 1$ or $d = 1$. If $x \in R$ is a non-zero non-unit, we prove the result by induction on $N(x)$. If x is not already irreducible, we can write $x = ab$ with $N(x) > N(a)$ and $N(x) > N(b)$. But then by induction, both a and b can be factored into irreducibles and hence also x , as required. $\diamond$

4.4.4 Example of a non-factorisation domain.

Consider the ring $R = \text{Complex entire functions}$ (1.8.8). This is a commutative integral domain with 1. The units in this ring are precisely the *nowhere vanishing* entire functions. It is easy to see that the only irreducible elements are the associates of the linear polynomial functions, namely, $\{z - \alpha \mid \alpha \in \mathbb{C}\}$. (Incidentally, we note that a linear polynomial $z - \alpha$ is a prime too and hence every irreducible element in this ring is also prime.) If R were a factorisation domain, it would imply that every element in R is an associate of a polynomial function which means that any entire function, (eg., $\sin z$), has only

a finite number of zeros which is absurd.

4.4.5 Remark: Theorem (4.4.2) above is a particular case of a more general theorem of which Proposition (4.4.3) above, is a corollary. It is the following.

Theorem: *Every Noetherian domain is a factorisation domain.*

We shall study Noetherian rings in § 6.5 below. The proof of this general theorem is identical with that of Theorem (4.4.2) above, where the fact proved in the *Claim* therein is simply a property of Noetherian rings. Secondly, the rings such as $\mathbb{Z}[i\sqrt{d}]$, $\mathbb{Z}[\sqrt{d}]$ are Noetherian being quotients of the Noetherian ring $\mathbb{Z}[X]$.

4.4.6 Corollary: *The ring of Complex entire functions is not Noetherian (since it is not even a factorisation domain).*

(See Theorem (6.5.13) below, for another proof.) ■

4.5 Unique Factorisation Domains

4.5.1 Definition: A domain R is called a *unique factorisation domain* (UFD) if

1. R is a factorisation domain, i.e., every non-zero element can be factored into a unit times a finite product of irreducibles and
2. the factorisation into irreducibles is unique upto order and associates, i.e., if $x \in R^*$ is factored as

$$x = u \cdot a_1 \cdot a_2 \cdots a_r = v \cdot b_1 \cdot b_2 \cdots b_s$$

where u, v are units and a_i 's, b_j 's are irreducibles, then $r = s$ and each a_i is an associate of a b_j and vice-versa.

4.5.2 Theorem: *In a UFD, every irreducible element is a prime.*

Proof: Let a be an irreducible element in a UFD R . Let $x, y \in R^*$ be such that $a \mid xy$. We have to show that either $a \mid x$ or $a \mid y$. Since $a \mid xy$, $\exists b \in R^*$ such that $ab = xy$. Since R is a UFD, there exist units u, v and irreducibles p_i, q_j ; $1 \leq i \leq r$, $1 \leq j \leq s$ such that

$$x = up_1p_2 \cdots p_r \text{ and } y = vq_1q_2 \cdots q_s.$$

Now we have $ab = xy = uv p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$. Since the irreducible

a occurs in one factorisation of xy , it should be an associate of some irreducible occurring in any other factorisation of xy into irreducibles. Hence a is an associate of some p_i or a q_j . Say, $a\alpha = p_i$ for some unit α . Thus we get that

$$x = up_1p_2 \cdots p_r = up_1p_2 \cdots p_{i-1}a\alpha p_{i+1} \cdots p_r$$

which gives $x = ax'$ for some $x' \in R^*$ and hence $a \mid x$, as required. $\diamond$

4.5.3 Theorem: *A domain R is a UFD if and only if R is an FD in which every irreducible element is a prime.*

Proof: The implication ‘ $\Rightarrow$ ’ is the theorem above. To prove the reverse implication $\Leftarrow$, we have only to prove the uniqueness of factorisation. This is quite easy. Let $x \in R^*$ have two factorisations into irreducibles (i.e., primes), say, $x = up_1p_2 \cdots p_r = vq_1q_2 \cdots q_s$ with u, v units and p_i, q_j primes. Now proceed by induction on r . If $r = 0$, then x is a unit implying that any factor of x is a unit and hence $s = 0$. Assume that $r \geq 1$ and the induction hypothesis. Note then that $s \geq 1$. Since $p_1 \mid x$ and p_1 is a prime, we get that $p_1 \mid q_j$ for some j . Since q_j is also a prime, it follows that p_1 and q_j are associates, and so there exists a unit $\alpha \in R$ such that $q_j = \alpha p_1$. Upon substituting for q_j in the factorisations of x and cancelling p_1 , we get that

$$x' = up_2 \cdots p_r = v\alpha q_1q_2 \cdots q_{j-1}q_{j+1} \cdots q_s.$$

The result follows by induction applied to x' in place of x . $\diamond$

4.5.4 Corollary: *A domain R is a UFD if and only if every non-zero non-unit in R can be factored into a finite product of primes.*

This is merely a restatement of the above theorem. The point to be emphasized is that if the factorisation is into *primes* instead of *irreducibles*, then *uniqueness* of factorisation is *automatic*.

4.5.5 Corollary: *Every PID is a UFD* (by Theorems (4.3.3)(1) and (4.4.2) above).

4.5.6 Remark: The conditions “FD” and “irreducible is prime” in Theorem (4.5.3) above, are independent of each other and both are essential. For instance, we look at the examples.

1. The ring $\mathbb{Z}[i\sqrt{3}]$ is an FD by (4.4.3) above, but it is not a UFD since the element $1 + i\sqrt{3}$ is irreducible but not a prime. (See the Example

after (4.1.8) above.) Likewise, $\mathbb{Z}[i\sqrt{19}]$ is an FD but not a UFD (since $1 + i\sqrt{19}$ is irreducible but not a prime).

2. The ring of Complex entire functions (1.8.8) is not an FD but every irreducible element therein is a prime (4.4.4).

4.5.7 Remark: In a UFD, “gcd” and “lcm” exist. However, *unlike* in a PID, it is not true that $(d) = (a) + (b)$ if $d = \gcd(a, b)$. In other words, this equality (as proved in Theorem (4.3.5)(1) above) is very special for PID’s. In fact, this property of gcd characterises PID’s with the *additional* hypothesis that ideals are finitely generated. See Ex.(6.8.25) below.

To see the existence: let $a, b \in R^*$. By unique factorisation, there exist units u, v and primes $p_i, 1 \leq i \leq r$ such that

$$a = up_1^{e_1} \cdots p_r^{e_r} \quad \text{and} \quad b = vp_1^{f_1} \cdots p_r^{f_r}$$

for some non-negative integers e_i and $f_i, 1 \leq i \leq r$. Now define $d_i = \min(e_i, f_i)$ and $m_i = \max(e_i, f_i), 1 \leq i \leq r$. Then we have

$$\gcd(a, b) = p_1^{d_1} \cdots p_r^{d_r} \quad \text{and} \quad \text{lcm}(a, b) = p_1^{m_1} \cdots p_r^{m_r}.$$

Note: Given finitely many elements $a_i \in R^*, 1 \leq i \leq r$, in a UFD, the definition and existence of gcd or lcm of a_i ’s is obvious. If $d = \gcd(a_1, \dots, a_r)$, then writing $a'_i = a_i/d, 1 \leq i \leq r$, we find that $a'_1, \dots, a'_r$ are collectively coprime, i.e., $1 = \gcd(a'_1, \dots, a'_r)$. Note that if $\ell = \text{lcm}(a_1, \dots, a_r)$, then $d\ell$ and $a_1 \cdots a_r$ are associates. $\diamond$

A Theorem of Gauss for UFD’s

To prove the most important theorem of Gauss for UFD’s, we need the following considerations. In what follows, unless otherwise stated, R stands for a UFD and $K = Q(R)$ its field of fractions.

4.5.8 Content of a polynomial: Given a non-zero polynomial $f(X)$ in $R[X]$, the gcd of the coefficients of $f(X)$ is called the *content* of $f(X)$ and is denoted by $c(f(X))$ or simply $c(f)$.

4.5.9 Primitive polynomial: A non-zero polynomial $f(X)$ is called *primitive* if its content is 1, i.e., its coefficients are collectively coprime.

Note: (1) Any non-zero polynomial $f(X)$ can be written as a product of a non-zero scalar and a primitive polynomial because $f(X)/c(f)$ is primitive and $c(f)$ is a non-zero scalar.

(2) Any irreducible polynomial is primitive.

4.5.10 Proposition: *The content of a product of polynomials is the product of their contents and in particular, the product of primitive polynomials is primitive.*

Proof: In view of the note above, it suffices to prove the result for the case of primitive polynomials. Let $f(X), g(X)$ primitive in $R[X]$. Let $h(X) = f(X)g(X)$. We have to show that $c(h)$ is a unit in R . If not, take a prime divisor p of $c(h)$. Write

$f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ where $a_mb_n \neq 0$. Since $c(f) = c(g) = 1$, we can find r, s least such that p is not a divisor of a_r or b_s , $0 \leq r \leq m$, $0 \leq s \leq n$. Note that $p \mid a_i$, $0 \leq i \leq r-1$ and $p \mid b_j$, $0 \leq j \leq s-1$ by the choice of r and s . Now look at the coefficient of $h(X)$, namely, $\sum_{i+j=r+s} a_ib_j$. Since p is a divisor of $c(h)$, it is a divisor of this coefficient of $h(X)$. On the other hand, since p is a divisor of a_i , $0 \leq i \leq r-1$ and of b_j , $0 \leq j \leq s-1$, it follows that p is a divisor of a_rb_s which is a contradiction to the fact that p is not a divisor of a_r or b_s . Hence $c(h) = 1$, as required. $\diamond$

4.5.11 Gauss Lemma: *A primitive polynomial $f(X) \in R[X]$ is irreducible in $R[X]$ if and only if $f(X)$ is irreducible in $K[X]$ where K is the field of fractions of R .*

Proof: Assume that $f(X)$ is primitive and irreducible in $R[X]$. Let, if possible, $f(X)$ be reducible in $K[X]$, say $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$. We can write $g(X) = (a/b)p(X)$ and $h(X) = (c/d)q(X)$ with $a, b, c, d \in R^*$, $p(X), q(X) \in R[X]^*$ and both $p(X)$ and $q(X)$ primitive.

Now substituting, we can write $f(X) = (\alpha/\beta)p(X)q(X)$ for some $\alpha, \beta \in R^*$ with α, β coprime. Thus we get $\beta f(X) = \alpha p(X)q(X)$ and hence comparing contents on either side, we have $\beta c(f) = \alpha c(p)c(q)$, i.e., $\beta = \alpha$ which means $f(X) = p(X)q(X)$ in $R[X]$ contradicting the irreducibility of $f(X)$. Conversely, if $f(X) \in R[X]$

is irreducible in $K[X]$, then it is obviously irreducible in $R[X]$ since $f(X)$ is primitive. $\diamond$

4.5.12 Theorem (Gauss): *Let R be a domain. Then $R[X]$ is a UFD if and only if R is a UFD.*

Proof: If $R[X]$ is an FD so is R since (for degree reasons) all factors in $R[X]$ of an element in R belong to R . Moreover, elements of R are irreducible (resp. prime) in R if and only if they are irreducible (resp. prime) in $R[X]$. Consequently, if $R[X]$ is a UFD and $a \in R$ is irreducible, then a is prime in $R[X]$ and so a prime in R . Thus R is a UFD. The converse is the non-trivial part of the theorem.

Suppose that R is a UFD. Since R is an FD, it is easy to see, for degree reasons, that $R[X]$ is also an FD. The difficult part is the uniqueness of factorisation. It suffices to prove, by Theorem (4.5.3) above, that every irreducible polynomial in $R[X]$ is a prime. This is assured by Gauss Lemma. To see this; let $p(X)$ be irreducible in $R[X]$ and suppose that $p(X) \mid f(X)g(X)$ in $R[X]$. Since $p(X)$ is irreducible in $R[X]$, by Gauss Lemma, it is irreducible in $K[X]$. But $K[X]$ is a UFD since K is a field. Hence $p(X)$ is a prime in $K[X]$ and so $p(X) \mid f(X)$ or $g(X)$ in $K[X]$, say $p(X) \mid f(X)$, i.e., $f(X) = p(X)q(X)$ for some $q(X) \in K[X]$. We can write $c(X) = (a/b)q_0(X)$ with $a, b \in R^*$, a, b coprime and $q_0(X) \in R[X]^*$, $q_0(X)$ primitive. Now substituting we get $bf(X) = ap(X)q_0(X)$ in $R[X]$. Taking contents on either side, we get $bc(f) = a$ and hence on cancellation we get that $f(x) = c(f)p(X)q_0(X)$ in $R[X]$ which means $p(X) \mid f(X)$ in $R[X]$ implying $p(X)$ is a prime in $R[X]$, as required. $\diamond$

4.5.13 Corollary: *The polynomial ring over a UFD is a UFD. (The number of variables may be finite or infinite.)*

Proof: Let R be a UFD.

(1) Let the variables be finite, say $X_1, \dots, X_n$. By Gauss theorem, we get that $R[X_1]$ is a UFD and hence $R[X_1, X_2] = R[X_1][X_2]$ is a UFD. Repeating this several times, we get $R[X_1, \dots, X_n]$ is a UFD.

(2) Let the set of variables be $\{X_i \mid i \in \Lambda\}$, Λ an arbitrary non-empty set. If $f \in S^*$ where $S = R[X_i, i \in \Lambda]$, f involves only some finitely

many variables and hence can be written as a product of irreducible elements for degree reasons. Thus S is a factorisation domain. It remains to check that irreducibles in S are prime. Let $p \in S$ be irreducible and $p \mid fg$ in S , say $fg = pq$ for some $q \in S$. Now p, f, g and q involve only a finite number of variables, say $X_{i_1}, \dots, X_{i_n}$. Then p is a prime in the UFD $S' = R[X_{i_1}, \dots, X_{i_n}]$ and hence $p \mid f$ or $p \mid g$ in S' and hence in S , as required. $\diamond$

4.5.14 Remark: Euclidean domains are PID's and PID's are UFD's and both of these inclusions are strict.

For instance, $\mathbb{Z}[X]$ is a UFD (by Gauss theorem) but not a PID, as noted already. We have seen that a PID need not be Euclidean. (See (4.3.2) and (4.3.7) above.)

4.5.15 Remark: A subring/quotient of a UFD need not be a UFD. To see this, take a commutative integral domain R with 1 which is not a UFD, for example $R = \mathbb{Z}[i\sqrt{3}]$. Let $K = Q(R)$ be the field of fractions of R . It is trivial that K is a UFD containing R as a subring which is not a UFD. On the other hand, we know that $\mathbb{Z}[X]$ is a UFD but its quotient $\mathbb{Z}[i\sqrt{3}] \simeq \mathbb{Z}[X]/(X^2 + 3)$ is not a UFD.

4.5.16 Remark: In a UFD R , if $d = \gcd(a, b)$, then $(d) \supset (a) + (b)$ but equality need not hold in general (unless R is a PID, see (4.3.5) and (4.5.7) above).

To see this, take $R = K[X, Y]$, K a field. Then $1 = \gcd(X, Y)$, but $R = (1) \neq (X) + (Y)$. $\blacksquare$

4.6 Eisenstein's Criterion

4.6.1 Theorem (Eisenstein's Criterion): Let R be a UFD and $f(X) \in R[X]^*$ be a primitive polynomial, say $f(X) = a_0 + a_1X + \dots + a_rX^r$, $a_r \neq 0$. Suppose there is a prime p in R such that

(i) $p \mid a_i, 0 \leq i \leq r-1$ and $p \nmid a_r$, i.e., p divides all but the leading coefficient and (ii) $p^2 \nmid a_0$. Then $f(X)$ is irreducible.

Proof: Let $f(X)$ be reducible, say $f(X) = g(X)h(X)$ where $g(X) = b_0 + b_1X + \dots + b_mX^m$ and $h(X) = c_0 + c_1X + \dots + c_nX^n$ with $b_m a_n \neq 0$. We shall prove that either $g(X)$ or $h(X)$ is a unit.

Since $f(X)$ is primitive, so are $g(X)$ and $h(X)$ by Gauss lemma. Since $p \mid a_0 = b_0 c_0$, we get that $p \mid b_0$ or $p \mid c_0$, say $p \mid b_0$. Furthermore, p cannot divide c_0 since p^2 does not divide a_0 . On the other hand, since p does not divide $a_r = b_m c_n$, p cannot divide b_m or c_n . Let ℓ be least such that p does not divide b_ℓ . We get that $1 \leq \ell \leq m$. If $n \neq 0$, we get that $\ell \leq m < m + n = r$. But then, $p \mid a_\ell$ where $a_\ell = \sum_{i+j=\ell} b_i c_j$ implying that $p \mid b_\ell c_0$ (since $p \mid b_i, 0 \leq i \leq \ell - 1$ and $p \mid a_\ell$). This is a contradiction. Hence $n = 0$ which means that c_0 is a unit since $h(X) = c_0$ is primitive. Thus $f(X)$ is irreducible, as required. $\diamond$

4.6.2 Remark: The Eisenstein's criterion for irreducibility can also be stated interchanging the roles of the constant term and the leading coefficient. The proof above is obviously symmetric with respect to these two entities.

4.6.3 Corollary: *The double sequence $\{X^n - p\}$, as p varies over primes in $\mathbb{Z}$ and $n \in \mathbb{Z}^+$, consists of all irreducible polynomials and mutually non-associates in $\mathbb{Z}[X]$. In particular, there are infinitely many irreducibles in $\mathbb{Z}[X]$ (in each degree).*

4.6.4 Remark ; The Eisenstein's criterion is only a sufficient condition but not necessary.

For example, the polynomial $f(X) = 1 + X + X^2 + \dots + X^{p-1}$ is irreducible in $\mathbb{Z}[X]$ for any prime number p in $\mathbb{Z}$, yet obviously there is no prime satisfying the conditions of the criterion.

To see the irreducibility of $f(X)$, first note that $f(X)$ is irreducible if and only if $f(X + 1)$ is irreducible (see Ex.(4.7.17) below). We have $f(X) = (X^p - 1)/(X - 1)$ and so

$$\begin{aligned} f(X + 1) &= [(X + 1)^p - 1] / X \\ &= X^{p-1} + pX^{p-2} + \dots + \binom{p}{i} X^{p-i-1} + \dots + \binom{p}{2} X + p. \end{aligned}$$

This is a monic polynomial for which Eisenstein's criterion can be applied with the prime p and hence irreducible, as required. $\blacksquare$

4.7 Exercises

In this section, unless otherwise specified, a ring means a commutative integral domain with 1. Given a prime number p and a positive integer n , a finite field having exactly p^n elements is denoted by $\mathbb{F}_{p^n}$. For instance, we have $\mathbb{F}_p = \mathbb{Z}_p$. Some of the following exercises can be done much more quickly if the reader has a little exposure to field extensions. However, it is not essential.

1. Show that the set of units in the ring $\mathbb{Z}[i\sqrt{5}]$ is $\{\pm 1\}$ and that $2 + i\sqrt{5}$ is irreducible but not a prime.
2. Show that $1 + 2i\sqrt{5}$ is irreducible in $\mathbb{Z}[i\sqrt{5}]$. Is it a prime?
3. Show that the gcd of 3 and $1 + 2i\sqrt{5}$ exists in $\mathbb{Z}[i\sqrt{5}]$. Examine the same for the pair $1 + 2i\sqrt{5}$ and $2 + i\sqrt{5}$.
4. Show that in the ring $\mathbb{Z}[i]$, the elements $3 + 4i$ and $4 - 3i$ are associates whereas $11 + 7i$ is coprime to $18 - i$.
5. In the ring $\mathbb{Q}^p$ (1.8.7), given non-zero elements x and y , show that either $x \mid y$ or $y \mid x$. Show that the same is true in $\mathbb{Q}^p[[X]]$ as well. Is it true also in $\mathbb{Q}^p[[X, Y]]$?

Let R be a ring and $f(X) \in R[X]$ be a non-constant polynomial. We know that the number of roots of $f(X)$ in R has *no* relation to its degree if R is *not commutative* or *commutative but not a domain*. (See Exs.(1.13.15) and (1.13.16) above.) However, we have the following.

6. Show that the number of roots of a non-zero polynomial over a commutative integral domain R is at most its degree. (Hint: Use the Remainder theorem and unique factorisation in $Q(R)[X]$ where $Q(R)$ is the field of fractions of R .)
7. Let K be a field and $f(X)$ a non-constant polynomial in $K[X]$. Suppose that $\deg f(X) \leq 3$. Show that $f(X)$ is irreducible if and only if $f(X)$ has no roots in K . Give an example to show that the “if” part of this result need not be true when $\deg f(X) \geq 4$.
8. Show that $1 + X^2$ is prime and is coprime to $1 + X + X^3 + X^6$ in $\mathbb{Z}[X]$.
9. Show that $1 + X + X^3 + X^6$ is *not* irreducible in $R[X]$ for any domain R with 1.

The following 7 exercises (which have some overlaps too) lead to a *complete information* about the set of primes in the Euclidean domain $\mathbb{Z}[i]$ and the residue fields thereof, namely,

Theorem: *Every prime number p in $\mathbb{Z}$ either remains a prime or splits into a product $p = p_1 p_2$ of two non-associate primes p_1 and p_2 in $\mathbb{Z}[i]$ and conversely every prime is of the form p or p_1 or p_2 . Furthermore, the residue fields at these primes are respectively given by $\mathbb{Z}[i]/(p) = \mathbb{F}_{p^2}$ and $\mathbb{Z}[i]/(p_1) = \mathbb{Z}_p = \mathbb{Z}[i]/(p_2)$.*

10. Let K be a field. Show that the polynomial $1 + X^2$ is irreducible in $K[X]$ if and only if -1 is *not* a square in K . Hence or otherwise, test for its irreducibility in $\mathbb{Z}_p[X]$ for $p = 3, 7, 11$, etc. Do the same for $p = 2, 5, 13$, etc.
11. If p is a prime number such that -1 is not a square in $\mathbb{Z}_p$, show that the residue field $\mathbb{Z}_p[X]/(1 + X^2)$ has exactly p^2 elements. In particular, we have $\mathbb{Z}_p[X]/(1 + X^2) = \mathbb{F}_{p^2}$ for $p = 3, 7, 11$, etc.
12. In the ring $\mathbb{Z}[i]$, show that a non-zero non-unit $x = m + in$ is irreducible if and only if its norm $N(x) = m^2 + n^2$ is a prime in $\mathbb{Z}$. Write down some primes in $\mathbb{Z}$ which can be expressed as a sums of two squares in $\mathbb{Z}$ and some others which cannot be. Are there infinitely many primes of either kind?
13. Show that the primes $p = 3, 7, 11, \dots$ remain irreducible in $\mathbb{Z}[i]$ with the residue fields given by $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$. (This is a special case of the following.)
14. Let p be a prime in $\mathbb{Z}$. Show that p remains a prime in $\mathbb{Z}[i]$ if and only if p is *not* a sum of two squares. Furthermore, show that the residue field $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$ if p remains a prime in $\mathbb{Z}[i]$. (Now look at the remaining primes p in $\mathbb{Z}$.)
15. Show that a prime p in $\mathbb{Z}$ is a sum of two squares if and only if -1 is a square in $\mathbb{Z}_p$.
16. Let p be a prime number which is a sum of two squares in $\mathbb{Z}$. Show that p splits into a product $p = xy$ of two non-associate primes x and y in $\mathbb{Z}[i]$ with isomorphic residue fields, namely, $\mathbb{Z}[i]/(x) \simeq \mathbb{Z}_p \simeq \mathbb{Z}[i]/(y)$.
17. Let R be a domain and $f(X) \in R[X]$ be a polynomial of positive degree. Show that $f(X)$ is irreducible if and only if $f(X + a)$ is irreducible for any $a \in R$.

18. Let $R = \mathbb{Z}[\sqrt{5}]$ and $N(x) = |m^2 - 5n^2|$ for $x = m + n\sqrt{5}$. Show that
 - for a non-zero non-unit $x \in R$, $N(x) \geq 4$,
 - x is irreducible if $4 \leq N(x) < 16$ and
 - 4 splits into irreducibles but not uniquely.
 Consequently, $\mathbb{Z}[\sqrt{5}]$ is not a UFD.
19. Let $f(X)$ be a monic polynomial in $\mathbb{Z}[X]$. Suppose that a rational number r is a root of $f(X)$. Then show that r is an integer.
 Generalise this statement to an arbitrary UFD R in place of $\mathbb{Z}$, i.e., if an element x of $Q(R)$ is a root of a monic polynomial in $R[X]$, then show that $x \in R$.
20. Show that every non-zero *minimal prime* ideal in a UFD is principal. (Hint: Take a prime divisor p of any non-zero element in such an ideal P and conclude that $(p) = P$.)
21. Let R be a UFD. Then show that R is a PID if every prime (resp. maximal) ideal is principal.
22. Show that there are infinitely many mutually non-associate primes in $K[X]$ for any field K . (Hint: If there are only finitely many primes $p_1, \dots, p_n$, take a prime divisor of $1 + \prod_{i=1}^n p_i$.)
23. Show that $\mathbb{Q}^{(p_1, \dots, p_n)}$ (2.8.10) is a PID having only finitely many primes (upto associates), namely, $p_1, \dots, p_n$. Why does the hint given above fail here?
24. Show that for all $n \in \mathbb{N}$, there are infinitely many irreducible elements in $\mathbb{Q}[X]$ of degree n . (Hint: Use Eisenstein's criterion in $\mathbb{Z}[X]$ and Gauss lemma.)
25. Let R be a local domain (2.8.2) with its maximal ideal M . Show that R is a PID if and only if M is a principal ideal. (Hint: If $M = (\pi)$, then π is a prime in R and every non-zero element of R is an associate of π^n for some $n \in \mathbb{Z}^+$.)
26. Show that every ideal in a PID can be written as a product of prime ideals. Is this true also in a UFD? (Hint: If $a = p_1 \cdots p_n$ is a product of primes, then $(a) = (p_1) \cdots (p_n)$.)
27. Let R be a UFD and P a prime ideal in R . Show that the localisation R_P (3.6.17) of R at P is a UFD and that its primes (upto

- associates) are precisely those of R contained in P . In particular, R_P is a PID if P is a minimal (non-zero) prime ideal.
28. Show that the Laurent polynomial ring $R[X, X^{-1}]$ is a UFD for every UFD R . (Hint: A prime in $R[X]$ becomes a unit or remains a prime in $R[X, X^{-1}]$.)
 29. Let $R = \mathbb{C}[X^2, X^3]$, the subring of $\mathbb{C}[X]$ generated by $\mathbb{C}, X^2$ and X^3 . Show that R is a factorisation domain but not a UFD. (Hint: X^2 is irreducible but not a prime.)
 30. Show that there are natural isomorphisms of rings between the following.
 - $\mathbb{Z}[X]/(1 + X^2) \simeq \mathbb{Z}[i]$,
 - $\mathbb{Q}[X]/(1 + X^2) \simeq \mathbb{Q}[i]$ and
 - $\mathbb{R}[X]/(1 + X^2) \simeq \mathbb{C} \simeq \mathbb{R}[X]/(1 + X + X^2)$.
 31. Show that every finitely generated ideal in the ring of Complex entire functions (1.8.8) is principal. (See Ex.(6.9.26) below.) ■

4.8 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counter-example if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be. Unless stated otherwise, R stands for a commutative integral domain with 1.

1. The polynomial $2 + 2X + 3X^3$ is irreducible in $\mathbb{Q}[X]$.
2. The element X is a prime in $R[X]$.
3. The element $1 + i\sqrt{3}$ is a prime in $\mathbb{Z}[i\sqrt{3}]$.
4. The element 6 is a prime in $\mathbb{Q}^3$ (1.8.7).
5. Any element in $\mathbb{Z}[i]$ is an associate of its complex conjugate.
6. The prime number 17 is not a prime in $\mathbb{Z}[i]$.
7. The prime number 19 is a prime in $\mathbb{Z}[i]$.
8. In a PID, every prime ideal is a maximal ideal.
9. In a PID, every non-zero prime ideal is a maximal ideal.
10. $R[X]$ is Euclidean if and only if $R[X]$ is a PID.

11. For a prime p in $\mathbb{Z}$, $1 + X + X^2 + \cdots + X^p$ is irreducible in $\mathbb{Z}[X]$.
12. For a prime p in $\mathbb{Z}$, $1 + X + X^2 + \cdots + X^{p-1}$ is irreducible in $\mathbb{Z}[X]$.
13. For a prime p in $\mathbb{Z}$, the polynomial $1 + X + X^2 + \cdots + X^p$ is irreducible in $\mathbb{Z}/(2)[X]$ only if $p \neq 2$.
14. The quadratic $aX^2 + bX + c$ in $\mathbb{R}[X]$ (with $a \neq 0$), is irreducible if and only if $b^2 - 4ac < 0$.
15. Subring of a PID is a PID.
16. $\mathbb{Z}[i\sqrt{5}]$ is a PID.
17. Subring of a Euclidean domain is Euclidean.
18. The ring $\mathbb{C}[X, Y]$ is Euclidean.
19. If K is a field, every non-zero element of $K[[X]]$ is an associate of X^n for some $n \geq 0$.
20. Product of prime ideals is a prime ideal.
21. Homomorphic images of associates are associates under a unitary monomorphism of commutative integral domains.
22. Every factorization domain is a unique factorization domain.
23. Subrings and quotient rings of a UFD are UFD's.
24. The set of units in $\mathbb{Z}[i\sqrt{d}]$ is $\{\pm 1\}$ for all $d \in \mathbb{N}$.
25. The ring $\mathbb{Z}[\sqrt{d}]$ is a factorisation domain for all $d \in \mathbb{N}$.
26. The ring $\mathbb{Z}[i\sqrt{3}]$ is a UFD.
27. The ring $\mathbb{Z}[i\sqrt{5}]$ is a PID.
28. The ring $\mathbb{Z}[i\sqrt{d}]$ is a factorisation domain for all $d \in \mathbb{N}$.
29. Any irreducible element in the ring $\mathbb{Z}[i\sqrt{2}]$ is a prime.
30. An irreducible element is prime in an FD $\iff$ it is a UFD.
31. R is a UFD $\iff$ every irreducible element is prime in R .
32. The ring of Complex entire functions (1.8.8) is an FD.
33. In the ring of Complex entire functions, an irreducible is prime.
34. If R is an FD (but not necessarily a UFD) then so is $R[X]$. ■

Part II

MODULES

Chapter 5

Modules

In this chapter, we shall formulate and study an extension of the concept of a “vector space” over a field to the so called “modules” over arbitrary rings. As we shall notice, “vector spaces” are too good, in fact, excellent, when compared to the modules in general. However, these limitations make the study of modules even more interesting. Ideals in rings become special cases of modules and often serve to illustrate or counter illustrate certain aspects of modules in general. Just as the linear transformations between vector spaces, we have homomorphisms between modules whose formal properties have to be gone through. As in the case of groups and rings, we have the notion of quotient modules whose properties are exactly as one would expect. We end the chapter with the study of modules over PID’s. These are next to vector spaces in sharing some good properties but are almost like “abelian groups” which are, after all, modules over $\mathbb{Z}$ which is a special PID. We have not touched upon the case of matrices over PID’s, their canonical forms, elementary divisors, etc., in the context of linear transformations between free modules over PID’s.

5.1 Definitions and Examples

5.1.1 Left module: Let R be any ring (with or without 1 and commutative or not). By a *left R -module* M , we mean, an abelian group $(M, +)$ together with a map $R \times M \rightarrow M$, $(a, x) \mapsto ax$, called the *scalar multiplication* or the *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 $x \in M$ and
3. $(ab)x = a(bx)$, $\forall a, b \in R$ and $x \in M$.

Elements of R are called *scalars*.

5.1.2 Proposition: Let M be an R -module. Then we have

1. $0_R x = a 0_M = 0_M$, $\forall a \in R$ and $x \in M$,
2. $-(ax) = (-a)x = a(-x)$, $\forall a \in R$ and $x \in M$ and
3. $mn(ax) = (mna)x = a(mnx) = (ma)(nx) = (na)(mx)$,
 $\forall a \in R, x \in M$ and $m, n \in \mathbb{Z}$.

Proof: Easy verification. ◇

5.1.3 Remark: If M is a left R -module, sometimes we also say that the abelian group $(M, +)$ has a *left R -module structure*. In case the scalar multiplication is trivial, i.e., $ax = 0$, $\forall a \in R$ and $x \in M$, then the left R -module M is same as the abelian group $(M, +)$. This is called the *trivial module structure* of R on M . In case $M = (0)$ whatever be R , a left R -module on M is the obvious scalar multiplication, $a0 = 0$, $\forall a \in R$. This is called the *zero module* over R .

In case R has 1 and the scalar multiplication $1 \cdot x_0 = 0$ for any $x_0 \in M$, then $ax_0 = (a \cdot 1)x_0 = a(1 \cdot x_0) = a \cdot 0 = 0$, $\forall a \in R$. Thus if $1 \cdot x = 0$, $\forall x \in M$, then it follows that $ax = 0$, $\forall a \in R$ and $x \in M$ which means that M is a trivial left R -module.

5.1.4 Unitary module: A left R -module M is said to be *unitary left R -module* if $1 \cdot x = x$, $\forall x \in M$.

5.1.5 Right module: An abelian group $(M, +)$ is called a *right R -module* if there is a map from $M \times R \rightarrow M$ denoted by $(x, a) \mapsto xa$ such that

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

If R has unity and $x \cdot 1 = x$, $\forall x \in M$, then M is called *unitary right R -module*.

5.1.6 Proposition: For an abelian group M , let $\text{End}_{\mathbb{Z}}(M)$ be the

ring of all (additive) endomorphisms of M . Let R any ring. Then we have the following.

1. M is a left R -module $\iff$ there exists a homomorphism of rings $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$.
2. M is a right R -module $\iff$ there exists an anti-homomorphism of rings $\Psi' : R \rightarrow \text{End}_{\mathbb{Z}}(M)$, i.e., Ψ' preserves addition but reverses the multiplication.
3. M is R -unitary $\iff \Psi(1_R) = \text{id}_M$ (resp. $\Psi'(1_R) = \text{id}_M$).

Proof: (1) Let M be a left R -module with scalar multiplication, $R \times M \rightarrow M$, $(a, x) \mapsto ax$. Now define $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ by $a \mapsto \Psi(a)$, where $\Psi(a) : M \rightarrow M$ is defined by $\Psi(a)(x) = ax$, $\forall a \in R$ and $x \in M$.

Claim (i): Ψ is a homomorphism of rings.

For, let $a, b \in R$ and $x \in M$. We have

$$\Psi(a+b)(x) \stackrel{\text{def}}{=} (a+b)x = \Psi(a)(x) + \Psi(b)(x) = [\Psi(a) + \Psi(b)](x).$$

Thus $\Psi(a+b) = \Psi(a) + \Psi(b)$. Similarly, we have for $x \in M$,

$$\begin{aligned} \Psi(ab)(x) &\stackrel{\text{def}}{=} (ab)(x) = a(bx) = a(\Psi(b)(x)) \\ &= \Psi(a)(\Psi(b)(x)) = (\Psi(a) \circ \Psi(b))(x). \end{aligned}$$

Thus $\Psi(ab) = \Psi(a)\Psi(b)$ and hence Ψ is a homomorphism of rings.

Conversely, suppose that $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ is a homomorphism of rings. Now define the scalar multiplication by

$$R \times M \rightarrow (a, x) \mapsto ax = (\Psi(a))(x).$$

Claim (ii): This defines a left R -module structure on M .

For, let $a, b \in R$ and $x, y \in M$. Since $\Psi(a) \in \text{End}_{\mathbb{Z}}(M)$, we have

$$a(x+y) \stackrel{\text{def}}{=} (\Psi(a))(x+y) = \Psi(a)(x) + \Psi(a)(y) \stackrel{\text{def}}{=} ax + ay.$$

Similarly, we have

$$\begin{aligned} (a+b)(x) &\stackrel{\text{def}}{=} \Psi(a+b)(x) = [\Psi(a) + \Psi(b)](x) \\ &= \Psi(a)(x) + \Psi(b)(x) \stackrel{\text{def}}{=} ax + bx \text{ and} \end{aligned}$$

$$\begin{aligned}
 (ab)(x) &\stackrel{\text{def}}{=} \Psi(ab)(x) = (\Psi(a) \circ \Psi(b))(x) \\
 &= \Psi(a)(\Psi(b)(x)) \stackrel{\text{def}}{=} \Psi(a)(bx) \stackrel{\text{def}}{=} a(bx).
 \end{aligned}$$

Thus M is an R -module. Proof of (2) is similar to (1).

(3) Suppose M is R -unitary and $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ is the corresponding homomorphism of rings. We have $\Psi(1) : M \rightarrow M, x \mapsto \Psi(1)(x) = 1 \cdot x = x$. Hence $\Psi(1_R) = \text{id}_M$.

Conversely, suppose that $\Psi(1_R) = \text{id}_M$ where $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$ is a homomorphism of rings. Look at the scalar multiplication defined as above, $R \times M \rightarrow M, (a, x) \mapsto ax = (\Psi(a))(x)$. We have $1 \cdot x = (\Psi(1))(x) = \text{id}_M(x) = x$, as required. $\diamond$

5.1.7 Corollary: *M is a left R -module implies that M is a right R^0 -module where R^0 is the ring opposite to R (1.11.1).*

Proof : We have a homomorphism of rings $\Psi : R \rightarrow \text{End}_{\mathbb{Z}}(M)$. Compose this with the identity map $\text{id} : R^0 \rightarrow R$ which is an anti-isomorphism, to get an anti-homomorphism $R^0 \rightarrow \text{End}_{\mathbb{Z}}(M)$ which means M is a right R^0 -module.

Conversely, suppose that we have an anti-homomorphism of rings $\Psi' : R^0 \rightarrow \text{End}_{\mathbb{Z}}(M)$. Compose this with the identity map $\text{id} : R \rightarrow R^0$ which is an anti-isomorphism, to get a homomorphism $R \rightarrow \text{End}_{\mathbb{Z}}(M)$. Therefore M is a left R -module. $\diamond$

5.1.8 Remarks: 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 .

Henceforth, we confine ourselves to the study of left modules. All modules are assumed unitary unless otherwise stated.

5.1.9 Submodule: Let M be an R -module. A non-empty subset N of M is called an R -submodule of M if

1. N is an additive subgroup of M , i.e., $x, y \in N \Rightarrow x - y \in N$ and
 2. N is closed for scalar multiplication, i.e., $x \in N, a \in R \Rightarrow ax \in N$.
- In other words, the restrictions to N of addition and scalar multiplication in M make N into an R -module in its own right.

5.1.10 Examples of modules: 1. *Unitary modules over $\mathbb{Z}$ are simply abelian groups.*

For, suppose, M is an abelian group. We have the natural map $\eta : \mathbb{Z} \times M \rightarrow M, (n, x) \mapsto nx$ where

$$nx = \begin{cases} x + x + \cdots + x \text{ (} n \text{ times)}, & \text{if } n \geq 0, \\ -x - x - \cdots - x \text{ (} |n| \text{ times)}, & \text{if } n \leq 0. \end{cases}$$

Then we have

$$\begin{aligned} n(x + y) &= \underbrace{(x + y) + (x + y) + \cdots + (x + y)}_{n \text{ times}} \\ &= \underbrace{(x + x + \cdots + x)}_{n \text{ times}} + \underbrace{(y + y + \cdots + y)}_{n \text{ times}} = nx + ny. \end{aligned}$$

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 $\mathbb{Z} \times M \rightarrow M, (n, x) \mapsto n \cdot x$, we show that $n \cdot x = nx$ for all $n \in \mathbb{Z}$. For $n \geq 0$, we have

$$\begin{aligned} n \cdot x &= \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ times}} \cdot x = 1 \cdot x + 1 \cdot x + \cdots + 1 \cdot x \\ &= x + x + \cdots + x = nx. \end{aligned}$$

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

2. *If R is any ring, R is naturally a left R -module and also a right R -module with usual multiplication in R as the scalar multiplication.*

• **Left module structure:** $R \times (R, +) \rightarrow (R, +), (a, x) \mapsto ax,$

• **Right module structure:** $R \times (R, +) \rightarrow (R, +), (a, x) \mapsto xa.$

If R has 1, these two module structures on R are both unitary. Sometimes we use the symbol, ${}_R R$ for the left R -module R and the symbol R_R for the right R -module R .

3. Suppose S is a subring of a ring R . Then R can be considered as a left (resp. right) S -module in a natural way, namely, with regard to multiplication in R , i.e., for all $a \in S$, $x \in R$ we have

$$S \times R \rightarrow R, (a, x) \mapsto ax \text{ (resp. } xa).$$

The module R over any of its subrings need not be unitary in general. However, if S has unity 1_S and $1_S = 1_R$, then R is unitary as an S -module. Secondly, a subring S is a module over the whole ring only if S is an ideal in R .

4. $\mathbf{H}$ is a module over $\mathbf{H}$, $\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}$ or $\mathbf{Z}$.

5. Any abelian group M is naturally a unitary left module over $R = \text{End}_{\mathbf{Z}} M$. The structure map $R \times M \rightarrow M$ is the evaluation $(f, x) \mapsto f(x)$. Since $(\text{id}, x) \mapsto \text{id}(x) = x$, it is a unitary module.

5.1.11 Direct product: Let R be any ring and M, N be (left) R -modules, then the Cartesian product $M \times N$ can be made into an R -module, called the *direct product* of M and N , in a natural way,

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

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

Special cases: 1. $R^2 = R \times R$.

$$2. R^n = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}}.$$

$$3. R^I = \prod_{\alpha \in I} R_\alpha, R_\alpha = R, \forall \alpha \in I.$$

$$4. R^\infty = \prod_1^\infty R.$$

5.1.12 Sum of submodules: 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 $P + Q = \{x + y \mid x \in P, y \in Q\}$.

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 , i.e.,

$$\sum_{\alpha \in I} P_\alpha = \{\sum_{\alpha \in I} x_\alpha \mid x_\alpha \in P_\alpha, x_\alpha = 0 \text{ except for finitely many } \alpha\text{'s}\}.$$

This is the smallest submodule of M containing each P_α , $\alpha \in I$. ■

5.2 Direct Sums

5.2.1 Direct sum: 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, $M = \{(x, 0) \in P \mid x \in M\} \subseteq P$ 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.

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

5.2.2 Proposition: 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 uniquely written as $z = x + y$ with $x \in M$ and $y \in N$.

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

Conversely, suppose every element of $M + N$ has a unique decomposition. Let $z \in M \cap N$. Now $0 = z + (-z) = 0 + 0 \in M + N$, $z \in M$, $-z \in N$. By uniqueness of decomposition we get $z = 0$, i.e., $M \cap N = (0)$. $\diamond$

5.2.3 Definition: A module P over R is called a *direct sum of 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 α 's. We write $P = \oplus_{\alpha \in I} P_\alpha$.

5.2.4 Remark: It is easy to see that $\oplus_{\alpha \in I} P_\alpha \subseteq \prod_{\alpha \in I} P_\alpha$ and equality holds if and only if I is finite.

5.2.5 Direct summand: A submodule P of a module M is said to be a *direct summand* or simply a *summand* of M if there exists

a submodule Q of M such that $M = P \oplus Q$. Such a Q is called a *supplement* of P .

5.2.6 Remark: *A submodule need not be a summand or if it is, its supplement need not be unique.*

For instance, a non-zero proper subgroup (n) of $\mathbb{Z}$ is not a summand since a supplement (which is infinite cyclic) has to be isomorphic to the quotient group $\mathbb{Z}/(n)$ which is not possible. Secondly, for the vector space $\mathbb{R}^2$ over $\mathbb{R}$, given a line L through the origin, any other line through the origin is a supplement to L . In fact, every subspace of $\mathbb{R}^n$ is a summand. ■

5.3 Free Modules

5.3.1 Definition: Suppose M is an R -module and X a subset of M , then the *submodule generated* or *spanned* by X is defined as the smallest submodule of M containing X , or equivalently, it is the intersection of all the submodules N of M each containing X . Note that this intersection is over a non-empty family because M is a member of this family. It can be seen to be equal to $\{\sum_i^{\text{finite}} a_i x_i \mid a_i \in R, x_i \in X\}$ if R is with 1 and M is unitary. Otherwise, it is equal to $\{\sum_i^{\text{finite}} (n_i + a_i) x_i \mid a_i \in R, x_i \in X \text{ and } n_i \in \mathbb{Z}\}$.

5.3.2 Remarks: 1. The submodule generated by $\emptyset$ is (0) .

2. If $X = \{x\}$, then the submodule generated by x is $\{ax \mid a \in R\}$ if R is with 1 or $\{ax + nx \mid a \in R, n \in \mathbb{Z}\}$, otherwise. This is called the *cyclic* or *monogenic* submodule generated by x .

5.3.3 Finitely generated module: An R -module M is said to be *finitely generated* over R if there is a finite subset X of M such that M is the submodule generated by X , i.e., if $X = \{x_1, \dots, x_r\}$, then (assuming R has 1 and M is unitary) we have

$$M = \{\sum_{i=1}^r a_i x_i \mid a_i \in R\}.$$

5.3.4 Linear independence: Let M be an R -module. A subset B of M is said to be *linearly independent* over R if for any finite subset $\{b_1, b_2, \dots, b_r\} \subseteq B$, $\sum_{i=1}^r a_i b_i = 0$ with $a_i \in R$, then $a_i = 0, \forall i$.

5.3.5 Free module: An R -module M is called a *free module* if M has a *basis* B , i.e., a linearly independent subset B of M such that M is spanned by B over R , i.e., every element $x \in M$ can be written uniquely as $x = \sum_{b \in B} \lambda_b \cdot b$, $\lambda_b \in R$, $\lambda_b = 0$ except for finitely many b 's, i.e., x is finite linear combination of elements in B , the scalars being unique for x .

5.3.6 Examples: 1. For any ring R with 1, the left R -module ${}_R R$ is free with basis $\{1\}$ or $\{u\}$, u any unit in R .

In fact, an element $b \in {}_R R$ is linearly independent if and only if b is not a right zero-divisor in R , i.e., $ab = 0 \Rightarrow a = 0$. Furthermore, $\{b\}$ is an R -basis of ${}_R R$ if and only if b has a left inverse and is not a right zero-divisor.

2. $R^n = \underbrace{R \times \cdots \times R}_{n \text{ times}}$, 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 .

3. *Direct sum of free modules is a free module.*

For, suppose M and N are free R -modules with bases A and B respectively. Now $M \oplus N = M \times N$ is free R -module because $(A \times \{0\}) \cup (\{0\} \times B)$ is an R -basis for $M \times N$. More generally, for any family of free R -modules, $\{M_i \mid i \in I\}$, with basis A_i , $M = \oplus_{i \in I} M_i$ is a free module with a basis $A = \cup_{i \in I} A_i$.

5.3.7 Example of a non-free module.

Any finite abelian group is not free as a module over $\mathbb{Z}$. In fact, any abelian group M which has a non-trivial element of finite order cannot be free as a module over $\mathbb{Z}$. For, suppose M is free. Say B is a basis for M over $\mathbb{Z}$. Let $0 \neq x \in M$ be such that $nx = 0$ for some $n \in \mathbb{N}$, $mx \neq 0$ for $m < n$ and $n \geq 2$. Now we have $x = n_1 b_1 + n_2 b_2 + \cdots + n_r b_r$ for some $b_1, b_2, \dots, b_r \in B$ and $n_1, n_2, \dots, n_r \in \mathbb{Z}$. Hence $0 = nx = n[n_1 b_1 + n_2 b_2 + \cdots + n_r b_r] = nn_1 b_1 + nn_2 b_2 + \cdots + nn_r b_r \Rightarrow nn_1 = 0, nn_2 = 0, \dots, nn_r = 0$ (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. ■

5.4 Vector Spaces

So far, we have been referring to a “Vector Space” V to mean a unitary module over a field K . In proving most of the familiar properties of vector spaces, one does not really use the fact that the base field K is commutative, but what is essentially used is that V is unitary and K is a division ring. That is to say, a vector space may well be defined as a unitary module over a division ring D . But then we will have a left vector space or a right vector space V according as V is a left/right module over D . As per our convention, we shall be concerned with left vector spaces. For the sake of completeness we shall go through a few familiar properties of vector spaces in the general setup.

5.4.1 Vector space: A (left) unitary module over a division ring is called a (*left*) *vector space*.

5.4.2 Theorem: *A vector space is a free module.*

Proof: Let V be a non-zero vector space over a division ring D . Let $\mathcal{F}$ be the family of all linearly independent subsets of V , i.e.,

$$\mathcal{F} = \{A \subseteq V \mid A \text{ is linearly independent over } D\}.$$

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

Claim: *B is a basis for V .*

For, we have only to show that B spans V . If not, there exists $v \in V$ such that v is not a linear combination of any finite subset of B . Now $B' = B \cup \{v\}$ is linearly independent because $\alpha v + \sum_{i=1}^r \alpha_i b_i = 0$
 $\Rightarrow \alpha \neq 0$ (otherwise $\alpha = \alpha_1 = \dots = \alpha_r = 0$)
 $\Rightarrow v = -\alpha^{-1}[\alpha_1 b_1 + \dots + \alpha_r b_r] = -\alpha^{-1} \alpha_1 b_1 - \alpha^{-1} \alpha_2 b_2 \dots - \alpha^{-1} \alpha_r b_r$
 $\Rightarrow v \in \text{span}(B)$ which is a contradiction. Thus $B' \notin \mathcal{F}$ which contradicts the maximality of B . Hence B spans V over D . $\diamond$

5.4.3 Theorem: *Let V be a vector space over a division ring D , then we have the following.*

1. *Every linearly independent subset of V can be extended to a basis of V . In particular, every non-zero vector can be extended to a basis.*

2. Every subset which spans V contains a basis of V .
 3. Any two bases of V are either both finite or both infinite and their cardinalities are equal. This common value is called the dimension of V and is denoted by $\dim_D(V)$.

Proof: Proofs of (1) and (2) are similar to (5.4.2) above, with Zorn's lemma respectively applied to

1. $\mathcal{F}_A = \{B \subseteq V \mid B \text{ is linearly independent over } D \text{ and } A \subseteq B\}$, for any linearly independent subset A of V or
 2. $\mathcal{F}_X = \{A \subseteq X \mid A \text{ is linearly independent over } D\}$ for any subset X spanning V over D .

Maximal elements in these families give bases for V . In order to prove (3), we first prove the following.

5.4.4 Lemma: *A subset $S = \{v_1, v_2, \dots, v_n\}$ of non-zero elements of a vector space V over a division ring D is linearly dependent if and only if some v_k , $2 \leq k \leq n$, can be expressed as linear combination of its preceding vectors.*

Proof: Suppose that v_k can be expressed as a linear combination of the preceding ones, then the set of $\{v_1, v_2, \dots, v_k\}$ is linearly dependent. Conversely, let $\{v_1, v_2, \dots, v_n\}$ be linearly dependent, say, $\sum_{i=1}^k b_i v_i = 0$ with $k \geq 1$ and $b_k \neq 0$. Now $-v_k = \sum_{i=1}^{k-1} b_k^{-1} b_i v_i$, i.e., v_k is a linear combination of its preceding vectors v_i , $i \leq k-1$. $\diamond$

Now we proceed to prove (5.4.3) (3). Let $B_1 = \{v_1, v_2, \dots, v_m\}$ be finite basis for V . If B_2 is another basis, then B_2 is also finite because it is easy to see that $B_1 \subseteq \text{span}(\{w_1, w_2, \dots, w_n\})$ for some finite subset $\{w_1, w_2, \dots, w_n\}$ of B_2 and hence we get that $B_2 = \{w_1, w_2, \dots, w_n\}$. We have to prove that $m = n$.

Since w_1 can be written as a linear combination of $v_1, v_2, \dots, v_m$, the set $\{w_1, v_1, v_2, \dots, v_m\}$ is linearly dependent. Then by (5.4.4), we can find $v_k \neq w_1$ such that $v_k = bw_1 + \sum_{i=1}^{k-1} a_i v_i$ and the set $B_3 = \{w_1, v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_m\}$ spans V .

Now consider $w_2 \in B_2$. Since w_2 is a linear combination of elements of B_3 , the set $B_4 = \{w_2, w_1, v_1, v_2, \dots, \hat{v}_k, \dots, v_m\}$ spans V , where

$\hat{v}_k$ means v_k omitted. Proceeding as above, at each step we include a w from B_2 and exclude a v from B_1 . We notice that the set B_1 of v 's cannot be exhausted before the set B_2 of w 's is included; for otherwise, we get V as a linear span of a proper subset of B_2 which contradicts the fact that B_2 is a basis for V . Hence we get a basis of the form $\{w_n, w_{n-1}, \dots, w_2, w_1, v_{i_1}, v_{i_2}, \dots, v_{i_t}\}$, $0 \leq i_t \leq m$, i.e., $n \leq m$. Similarly, interchanging the roles of B_1 and B_2 , we get that $m \leq n$. Thus we have $n = m$, as required.

In general, when V has no finite basis, an argument using Zorn's lemma can be given to show that the cardinalities of any two bases are the same. The details are rather technical and hence omitted. ■

5.5 Some Pathologies

It is natural to ask the following question.

5.5.1 Question: *To what extent do Theorems (5.4.2) and (5.4.3) above, hold for*

1. modules over arbitrary rings,
2. free modules over arbitrary rings and
3. free modules over commutative rings?

By (5.3.7) above, Theorems (5.4.2) and (5.4.3) are not applicable for modules over arbitrary rings. Answers to the others are given in the Table 5.1 below and we now give examples in support thereof.

5.5.2 Example of a free module in which a linearly independent subset cannot be extended to a basis.

Take $R = \mathbb{Z} = M$. As a $\mathbb{Z}$ -module, $\mathbb{Z}$ is free with a basis $\{1\}$ or $\{-1\}$. (In fact, it has no other basis.) Now $\{2\}$ is linearly independent over $\mathbb{Z}$. We note that 2 cannot generate $\mathbb{Z}$ over $\mathbb{Z}$. If at all there is a basis B containing 2, B should have at least one more element, say b . We have $b \cdot 2 - 2 \cdot b = 0$, i.e., $\{2, b\}$ is linearly dependent subset of B which is absurd.

5.5.3 Example of a free module M for which a subset X spans M but X does not contain a basis.

Table 5.1: See (5.5.1) above.

VECTOR SPACES		FREE MODULES over	
		arb. rings	com. rings
1	Any linearly independent subset can be extended to a basis	Not true	Not true
2	Any spanning subset contains a basis	Not true	Not true
3	Any subspace of a vector space is again a vector space	Not true	Not true
4	Any subspace of a finitely generated vector space is again finitely generated	Not true	Not true
5	Any two bases have the same cardinality	Not true	True See (5.6.5)
NOTE: In case of free modules over PID's, the statements 3 and 4 are also true (besides 5), as shown in § 5.9 below.			

Again take $R = \mathbb{Z} = M$ and $X = \{m, n\}$ with m and n non-units and $(m, n) = 1$. For instance, $X = \{2, 3\}$. We have $1 = am + bn$ for some $a, b \in \mathbb{Z}$. Therefore, $x = xam + xbn$, $\forall x \in \mathbb{Z}$, i.e., $\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$. We know that X is linearly dependent hence X is not a basis for $\mathbb{Z}$. It is clear that $m\mathbb{Z} \neq \mathbb{Z}$ and $n\mathbb{Z} \neq \mathbb{Z}$ which means X does not contain any basis for $\mathbb{Z}$.

5.5.4 Example of a finitely generated free module M having a submodule which is neither free nor finitely generated.

Let K be a field and $R = K[X_1, X_2, \dots, X_n, \dots]$. This is a commutative ring. Now $M = R$ is a free module with basis $\{1\}$. Submodules of M are ideals of R . Now let N be the ideal of all polynomials with constant term zero, i.e., N is generated by $(X_1, X_2, \dots, X_n, \dots)$.

Claim: N is not finitely generated.

For, suppose N is finitely generated as an ideal in R , say generated by $\{f_1, f_2, \dots, f_r\}$. It is clear that there exists a positive integer $n \gg 0$ such that $f_i \in K[X_1, X_2, \dots, X_n]$ which is a subring of R . Since $X_i \in N$, for all i , we can write $X_{n+1} = \sum_{i=1}^r a_i f_i$ for some $a_i \in R$. Since the f_i 's are all without constant term, specialising

$X_1 = X_2 = \dots = X_n = 0$, we get that

$$\begin{aligned} X_{n+1} &= \sum_{i=1}^r a_i(0, 0, \dots, 0, X_{n+1}, \dots) f_i(0, 0, \dots, 0) \\ &= \sum_{i=1}^r a_i(0, 0, \dots, 0, X_{n+1}, \dots) \cdot 0 = 0 \end{aligned}$$

which is absurd. Since N is not finitely generated, it cannot be obviously a principal ideal and hence it is not free because the only ideals of R which are free as R -modules are non-zero principal ideals.

5.5.5 Example of a free module M which has bases having different cardinalities.

Let V be a vector space of *countably infinite dimension* over a division ring D . Let $R = \text{End}_D(V)$. We know that R is free over R with basis $\{1\}$. We shall prove that given a positive integer n , there is an R -basis $B_n = \{f_1, \dots, f_n\}$ for R having n elements.

Let $B = \{e_k\}_{k=1}^\infty$ be a basis of V over D . Define $f_1, \dots, f_n \in R$ by specifying their values on B as in the Table 5.2 below.

Table 5.2: See (5.5.5) above.

	f_1	f_2	f_3	$\cdots$	f_n
e_1	e_1	0	0	$\cdots$	0
e_2	0	e_1	0	$\cdots$	0
$\vdots$				$\ddots$	
e_n	0	0	0		e_1
e_{n+1}	e_2	0	0		0
e_{n+2}	0	e_2	0	$\cdots$	0
$\vdots$				$\ddots$	
e_{2n}	0	0	0		e_2
e_{kn+1}	e_{k+1}	0	0	$\cdots$	0
e_{kn+2}	0	e_{k+1}	0	$\cdots$	0
$\vdots$				$\ddots$	
$e_{(k+1)n}$	0	0	0	$\cdots$	e_{k+1}
		$\vdots$	$\vdots$	$\vdots$	$\vdots$

It is a simple matter to check that B_n is an R -basis of R . In fact, if $\sum_{i=1}^n \alpha_i f_i = 0$ with $\alpha_i \in R$, then evaluating on the successive blocks of n vectors, namely, $e_{kn+1}, \dots, e_{(k+1)n}$, $k = 0, 1, \dots$, we get $\alpha_i(e_{k+1}) = 0$ for all k and $1 \leq i \leq n$; i.e., $\alpha_i \equiv 0$ for all i showing that B_n is linearly independent over R . Secondly, if $f \in R$, then $f = \sum_{i=1}^n \alpha_i f_i$, where $\alpha_i \in R$ are defined by their values on B as in the Table 5.3 below. Thus B_n is an R -basis for R , as required. We note that $B_1 = \{1_R\}$, which is the standard basis.

5.5.6 Remark: The vector space V , considered as an R -module under *evaluation as scalar multiplication*, has no non-trivial submodules because given $v \in V$, $v \neq 0$ and $w \in V$, there exists an $f \in R$ such that $w = f(v)$. Furthermore, we have an isomorphism of R -modules

$$R \xrightarrow{\sim} \prod_{b \in B} V_b, \quad f \mapsto (f(b))_{b \in B}, \quad V_b = V, \quad \forall b \in B$$

where B is a basis of V over D . This isomorphism depends on the choice of the basis B . ■

Table 5.3: See (5.5.5) above.

	α_1	α_2	α_3	α_n	
e_1	$f(e_1)$	$f(e_2)$	$f(e_3)$	$\cdots$	$f(e_n)$
e_2	$f(e_{n+1})$	$f(e_{n+2})$	$f(e_{n+3})$	$\cdots$	$f(e_{2n})$
$\vdots$				$\ddots$	
e_n	$f(e_{(n-1)n+1})$	$f(e_{(n-1)n+2})$	$f(e_{(n-1)n+3})$	$\cdots$	$f(e_{n^2})$
e_{n+1}	$f(e_{n^2+1})$	$f(e_{n^2+2})$	$f(e_{n^2+3})$	$\cdots$	$f(e_{n^2+n})$
e_{n+2}	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
$\vdots$				$\ddots$	
e_{2n}	$f(e_{2n^2-n+1})$	$f(e_{2n^2-n+2})$	$f(e_{2n^2-n+3})$	$\cdots$	$f(e_{2n^2})$
$\vdots$			$\vdots$	$\vdots$	$\vdots$
e_{kn+1}	$f(e_{kn^2+1})$	$f(e_{kn^2+2})$	$f(e_{kn^2+3})$	$\cdots$	$f(e_{kn^2+n})$
e_{kn+2}	$\cdot$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
$\vdots$				$\ddots$	
$e_{(k+1)n}$			$\cdot$	$\cdots$	$f(e_{(k+1)n^2})$
		$\vdots$	$\vdots$	$\vdots$	$\vdots$

5.6 Quotient Modules

5.6.1 Definition: Given a submodule N of an R -module M , the *quotient group* M/N has a natural structure of an R -module, namely, $R \times (M/N) \rightarrow M/N$, $(a, x + N) \mapsto ax + N$, $\forall a \in R$ 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 R -module, called the *quotient* of M modulo N .

5.6.2 Proposition: Suppose N is a submodule of an R -module M . Then the set of submodules of M/N is naturally bijective with the set of all submodules of M containing N .

Proof: Let $P_0 = \{x \in M \mid x + N \in P\}$ for a submodule P of M/N . Since $x + N = N \in P$, $\forall x \in N$, we have $N \subseteq P_0$.

Claim: P_0 is a submodule of M .

For, let $u, v \in P_0$. Since P is a submodule, we have $(u + N) - (v + N) = (u - v) + N \in P \Rightarrow u - v \in P_0$. Now let $x \in P_0$, i.e., $x + N \in P$. Let $a \in R$. Since P is a submodule of M/N , we have $a(x + N) = ax + N \in P \Rightarrow ax \in P_0$. Hence P_0 is a submodule of M .

It is easy to see that $P \subseteq P'$ in $M/N \iff P_0 \subseteq P'_0$ in M . Hence $P \neq P'$ in $M/N \iff P_0 \neq P'_0$ in M . Finally, if K is a submodule in M containing N , then $\widetilde{K} = \{x + N \mid x \in K\}$ is a submodule of M/N and furthermore, we have

$$(\widetilde{K})_0 = \{x \in M \mid x + N \in \widetilde{K}\} = \{x \in M \mid x \in K\} = K,$$

as required. $\diamond$

5.6.3 Remark: Let R be any ring and let I be any left ideal of R . Considering R as a left R -module, we know that I is then an R -submodule of R . Hence we can talk about the quotient module R/I . We note that R/I is not a ring unless I is a 2-sided ideal of R .

5.6.4 Remark: Let M be an R -module and I be a 2-sided ideal contained in $\{a \in R \mid ax = 0, \forall x \in M\}$, the *annihilator* of M . Then M can be naturally considered as an R/I -module and the two module structures on M (over R and R/I) coincide, i.e., any R -submodule of

M is also an R/I -submodule and vice-versa.

The R/I -module structure on M is given by the map

$$(R/I) \times M \longrightarrow M, (a + I, x) \longmapsto ax$$

(which is well-defined since I annihilates M and hence) gives a scalar multiplication on M . The other assertions are obvious since the scalar multiplications on M over R and R/I are the same.

5.6.5 Theorem: *The cardinalities of any two bases of a free module F over a commutative ring R with 1 are equal and the common value is called the dimension or the rank of F and is denoted by $\dim_R(F)$ or $\text{rank}_R(F)$.*

Proof: Let R be a commutative ring with unity and F a free R -module with a basis B . Choose a maximal ideal M of R and let $K = R/M$ which is a field. Let MF be the submodule of F generated by elements of the form ax with $a \in M$ and $x \in F$. Let $V = F/MF$ which is an R -module and also a K -module since M annihilates V , i.e., V is a vector space over K . It is easy to check that $\widetilde{B} = \{x + MF \mid x \in B\}$ is a K -basis of V and the cardinalities of B and $\widetilde{B}$ are equal. Thus if B_1 and B_2 are two bases of F over R , then $\widetilde{B}_1$ and $\widetilde{B}_2$ are two bases of the vector space V over K and hence their cardinalities are the same, as required. ■

5.7 Homomorphisms

5.7.1 Homomorphism: Given R -modules M and N , by an R -linear homomorphism $f : M \rightarrow N$, we mean a map which is additive and commutes with scalar multiplication, i.e.,

$$f(x + y) = f(x) + f(y) \text{ and } f(ax) = af(x), \quad \forall x, y \in M \text{ and } a \in R.$$

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

5.7.3 Definitions: A homomorphism $f : M \rightarrow N$ of R -modules M and N is called

- a *monomorphism* if f is injective,

- an *epimorphism* if f is surjective,
- an *isomorphism* if f is bijective,
- an *endomorphism* if $M = N$ and
- an *automorphism* if $M = N$ and f is an isomorphism.

Notation: For R -modules M and N , we write

- $\text{Hom}_R(M, N) = \{f : M \rightarrow N \mid f, R\text{-linear}\},$
- $\text{End}_R(M) = \text{Hom}_R(M, M)$ and

• If M is isomorphic to N by means of an isomorphism $\varphi : M \rightarrow N$, then we write $M \xrightarrow{\varphi} N$ or $M \xrightarrow{\sim} N$ or $M \xrightarrow{\cong} N$ or simply $M \approx N$.

5.7.4 Abelian group structure on $\text{Hom}_R(M, N)$: Let $f, g : M \rightarrow N$ be R -linear homomorphisms. Then define

$$f + g : M \longrightarrow N, \quad x \longmapsto f(x) + g(x)$$

which can be seen to be R -linear. Under this addition, $\text{Hom}_R(M, N)$ is an abelian group.

5.7.5 Remark: The abelian group $\text{Hom}_R(M, N)$ has a natural structure of an R -module if R is commutative under the scalar multiplication given by

$$R \times \text{Hom}_R(M, N) \longrightarrow \text{Hom}_R(M, N), \quad (a, f) \longmapsto af$$

where af is defined by

$$af : M \longrightarrow N, \quad x \longmapsto (af)(x) = a f(x), \quad \forall x \in M.$$

If R is not commutative, we note that in general “ af ” is additive but not necessarily R -linear.

5.7.6 Proposition: Suppose R is a commutative ring with 1 and M and N are unitary free R -modules. Then $P = \text{Hom}_R(M, N)$ is a free R -module if M is finitely generated.

Proof: We know that P is an R -module by (5.7.5) above. We have to show that it has a basis. If $A = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ is a basis of M , then it is easy to see that the map (depending on A), namely,

$$\text{Hom}_R(M, N) = P \longrightarrow N^n, \quad f \longmapsto (f(\alpha_1), \dots, f(\alpha_n))$$

is an isomorphism. But N^n is free with a basis B^n where B is a basis of N (by (5.3.6)(3) above).

In case N also has a finite basis, say $B = \{\beta_1, \beta_2, \dots, \beta_m\}$, then a basis of P is given as follows. Define $f_{\mu k} : M \rightarrow N$ by

$$f_{\ell k}(\alpha_i) = \begin{cases} 0 & \text{if } i \neq k, \ 1 \leq i, k \leq n, \\ \beta_\ell & \text{if } i = k, \ 1 \leq \ell \leq m. \end{cases}$$

Claim 1: $f_{\ell k}$'s span P .

For, let $f \in P$ and let $f(\alpha_i) = \sum_{\ell=1}^m a_{\ell i} \beta_\ell$ for some $a_{\ell i}$'s in R . Now consider $\sum_{\ell=1}^m \sum_{k=1}^n a_{\ell k} f_{\ell k} \in \text{Hom}_R(M, N)$. We have

$$\begin{aligned} \sum_{\ell=1}^m \sum_{k=1}^n a_{\ell k} f_{\ell k}(\alpha_i) &= \sum_{\ell=1}^m a_{\ell 1} f_{\ell 1}(\alpha_i) + a_{\ell 2} f_{\ell 2}(\alpha_i) + \cdots + a_{\ell m} f_{\ell m}(\alpha_i) \\ &= \sum_{\ell=1}^m a_{\ell i} f_{\ell i}(\alpha_i) = f(\alpha_i). \end{aligned}$$

This shows that $f = \sum_{\ell=1}^m \sum_{k=1}^n a_{\ell k} f_{\ell k}$. Hence $f_{\ell k}$'s span P .

Claim 2: $f_{\ell k}$'s are linearly independent.

For, let $b_{\ell k} \in R$ be such that $\sum_{\ell=1}^m \sum_{k=1}^n b_{\ell k} f_{\ell k} = 0$. Then

$$\begin{aligned} \sum_{\ell=1}^m \sum_{k=1}^n b_{\ell k} f_{\ell k}(\alpha_i) &= 0, \ \forall \alpha_i \in A, \text{ i.e.,} \\ \sum_{\ell=1}^m b_{\ell 1} f_{\ell 1}(\alpha_i) + \sum_{\ell=1}^m b_{\ell 2} f_{\ell 2}(\alpha_i) + \cdots + \sum_{\ell=1}^m b_{\ell n} f_{\ell n}(\alpha_i) &= 0 \\ \Rightarrow \sum_{\ell=1}^m b_{\ell i} f_{\ell i}(\alpha_i) &= 0, \text{ i.e., } \sum_{\ell=1}^m b_{\ell i} \beta_\ell = 0 \Rightarrow b_{\ell i} = 0, \ \forall \ell \end{aligned}$$

(since $\{\beta_1, \dots, \beta_m\}$ is a basis for N). Thus P is a free module. $\diamond$

The proofs of the following theorems are identical with the corresponding ones in Rings. So we omit the details. The reader is urged to go through the details, replacing rings by modules and 2-sided ideals by submodules in § 3.2 above.

5.7.7 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 η is the natural map given by $\eta : M \rightarrow M/P, x \mapsto x + P$, i.e., the following diagram is commutative.

$$\begin{array}{ccc}
 M & \xrightarrow{f} & N \\
 \eta \searrow & & \nearrow \widetilde{f} \\
 & M/P &
 \end{array}$$

5.7.8 Theorem (Quotient of a quotient): Suppose $P \subseteq N \subseteq M$ are R -submodules of an R -module M . Then there exists a natural isomorphism $\widetilde{\eta} : (M/P)/(N/P) \xrightarrow{\sim} M/N$ making the following diagram commutative.

$$\begin{array}{ccc}
 & M & \\
 \eta_P \swarrow & & \searrow \eta_N \\
 M/P & \xrightarrow{\eta_{PN}} & M/N \\
 \eta_{N/P} \searrow & & \nearrow \widetilde{\eta} = \widetilde{\eta}_{PN} \\
 & (M/P)/(N/P) &
 \end{array}$$

where $\eta_{PN} : x + P \mapsto x + N, \forall x \in M$. ◇

5.7.9 Theorem (Quotient of a sum): Suppose P, N are submodules of a module M . Then there exist natural isomorphisms

$$(1) \quad \frac{P + N}{P} \approx \frac{N}{N \cap P} \quad \text{and} \quad (2) \quad \frac{P + N}{N} \approx \frac{P}{P \cap N}.$$

Proof: This has no parallel in rings and so we give details. We shall prove (1) and the other is similar. Define $g : P + N \rightarrow N/(N \cap P)$ as $g(x + y) = y + (N \cap P)$ for all $x \in P$ and $y \in N$. This g is well-defined because if $x_1 + y_1 = x_2 + y_2$ for some $x_1, x_2 \in P$ and $y_1, y_2 \in N$, then $x_1 - x_2 = y_2 - y_1$. But P and N being submodules, $x_1 - x_2 \in P$ and $y_2 - y_1 \in N$. Hence $y_2 - y_1 \in P \cap N$. Thus $y_1 + (N \cap P) = y_2 + (N \cap P)$, i.e., $g(x_1 + y_1) = g(x_2 + y_2)$, as required. It is easy to check that g is an epimorphism and $\text{Ker}(g) = N/(N \cap P)$ and hence by the epimorphism theorem, $(P + N)/P$ is isomorphic to $N/(N \cap P)$. ◇

5.7.10 Remark: Suppose P and N are submodules of M , then the natural map $\eta_{PN} : M/P \rightarrow M/N, x + P \mapsto x + N$, is well defined $\iff P \subseteq N$. (This is required in the proof of (5.7.8) above.)

5.7.11 Proposition: Any unitary module over a ring with unity is a quotient of a free module.

Proof: Let M be an R -module. Take a set of generators X for M . For example, $X = M$. Now consider the free module F with basis X , i.e., $F = \bigoplus_{x \in X} R_x$ with $R_x = R$, $\forall x \in X$. We have $F = \{\sum_{x \in X} a_x e_x \mid a_x \in R, a_x = 0 \text{ for almost all } x \text{ and } e_x = 1, \forall x\}$. Now consider the map $f: F \rightarrow M$, $f(\sum_{x \in X} a_x e_x) \mapsto \sum_{x \in X} a_x x$. This is an R -linear epimorphism since M is generated by X and hence by the epimorphism theorem, we get that $F/\text{Ker}(f) \approx M$. $\diamond$

5.7.12 Corollary: If an R -module M is generated by n elements, then M can be realised as a quotient of R^n .

For, following the proof of (5.7.11), we note that, if M is generated by n elements, then the free module in question is $F = R^n$. $\diamond$

5.7.13 Homothecy: Let M be an R -module and $a \in R$. Then the map $\lambda_a: M \rightarrow M$ given by $x \mapsto ax$ is called the *homothecy* defined by a . (Note that λ_a is additive but not necessarily R -linear if R is not commutative.)

5.7.14 Remark: The set of homothecies $\{\lambda_a \mid a \in R\}$ is a subring of $\text{End}_{\mathbb{Z}}(M)$. In fact, it is the image of the ring homomorphism $\Psi: R \rightarrow \text{End}_{\mathbb{Z}}(M)$ defining the module structure on M . $\blacksquare$

5.8 Simple Modules

5.8.1 Maximal submodule: 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 a submodule of $M \Rightarrow P = N$ or $P = M$,
i.e., the only submodules of M containing N are N and M .

5.8.2 Minimal submodule: A submodule N of a module M is called a *minimal submodule* if

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

5.8.3 Simple module: A module M is called a *simple module* if

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

5.8.4 Remarks: 1. Any minimal submodule is simple.

2. A submodule N of M is maximal in $M \iff M/N$ is simple.

5.8.5 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., $f(x_0) \neq 0$ 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., $f \equiv 0$ or f is onto. But $f \neq 0$ 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. $\diamond$

5.8.6 Remark: We note the *difference* between the two notions, namely, a ring R as a simple left R -module and R as a simple ring.

By definition, ${}_R R$ is simple $\iff R$ has no non-trivial left ideals and hence by (2.4.9) above, R is a division ring. On the other hand, R is a simple ring means that it has no non-trivial 2-sided ideals, but may have non-trivial left/right ideals. For example, $R = M_n(D)$, D a division ring, is a simple ring but not a simple R -module if $n \geq 2$.

5.8.7 Proposition: An R -module M is simple if and only if $M \approx R/I$ for some maximal left ideal I 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 the only R -submodules of R/I are (0) and R/I (by (5.8.4) above). Hence R/I is simple, i.e., M is simple.

Conversely, let M be a simple R -module ($\Rightarrow M \neq (0)$). Take any

$x_0 \in M$, $x_0 \neq 0$. Now 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. Look at the map $f: R \rightarrow M$, $a \mapsto ax_0$ which is R -linear and surjective. Hence by (5.7.7) above, we get that $R/\text{Ker}(f) \approx M$, i.e., $\text{Ker}(f)$ is a maximal left ideal, as required. $\diamond$

5.8.8 Corollary: *The annihilator of any non-zero element of a simple module is a maximal left ideal and vice-versa.*

For, if M is simple, $0 \neq x_0 \in M$ and $f: R \rightarrow M$, $a \mapsto ax_0$, 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 $\mathfrak{m}$ is a maximal left ideal of R , then $\mathfrak{m}$ is the annihilator of the non-zero element $x_0 = 1 + \mathfrak{m}$ of the simple module $R/\mathfrak{m}$, as required. $\diamond$

5.8.9 Corollary: *Intersection of the annihilators of all elements of a simple module M is a 2-sided ideal of R because $\text{Ann}_R(M)$ is 2-sided and $\text{Ann}_R(M) = \bigcap_{x \in M} \text{Ann}_R(x) = \bigcap_{0 \neq x \in M} \text{Ann}_R(x)$.* ■

5.9 Modules over PID's

In this section, we shall establish some elementary and standard facts about modules over principal ideal domains. These are natural generalisations of well-known properties of abelian groups. But abelian groups are modules over $\mathbb{Z}$ which is a PID. The proofs in the general setup are, in fact, natural extensions of their forerunners over $\mathbb{Z}$. In what follows R denotes a PID with 1 and all R -modules considered are assumed to be unitary.

5.9.1 Theorem: *Let F be a free module over R and M be a submodule of F . Then M is also free and $\dim_R M \leq \dim_R F$. (See (5.9.13) below, for a stronger version of this result.)*

Proof: To appreciate the proof better, we shall assume that F has finite dimension. (The general case involves some transfinite induction which is rather technical.) Let $B = \{x_1, \dots, x_n\}$ be a basis of F . We have to prove that a submodule M of F is free and has a basis having at most n elements.

Let $M_r = M \cap \text{Span}(x_1, \dots, x_r)$, $1 \leq r \leq n$. We have $M_n = M$. We proceed by induction on r . If $r = 1$, we have $M_1 = \{x \in M \mid x = ax_1 \text{ for some } a \in R\}$. Let $I = \{a \in R \mid ax_1 \in M_1\}$. It is clear that I is an ideal in R and so $I = (a_1)$ for some $a_1 \in I$. But then $M_1 = (a_1x_1)$ and $M_1 = (0) \iff a_1 = 0$ and obviously M_1 is free with a basis $\emptyset$ or $\{a_1x_1\}$ according as M_1 is (0) or not.

Assume that for each $r \leq n-1$, M_r is free with basis B_r such that cardinality of $B_r \leq r$. Let

$$J = \{a \in R \mid ax_{r+1} + \sum_{i=1}^r a_i x_i \in M_{r+1} \text{ for some } a_i \in R\}$$

which is an ideal in R and so $J = (a_{r+1})$ for some $a_{r+1} \in J$. It follows that $a_{r+1} = 0 \iff M_r = M_{r+1}$. Hence, if $a_{r+1} = 0$, we are through by induction. Suppose $a_{r+1} \neq 0$. Let $x_0 \in M_{r+1}$ be such that $x_0 = a_{r+1}x_{r+1} + \sum_{i=1}^r a_i x_i$ for some $a_i \in R$. Now for any $y \in M_{r+1}$, we have $y = \sum_{i=1}^{r+1} b_i x_i$ for some $b_i \in R$. But then $b_{r+1} \in J$ and so $b_{r+1} = aa_{r+1}$ for some $a \in R$. This gives that $ax_0 - y = \sum_{i=1}^r (a a_i - b_i) x_i \in M_r$, i.e., $y \in M_r + Rx_0$ and hence $M_{r+1} = M_r + Rx_0$. On the other hand, we see easily that $M_r \cap Rx_0 = (0)$. Thus $M_{r+1} = M_r \oplus Rx_0$ which shows that $B_{r+1} = B_r \cup \{x_0\}$ is a basis for M_{r+1} , as required. $\diamond$

5.9.2 Corollary: *A submodule of a finitely generated module over a PID is finitely generated.*

Proof: Let M be generated by n elements. We shall show that any submodule N of M is generated by n or fewer elements. By (5.7.11) above, we know that M is a quotient of the free module R^n , say, $M \approx R^n/P$ for some submodule P of R^n . But then N gives rise to a submodule $Q \supseteq P$ of R^n such that $N \approx Q/P$. Since Q is free of dimension $m \leq n$, we have $Q \approx R^m$ and so $N \approx R^m/P$. It is clear that N is generated by the residues mod P of a basis of R^m . $\diamond$

5.9.3 Torsion module: A module is said to be a *torsion module* if every element is a torsion element.

5.9.4 Torsion free module: 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.)

5.9.5 Torsion part of a module: 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 is denoted by M_t . (It is the largest torsion submodule of M and saying that M is torsion free is the same as saying that its torsion part M_t is (0) .)

5.9.6 Proposition: *For any module M over a commutative integral domain, the quotient M/M_t is torsion free.*

Proof: Let $\bar{x} = x + M_t$ ($x \in M$) be a torsion element of M/M_t , i.e., $a\bar{x} = 0$ for some $a \neq 0$, i.e., $ax \in M_t$ and so $b(ax) = 0$ for some $b \in R$, $b \neq 0$. But then $ba \neq 0$ and so x is a torsion element of M , i.e., $x \in M_t$, as required. $\diamond$

5.9.7 Example of a torsion free module which is not free.

Take $R = \mathbb{Z}$ and $M = (\mathbb{Q}, +)$ which is obviously torsion free, i.e., has no elements of finite additive order except 0. But $(\mathbb{Q}, +)$ is not free because any two elements of $(\mathbb{Q}, +)$ are linearly dependent over $\mathbb{Z}$ and $(\mathbb{Q}, +)$ is not cyclic itself. (The following theorem shows that the source of trouble is that $(\mathbb{Q}, +)$ is not finitely generated over $\mathbb{Z}$.)

5.9.8 Theorem: *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

$$(*) \quad a_i x_i + \sum_{j=1}^m a_{ij} x_j = 0.$$

Since B is linearly independent, it is clear that $a_i \neq 0$, $\forall i$. Let $a = a_1 a_2 \cdots a_n$ so that $a \neq 0$. From $(*)$, $a_i x_i \in F$ and so $ax_i \in F$, $\forall i$, i.e., $aM \subseteq F$. Now the map $f: M \rightarrow F$, $x \mapsto ax$, 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 by (5.9.1) above, i.e., M is free, as required. $\diamond$

5.9.9 Theorem: *A finitely generated module M over a PID is a direct sum of its torsion part M_t and a free submodule M_f .*

Proof: Let $\widehat{B} = \{x_i + M_t \mid x_i \in M, 1 \leq i \leq n\}$ be a basis of the free module M/M_t (of finite dimension). Let $B = \{x_1, \dots, x_n\}$. It is obvious that B is linearly independent. Let $M_f = \text{span } B$ which is a free submodule of M . Since M_t is a torsion module, we have $M_f \cap M_t = (0)$. Hence $M_f + M_t = M_f \oplus M_t$.

Claim: $M = M_f \oplus M_t$.

For, it suffices to show that $M = M_f + M_t$. Let $\eta : M \rightarrow M/M_t$ be the natural map. For $x \in M$, write $\eta(x) = \sum_{i=1}^n a_i (x_i + M_t)$ for unique $a_i \in R$. Now we have

$$\eta(x - \sum_{i=1}^n a_i x_i) = 0 \Rightarrow y = x - \sum_{i=1}^n a_i x_i \in M_t = \text{Ker}(\eta), \text{ i.e.,}$$

$$x = (\sum_{i=1}^n a_i x_i) + y \in M_f + M_t, \text{ as required.} \quad \diamond$$

5.9.10 Remarks: Suppose that M is a finitely generated module over a PID and M_t is its torsion part. Then we have the following.

1. If $n = \dim_R(M/M_t)$, then any $n + 1$ elements in M are linearly dependent (because their residues mod M_t are linearly dependent and M_t is torsion).
2. While the torsion part M_t of M is unique, its supplement M_f is not unique since different bases for M/M_t give rise to different supplements for M_t . However,
3. M_f is unique upto isomorphism (being isomorphic to M/M_t) and is called a *free part* of M .
4. The uniquely determined integer $n = \dim_R(M/M_t)$ is called the *rank* of M is denoted by $\text{rank}_R(M)$.
5. Torsion modules are nothing but modules of rank 0.
6. Finitely generated torsion modules over $\mathbb{Z}$ are nothing but finite abelian groups.

Information about finitely generated modules over PID's would be complete provided we know the nature of the finitely generated torsion modules, i.e., the structure of finitely generated torsion modules. This goes exactly parallel to the structure of finite abelian groups and the proofs are also natural extensions. However, we shall *merely state the results without proofs* for the simple reasons that we do not use these results in the rest of these notes and secondly, the proofs in essence depend on more of group-theoretic considerations than that of rings. Proofs can be found in books like, "ALGEBRA" by S. Lang, 2 ed.,

Addison-Wesley Publishing Co., Inc., California (1984).

5.9.11 Theorem: *A finitely generated non-zero torsion module M over a PID is a direct product of cyclic modules. To be precise, there exists a finite set of primes $\mathcal{P}_M$ in R , (unique upto associates), with*

1. $M = \prod_{p \in \mathcal{P}_M} M_p$ where
2. $\forall p \in \mathcal{P}_M, \exists$ unique integers $1 \leq n_1 \leq \dots \leq n_r$ such that $M_p = \prod_{i=1}^{n_r} R/(p^{n_i})$.

◇

A slight rearrangement of the cyclic factors $R/(p^{n_i})$ in this decomposition leads to the following.

5.9.12 Theorem: *If M is as above, then there exist non-zero elements $q_1, \dots, q_m$ of R , unique (upto associates), called the invariants of M , such that*

1. $M = \prod_{i=1}^m R/(q_i)$ and
2. $q_1 \mid q_2 \mid \dots \mid q_{m-1} \mid q_m$.

◇

The following is also another formulation of the above.

5.9.13 Theorem (Elementary Divisors): *If F is a free module of dimension n and M a submodule of F , there exists a basis $B_F = \{x_1, \dots, x_n\}$ of F and non-zero elements $a_1, \dots, a_r$, ($r \leq n$), (unique upto associates) in R , called the invariants or elementary divisors of M in F , such that*

1. $B_M = \{a_1 x_1, \dots, a_r x_r\}$ is a basis of M and
2. $a_1 \mid a_2 \mid \dots \mid a_r$.

◇

5.9.14 Remark: The submodules M_p above, correspond to the Sylow subgroups in the case of finite abelian groups. ■

5.10 Exercises

In this section, a ring means a ring with 1, commutative or not. A module means a unitary left module (over a base ring which may or may not be explicitly mentioned).

1. Give an example of a homomorphism $f: M \rightarrow N$ of R -modules M and N and a scalar $a \in R$ such that af , defined by $x \mapsto af(x)$, is not R -linear.
2. Do Exs.(3.6.2) and (3.6.4) above, for submodules and homomorphisms of modules.
3. Show that the annihilator of an element of a module is a left ideal but not necessarily 2-sided. However, show that the annihilator of a module is a 2-sided ideal.
4. Show that the annihilator ideals of isomorphic modules are equal (not just isomorphic) but modules whose annihilators are equal need not be isomorphic.
5. Let R be a ring and $S = R \times R$. Show that both $R \times \{0\}$ and $\{0\} \times R$ are 2-sided ideals of S but are not isomorphic as S -modules.
6. Give an example of a module M and a submodule N which is not a direct summand.
7. Show that a direct summand of a direct summand is a direct summand.
8. Let M be an R -module and $p \in \text{End}_R(M)$ be a *projection*, i.e., an idempotent ($p^2 = p$). Show that
 - $p(x) = x$ for all $x \in p(M)$,
 - $M = \text{Ker}(p) \oplus p(M)$,
 - $q = 1 - p$ is also a projection (where $1 = \text{Id}_M$),
 - p and q are orthogonal projections, i.e., $p \circ q = 0 = q \circ p$ and
 - $\text{Ker}(p) = q(M)$ and $\text{Ker}(q) = p(M)$.
9. Show that a submodule P of an R -module M is a direct summand of M if and only if there is a projection p of M onto P , i.e., $p(M) = P$.
10. Let $M_i, 1 \leq i \leq n$, be submodules of a module M . Show that $M = \bigoplus_{i=1}^n M_i$ if and only if there exist projections p_i of M onto M_i , mutually pairwise orthogonal and form a *partition of unity*, i.e., $\text{Id}_M = 1 = \sum_{i=1}^n p_i$.

11. Show that a left ideal I of a ring R is a direct summand in R if and only if I is generated by an idempotent. Deduce that a non-zero ideal in a local ring is not a direct summand.
12. Show that a finitely generated left ideal I of ring R is a direct summand in R if $I^2 = I$.
13. Let e be a non-trivial idempotent in a ring R . Show that the principal left ideal $(e)_\ell$ is minimal (resp. maximal) if and only if the principal right ideal $(e)_r$ is so. (Hint: Use the anti-isomorphism (5.1.6) $\text{Id}: R \rightarrow R^0$ where R^0 is the ring opposite to R (1.11.1).)
14. Let e and f be two orthogonal idempotents in a ring R . Show that the principal left (resp. right) ideal generated by $e + f$ is the direct sum of the principal left (resp. right) ideals generated by e and f . (Use Ex.(2.9.4) above.)
15. Let R be a ring such that it is a direct sum of a family $\{I_\lambda \mid \lambda \in \Lambda\}$ of distinct left ideals. Show that
 - Λ is finite, (say) $\Lambda = \{\lambda_1, \dots, \lambda_n\}$,
 - I_{λ_j} is generated by an idempotent e_j , $1 \leq j \leq n$ and
 - $\{e_j \mid 1 \leq j \leq n\}$ is a set of pairwise orthogonal idempotents forming a partition of unity.

Conversely, show that any set of pairwise orthogonal idempotents giving a partition of unity decomposes R into a direct sum of suitable left (resp. right) ideals.
16. Decompose the matrix ring $M_n(R)$ into a direct sum of n left (resp. right) ideals for any ring R (with 1). Describe the corresponding set of orthogonal idempotents.
17. Let N be a minimal submodule of a module M . For any submodule P of M , show that $N \subseteq P$ or $N + P = N \oplus P$. Hence or otherwise, deduce that a sum $\sum_{i=1}^n N_i$ of finitely many *minimal* submodules N_i is a *direct sum* of a subset of them, i.e., $\exists r \geq 1$ and $1 \leq i_1 < \dots < i_r \leq n$ such that $\sum_{i=1}^n N_i = \oplus_{j=1}^r N_{i_j}$. Generalise this to a family of minimal submodules as follows.
18. Let M be a module which is a sum of a family $\{N_\lambda \mid \lambda \in \Lambda\}$ of distinct *minimal* submodules N_λ . Then show that M is a *direct sum* of a subfamily $\{N_\lambda \mid \lambda \in \Omega\}$ for some $\Omega \subseteq \Lambda$. Furthermore, give an

example for which Λ is infinite but Ω is finite. (Hint: Apply Zorn's lemma to

$$\mathcal{F} = \{\Gamma \subseteq \Lambda \mid \sum_{\gamma \in \Gamma} N_\gamma = \bigoplus_{\gamma \in \Gamma} N_\gamma\},$$

partially ordered under set inclusion.)

19. A module is said to be *semi-simple* if it is a direct sum of a family of minimal submodules. Show that every submodule N of a semi-simple module M is a direct summand of M . (Hint: Apply Zorn's lemma to the set of submodules P of M , namely, $\mathcal{F}_N = \{P \subseteq M \mid N + P = N \oplus P\}$, partially ordered under set inclusion.)
20. Show that a supplement of a minimal submodule of a semi-simple module is maximal and vice-versa.
21. A ring is said to be *left semi-simple* if it is semi-simple as a left module over itself. Show that a ring is left semi-simple if and only if it is right semi-simple. (Hint: Use Exs.11 and 15 above.)
22. Show that a local ring (2.8.2) is semi-simple if and only if it is a division ring.
23. Show that a commutative ring is semi-simple if and only if it is a finite direct product of fields,
24. Show that the matrix ring $R = M_n(D)$, over a division ring D , is semi-simple.
25. Show that $R = M_n(\mathbb{Z})$ is not semi-simple for any $n \in \mathbb{N}$. (Hint: Minimal left ideals exist in a semi-simple ring.)
26. Show that a submodule (resp. a quotient) of a semi-simple module is semi-simple.
27. Show that a finite sum of finitely generated submodules is finitely generated and that a quotient of a finitely generated module is finitely generated. However, give an example of two submodules P and Q of a module M such that both P and $P + Q$ are finitely generated but Q is not. Verify that for such a pair, $P \cap Q \neq (0)$.
28. Give examples to show that maximal or minimal submodules need not exist in a non-zero module.

29. Show that maximal submodules exist in a finitely generated non-zero module (but minimal ones need not). (Hint: Imitate the proof of (2.2.5) above, using Zorn's lemma.)
30. Show that a semi-simple module is finitely generated if and only if it is a sum of finitely many minimal submodules.
31. Give an example of a module which is not semi-simple.
32. Show that an R -module M is cyclic or *monogenic*, i.e., generated by one element, if and only if $M \simeq R/I$ for some left ideal I of R . Deduce that M is simple if and only if I is a maximal left ideal. However, give an example of a maximal 2-sided ideal I such that R/I is not simple.
33. Show that a simple R -module M is free if and only if R is a division ring and M is of dimension 1 over R .
34. Show that the multiplicative group of *positive* rational numbers, considered as a module over $\mathbb{Z}$, is a free module with the set of all positive prime numbers as a basis. (Hint: Use unique factorisation in $\mathbb{Z}$.)
Is the multiplicative group of all non-zero rational numbers a free module over $\mathbb{Z}$?
35. Considering R as a left module over itself, show that the ring $\text{End}_R(R)$ is naturally isomorphic to the opposite ring R^0 (1.11.1). (Hint: Any R -linear endomorphism of R is a right homothety, (i.e., multiplication on the right) by some element of R (5.7.13).)
36. Show that
 - $\text{End}_{\mathbb{Z}}(\mathbb{Q}) = \mathbb{Q} = \text{End}_{\mathbb{Q}}(\mathbb{Q})$ but
 - $\text{End}_{\mathbb{Z}}(\mathbb{R}) \neq \mathbb{R} = \text{End}_{\mathbb{R}}(\mathbb{R})$.
37. Prove Theorems (5.9.11), (5.9.12) and (5.9.13) above.
38. Let R be a ring with 1 and G be a finite group with its identity e (G multiplicatively written even if it is abelian). Let $R[G]$ be the set of all R -valued set-theoretic maps on G . For $x \in G$, let $\chi_x: G \rightarrow R$ be the *characteristic function* of $\{x\}$, i.e., $\chi_x(x) = 1$ and $\chi_x(y) = 0$ for $y \neq x$. Define addition and multiplication on $R[G]$ as follows.
 $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x)$, $\forall x \in G$.
 Show that
 - $\chi_x \chi_y = \chi_{xy}$, $\forall x, y \in G$,
 - $\chi(G) = \{\chi_x \mid x \in G\}$ is a basis of $R[G]$ as an R -module and

• $R[G]$ is a ring with $1 = \chi_e$ containing R as a subring.
This $R[G]$ is called the *group ring* of G over R .

39. With notation as above, show that
- $\chi(G)$ is a subgroup of the group $\mathcal{U}(R[G])$ of units in $R[G]$,
 - G is isomorphic to $\chi(G)$ and
 - $R[G]$ is commutative if and only if both R and G are so.
40. Let G be a cyclic group generated by x . Show that the map, $x \mapsto X + (X^n - 1)$, extends to an R -linear isomorphism of the group ring $R[G]$ onto $R[X]/(X^n - 1)$.
41. Let $C_1, \dots, C_h$ be all the distinct *conjugacy classes* of G . Let $z_i = \sum_{x \in C_i} x$, $1 \leq i \leq h$. Show that
- $z_i \in \text{Centre}(R[G])$, $\forall i$,
 - $z_i z_j = \sum_{k=1}^h m_{ijk} z_k$, with $m_{ijk} \in \mathbb{Z}^+$ for all i, j and
 - $\text{Centre}(R[G])$ is a free R -module with a basis $\{z_1, \dots, z_h\}$.
42. Let K be a field. Show that $K[G]$ is a simple ring if and only if $G = \{e\}$. (Hint: Look at the ideal generated by $z = \sum_{x \in G} x$.)
43. Let K be a field of non-zero characteristic p . Show that $K[G]$ has a non-trivial nilpotent ideal if $p \mid n$ where n is the order of G . (Hint: Consider the square of the ideal (z) where z is as above.)
44. With notation and hypothesis as above, show that the ideal (z) is not a direct summand of $K[G]$. (Hint: Use Ex.(5.10.11) and the fact that the ideal (z) does not contain non-trivial idempotents.)
45. If $f: G \rightarrow H$ is a homomorphism of groups, show that the induced map $\tilde{f}: R[G] \rightarrow R[H]$, sending $\chi_x \mapsto \chi_{f(x)}$, $x \in G$, extends to an R -linear homomorphism which is
- a unitary homomorphism of rings and that
 - it is a monomorphism (resp. an epimorphism) $\iff f$ is so. ■

5.11 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counter-example if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be. (Here R stands for a ring with 1, commutative or not.)

1. A simple ring R is simple as a left R -module.
2. Minimal submodules are simple modules.
3. Any simple module M over R is isomorphic to some minimal left ideal of R .
4. Any simple R -module is isomorphic to some quotient of R .
5. The additive group $(\mathbf{Q}, +)$ is finitely generated.
6. The additive group $(\mathbf{Q}, +)$ is torsion-free.
7. The additive group $(\mathbf{Q}, +)$ is free.
8. Any two bases of a finitely generated free $\text{End}_D(V)$ -module have the same cardinality if V is of finite dimension over a division ring D .
9. Any set spanning a free-module contains a basis.
10. $M_n(R)$ is a free R -module for all $n \in \mathbf{N}$.
11. Every module is a quotient of a free module.
12. Any two bases of a free module have the same cardinality.
13. Any two bases of a free module over a commutative ring have the same cardinality.
14. Submodule of a free module is free.
15. A quotient of a free module is free.
16. The multiplicative group $(\mathbf{Q}^*, \cdot)$ is a free $\mathbf{Z}$ -module.
17. The multiplicative group $(\mathbf{Q}^{>0}, \cdot)$ is a free $\mathbf{Z}$ -module.
18. Submodule of a free module over a PID is free.
19. A quotient of a free module over a PID is free.
20. A torsion-free module over a PID is free.
21. A simple module over a simple ring is free.
22. A simple module is semi-simple.

- 23. A vector space is semi-simple.
- 24. The matrix ring $M_n(D)$ over a division ring D is both a simple ring and a semi-simple module over itself.
- 25. A quotient of a semi-simple module M is isomorphic to a submodule of M .
- 26. A finitely generated torsion-free module over a PID is free.
- 27. R is the ring of endomorphisms of a suitable module over some ring.
- 28. Any endomorphism of a simple module is an isomorphism.
- 29. The only simple modules over $\mathbb{Z}$ are cyclic groups of prime order.
- 30. The only simple modules over a PID R are of the form $R/(p)$ for some prime p in R .
- 31. The only simple modules over a UFD R are of the form $R/(p)$ for some prime p in R .
- 32. The ring of endomorphisms of a simple module is a division ring.
- 33. The only simple and free modules are one dimensional vector spaces.
- 34. Any local ring is semi-simple.
- 35. A local ring is semi-simple if and only if it is a division ring.
- 36. Any cyclic module over a PID is simple. ■

Chapter 6

Modules with Chain Conditions

In this concluding chapter, we shall study the basic properties of an important class of modules and rings, (“Artinian” and “Noetherian”), which have some very special properties. Unless otherwise stated, R stands for a ring with 1 (commutative or not) and all modules considered are assumed to be unitary modules.

6.1 Artinian Modules

6.1.1 Theorem: *The following are equivalent for an R -module M .*

- 1. Descending chain condition (d.c.c) holds for submodules of M , i.e., any descending chain $M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots \supseteq \cdots$ of submodules of M is stationary in the sense that $M_r = M_{r+1} = \cdots$ for some r . (We write this as $M_r = M_{r+1}$, $\forall r \gg 0$).*
- 2. Minimum condition for submodules holds for M , in the sense that any non-empty family of submodules of M has a minimal element.*

Proof: (1) $\Rightarrow$ (2): Let $\mathcal{F} = \{M_i, i \in I\}$ be a non-empty family of submodules of M . Pick any index $i_1 \in I$ and look at M_{i_1} . If M_{i_1} is minimal in $\mathcal{F}$, we are through. Otherwise, there is an $i_2 \in I$ such that $M_{i_1} \supset M_{i_2}$, $M_{i_1} \neq M_{i_2}$. If this M_{i_2} is minimal in $\mathcal{F}$, we are through again. Proceeding thus, if we do not find a minimal element at any finite stage, we would end up with a non-stationary descending chain of submodules of M , namely, $M_{i_1} \supset M_{i_2} \supset \cdots \supset M_{i_n} \supset \cdots$ contradicting (1).

(2) $\Rightarrow$ (1): Let $M_1 \supseteq M_2 \supseteq \dots \supseteq M_n \supseteq \dots \supseteq \dots$ be a descending chain of submodules of M . Consider the non-empty family $\mathcal{F} = \{M_i \mid i \in \mathbb{N}\}$ of submodules of M . This must have a minimal element, say M_r , for some r . Now we have $M_s \subseteq M_r$, $\forall s \geq r$ which implies by minimality of M_r that $M_s = M_r$, $\forall s \geq r$. $\diamond$

6.1.2 Artinian module: A module M is called *Artinian* if d.c.c (or equivalently, the minimum condition) holds for M .

6.1.3 Remark: 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 .

6.1.4 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. (Verify.)

3. Infinite cyclic groups are *not* Artinian. For instance, $\mathbb{Z}$ has a non-stationary descending chain of subgroups, namely,

$$\mathbb{Z} = (1) \supset (2) \supset (4) \supset \dots \supset (2^n) \supset \dots \supset \dots$$

6.1.5 Theorem: 1. *Submodules and quotient modules of Artinian modules are Artinian.*

2. *If a module M is such that it has a submodule N with both N and M/N are Artinian, then M is Artinian.*

Proof : (1) Let M be Artinian 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 descending chain of submodules of M/N corresponds to one in M (wherein each member contains N) and hence the result.

(2) Let $M_1 \supseteq M_2 \supseteq \dots \supseteq M_n \supseteq \dots \supseteq \dots$ be a descending chain in M . Intersecting with N gives the descending chain in N , namely, $N \cap M_1 \supseteq N \cap M_2 \supseteq \dots \supseteq N \cap M_n \supseteq \dots \supseteq \dots$ which must be stationary, say $N \cap M_r = N \cap M_{r+1} = \dots$ for some r . On the other hand, we have the descending chain in M/N , namely,

$$(N + M_1)/N \supseteq (N + M_2)/N \supseteq \dots \supseteq (N + M_n)/N \supseteq \dots \supseteq \dots$$

which must be also stationary, say $(N + M_s)/N = (N + M_{s+1})/N = \dots$ for some s . Now we prove the following.

Claim: $M_n = M_{n+1}$, $\forall n \geq (r + s)$.

This is an immediate consequence of the four facts, namely,

1. $M_n \supseteq M_{n+1}$, $\forall n \in \mathbb{N}$,
2. $N \cap M_n = N \cap M_{n+1}$, $\forall n \geq r$,
3. $(N + M_n)/N = (N + M_{n+1})/N$, $\forall n \geq s$ and
4. $(N + M_n)/N \simeq M_n/(N \cap M_n)$, $\forall n \in \mathbb{N}$.

Putting together we get that

$M_n/(N \cap M_n) = (N + M_n)/N = (N + M_{n+1})/N = M_{n+1}/(N \cap M_{n+1})$
which implies the claim and hence the result. $\diamond$

6.1.6 Corollary: *Every non-zero submodule of an Artinian module contains a minimal submodule.* (Obvious by Remark (6.1.3).)

6.1.7 Corollary: *Sums and direct sums of finitely many Artinian modules are Artinian.*

For, let $M_1, \dots, M_n$ be Artinian submodules of a module M . Let $N = \sum_{i=1}^n M_i$. To prove N is Artinian, proceed by induction on n . If $n = 1$, there is nothing to prove. Let $n \geq 2$ and assume, by induction, that $N' = \sum_{i=1}^{n-1} M_i$ is Artinian. Now look at

$$N/M_n = (N' + M_n)/M_n \simeq N'/(N' \cap M_n)$$

which is Artinian being a quotient of the Artinian module N' . Thus both M_n and N/M_n are Artinian and hence N is Artinian, as required. The case of a direct sum is an immediate consequence because if $M = \oplus_{i=1}^n M_i$, then M is a finite sum of the Artinian submodules M_i and hence Artinian. $\diamond$

6.1.8 Remark: 1. *Direct sum of an infinite family of non-zero Artinian modules is not Artinian* (because it contains non-stationary descending chains). (Verify.)

2. *However, a sum of an infinite family of distinct Artinian modules could be Artinian.* (For example, the Euclidean plane $\mathbb{R}^2$ is a sum of all the lines passing through the origin and is a direct sum of any two of them.) $\blacksquare$

6.2 Noetherian Modules

A major part of this section (but not entirely though) is *dual* to the previous one, by respectively changing “descending”, “minimum”, etc., to “ascending”, “maximum”, etc. However, full details are given to facilitate an easy access to the reader.

6.2.1 Theorem: *The following are equivalent for an R -module M .*

1. *Ascending chain condition (a.c.c) holds for submodules of M , i.e., any ascending chain $M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq \dots$ of submodules of M is stationary in the sense that $M_r = M_{r+1} = \dots = \dots$ for some r . (We write this as $M_r = M_{r+1}, \forall r \gg 0$).*
2. *Maximum condition holds for M in the sense that any non-empty family of submodules of M has a maximal element.*
3. *Finiteness condition holds for M in the sense that every submodule of M is finitely generated (i.e., spanned).*

Proof: (1) $\Rightarrow$ (2): Let $\mathcal{F} = \{M_i, i \in I\}$ be a non-empty family of submodules of M . Pick any index $i_1 \in I$ and look at M_{i_1} . If M_{i_1} is maximal in $\mathcal{F}$, we are through. Otherwise, there is an $i_2 \in I$ such that $M_{i_1} \subset M_{i_2}, M_{i_1} \neq M_{i_2}$. If this M_{i_2} is maximal in $\mathcal{F}$, we are through again. Proceeding thus, if we do not find a maximal element at any finite stage, we would end up with a non-stationary ascending chain of submodules of M , namely, $M_{i_1} \subset M_{i_2} \subset \dots \subset M_{i_n} \subset \dots$ contradicting (1).

(2) $\Rightarrow$ (3): Let N be a submodule of M . Consider the family $\mathcal{F}$ of all finitely generated submodules of N . This family is non-empty since the submodule (0) is a member. This family has a maximal member, say $N_0 = (x_1, \dots, x_r)$. If $N_0 \neq N$, pick an $x \in N, x \notin N_0$. Now $N_1 = N_0 + (x) = (x, x_1, x_2, \dots, x_r)$ is a finitely generated submodule of N and hence $N_1 \in \mathcal{F}$. But then this contradicts the maximality of N_0 in $\mathcal{F}$ since $N_0 \subset N_1, N_0 \neq N_1$ and so $N_0 = N$ is finitely generated.

(3) $\Rightarrow$ (1): Let $M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq \dots$ be an ascending chain of submodules of M . Consider the submodule $N = \bigcup_{i=1}^{\infty} M_i$ of M which must be finitely generated, say $N = (x_1, x_2, \dots, x_n)$. It follows that $x_i \in M_r, \forall i, 1 \leq i \leq n$ for some $r (\gg 0)$. Now we have

$N \subseteq M_s \subseteq N, \forall s \geq r$ and so $N = M_r = M_{r+1} = \dots$

◇

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

Note: The “finiteness condition” has no parallel in the Artinian case. This additional property makes Noetherian modules rather special and the study more interesting.

6.2.3 Remarks: 1. *Maximal submodules exist in a non-zero Noetherian module* (because a maximal submodule is simply a maximal element in the family of all (proper) submodules N of $M, N \neq M$).

2. *However, maximal submodules exist in any finitely generated non-zero module, even if the module is not Noetherian.* (This is a simple consequence of Zorn’s lemma applied to the family of all proper submodules of such a module.) (See (6.2.9)(4) below, for an example of a finitely generated module which is not Noetherian.)

6.2.4 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.

3. Unlike the Artinian case, infinite cyclic groups are Noetherian because every subgroup of a cyclic group is again cyclic.

6.2.5 Theorem: 1. *Submodules and quotient modules of Noetherian modules are Noetherian.*

2. *If a module M is such that it has a submodule N with both N and M/N are Noetherian, then M is Noetherian.*

Proof: (1) 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.

(2) Let $M_1 \subseteq M_2 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq \dots$ be an ascending chain

in M . Intersecting with N gives the ascending chain in N , namely, $N \cap M_1 \subseteq N \cap M_2 \subseteq \dots \subseteq N \cap M_n \subseteq \dots \subseteq \dots$ which must be stationary, say $N \cap M_r = N \cap M_{r+1} = \dots =$ for some r . On the other hand, we have the ascending chain in M/N , namely,

$$(N + M_1)/N \subseteq (N + M_2)/N \subseteq \dots \subseteq (N + M_n)/N \subseteq \dots \subseteq \dots$$

which must be also stationary, say, $(N + M_s)/N = (N + M_{s+1})/N = \dots =$ for some s . Now we prove the following.

Claim: $M_n = M_{n+1}$, $\forall n \geq (r + s)$.

This is an immediate consequence of the four facts, namely,

1. $M_n \subseteq M_{n+1}$, $\forall n \in \mathbb{N}$,
2. $N \cap M_n = N \cap M_{n+1}$, $\forall n \geq r$,
3. $(N + M_n)/N = (N + M_{n+1})/N$, $\forall n \geq s$ and
4. $(N + M_n)/N \simeq M_n/(N \cap M_n)$, $\forall n \in \mathbb{N}$.

Putting together we get that

$$M_n/(N \cap M_n) = (N + M_n)/N = (N + M_{n+1})/N = M_{n+1}/(N \cap M_{n+1})$$

which implies the claim and hence the result. $\diamond$

6.2.6 Corollary : *Every non-zero submodule of a Noetherian module is contained in a maximal submodule.* (Obvious by Remark (6.2.3) above.)

6.2.7 Corollary: *Sums and direct sums of finitely many Noetherian modules are Noetherian.*

For, let $M_1, \dots, M_n$ be Noetherian submodules of a module M . Let $N = \sum_{i=1}^n M_i$. To prove N is Noetherian, proceed by induction on n . If $n = 1$, there is nothing to prove. Let $n \geq 2$ and assume, by induction, that $N' = \sum_{i=1}^{n-1} M_i$ is Noetherian. Now look at

$$N/M_n = (N' + M_n)/M_n \simeq N'/(N' \cap M_n)$$

which is Noetherian being a quotient of the Noetherian module N' . Thus both M_n and N/M_n are Noetherian and hence N is Noetherian, as required. The case of a direct sum is an immediate consequence because if $M = \oplus_{i=1}^n M_i$, then M is a finite sum of the Noetherian submodules M_i and hence Noetherian. $\diamond$

6.2.8 Remark: *Direct sum of an infinite family of non-zero Noetherian modules is not Noetherian* (because it contains non-

stationary ascending chains). (Verify.)

6.2.9 Some Pathologies:

1. An Artinian module need not be finitely generated.
2. Maximal submodules need not exist in an Artinian module.
3. An Artinian module need not be Noetherian.
4. A finitely generated module need not be Noetherian.
5. Minimal submodules need not exist in a Noetherian module.
6. A Noetherian module need not be Artinian.
7. There are modules which are neither Artinian nor Noetherian.

Before we give counter-examples to justify the statements above, first we consider the abelian group μ_{p^n} of all complex $(p^n)^{th}$ roots of unity for a fixed prime number p and all $n \in \mathbb{N}$. For each positive integer n , let μ_{p^n} denote the cyclic group of all complex $(p^n)^{th}$ roots of unity so that we have $\mu_p \subset \mu_{p^2} \subset \cdots \subset \mu_{p^n} \subset \cdots$ and hence

$$\mu_{p^\infty} = \bigcup_{n=1}^{\infty} \mu_{p^n}.$$

Furthermore, we notice the following special features in this group.

- (a) It is infinite and non-cyclic.
- (b) Every proper subgroup is finite and is equal to μ_{p^n} for some n .
- (c) Every finitely generated subgroup is proper and hence finite.
- (d) In particular, μ_{p^∞} is not finitely generated.

These properties can be easily verified using the fact that any $x \in \mu_{p^{n+1}}$, $x \notin \mu_{p^n}$ generates $\mu_{p^{n+1}}$.

Now we give the required counter-examples.

Example 1: The group μ_{p^∞} is Artinian but not Noetherian, not finitely generated and does not have maximal subgroups. This justifies the statements (1),(2) and (3).

Example 2: Let $R = \mathbb{Z}[X_1, X_2, \dots, X_n, \dots]$ be the polynomial ring in *infinitely many variables*. We know that R , as a module over itself, is generated by $\{1\}$ but R is not Noetherian because it has a non-stationary ascending chain of ideals, namely,

$$(X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n) \subset \cdots$$

This serves the purpose for statement (4).

Example 3: The infinite cyclic group $\mathbb{Z}$ is Noetherian but not Artinian and it has no minimal subgroups. This justifies statements (5) and (6).

Example 4: Direct sum of any infinite family of non-zero modules, in particular, an infinite dimensional vector space, is neither Artinian nor Noetherian. ■

6.3 Modules of Finite Length

6.3.1 Simple module: A module M is called *simple* if

1. $M \neq (0)$ and
2. M has no submodules other than (0) and M .

6.3.2 Remark : A non-zero module M is simple $\Leftrightarrow (0)$ is a maximal submodule of $M \Leftrightarrow M$ is a minimal submodule of $M \Leftrightarrow$ every non-zero element of M generates M .

6.3.3 Examples:

1. Any one-dimensional vector space is simple.
2. Any minimal submodule of a module is simple.
3. A submodule N of M is maximal in $M \Leftrightarrow M/N$ is simple.

6.3.4 Remark: Simple submodules exist in a non-zero Artinian module while simple quotients exist for a non-zero Noetherian one.

6.3.5 Composition series: By a *composition series* of a non-zero module M , we mean a finite descending chain of submodules of M starting with M and ending with (0) , say

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = (0)$$

such that the successive quotients M_i/M_{i+1} are simple $\forall i$. The integer m is called the *length* of the series. (It is one less than the number of terms in the series.) A composition series is also called a *Jordan-Hölder filtration* or simply a *filtration*.

6.3.6 Remark: For a non-zero module M , a composition series may or may not exist. If one exists, we notice that M would have a simple submodule M_{m-1} and a maximal submodule M_1 (i.e., a simple quotient M_0/M_1).

6.3.7 Examples: 1. A vector space V having a finite basis $\{v_1, \dots, v_m\}$ has a composition series of length m , namely,

$$V = V_0 \supset V_1 \supset \dots \supset V_m = (0)$$

where $V_i = \text{span of } \{v_{i+1}, v_{i+2}, \dots, v_m\}$ for all $i, 0 \leq i \leq m$ with $V_m = (0)$. (However, a vector space having an infinite basis cannot have a composition series. Verify.)

2. A finite abelian group has a composition series. (Check.)

3. An infinite cyclic group cannot have a composition series since it has no minimal submodules.

6.3.8 Modules of finite length: A module is called a *module of finite length* if it is either zero or has some composition series.

6.3.9 Theorem : *A module is of finite length $\Leftrightarrow$ it is both Artinian and Noetherian.*

Proof: Let M be a module of finite length. If $M = (0)$, the result is obvious. Suppose $M \neq (0)$ and has a composition series, say

$$M = M_0 \supset M_1 \supset \dots \supset M_m = (0).$$

Now proceed by induction on m . If $m = 1$, then M is simple and hence trivially M is both Artinian and Noetherian. Assume that $m \geq 2$ and the induction hypothesis that any module having some composition series of length at most $m - 1$ is both Artinian and Noetherian. Now look at M_1 which has the composition series, namely, $M_1 \supset \dots \supset M_m = (0)$, of length $m - 1$. Hence M_1 is both Artinian and Noetherian. On the other hand, the quotient M/M_1 , being simple, is also both Artinian and Noetherian and hence it follows, by (6.1.5) and (6.2.5), that M is both Artinian and Noetherian, as required.

Conversely, suppose M is both Artinian and Noetherian, we may assume that $M \neq (0)$. Since M is Noetherian, it has a maximal submodule, say M_1 . If $M_1 = (0)$, then M is simple and hence it is a module of finite length. Otherwise M_1 , also being Noetherian, has a maximal submodule, say M_2 . If $M_2 = (0)$, we have a composition series for M , namely, $M = M_0 \supset M_1 \supset M_2 = (0)$. Proceeding thus, at any finite stage n , if $M_n \neq (0)$, we get a maximal submodule M_{n+1} of M_n and so on, yielding an infinitely descending chain of submodules of M , namely, $M = M_0 \supset M_1 \supset \dots \supset M_n \supset \dots \supset \dots$ (with M_n/M_{n+1}

simple for all n), contradicting that M is Artinian. Hence $M_m = (0)$ for some m , as required. $\diamond$

6.3.10 Theorem: 1. *Submodules and quotient modules of a module of finite length are modules of finite length.*

2. *If a module M has a submodule N such that both N and M/N are of finite length, then M is of finite length.*

Proof: *We shall give two proofs.*

First proof: Put together (6.3.9), (6.1.5) and (6.2.5) above. $\diamond$

Second proof: *This is from first principles.* Here the details may appear a little messy but we have the advantage of not using any other results. Let M be a module of finite length having a composition series, say

$$(\star) \quad M = M_0 \supset M_1 \supset \cdots \supset M_m = (0).$$

Let N be a submodule of M . Intersecting $(\star)$ with N we get a descending chain, namely,

$$N = N \cap M_0 \supseteq N \cap M_1 \supseteq \cdots \supseteq N \cap M_m = (0).$$

For each i , we find that either $N \cap M_i = N \cap M_{i+1}$ or else

$(N \cap M_i)/(N \cap M_{i+1}) \simeq M_i/M_{i+1}$ is simple. Deleting repetitions, if any, we get a composition series for N of the form

$$N = N \cap M_0 \supset N \cap M_{i_1} \supset \cdots \supset N \cap M_{i_r} = (0) \quad \text{where}$$

$$N \cap M_0 = N \cap M_1 = \cdots = N \cap M_{i_1-1} \neq N \cap M_{i_1},$$

$$N \cap M_{i_1} = N \cap M_{i_1+1} = \cdots = N \cap M_{i_2-1} \neq N \cap M_{i_2},$$

$$\vdots \quad \quad \quad \vdots$$

$$N \cap M_{i_{r-1}} = N \cap M_{i_{r-1}+1} = \cdots = N \cap M_{i_r-1} \neq N \cap M_{i_r} \quad \text{and}$$

$$N \cap M_{i_r} = N \cap M_{i_r+1} = \cdots = N \cap M_m = (0).$$

This proves that N is of finite length. Let $\eta : M \rightarrow M/N$ be the natural homomorphism. Look at the image of the filtration $(\star)$ above under η , namely, $M/N = \eta(M_0) \supseteq \eta(M_1) \supseteq \cdots \supseteq \eta(M_m) = (0)$, i.e.,

$$M/N = (M_0 + N)/N \supseteq (M_1 + N)/N \supseteq \cdots \supseteq (M_m + N)/N = (0).$$

For each i , we find that either $(N + M_i)/N = (N + M_{i+1})/N$ or else $((N + M_i)/N)/((N + M_{i+1})/N) \simeq M_i/M_{i+1}$ is simple. Hence deleting repetitions, if any, we get a composition series for M/N of the form

$$M/N = \eta(M_0) \supset \eta(M_{j_1}) \supset \cdots \supset \eta(M_{j_s}) = (0).$$

This proves (1). Let N be a submodule of M such that both N and M/N are of finite length, with respective composition series (of lengths n and m), $N = N_0 \supset N_1 \supset \cdots \supset N_n = (0)$ and

$$M/N = (M/N)_0 \supset (M/N)_1 \supset \cdots \supset (M/N)_m = (0).$$

Let $M_i = \eta^{-1}((M/N)_i)$, $0 \leq i \leq m$, so that we have

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = N$$

with $M_i/M_{i+1} \simeq ((M/N)_i)/((M/N)_{i+1})$ simple for $0 \leq i \leq m-1$.

Now we have a composition series for M (of length $n+m$),

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = N = N_0 \supset N_1 \supset \cdots \supset N_n = (0). \quad \diamond$$

6.3.11 Theorem (Jordan–Hölder): *Any two composition series of a non-zero module are equivalent in the sense that both have the same length and the same simple quotients upto order and isomorphisms. To be more precise, let $M = M_0 \supset M_1 \supset \cdots \supset M_m = (0)$ and $M = N_0 \supset N_1 \supset \cdots \supset N_n = (0)$ be any two composition series for M . Then (i) $m = n$ and (ii) $\forall i$, $0 \leq i \leq m-1$, $\exists j = j(i)$, $0 \leq j \leq n-1$ such that $M_i/M_{i+1} \simeq N_j/N_{j+1}$ and vice-versa.*

Proof: We prove the result by induction on the length of one of the composition series, say m of the first. If $m = 1$, then M is simple and hence $N_1 = (0)$, i.e., $n = 1$ and the result follows. Suppose $m \geq 2$ and assume the induction hypothesis that the theorem is true for any module having some composition series of length at most $m-1$. We distinguish two possibilities.

Case 1: $M_1 = N_1$.

Now we find that M_1 has two composition series, namely,

$$M_1 \supset M_2 \supset \cdots \supset M_m = (0) \text{ and}$$

$$N_1 \supset N_2 \supset \cdots \supset N_n = (0).$$

Since the first one is of length $m-1$, we get by induction that

1. $m-1 = n-1$, i.e., $m = n$ and
2. $\forall i$, $1 \leq i \leq m-1$, $\exists j = j(i)$, $1 \leq j \leq n-1$ such that $M_i/M_{i+1} \simeq N_j/N_{j+1}$ and vice-versa.

Since $M/M_1 = M/N_1$, the result follows.

Case 2: $M_1 \neq N_1$.

Let $M' = M_1 + N_1$ which is a submodule of M containing the maximal

submodules M_1 and N_1 and so $M' = M$. furthermore, we have

(★★) $\begin{cases} M/M_1 = (M_1 + N_1)/M_1 \simeq N_1/(M_1 \cap N_1) = N_1/K = \text{simple,} \\ M/N_1 = (M_1 + N_1)/N_1 \simeq M_1/(M_1 \cap N_1) = M_1/K = \text{simple,} \end{cases}$
 where $K = (M_1 \cap N_1)$ which is a submodule of a module of finite length M and so K is also a module of finite length and hence has some composition series, say $K = K_0 \supset K_1 \supset \cdots \supset K_r = (0)$. Thus we get 4 composition series for $M = (M_1 + N_1)$, namely,

$$\begin{aligned} M &= (M_1 + N_1) \supset M_1 \supset K \supset K_1 \supset \cdots \supset K_r = (0), \\ &= (M_1 + N_1) \supset M_1 \supset M_2 \supset \cdots \supset M_m = (0), \\ &= (M_1 + N_1) \supset N_1 \supset N_2 \supset \cdots \supset N_n = (0) \text{ and} \\ &= (M_1 + N_1) \supset N_1 \supset K \supset K_1 \supset \cdots \supset K_r = (0). \end{aligned}$$

Of these, the first two (resp. the last two) are equivalent by Case 1 whereas the first and last are equivalent by (★★) above and hence we get that the 2nd and 3rd are equivalent, as required. $\diamond$

6.3.12 Length of a module: For a module M of finite length, the length of any of its composition series (which is independent of the series) is called the *length of the module* and is denoted by $\ell_R(M)$ or simply $\ell(M)$ if there is no confusion about the base ring R . (If M has no composition series, we say set $\ell_R(M) = \infty$.)

6.3.13 Remark: 1. $\ell(M) \geq 0$ and equality holds $\Leftrightarrow M = (0)$.

2. $\ell(M) = 1 \Leftrightarrow M$ is simple.

3. $\ell(M)$ is a measure of departure of M from being simple for a non-zero module M .

6.3.14 Corollary: 1. Let N be a submodule of a module M of finite length. Then we have $\ell(M) = \ell(N) + \ell(M/N)$ and in particular, $\ell(M) \geq \ell(N)$ with equality $\Leftrightarrow M = N$.

2. Sum of finitely many submodules of finite length is a module of finite length and $\ell(\sum_{i=1}^n M_i) \leq \sum_{i=1}^n \ell(M_i)$ with equality if and only if the sum is a direct sum, i.e.,

$$\ell(\sum_{i=1}^n M_i) = \sum_{i=1}^n \ell(M_i) \iff \sum_{i=1}^n M_i = \oplus_{i=1}^n M_i.$$

3. If a vector space V over D has a finite basis, then any other basis is also finite and all bases have the same number of elements, namely, $\ell_D(V)$ ($= \dim_D(V)$).

Proof : (1) As we saw in the second proof of (6.3.10) above, if N

and M/N have composition series of lengths n and m respectively, then M has a composition series of length $n + m$, as required.

(2) Proceed by induction on n and use the fact (1), namely,

$$\ell(M_1 + M_2) = \ell(M_1) + \ell(M_2) - \ell(M_1 \cap M_2)$$

via the isomorphism $(M_1 + M_2)/M_1 \approx M_2/(M_1 \cap M_2)$.

(3) Follows from Example (1) of (6.3.7) above. ■

6.4 Artinian Rings

6.4.1 Artinian ring: A ring R is called (*left*) *Artinian* if it is Artinian as a left module over itself, i.e., d.c.c or minimum condition holds for left ideals of R .

6.4.2 Examples: Fields, division rings, finite rings are all Artinian. The ring of integers $\mathbb{Z}$ is not Artinian.

6.4.3 Proposition: *A quotient ring of an Artinian ring is Artinian (whereas a subring need not be Artinian).*

Proof: If I is a 2-sided ideal of an Artinian ring R , then R/I is Artinian as an R -module. But the family of all left ideals of R/I is precisely the family of all left ideals of R each containing I and hence it follows that R/I is an Artinian ring, as required. The subring $\mathbb{Z}$ of the Artinian ring $\mathbb{Q}$ is not Artinian. ◇

6.4.4 Proposition: *A finitely generated module over an Artinian ring is Artinian.*

Proof: If a module M is generated by n elements, then M is a quotient of the Cartesian product R^n which is Artinian (since R is Artinian) and hence M is Artinian, as required. ◇

6.4.5 Corollary: *Matrix rings over Artinian rings with unity, (in particular, over division rings), are Artinian.*

Proof: Let R be Artinian and $S = M_n(R)$ be a matrix ring over R . It is clear that any left ideal of S is also an R -submodule of S . But

S is Artinian as an R -module since it is finitely generated over R , (in fact, it is a free R -module with a basis having n^2 elements). Hence S is an Artinian ring, as required. $\diamond$

6.4.6 Theorem: *Let R be an Artinian ring with unity. Then we have the following.*

1. *Every non-zero divisor in R is a unit. In particular, an Artinian integral domain is a division ring.*
2. *If R is commutative, every prime ideal is maximal. (In particular, a commutative Artinian integral domain is a field.)*

Proof: (1) Let $x \in R$ be not a zero-divisor. Note then that x^r is not a zero-divisor for any $r \in \mathbb{N}$. Since R is Artinian, the descending chain of principal left ideals, namely, $(x)_l \supset (x^2)_l \supset \cdots \supset (x^n)_l \supset \cdots$ must be stationary, say $(x^r)_l = (x^{r+1})_l = \cdots =$ for some $r \in \mathbb{N}$. Since $x^r \in (x^{r+1})_l$, we can write $x^r = yx^{r+1}$ for some $y \in R$. This gives $(1 - yx)x^r = 0$ and hence $1 = yx$ (on cancelling x^r which is not a zero-divisor). Now we have $x = x(yx) = (xy)x$ and hence $(1 - xy)x = 0$ implying $1 = xy$ (on cancelling x). Thus we get that $yx = 1 = xy$.

(2) If R is commutative Artinian and P is a prime ideal in R , then R/P is an Artinian integral domain and hence every non-zero element (being not a zero-divisor) is a unit, i.e., R/P is a field, i.e., P is a maximal ideal, as required. $\blacksquare$

6.5 Noetherian Rings

6.5.1 Noetherian ring: A ring R is called (*left*) *Noetherian* if it is Noetherian as a left module over itself, i.e., a.c.c or maximum condition holds for left ideals or every left ideal is finitely generated.

6.5.2 Examples: Fields, division rings, finite rings, principal ideal rings, etc., are all Noetherian. In particular, the ring of integers $\mathbb{Z}$ is Noetherian.

6.5.3 Proposition: *A quotient ring of a Noetherian ring is Noetherian (whereas a subring need not be Noetherian).*

Proof: If I is a 2-sided ideal of a Noetherian ring R , then R/I is Noetherian as an R -module. But the family of all left ideals of R/I is precisely the family of all left ideals of R each containing I and hence it follows that R/I is a Noetherian ring, as required.

We know that the ring $R = \mathbb{Z}[X_i, i \in \mathbb{N}]$ is not Noetherian (see Example 2 of (6.2.9) above), but it is a subring of its field of fractions which is Noetherian. $\diamond$

6.5.4 Proposition: *A finitely generated module over a Noetherian ring is Noetherian.*

Proof: If a module M is generated by n elements, then M is a quotient of the Cartesian product R^n which is Noetherian (since R is Noetherian) and hence M is Noetherian, as required. $\diamond$

6.5.5 Corollary: *Matrix rings over Noetherian rings with unity, (in particular, over division rings), are Noetherian.*

Proof: Let R be Noetherian and $S = M_n(R)$ be a matrix ring over R . It is clear that any left ideal of S is also an R -submodule of S . But S is Noetherian as an R -module since it is finitely generated over R , (in fact, it is a free R -module with a basis having n^2 elements). Hence S is a Noetherian ring, as required. $\diamond$

The following is a well-known theorem of Hilbert, called the "Hilbert Basis Theorem" and most useful too. The word "basis" is used in the sense of finite generation and not in the strict sense.

6.5.6 Hilbert Basis Theorem: *Let R be a ring with 1. Then R is Noetherian $\iff R[X]$ is Noetherian.*

Proof: If $R[X]$ is Noetherian, then $R \approx R[X]/(X)$ is Noetherian being a quotient of a Noetherian ring.

The converse is the non-trivial part. Let R be Noetherian. We shall show that every left ideal of $R[X]$ is finitely generated. Let J be a left ideal of $R[X]$. If $J = (0)$, we are through. Let $J \neq (0)$. We divide the proof into 2 main steps.

Step 1: For each $r \in \mathbb{Z}^+$, let I_r be the set of the leading coefficients of all non-zero elements of J of degree at most r together with 0. Then we have (i) I_r is a left ideal of R and (ii) $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_r \subseteq \cdots$

Obviously $I_r \neq \emptyset$. Let $a, b \in I_r, a \neq b$. Let $f(X) = aX^r + \cdots + a_0$ and $g(X) = bX^r + \cdots + b_0$ be in J corresponding to a and b in I_r . We have assumed that both f and g have the same degree, namely r , by multiplying with suitable powers of X if necessary. Now $a - b$ is the leading coefficient of $(f(X) - g(X)) \in J$ which is of degree r and hence $(a - b) \in I_r$. On the other hand, if $x \in R$ and $xa \neq 0$, then xa is the leading coefficient of $xf(X) \in J$ and so I_r is a left ideal of R . The assertion (ii) is obvious.

Since R is Noetherian, we have $\cup_{r=0}^{\infty} I_r = I_n$ for some $n \gg 0$ and each I_r is finitely generated, say, $I_r = (a_{r1}, a_{r2}, \dots, a_{rk_r})$ for some $a_{rj} \in I_r, 1 \leq j \leq k_r$ and $0 \leq r \leq n$. Let $f_{rj}(X) \in J$ be such that its leading coefficient is $a_{rj} \in I_r$. As before, we may assume that all the $f_{rj}(X)$'s have the same degree r , independent of j for $1 \leq j \leq k_r$.

Step 2: We have $J = (f_{rj}(X)), 0 \leq r \leq n$ and $1 \leq j \leq k_r$.

In fact, $J = \sum_{r=0}^{n-1} \sum_{j=1}^{k_r} R f_{rj}(X) + \sum_{j=1}^{k_n} R[X] f_{nj}(X)$. (★)

We have only to show that any element $f(X) \in J$ can be written as an $R[X]$ -linear combination of the $f_{rj}(X)$'s. To this end, take $0 \neq f(X) \in J$. Let the degree of $f(X)$ be m . Proceed by induction on m . If $m = 0$, then $f \in I_0 = (f_{0j}(X)), 1 \leq j \leq k_0$, as required.

Assume that $m \geq 1$ and the induction hypothesis that every element $g(X) \in J$ of degree at most $m - 1$ can be written as stated in (★) above. Look at the leading coefficient of $f(X)$, say a . Since $a \in I_m$, we can write $a = \sum_{j=1}^{k_m} \alpha_{mj} a_{mj}$ for some $\alpha_{mj} \in R$. Since $I_m = I_n$ for $m \geq n$, we note that $a = \sum_{j=1}^{k_n} \alpha_{nj} a_{nj}$ if $m \geq n$. Now consider

$$g(X) = \begin{cases} f(X) - X^{m-n} (\sum_{j=1}^{k_n} \alpha_{nj} f_{nj}(X)) & \text{if } m \geq n \\ f(X) - (\sum_{j=1}^{k_m} \alpha_{mj} f_{mj}(X)) & \text{if } m \leq n \end{cases}$$

which is an element of J and has degree at most $m - 1$ and so we can write $g(X)$ as in (★) above and hence also $f(X)$, as required. ◇

6.5.7 Corollary: 1. *A ring R is Noetherian $\iff R[X_1, X_2, \dots, X_n]$ is Noetherian for any finitely many variables.*

2. *A finitely generated algebra over a Noetherian ring, generated by a commuting set of generators, is Noetherian. In particular, the ring $\mathbb{Z}[\sqrt{d}]$ is Noetherian for any integer $d \in \mathbb{Z}$.*

Proof: (1) follows by a repeated use of Hilbert's theorem.

(2) Such a ring is a quotient of $R[X_1, X_2, \dots, X_n]$ for some n . The last is a quotient of $\mathbb{Z}[X]$ by the ideal $(X^2 - d)$. $\diamond$

6.5.8 Theorem : *Let V be a vector space over a division ring D and $R = \text{End}_D(V)$ be the ring of D -linear endomorphism of V . Then the following are equivalent.*

- 1.** *R is Artinian.*
- 2.** *V is finite dimensional over D .*
- 3.** *R is Noetherian.*

Proof: (1) $\Leftrightarrow$ (2) : Let R be Artinian. Suppose V is not finite dimensional over D . Pick up any countably infinite linearly independent subset $\{v_1, v_2, \dots, v_n, \dots\}$ of V . For each $i \in \mathbb{N}$, let V_i be the subspace spanned by first i vectors $v_1, v_2, \dots, v_i$. We get an infinitely ascending chain of subspaces of V , namely,

$$V_1 \subset V_2 \subset \dots \subset V_n \subset \dots \subset \dots$$

This gives an infinitely descending chain of left ideals of R , namely,

$$I_1 \supset I_2 \supset \dots \supset I_n \supset \dots \supset \dots$$

where $I_i = \{f \in R \mid f(V_i) = 0, i \in \mathbb{N}\}$ contradicting (1). Hence V is finite dimensional. Conversely, if V is finite dimensional, then $R \approx M_r(D)$ where $r = \dim_D(V)$ and so R is Artinian by (6.4.5) above.

(2) $\Leftrightarrow$ (3): If V is finite dimensional, then $R = M_r(D)$ which is Noetherian by (6.5.5) above. Conversely, suppose R is Noetherian and assume, if possible, V is not finite dimensional. As before choose any countably infinite linearly independent subset $\{w_1, w_2, \dots, w_n, \dots\}$ of V . For each $i \in \mathbb{N}$, let W_i be the subspace spanned by omitting the first $i - 1$ vectors. We get an infinitely descending chain of subspaces of V , namely, $W_1 \supset W_2 \supset \dots \supset W_n \supset \dots \supset \dots$

This gives an infinitely ascending chain of left ideals of R , namely,

$$J_1 \subset J_2 \subset \dots \subset J_n \subset \dots \subset \dots$$

where $J_i = \{f \in R \mid f(W_i) = 0, i \in \mathbb{N}\}$ contradicting (3). Hence V is finite dimensional, as required. $\diamond$

6.5.9 Corollary: *The ring $R = \text{End}_D(V)$ is a module of finite length as an R -module if and only if V is finite dimensional over D .*

Proof: Immediate from (6.5.8) and (6.3.9) above. $\diamond$

6.5.10 Remark: If $\dim_D(V) = r$, then $R = \text{End}_D(V)$ is a module of finite length as a module over D as well as over itself. Its lengths are given by $\ell_R(R) = r$ whereas $\ell_D(R) = r^2$. The second follows simply because $\dim_D(R) = \dim_D(M_r(D)) = r^2$. The first follows because R has a composition series, namely, $R = R_0 \supset R_1 \supset \dots \supset R_r = (0)$ where R_i is the left ideal consisting of all matrices whose first i columns are zero, $0 \leq i \leq r$.

In the rest of this section, R stands for a commutative ring with 1, integral domain or not.

6.5.11 Theorem (Cohen): *Let R be as above. Then R is Noetherian $\iff$ every prime ideal of R is finitely generated.*

Proof: The implication " $\implies$ " is obvious since every ideal is finitely generated. The converse is the interesting part.

Suppose every prime ideal of R is finitely generated. Let $\mathcal{F}$ be the family of all ideals of R which are not finitely generated. We want to show that $\mathcal{F} = \emptyset$. Assume otherwise and apply Zorn's lemma to $\mathcal{F}$. If $\mathcal{T}$ is a chain in $\mathcal{F}$ and $T_0 = \cup_{T \in \mathcal{T}} T$, then T_0 is clearly an ideal of R and T_0 cannot be finitely generated (otherwise, it would follow that $T_0 = T' \in \mathcal{T} \subseteq \mathcal{F}$ implying that $\mathcal{F}$ contains a finitely generated ideal T_0 which cannot be). Thus $T_0 \in \mathcal{F}$ is an upper bound for $\mathcal{T}$ and hence $\mathcal{F}$ has a maximal element, say J . Since J is not finitely generated, J cannot be a prime ideal. Hence $\exists x, y \in R$ such that $x \notin J$ and $y \notin J$ but $xy \in J$.

Now the ideal $J + yR \supset J, J + yR \neq J$ and so $J + yR$ is not a member of $\mathcal{F}$ which means that $J + yR$ is finitely generated, say $J + yR = (y_1, y_2, \dots, y_r)$. Each y_i can be written as $y_i = a_i + \alpha_i y$ for

some $a_i \in J$ and $\alpha_i \in R, 1 \leq i \leq r$. On the other hand, look at the ideal of R which contains J and the element x , namely,

$$J : yR = \{z \in R \mid zy \in J\}.$$

This again is not a member of $\mathcal{F}$ and so finitely generated, say $J : yR = (x_1, x_2, \dots, x_s)$. By definition, we have $b_j = x_j y \in J, 1 \leq j \leq s$. It is an easy exercise to see now that J is finitely generated, in fact, we have $J = (a_1, a_2, \dots, a_r; b_1, b_2, \dots, b_s)$ contradicting the fact that J is not finitely generated and so $\mathcal{F} = \emptyset$, as required. $\diamond$

6.5.12 Theorem: *A commutative Noetherian integral domain with 1 is a factorisation domain.*

Proof: Same as that of (4.4.2) above, as was already noted there. $\diamond$

6.5.13 Theorem : *The ring R of Complex entire functions is neither Artinian nor Noetherian.*

Proof: R is not Artinian because it is a commutative integral domain which is not a field. That R is not Noetherian follows because it is not even a factorisation domain. However, we shall now give a direct argument (from first principles) as follows.

Consider the discrete subset $\mathbb{N}$ of $\mathbb{C}$ which is without limit points. For each $r \in \mathbb{N}$, let I_r be the set of all entire functions vanishing at the integral points $m \in \mathbb{N}, \forall m \geq r$, i.e.,

$$I_r = \{f \in R \mid f(r) = f(r+1) = \dots = 0\}.$$

Thus we get an ascending chain of ideals of R , namely

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots \subset \dots$$

This chain is infinitely strictly ascending because of the following well-known theorem.

Theorem (Weierstrass): *For each positive integer r , there exists a Complex entire function $f(z)$ such that $f(r) \neq 0$ but $f(r+1) = f(r+2) = \dots = 0$, i.e., $f(z) \in I_{r+1}$ but $f(z) \notin I_r$.*

This is a very special case (for $D = \mathbb{N}$) of a much stronger theorem of Weierstrass which gives the existence of Complex entire functions with prescribed zeros (each of specified order) at any discrete set D without limit points. $\diamond$

6.5.14 Theorem: *In a commutative Noetherian ring, every ideal contains a product of prime ideals.*

Proof: Let $\mathcal{F}$ be the set of all ideals I in R such that I does not contain any product of prime ideals. If $\mathcal{F} \neq \emptyset$, it has a maximal element, say A . This A cannot be a prime ideal itself and hence there exist $x, y \in R$ such that $xy \in A$ with $x, y \notin A$. Now let $I = A + Rx$ and $J = A + Ry$ so that $A \subseteq I \cap J$ and $A \neq I$ and $A \neq J$. Hence by maximality of A in $\mathcal{F}$, we get that $I, J \notin \mathcal{F}$, i.e., both I and J contain some products of prime ideals. But then it follows that IJ contains a product of prime ideals and so does A because $xy \in A$ and so we have $IJ = (A + Rx)(A + Ry) \subseteq A + Rxy = A$. This contradiction proves that $\mathcal{F} = \emptyset$, as required. $\diamond$

6.5.15 Corollary: *In a commutative Noetherian ring the ideal (0) is a product of prime ideals, say*

$$(0) = P_1^{\epsilon_1} \cdot P_2^{\epsilon_2} \cdots P_n^{\epsilon_n} \quad (\star)$$

with P_i distinct prime ideals and $\epsilon_i \in \mathbb{N}$. Consequently, the set of minimal prime ideals of R is finite (it being the set of minimal elements in $\{P_1, \dots, P_n\}$).

This follows at once since any prime ideal contains the product in $(\star)$ and hence contains one of the P_i 's. $\blacksquare$

6.6 Radicals

6.6.0 Radical ideal: A two-sided ideal I in a ring R with 1 is called a *radical ideal* with respect to a specified property $\mathcal{P}$ if

1. the ideal I possesses the property $\mathcal{P}$ and
2. the ideal I is maximal for the property $\mathcal{P}$, i.e., if J is a 2-sided ideal of R having the property $\mathcal{P}$, then $J \subseteq I$.

There are several kinds of radicals defined and studied in a ring in various contexts. Notable among them are two radicals called the *nil radical* and the *Jacobson radical*. There are others like the *Amit-sur radical*, the *Brown-McCoy radical*, the *Levitzki radical*, etc. (See

“RINGS AND RADICALS” by N.J. Divinsky, George Allen and Unwin Ltd., London (1965).) We shall introduce the first two of these radicals and prove some basic properties thereof.

6.6n Nil Radical

6.6n.1 Nil radical: The *nil radical* of a ring R is defined to be the radical ideal with respect to the property that “A 2-sided ideal is nil” and is denoted by $N(R)$, i.e., $N(R)$ is the largest 2-sided ideal of R such that every element of $N(R)$ is nilpotent.

Before we prove the existence of the nil radical, let us note the following special cases.

6.6n.2 Examples: 1. If R has no non-trivial nilpotent elements, in particular, R an integral domain, then $N(R) = (0)$.

2. If R is commutative, then the set $N(R)$ of all nilpotent elements of R which is an ideal, is the nil radical of R . (If R has 1, then $N(R)$ is the intersection of all prime ideals of R .)

3. If R is a nil ring, i.e., every element of R is nilpotent, then $N(R) = R$. For instance, $R = 2\mathbb{Z}/4\mathbb{Z}$ or $R =$ strictly upper triangular matrices over any ring.

4. $N(M_r(D)) = (0)$ for any division ring D because $R = M_r(D)$ is not a nil ring and it has no 2-sided ideals other than (0) and R . (Note that R has nilpotent elements if $r \geq 2$ but they do not form an ideal.)

6.6n.3 Theorem: For any ring R , the nil radical $N(R)$ exists and it is characterised by

$N(R) = \{a \in R \mid \text{the principal 2-sided ideal } (a) \text{ is a nil ideal}\}.$

Proof: We have to first prove that $N = N(R)$ as above is a 2-sided ideal and secondly that it is the largest for that property.

1. Since $0 \in N$, $N \neq \emptyset$. If $a \in N$ and $x \in R$, then $(xa) \subseteq (a)$ and $(ax) \subseteq (a)$ and so both (xa) and (ax) are nil ideals hence $ax, xa \in N$. Thus we have only to prove the following.

2. N is an additive subgroup of R .

To see this, for $a, b \in N$, we have to show that $(a - b)$ is a nil ideal. Since $(a - b) \subseteq (a) + (b)$, every element $x \in (a - b)$ can be written as $x = y + z$ for some $y \in (a)$ and $z \in (b)$. Since (a) and (b) are nil ideals, both y and z are nilpotent, say $y^n = 0$ and $z^n = 0$ for some $n \gg 0$. Now look at $x^n = (y + z)^n = y^n + z' = 0 + z'$ where z' is a sum of monomials in y and z in each of which z is a factor, i.e., $z' \in (z) \subseteq (b)$ and so z' is nilpotent and hence x is nilpotent, i.e., $(a - b)$ is a nil ideal, as required.

Finally, let I be any 2-sided nil ideal of R . Then trivially, $(a) \subseteq I$, $\forall a \in I$ and hence (a) is a nil ideal, i.e., $I \subseteq N$, as required. $\diamond$

6.6n.4 Corollary: *We have $N(R/N(R)) = (0)$ for any ring R .*

Proof: Let $\bar{a} = a + N \in N(R/N)$ where $N = N(R)$ and $a \in R$. Then the 2-sided principal ideal $(\bar{a})$ is a nil ideal in R/N , i.e., the 2-sided ideal (a) in R is nil modulo N . Hence it follows that (a) is a nil ideal in R (since N is a nil ideal), i.e., $a \in N$ and so $\bar{a} = 0$, i.e., $a \in N$, as required. $\blacksquare$

6.6j Jacobson Radical

6.6j.1 Jacobson radical : The *Jacobson radical* of a ring R with 1 is defined as the radical ideal of R with respect to the property that “A 2-sided ideal I is such that $1 - a$ is a unit in R for all $a \in I$ ” and it is denoted by $J(R)$. In other words, $J(R)$ is the largest 2-sided ideal of R such that $1 - a$ is a unit for all $a \in J(R)$.

Before we prove the existence of the Jacobson radical, let us note the following special cases.

6.6j.2 Examples: 1. $J(\mathbb{Z}) = (0)$.

2. $J(M_r(D)) = (0)$, $\forall r \in \mathbb{N}$ and D a division ring (since $M_r(D)$ has no 2-sided ideals other than (0) and $M_r(D)$ and the latter cannot be a candidate).

3. If R is a commutative local ring with its unique maximal ideal M , then obviously $J(R) = M$.

To prove the existence of the Jacobson radical, first we define the so called *left and right Jacobson radicals* $J_l(R)$ and $J_r(R)$ and show them to be equal. Secondly, we show that $J_l(R) = J_r(R) = J(R)$ is the one we are looking for.

6.6j.3 Left Jacobson radical: For any ring R with 1, the intersection of all maximal left ideals of R is called the *left Jacobson radical* or simply the *left radical* of R and is denoted by $J_l(R)$.

(In case R is commutative, $J_l(R)$ is the intersection of all maximal ideals of R .)

6.6j.4 Examples: 1. The left radical of a division ring is (0) . More generally, the left radical of $M_n(D)$ is (0) ($\forall n \in \mathbb{N}$) where D is a division ring.

2. The (left) radical of $\mathbb{Z}$ is (0) .

3. The (left) radical of a local ring is its unique maximal ideal.

4. The (left) radical of $\mathbb{Z}/n\mathbb{Z}$ is $m\mathbb{Z}/n\mathbb{Z}$ where m is the product of all distinct prime divisors of n . For instance, $J_l(\mathbb{Z}/36\mathbb{Z}) = 6\mathbb{Z}/36\mathbb{Z}$, $J_l(\mathbb{Z}/64\mathbb{Z}) = 2\mathbb{Z}/64\mathbb{Z}$ and $J_l(\mathbb{Z}/180\mathbb{Z}) = 30\mathbb{Z}/180\mathbb{Z}$.

6.6j.5 Theorem : For any ring R , its left radical $J_l(R)$ is the intersection of the annihilators of all simple left modules over R . In particular, $J_l(R)$ is a 2-sided ideal of R .

Proof: (1) If $\mathfrak{m}$ is a maximal left ideal of R , then $\mathfrak{m}$ is the annihilator of the non-zero element $\bar{1} = 1 + \mathfrak{m}$ in the simple R -module $S = R/\mathfrak{m}$.

(2) If S is a left simple R -module and $x \in S$ is a non-zero element, then $S = Rx$ and the natural map $f_x : R \rightarrow S$, defined by $f_x(a) = ax$, $\forall a \in R$ is an epimorphism whose kernel is the annihilator of the element x . Thus we have $R/\text{Ker}(f_x) \approx Rx = S$ which is simple and hence $M_x = \text{Ker}(f_x)$ is a maximal left ideal of R . This shows that the annihilator of any non-zero element of a simple module is a maximal left ideal of R . In other words, the family of all maximal left ideals of R is the same as that of the annihilators of non-zero elements of all simple left modules over R .

(3) The annihilator of any left module M is a 2-sided ideal of R and it is the intersection of the annihilators of all elements of M .

(4) If $\mathcal{M}$ is the set of all maximal left ideals of R and $\mathcal{L}$ is the family of all simple left modules over R , then we have $J_\ell(R) = \bigcap_{M \in \mathcal{M}} M$ which in turn can be written as

$$J_\ell(R) = \bigcap_{S \in \mathcal{L}} (\bigcap_{x \in S} M_x) = \bigcap_{S \in \mathcal{L}} \text{Ann}_R(S)$$

(where M_x is the annihilator of the element $x \in S$) and so $J_\ell(R)$ is the intersection of the family $\{\text{Ann}_R(S) \mid S \in \mathcal{L}\}$ of 2-sided ideals and hence 2-sided, as required. $\diamond$

6.6j.6 Proposition: *Given a ring R with its left radical $J_\ell(R)$, the left radical of the quotient $R/J_\ell(R)$ is zero, i.e., $J_\ell(R/J_\ell(R)) = (0)$.*

Proof: Let $\eta: R \rightarrow R/J_\ell(R)$ be the natural homomorphism. Then the assignment $M \mapsto \eta(M)$ is a bijection between the set $\mathcal{M}_R$ of all maximal left ideals of R and that of $R/J_\ell(R)$ since each $M \in \mathcal{M}_R$ contains $J_\ell(R)$. Hence it follows that

$$J_\ell(R/J_\ell(R)) = \bigcap_{M \in \mathcal{M}_R} \eta(M).$$

But then we have

$$\bigcap_{M \in \mathcal{M}_R} \eta(M) = \eta(\bigcap_{M \in \mathcal{M}_R} M) = \eta(J_\ell(R)) = (0). \quad \diamond$$

6.6j.7 Theorem: $J_\ell(R) = \{x \in R \mid 1 - yx \text{ is a unit, } \forall y \in R\}$.

Proof: $(\Rightarrow)$: Let $x \in J_\ell(R)$. For any $y \in R$, if $1 - yx$ has no left inverse in R , we can find a maximal left ideal M containing $1 - yx$. But then $1 = (1 - yx) + yx$ would be in M since M is a left ideal containing x and $1 - yx$ which is a contradiction. Let $z \in R$ be such that $z(1 - yx) = 1$. If this z has no left inverse, we can find another maximal left ideal M' containing z . But then M' contains z as well as x and hence it contains $1 = z(1 - yx) = z - zyx$ which is again a contradiction. Thus z is invertible whose inverse is $1 - yx$, i.e., $1 - yx$ is a unit, as required.

$(\Leftarrow)$: Let $x \in R$ be such that $1 - yx$ is a unit for all $y \in R$. If $x \notin J_\ell(R)$, then $x \notin M$ for some $M \in \mathcal{M}$. But then we get that $M + Rx = R$ and so we can write that $1 = z + ax$ for some $z \in M$ and $a \in R$ which means that $z = 1 - ax$ is invertible and is an element of the maximal left ideal M , a contradiction. Hence $x \in J_\ell(R)$. $\diamond$

6.6j.8 Theorem: $J_\ell(R)$ is the largest left ideal of R such that $1 - a$ is a unit for every $a \in J_\ell(R)$.

Proof: By the theorem above, it is obvious that $1 - x$ is a unit for all $x \in J_\ell(R)$. Let now I be a left ideal of R such that $1 - a$ is a unit for every $a \in I$. Let $x \in I$ and $y \in R$. then $yx \in I$ since I is a left ideal of R . But then by assumption $1 - yx$ is a unit (no matter what y is) and so $x \in J_\ell(R)$, i.e., $I \subseteq J_\ell(R)$, as required. $\diamond$

6.6j.9 Right Jacobson radical: For any ring R with 1, the intersection of all maximal right ideals of R is called the *right Jacobson radical* or simply the *right radical* of R and is denoted by $J_r(R)$.

6.6j 10 Remarks: Proceeding as above, we can prove that $J_r(R)$ has the following properties.

1. $J_r(R)$ is a 2-sided ideal of R .
2. $J_r(R) = \{x \in R \mid 1 - xy \text{ a unit, } \forall y \in R\}$.
3. $J_r(R)$ is the largest right ideal of R such that $1 - b$ is a unit for all $b \in J_r(R)$.

6.6j.11 Theorem: For any ring R , the left and right Jacobson radicals coincide and the 2-sided ideal $J(R) = J_\ell(R) = J_r(R)$ is the Jacobson radical of R . In particular, the Jacobson radical of a local ring is its (unique) maximal ideal.

Proof: We have $J_r(R) \subseteq J_\ell(R)$ since $J_r(R)$ (being 2-sided) is also a left ideal such that $1 - a$ is a unit for all $a \in J_r(R)$. Similarly, $J_\ell(R) \subseteq J_r(R)$, as required. $\diamond$

6.6j.12 Proposition: For any ring R , $N(R) \subseteq J(R)$ and equality need not hold.

Proof: Let $a \in N(R)$. Since $N(R)$ is a nil ideal, a is nilpotent, say $a^n = 0$ for some $n \in \mathbb{N}$. Now we have $1 = 1 - a^n = (1 - a)(1 + a + a^2 + \cdots + a^{n-1})$ implying that $1 - a$ is a unit in R and so $a \in J(R)$, as required. $\diamond$

Note : For the local ring $\mathbb{Q}^p = \{a/b \in \mathbb{Q}, (p, b) = 1\}$ where p is a fixed prime number, we have $N(\mathbb{Q}^p) = (0)$ whereas $J(\mathbb{Q}^p) = (p) \neq (0)$.

6.6j.13 Nakayama Lemma: If M is a finitely generated module over a ring R such that $J(R)M = M$, then $M = (0)$.

(Recall (2.5.3) that for any subset A of R , the set AM stands for the submodule of M generated by elements of the form ax for all $a \in A$ and $x \in M$.)

Proof : Suppose M is generated by $X = \{x_1, x_2, \dots, x_r\}$, a finite subset of M . We may assume that X is a minimal set of generators in the sense that no proper subset of X generates M . Since $J = J(R)$ is a right ideal of R , we find that JM is the submodule of M generated by $\{ax_i \mid \forall a \in J, 1 \leq i \leq r\}$. Since $x_1 \in M = JM$ and J is a left ideal, we can write $x_1 = \sum_{i=1}^r a_i x_i$ for some $a_i \in J, 1 \leq i \leq r$. This gives $(1 - a_1)x_1 = \sum_{i=2}^r a_i x_i$. Since $a_1 \in J$, $(1 - a_1)$ is a unit in R and so by multiplying on the left with $b_1 = (1 - a_1)^{-1}$, we get $x_1 = \sum_{i=2}^r b_1 a_i x_i$ which means that x_1 is an R -linear combination of the x_i 's, $2 \leq i \leq r$, i.e., the proper subset $X' = \{x_i, 2 \leq i \leq r\}$ of X generates M , a contradiction and so $X = \emptyset$, i.e., $M = (0)$. $\diamond$

6.6j.14 Remark: The assumption that M is finitely generated is necessary in the Nakayama lemma. For instance, we have $J(\mathbb{Q}^p)\mathbb{Q} = (p)\mathbb{Q} = \mathbb{Q}$ but $\mathbb{Q} \neq (0)$ because $\mathbb{Q}$ is not finitely generated over $\mathbb{Q}^p$ (see (5.9.7) above). $\blacksquare$

6.7 Radical of an Artinian Ring

6.7.1 Proposition: *The Jacobson radical of an Artinian ring is the intersection of some finitely many maximal left (resp., right) ideals.*

Proof: Let R be an Artinian ring. Let $\mathcal{M}$ be the set of all maximal left ideals of R . Let $\mathcal{F}$ be the family of all left ideals of R each of which is an intersection of finitely many maximal left ideals of R . Obviously this family is non-empty since $\mathcal{M} \subseteq \mathcal{F}$. Since R is Artinian, $\mathcal{F}$ has a minimal member, say $J_0 = \bigcap_{i=1}^n M_i, M_i \in \mathcal{M}$. We have $J \subseteq J_0$ where $J = J(R)$. On the other hand, if $M \in \mathcal{M}$, then $J_0 \cap M$ being a member of $\mathcal{F}$ must be equal to J_0 by the minimality of J_0 which means that $J_0 \subseteq M, \forall M \in \mathcal{M}$. Thus we get that $J \subseteq J_0 \subseteq \bigcap_{M \in \mathcal{M}} M = J$ and hence $J = J_0$, as required. $\diamond$

6.7 2 Theorem: *The Jacobson radical of an Artinian ring R*

is nilpotent. In fact, $J(R)$ is the largest nilpotent (left or right or 2-sided) ideal of R and consequently, $N(R) = J(R)$.

Proof: Since R is Artinian, the descending chain of ideals

$$J \supseteq J^2 \supseteq \dots \supseteq J^n \supseteq \dots \supseteq \dots$$

is stationary where $J = J(R)$. Say, $J^m = J^{m+1} = \dots =$ for some $m \gg 0$. Write $I = J^m$. Now we have $I = I^2$ and $JI = I$. (If we know that I is finitely generated then Nakayama lemma would have implied that $I = (0)$ which is what we are looking for. But there seems no way to ensure this crucial fact.) The following is an elementary but a subtle argument to achieve the goal.

Assume, if possible, that $I \neq (0)$. Consider the family $\mathcal{F}$ of all left ideals K of R such that $IK \neq (0)$. Since $I^2 = I \neq (0)$, $I \in \mathcal{F}$ and so $\mathcal{F} \neq \emptyset$. Note that $(0) \notin \mathcal{F}$. Since R is Artinian, $\mathcal{F}$ has a minimal member, say K , i.e., K is a left ideal of R such that $IK \neq (0)$ and K is minimal for this property. On the other hand, since $IK \neq (0)$, we can find $a \in I$ and $b \in K$ such that $ab \neq 0$ which implies that $I(Rb) \neq (0)$, i.e., $Rb \in \mathcal{F}$. But $Rb \subseteq K$ and so $Rb = K$ by minimality of K . Thus K is a principal left ideal of R .

Finally, we have $(IJ) \cdot Rb = I \cdot Rb = Ib \neq (0)$ and $J \cdot Rb = J \cdot b \subseteq Rb$ and $J \cdot Rb \neq (0)$ which give, (again by minimality of $K = Rb$ in $\mathcal{F}$), that $J \cdot Rb = Rb$. Now Nakayama lemma gives that $K = Rb = (0)$, a contradiction to the assumption that $I \neq (0)$. Hence $I = J^n = (0)$. $\diamond$

6.7.3 Corollary: *In an Artinian ring, every nil ideal is nilpotent (since such an ideal is contained in the radical which is nilpotent).*

6.7.4 Theorem: *There are only finitely many maximal ideals in a commutative Artinian ring, i.e., it is a semi-local ring.*

Proof: Let R be Artinian. We know by (6.7.1) above, that $J = J(R)$ is an intersection of finitely many maximal ideals, say

$$J = \bigcap_{i=1}^n M_i \supseteq M_1 \cdot M_2 \cdots M_n.$$

Claim: *The only maximal ideals of R are the M_i 's, $1 \leq i \leq n$.*

For, since J is nilpotent, we have $J^r = (0)$ for some $r \in \mathbb{N}$ and

$$(0) = J^r \supseteq (M_1 \cdot M_2 \cdots M_n)^r = M_1^r \cdot M_2^r \cdots M_n^r.$$

If M is any maximal ideal of R , then $M \supseteq (0) = M_1^r \cdot M_2^r \cdots M_n^r$ and hence $M \supseteq M_i^r$, for some i ($1 \leq i \leq n$). But then $M \supseteq M_i$ (because M is a prime ideal). Now both being maximal, it follows that $M = M_i$, as required. $\diamond$

6.7.5 Remark: We have seen examples of Artinian modules which are not Noetherian and vice-versa and some which are neither. On the other hand, there are Noetherian rings which are not Artinian and some which are neither. However, it is a remarkable fact that

“EVERY ARTINIAN RING IS NOETHERIAN”.

We shall first prove this in the commutative case and offer a comment about the other case. We begin with the following easy but crucial step.

6.7.6 Theorem: *Let R be a commutative local ring whose maximal ideal is nilpotent. Then R is Artinian if and only if it is Noetherian.*

Proof: Let M be the maximal ideal of R with $M^r = (0)$. Let $K = R/M$ be the residue field of R . It is obvious that R is Artinian (resp. Noetherian) if and only if M is so. Now M is Artinian (resp. Noetherian) if and only if both M/M^2 and M^2 are so, etc. Secondly, since M annihilates M^i/M^{i+1} , it is a vector space over the field K and the R -module structure is the same as the vector space structure. But then we know that M^i/M^{i+1} is Artinian (resp. Noetherian) if and only if M^i/M^{i+1} is finite dimensional over K .

Suppose R is Artinian (resp. Noetherian). Then M^i/M^{i+1} is Artinian (resp. Noetherian) and hence finite dimensional over K , for all $i = 0, 1, \dots, r-1$. Consequently, each is Noetherian (resp. Artinian). Now $M^{r-1} = M^{r-1}/M^r$ and M^{r-2}/M^{r-1} are both Noetherian (resp. Artinian) implies that M^{r-2} is Noetherian (resp. Artinian), etc. Proceeding thus we get that M is Noetherian (resp. Artinian). $\diamond$

6.7.7 Example of a commutative local ring R whose maximal ideal is nilpotent but R is not Artinian (hence not Noetherian).

Let K be a field and $R = K[X_i, i \in \mathbb{N}]/M^2$ where M is the ideal generated by $X_i, i \in \mathbb{N}$. The maximal ideal of R is of square 0 and is infinite dimensional over its residue field K .

6.7.8 Theorem : *A commutative Artinian ring is Noetherian and conversely a commutative Noetherian ring in which every prime ideal is maximal is Artinian.*

Proof: Let R be a commutative Artinian ring. By (6.7.4) above, R is semi-local with its maximal ideals, (say) $M_1, \dots, M_n$ and $(0) = J^r = M_1^r \dots M_n^r$. Since the maximal ideals M_i are pairwise coprime, their powers M_i^r are also pairwise coprime, by Ex.(2.9.25) above. Consequently, by the Chinese Remainder Theorem, Ex.(3.6.6) above, we get that $R \simeq R/M_1^r \times \dots \times R/M_n^r$. Since each R/M_i^r is Artinian local ring whose maximal ideal, i.e., M_i/M_i^r , is nilpotent, it follows that it is Noetherian (by (6.7.6) above). Thus R is a finite direct product of Noetherian rings, as required.

Conversely, suppose R is Noetherian in which every prime ideal is maximal. Then each maximal ideal is also a minimal prime ideal and so it is semi-local (by (6.5.15) above). Furthermore, we have $(0) = M_1^{\epsilon_1} \dots M_r^{\epsilon_r}$ for some maximal ideals M_i and $\epsilon_i \in \mathbb{N}$, etc. But then it follows that $R \simeq R/M_1^{\epsilon_1} \times \dots \times R/M_r^{\epsilon_r}$ from where the argument is identical with the above. $\diamond$

6.7.9 Remark: The idea of the proof in the non-commutative Artinian case is just the same as above except for a little formalism required from the semi-simple rings (Ex.(5.10.21) above), to prove the crucial facts that both J and R/J are Noetherian (using of course that J is nilpotent).

We note that there is no parallel for the converse part of (6.7.8) in the non-commutative case. $\blacksquare$

6.8 Exercises

R stands for a ring with 1, commutative or not (unless specified otherwise) and J stands for its Jacobson radical. A module means a unitary R -module.

- Let P and Q be submodules of a module M such that both M/P and M/Q are Artinian (resp. Noetherian). Show that $M/(P \cap Q)$ and $M/(P + Q)$ are Artinian (resp. Noetherian). (Hint: Realise the first as a submodule and the other as a quotient of $M/P \times M/Q$, via maps $x \mapsto (x+P, x+Q)$ and $(x+P, y+Q) \mapsto (x+y)+(P+Q)$, $\forall x, y \in M$.)
- Let M be a Noetherian R -module with its annihilator ideal $I = \text{Ann}_R(M)$. Show that R/I is a Noetherian ring. (Hint: Realise R/I as a submodule of M^n if M is generated by n elements.)
Give an example to show that the above need not be true for the Artinian case. (Try $M = \mu_{p^n}$ (6.2.9).)
- Show that a monomorphism $f \in \text{End}_R(M)$ of an Artinian module M is an automorphism. (Hint: Look at the descending chain of submodules $f^n(M)$, $n \in \mathbb{N}$.) However, give an example to show that it is not true for the Noetherian case.
- Give an example of a finitely generated 2-sided ideal I in a ring R such that R/I is Artinian (resp. Noetherian) but R is not. (Hint: Use a construction similar to Ex.(1.13.1).)
However, show that R is Artinian (resp. Noetherian) if I is nilpotent. (Hint: For each i , I^i/I^{i+1} is Artinian (resp. Noetherian).)
- Give an example of a ring R and an element which has a left inverse but not a unit. (Try $\text{End}_D(V)$ for an infinite dimensional vector space V over a division ring D .)
However, show that such a thing is not possible in a left Noetherian ring. (Hint: If $ab = 1 \neq ba$, then $\{e_i \mid i \in \mathbb{N}\}$ is an infinite set of pairwise orthogonal idempotents where $e_i = b^{i-1}a^{i-1} - b^i a^i$. Now use Ex.(5.10.14) to deduce that $\{R(e_1 + \cdots + e_n) \mid n \in \mathbb{N}\}$ is ascending but not stationary.)
- Give an example to show that $\sqrt{I}$ (2.9.10) need not be finitely generated if the ideal I is finitely generated (in a commutative ring).
- If $\sqrt{I}$ is finitely generated, show that $\sqrt{I}^n \subseteq I$ for some $n \in \mathbb{N}$. Hence, the nil radical of a commutative Noetherian ring is nilpotent.

8. Show that for a Boolean ring R , the following are equivalent.
 - R is Artinian.
 - R is Noetherian.
 - R is a finite Cartesian power of the field of 2 elements.
9. Suppose that all the coefficients of an element $f(X) \in R[[X]]$ are nilpotent where R is a commutative Noetherian ring. Then show that $f(X)$ is nilpotent. (Hint: Same as for Ex.(1.13.13) above.)
10. Show that the localisation R_P (3.6.17) of a commutative Noetherian integral domain R at any prime ideal P is Noetherian.
11. Let R be a commutative Noetherian local ring with its maximal ideal M . Show that $I = \bigcap_{i=1}^{\infty} M^i = (0)$. (Hint: Apply Nakayama to I .)
12. Show that for any simple R -module S , (R commutative or not), $JS = (0)$. (Hint: Apply Nakayama to S if $JS = S$.)
13. Let N be a submodule of a finitely generated R -module M such that $M = N + JM$. Then show that $N = M$. (This is another version of Nakayama lemma.) (Hint: Apply Nakayama to M/N .)
14. Show that R is Noetherian if and only if $R[[X]]$ is. (Hint: Imitate the proof of Hilbert Basis Theorem (6.5.6) replacing "leading coefficient" by "coefficient of lowest degree term".)
15. Let $R = \left\{ \begin{pmatrix} m & 0 \\ x & y \end{pmatrix} \mid m \in \mathbb{Z} \text{ and } x, y \in \mathbb{Q} \right\}$. Show that R is a left Noetherian ring but not right Noetherian.
 (Hint: Show that $I = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \mid x \in \mathbb{Q} \right\}$ is a minimal left ideal and that $R/I = \left\{ \begin{pmatrix} m & 0 \\ x & 0 \end{pmatrix} \mid m \in \mathbb{Z} \text{ and } x \in \mathbb{Q} \right\}$ is Noetherian. Furthermore, show that $\{I_n, n \in \mathbb{N}\}$ is a non-stationary ascending chain of right ideals where $I_n = \left\{ \begin{pmatrix} 0 & 0 \\ m/2^n & 0 \end{pmatrix} \mid m \in \mathbb{Z} \right\}$.)
16. Let $R = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{Q} \right\}$. Show that R is a left Artinian ring but not right Artinian. (Note that R is without 1.)
 (Hint: Show that $I = \left\{ \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{Q} \right\}$ is a minimal left ideal and that $R/I = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \mid x \in \mathbb{Q} \right\}$ is Artinian. Furthermore, show that

$\{I_n, n \in \mathbb{N}\}$ is a non-stationary descending chain of right ideals where
 $I_n = \left\{ \begin{pmatrix} 0 & 0 \\ 2^n m & 0 \end{pmatrix} \mid m \in \mathbb{Z} \right\}.$

17. Let R be a ring of finite length, viz., $R = M_n(D)$ where D is a division ring. Let M be a free R -module having a finite basis B . Then show that M is a module of finite length and $\ell_R(M) = \ell_R(R) \cdot \text{Card}(B)$. Deduce that any other basis C for M also must be finite and $\text{Card}(C) = \text{Card}(B)$, i.e., any two bases of a finitely generated free $M_n(D)$ -module have the same cardinality.
18. Show that a semi-simple (5.10.21) ring is of finite length. However, for a prime number p , show that $\mathbb{Z}_p$ is a ring of finite length but not semi-simple.
19. Show that the following are equivalent for a semi-simple module M .
 - M is finitely generated.
 - M is Artinian.
 - M is Noetherian.
 - M is of finite length.
20. Let $R[G]$ be the group ring (Ex.(5.10.38)) over R of a finite group G . Show that $R[G]$ is a ring of finite length (6.3.8) if R is one such.
21. Let K be a field and $K[G]$ be as above. Let $f \in \text{End}_K(K[G])$, i.e., f is a K -linear endomorphism of $K[G]$ as a vector space over K . Let $\tilde{f} = \sum_{x \in G} \ell_{x^{-1}} \circ f \circ \ell_x$ where ℓ_y stands for the left multiplication in $K[G]$ by χ_y for $y \in G$. Show that
 - $\tilde{f} \in \text{End}_{K[G]}(K[G])$, in fact, $\tilde{f} = r_z$, the right multiplication by $z = \sum_{x \in G} \chi_{x^{-1}} f(\chi_x)$ and
 - $\tilde{f} = nf$ if $f \in \text{End}_{K[G]}(K[G])$ where n is the order of G .
22. Prove Maschke's theorem that $K[G]$ is semi-simple (5.10.21) if and only if the characteristic of K is either 0 or a prime p not dividing n . (Hint: If I is a left ideal of $K[G]$ and f is a K -linear projection (5.10.9) of $K[G]$ onto I , then $(1/n)f$ is a $K[G]$ -linear projection of $K[G]$ onto I . Use Ex.(5.10.44) for the converse.)
23. Show that $K[G]$ is semi-simple if and only if $K[H]$ is so for every subgroup (resp. Sylow subgroup) H of G .

24. Show that the ring of real valued continuous functions on the closed interval $[0,1]$ is neither Artinian nor Noetherian.
25. Let R be a commutative integral domain with 1. Then R is a PID if and only if
- R is Noetherian and
 - $\gcd(a,b)$ exists and $(\gcd(a,b)) = (a) + (b)$, $\forall a,b \in R^*$.
- (See also (4.5.7) above.)
26. Do Ex.(4.7.31) above (using the existence of $\gcd$). ■

6.9 True/False Statements

Determine which of the following statements are true (T) or false (F) or partially true (PT). Justify your answers by giving a proof if (T) or a counter-example if (F)/(PT) and supplying the additional hypothesis needed to make it (T) (along with a proof) if (PT), as the case may be. (Here R stands for a ring with 1, commutative or not.)

1. If a ring R is Artinian, then $R[X]$ is Artinian.
2. If a ring R is Noetherian, then $R[X]$ is Noetherian.
3. If a ring R is Artinian, then $R[[X]]$ is Artinian.
4. If a ring R is Noetherian, then $R[[X]]$ is Noetherian.
5. Minimal submodules exist in a module of finite length.
6. Direct sum of two modules is of finite length if and only if each is.
7. The length of a finite Cartesian product of modules of finite length is the product of their lengths.
8. A module of finite length is finitely generated.
9. A finitely generated module over a PID is Noetherian.
10. A finitely generated module over $M_n(\mathbb{C})$ is both Artinian and Noetherian.
11. Homomorphic image of a module of finite length is Noetherian.
12. Subring of a Noetherian ring is Noetherian.
13. Subring of an Artinian ring is Artinian.
14. A quotient of a ring of finite length is both Artinian and Noetherian.

15. Minimal submodules exist in a finitely generated module over an Artinian ring.
16. Minimal submodules exist in a finitely generated module over a Noetherian ring.
17. Minimal and maximal submodules exist in a module of finite length.
18. In an Artinian ring, every prime ideal is maximal.
19. In a commutative Artinian ring, every prime ideal is maximal.
20. A finite ring is a ring of finite length.
21. The length of a finite ring is the number of its non-zero elements.
22. A ring of finite length is a finite ring.
23. A finite ring is a semi-simple ring.
24. The ring $\text{End}_D(V)$ is Noetherian but not Artinian (where V is a vector space over a division ring D).
25. A free module over $M_n(\mathbb{Q})$ has all its bases of the same cardinality.
26. Matrix rings over rings of finite length are rings of finite length.
27. If a module M has a submodule N such that N and M/N are simple, then M is semi-simple.
28. Sum of an infinite family of distinct Artinian (resp. Noetherian) submodules (of a module) could be one such.
29. Direct sum of an infinite family of distinct Artinian (resp. Noetherian) submodules cannot be one such.
30. The Jacobson radical of a Noetherian ring is nilpotent.
31. The nil and Jacobson radicals of an Artinian ring are equal. ■

Answers to True/False Statements

T = True, F = False and P = Partially True

Chapter 1 : Section 1.14

? T F T F F T T F T F F T T F F T F P T F T F T F T ?

Chapter 2 : Section 2.10

F P T F P F T F F T F T T T T F T F T F T F F T F

Chapter 3 : Section 3.7

P F F P F T F T F T T F T T T F T T F T T T T T F T T F T

Chapter 4 : Section 4.8

T T F T F T T F T T F T T T F F F F T F T F F P T F F T F T F F T
T

Chapter 5 : Section 5.11

F T F T F T F T F T T F T F F F T T F F F T T T T T P T T F T T
F T F

Chapter 6 : Section 6.9

F T F T T T F T T T T F F T T F T P T T F F F F T T F T T F T

Index

A

a.c.c 154
abelian group 4
 Lie ring 30
addition 3
additive identity 4
 inverse 4
 of fractions 78
 of ideals 48
adjoint of a matrix 15
algorithm map 93
Amitsur radical 170
annihilator 132
anti-homomorphism 117
anti-isomorphism 118
anti-symmetric order 35
Artinian module 152
Artinian ring
ascending chain condition 154
associate 89
author's devil viii
automorphism of a module 134
 of a ring 68

B

basis 123
binary operation 3
Boolean ring 19
bounded above 35

below 35

Brown-McCoy radical 170

C

Cayley numbers 10
Cartesian product 22
central subfield 82
 subrig 82
centre of a ring 7
 of a Lie ring 30
chain condition, ascending 154
 descending 151
chain or totally ordered 35
Chinese Remainder thm. 83,
 179
characteristic function 70, 147
 of a ring 24
 of a Lie ring 30
 of a local ring 59
cofactor 15
Cohen's theorem 168
comaximal ideals 62
commutative ring 5
commutator 29
 of derivations 86
Complex entire functions 22
composition series 158
conjugacy class 148
conjugate of a quaternion 9

constant term 16
 content of a polynomial 103
 continuous function 10
 coprime elements 92
 ideals 62, 179
 cyclic module 147
 submodule 122

D

d.c.c 151
 degree of polynomial 16
 map 94
 dense 64
 derivation 86
 descending chain condition 151
 diagonal matrix 14
 dimension of a free module 133
 of a vector space 125
 direct product of rings 22
 product of modules 120
 sum of modules 121
 summand 121
 distributive laws 3
 divide 89
 dividend 93
 division algorithm 93
 ring 7
 ring of left quotients 80
 divisor 89, 93

E

Eisenstein's Criterion 106
 elementary divisors 143
 theorem 143
 endomorphism of a module 134
 of a ring 68
 epimorphism of modules 134
 of rings 68

 theorem for modules 135
 for rings 70
 equivalence relation 77
 Euclidean domains 92
 Euler's totient function 20

F

factorisation domains 99, 169
 factor 89
 field 54
 of fractions 79
 of meromorphic functions 80
 of rational functions 80
 filtration 158
 finite rank 76
 support 70
 finitely generated ideal 41
 module 122, 164
 finiteness condition 154
 fraction 78
 free module 123
 Frobenius map 84
 fundamental thm. of Arithmetic
 89
 thms. of homomorphisms
 70, 135

G

Gauss' lemma 104
 theorem 105
 Gaussian integers 21, 94
 Gaussian numbers 21
 generic point 64
 greatest common divisor 91
 group 3
 abelian 3
 of quaternions 21
 ring 148

H

Hilbert basis theorem 165
homomorphism 57, 67, 75, 117,
 144
 local 86
 of groups 90
 unitary 67
homothecy 137, 147

I

ideals 33, 34, 41, 48, 53,
ideal generated by 39
idempotent 5, 44, 53
identity matrix 14
integers modulo n 23
integral domain 7, 54
 quaternions 21
invariants 143
inverse 4
invertible element 5
irreducible element 90
isomorphism of modules 34
 of rings 68

J

Jacobi identity 30
Jacobson radical 170, 172, 173,
 175
Jordan–Hölder filtration 158
 theorem 161

K

kernel of a homomorphism 67,
 133

L

Laurent polynomial ring 18
Laurent series ring

leading coefficient 16
least common multiple 92
left annihilator 44
 Artinian ring 163
 ideal 33
 generated by 39
 identity 44
 Jacobson radical 172, 175
 module 115
 Noetherian ring 164
 zero-divisor 5
length of a composition series
 158
 of a module 162
Levitzki radical 170
Lie product 29
 ring 29
 subring 30
linear homomorphism 133
 independence 122
 transformations 115
local homomorphism 86
 ring 57
localisation 85
lower bound 35

M

Maschke's theorem 182
maximal element 35
 left ideal 34
 right ideal 34
 submodule 137, 155
 subring 34
 2-sided ideal 34
maximum condition 154, 164
minimal element 35
 left ideal 34

- right ideal 34
- submodule 137, 155
- 2-sided ideal 34
- minimum condition 151, 163
- module 115
 - of finite length 159
- modules over PID's 139
- monic polynomial 16
- monogenic module 147
 - submodule 122
- monomorphism of modules 133
 - of rings 68
- multiplication 3
 - of fractions 78
- multiplicative cancellation 8
 - identity 4
 - inverse 5

N

- Nakayama lemma 176
- nil ideal 50, 170
 - radical 170
- nilpotent coset 53
 - element 5
 - ideal 50, 177
- Noetherian modules 155
 - rings 101

O

- opposite ring 34
- orbit 90
- order of power series 18, 95
- Ore domains 80
- orthogonal idempotents 6
 - projections 144

P

- partial order 35

- partition of unity 144
- pathologies 6, 126, 157
- polynomial 16
 - part 18
- poset 35
- power of an ideal 50
 - series part 18
 - set 19
- prime element 90
 - field 83
 - ideal 37, 62
 - spectrum 63
 - subring 25
- primitive polynomial 103
- principal left ideal 40
 - ideal domain PID 41, 96
 - ring PIR 41
 - right ideal 40
 - 2-sided ideal 41
 - part 18
- product of ideals 49
- projection 182

Q

- quaternion group 21
- quaternions 8, 9, 21, 29
- quotient 93
 - group 132
 - module 132
 - rings 52
 - of a quotient 71, 136
 - of a sum 136

R

- radical ideal 170
 - of an ideal 60
- rank of a free module 133
 - module over a PID 142

rational quaternions 9
 real quaternions 8
 reflexivity 77
 remainder 93
 residue field 54, 109
 ring 52
 right ideal 33
 identity 44
 Jacobson radical 175
 module 116
 zero-divisor 5
 ring 3
 of endomorphisms 75, 116,
 167, 180
 of Complex entire functions
 22
 of continuous functions 11
 of matrices 14
 of p -adic integers 22, 70
 of polynomials 16, 23
 of power series 17, 23
 opposite to 24, 34

S

scalar matrix 14
 multiplication 115
 scalars 116
 Schur's lemma 138
 semi-group 4
 semi-local ring 59
 semi-simple module 146
 ring 146
 simple module 138, 158
 quotient 158
 ring 47
 skew-field 7
 smooth function 13, 29

square root of an ideal 60
 standard basis 123
 stationary 151, 154
 structure thm. for Boolean rings
 20
 subgroup generated by 39
 submodule 119
 subring 6
 generated by 39
 sum of ideals 48
 of submodules 120
 summand 121
 supplement 122
 symmetric difference 19
 symmetry 77

T

torsion element 140
 module 140
 part of a module 141
 totally ordered or chain 35
 transitive order 35
 transitivity 78
 trivial coset 51
 ideals 34
 idempotent 5
 module 116
 multiplication 6
 nilpotent 5
 ring 6
 subrings 6
 zero-divisor
 two sided ideal 33

U

unique factorisation domain 101
 unit 5
 ideal 34

unitary homomorphism 67
 module 116
unity 4
universal Boolean ring 20
upper bound 35
 triangular matrix (strict) 27

V

vector space 124

W

Weierstrass' theorem 170

Z

Zariski topology 64, 86

zero element 4

 ideal 34

 module 116

 ring 6

zero-divisor 5, 53

Zorn's lemma 35

Introduction to **RINGS AND MODULES**

Second Revised Edition

C. Musili

School of Mathematics & Computer/Information Sciences
University of Hyderabad
Hyderabad, India

This book is a self-contained elementary introduction to Rings and Modules, a topic constituting about half of a core course on Algebra.

The proofs are treated with full details retaining the class room flavour. The entire material including exercise is fully class tested. True/False statements are meant for a quick test of understanding of the main text.

Narosa Publishing House

NEW DELHI MADRAS BOMBAY CALCUTTA

ISBN 978-81-7319-037-7