A COURSE IN
ABSTRACT ALGEBRA
(Second Revised Edition)

VIJAY K KHANNA
Department of Mathematics
Kirori Mal College
University of Delhi

S K BHAMBRI
Department of Mathematics
Kirori Mal College
University of Delhi

VIKAS PUBLISHING HOUSE PVT LTD

VIKAS PUBLISHING HOUSE PVT LTD
576, Masjid Road, Jangpura, **New Delhi** - 110 014
Phones: 4314605, 4315313 • Fax: 91-11-4310879
E-mail: ***orders@vikas.gobookshopping.com***
First Floor, N.S. Bhawan, 4th Cross, 4th Main,
Gandhi Nagar, **Bangalore**-560 009 • Phone : 2204639

F-20, Nand Dham Industrial Estate, Marol,
Andheri (East), **Mumbai**-400 059 • Phone : 8502333, 85023

35, Palm Avenue, **Kolkata**-700 019 • Phone : 2872575

A-26, 4th floor, Nelson Chambers, Nelson Manickam Road,
Aminjikarai, **Chennai**-600 029
Distributors:
UBS PUBLISHERS' DISTRIBUTORS LTD
5, Ansari Road, **New Delhi**-110 002
Ph. 3273601, 3266646 • Fax : 3276593, 3274261
E-mail: orders@gobookshopping.com • Internet: www.gobookshopping.com
• 10, First Main Road, Gandhi Nagar, **Bangalore**-560 009 • Ph. 2263901
• 6, Sivaganga Road, Nungambakkam, **Chennai**-600 034 • Ph. 8276355
• 8/1-B, Chowringhee Lane, **Kolkata**-700 016 • Ph. 2441821, 2442910
• 5-A, Rajendra Nagar, **Patna**- 800 016 • Ph. 672856, 656169
• 80, Noronha Road, Cantonment, **Kanpur**-208 004 • Ph. 369124, 362665

Distributors for Western India:
PREFACE BOOKS
223, Cama Industrial Estate, 2nd Floor,
Sun Mill Compound, Lower Parel (W), **Mumbai**-400 013

Second Revised Edition 1998
Reprint 2002

Copyright © Vijay K Khanna & S K Bhambri, 1993

"No part of this publication which is material protected by this copyright notice may be reproduced or transmitted or utilized or stored in any form or by any means now known or hereinafter invented, electronic, digital or mechanical, including photocopying, scanning, recording or by any information storage or retrieval system, without prior written permission from the publisher."

All rights reserved. No part of this publication may be reproduced in any form without the prior written permission of the publishers.

Information contained in this book has been published by VIKAS Publishing House Pvt. Ltd. and has been obtained by its authors from sources believed to be reliable and are correct to the best of their knowledge. However, the publisher and its authors shall in no event be liable for any errors, omissions or damages arising out of use of this information and specifically disclaim any implied warranties or merchantability or fitness for any particular use.

Printed at Kumar Offset Printers, Delhi - 110 031

Contents

	Preface to the second edition	*ix*
	Preface to the first edition	*x-xi*
	Glossary of Symbols	*xii*
Chapter 1	**Preliminaries**	**1-39**
	Sets	1
	Subsets	2
	Relations	4
	Equivalence Classes	6
	Mappings or Functions	7
	Binary Compositions	11
	Permutations	12
	Cyclic Permutations	15
	Cycles of a Permutation	16
	Disjoint Permutations	18
	Some Results From Number Theory	23
	Prime Numbers	33
	Composite Numbers	34
	Congruences	34
Chapter 2	**Groups**	**40-86**
	Semi groups	49
	Subgroups	57
	Cyclic Groups	71
Chapter 3	**Normal Subgroups, Homomorphisms, Permutation Groups**	**87-137**
	Quotient Groups	95
	Homomorphisms – Isomorphisms	100
	The Dihedral Group	118

	Permutation Groups	123
	Generators of a Subgroup	133
	Cummutator	135
Chapter 4	**Automorphisms and Conjugate Elements**	**138-170**
	Inner Automorphism	140
	Characteristic Subgroups	147
	Conjugate Elements	152
	Similar Permutations	164
Chapter 5	**Sylow Theorems and Direct Products**	**171-219**
	Sylow *p*-subgroups	174
	Double Cosets	176
	Direct Products	199
	Finite Abelian Groups	209
Chapter 6	**Rings**	**220-252**
	Sub Rings	229
	Characteristic of a Ring	235
	Ideals	240
	Sum of Ideals	242
	Product of Ideals	246
Chapter 7	**Homomorphisms and Imbedding of Rings**	**253-286**
	Quotient Rings	253
	Homomorphisms	255
	Imbedding of Rings	264
	More On Ideals	274
	Maximal Ideals	277
Chapter 8	**Euclidean and Factorization Domains**	**287-349**
	Euclidean Domains	290
	Prime & Irreducible Elements	301
	Polynomial Rings	308
	Unique Factorisation Domains	324
Chapter 9	**Vector Spaces**	**350-398**
	Subspaces	352
	Sum of Subspaces	353
	Quotient Spaces	356

Homomorphisms Of Linear Transformations 357
Linear Span 365
Linear Dependence and Independence 367
Inner Product Spaces 386
Norm of a vector 389
Orthogonality 392
Orthonormal Set 392

Chapter 10 **Linear Transformations** **399-446**

Algebra Of Linear Transformations 402
Invertible Linear Transformations 410
Matrix of a Linear Transformation 415
Dual Spaces 425

Chapter 11 **Eigen Values and Eigen Vectors** **447-496**

Annihilating Polynomials 467
Invariant Subspaces 437
Direct Sum Decomposition 483
Invariant Direct Sums 487
Primary Decomposition Theorem 492

Chapter 12 **Fields** **497-595**

Algebraic Extensions 501
Roots of Polynomials 511
Splitting Fields 516
Ruler and Compass Constructions 525
Prime Subfields 531
Separable Extensions 533
Normal Extensions 540
Algebraically Closed Fields 545
Automorphisms of Field Extensions 556
Galois Extensions 567
Roots of Unity 576
Finite Fields 587

Index **597**

Preface to the Second Edition

Just as the old must make way for the young, first editions would always get replaced by second and subsequent editions. In fact, the revision for the first edition had started the day it hit the stands. The last chapter on Fields needed expansion and we have added seventy odd pages covering a wide range of topics in the hope of giving a better 'filled up' look to this chapter. Besides adding these new topics it has more or less been an attempt at smoothening the rough edges and trying to bring out a well chiselled form of the first edition. In the process some new (alternate) proofs and solutions along with good many new worked out problems have been added.

We received comments and suggestions from a large number of readers, both from home and abroad. It was not possible to write to all of them individually. So this seems to be an appropriate occasion to place on record our sincere thanks to them all and assure them that each and every suggestion of their's has been taken note of and incorporated wherever possible. A word of thanks to that vast majority of silent admirers who have contributed in making the book a success will also not be out of place here.

Finally, we express our sincere gratitude to all friends and colleagues who went through the book critically and offered their valuable opinions.

The 'job' is not yet complete. There is (and would always be) scope for improvement and we invite further comments and suggestions to make the book more purposeful.

VIJAY K. KHANNA
S.K. BHAMBRI

Preface to the First Edition

The present volume has grown out of our association with the teaching of Algebra to the Hons. and post graduate classes for the last several years and our exposure to the problems faced by the students in grasping the abstract nature of the subject. This experience is the foundation and, we hope, the strength of the text. Earnest efforts have been exerted to present the subject matter in a well-knit manner so as not only to stimulate the interest of the student but also to provide him with an insight into the complexities of a subject of great intrinsic beauty.

The book is intended to serve as a text for undergraduate students especially those opting for an Honours course in Mathematics. However, post graduate students will find it equally useful.

The first chapter on Preliminaries is a curtain-raiser to the main contents of the book. It gives a rather terse summery of the results from Set Theory (some of which we presume the reader would already be familiar with). A few results from Number Theory are incorporated in the later half of this chapter. We debated between ourselves whether or not to give a 'full chapter status' to Number Theory results and after a careful thought decided to keep these as only a part of the first chapter since we feared that a full chapter on these might impair the balance of the book.

The main text can be divided into four sections on Groups, Rings, Vector spaces (Linear Algebra) and Fields. Fairly sufficient ground has been covered in the first three sections. It is only in the last section on Fields that we can possibly be accused of being stingy. But then there are constraints and it was paucity of space and time (and not of ideas) that finally made us keep Galois Theory out. May be in a subsequent edition it would find its way in.

Different concepts have been explained with the help of examples. A large number of problems with solutions have been provided to assist one get a firm grip on the ideas developed. There is plenty of scope (in the form of exercises) for the reader to try and solve problems on his own. In all, a substantial variety of challenges (and rewards) is assured.

We are deeply indebted to all those authors whose books (research papers) on Algebra influenced our learning of the subject and take this opportunity to express our sincere gratitude to them. We are also thankful to those friends and colleagues with whom we had fruitful discussions from time to time.

It is our earnest belief that no 'work' is ever complete till it has had its share of criticism and hence we'll be only too glad to receive comments and suggestions for the betterment of the book.

VIJAY K. KHANNA
S.K. BHAMBRI

Glossary of Symbols

$\in$	:	Belongs to
$\notin$	:	Does not belong to
$\exists$	:	There exists
$\Rightarrow$	:	Implies
$\Leftrightarrow$	:	Implies and is implied by
iff	:	If and only if
$a \mid b$	:	a divides b or b is a multiple of a
$a \nmid b$	:	a does not divide b
φ	:	Empty set
$H \leq G$	:	H is a sub group of G
$H < G$	:	H is a proper subgroup of G
$i_G(H)$	:	Index of H in G
$[G : H]$	:	In groups, index of H in G. In fields, degree of G over H
$\mathbf{N}$	:	Set of natural numbers
$\mathbf{Z}$	:	Set of integers
$\mathbf{Q}$	:	Set of rational numbers
$\mathbf{R}$	:	Set of real numbers
$\mathbf{C}$	:	Set of complex numbers
$Z(G)$	:	Centre of group G
$o(G)$	:	Order of G
S_n	:	Symmetric group of degree n
$\cong$	:	is isomorphic to

Chapter 1

Preliminaries

Sets

The notion of a set is most fundamental in Mathematics, but it is not our endeavour in this text to enter into the axiomatic study of set theory. We'll, instead, borrow the word 'set' from the language and be content to refer to it as a collection of objects. To give it a more precise shape, by a set, we will mean a collection of objects such that given any object, it is possible to ascertain whether that object belongs to the given collection or not. For instance, we can talk of set of all natural numbers, set of all students in a particular class, etc. If x is an element (member) of a set A we say x belongs to A and express it as $x \in A$. If y is not a member of A we say y does not belong to A and write $y \notin A$. We shall use capital letters A, B, X, Y etc. for denoting sets and small letters, a, b, c, x, y etc. for the elements (or members or objects).

Two sets A and B are called *equal* if they contain precisely the same elements and we write $A = B$.

A set can be described in various ways. For example, if A is the set containing 1, 2, 3, 4, 5, 6, we can write it as

$$A = \{1, 2, 3, 4, 5, 6\}$$

$$A = \{1, 2, \ldots\ldots\ldots, 6\}$$

$$A = \{x \in \mathbf{N} \mid x \leq 6\}$$

where $\mathbf{N}$ is set of all natural numbers. The last notation reading as : those x in the set of natural numbers which satisfy the property that $x \leq 6$.

We do not repeat any element while writing the elements in a set. Again, the order in which the elements are written is immaterial. Thus $\{1, 2, 3\}$ and $\{2, 1, 3\}$ mean the same set.

A set having no element is called an *empty set* or a *null set* or a *void set.* It is denoted by Φ or φ. Obviously any two empty sets are equal. A set will be called *finite* if either it is empty or has finite number of elements, i.e. the elements can be listed by natural numbers such that the process of listing stops after a certain definite stage. A set with infinite number of elements is referred to as an infinite set.

The set $\{1, 2, 3, \ldots\ldots, 1000\}$ is a finite set, whereas the set of all integers is infinite. Again the set of all rational numbers whose square is 2 is an empty set.

Subsets

We say a set A is contained in a set B (in symbols $A \subseteq B$) if every element of A is in B. A is then called subset of B and B is called superset of A. If in addition to this there is at least one element in B which is not in A, we say A is strictly contained in B ($A \subset B$) and call A a proper subset of B. $A \not\subset B$ means A is not a subset of B. Also $A \subseteq B$ and $B \supseteq A$ mean the same.

It is clear then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. Also, $A \subseteq A$, $\varphi \subseteq A$ for any set A.

Definition : By *union* of two sets A and B, we mean the set $A \cup B$ which contains all the elements of A as well as B. Thus $A \cup B = \{x \mid x \in A \text{ or } x \in B \text{ (or both)}\}$.

By intersection of two sets A and B, we mean the set $A \cap B$ which contains all the elements of A and B. Thus $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.

The *difference* of two sets A and B is defined to be the set $A - B = \{x \mid x \in A, x \notin B\}$.

In case $B \subset A$, then $A - B$ is called the complement of B in A. If there is no confusion regarding the set A, complement of B in A is denoted by B'.

Example 1 : Let $A = \{1, 2, 3\}$, $B = \{3, 4, 5, 6\}$

Then $A \cap B = \{3\}$

$A \cup B = \{1, 2, 3, 4, 5, 6\}$

$A - B = \{1, 2\}$

Theorem 1 : *If A, B, C are sets then the following results hold* :-

(*i*) $A \cap A = A$, $A \cup A = A$

(*ii*) $A \cap \varphi = \varphi$, $A \cup \varphi = A$

(*iii*) $A \cap B = B \cap A$, $A \cup B = B \cup A$, $A \cap B \subseteq A \subseteq A \cup B$

(*iv*) $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$

(*v*) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(*vi*) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof : We will prove (*v*), and leave others for the reader to try as an exercise.

Let $x \in A \cap (B \cup C)$ be any element.

Then $x \in A$ and $x \in B \cup C$

$\Rightarrow x \in A$ and $x \in B$ or $x \in C$.

If $x \in B$, then as $x \in A$, $x \in A \cap B$

If $x \in C$, then as $x \in A$, $x \in A \cap C$.

i.e. $x \in A \cap B$ or $x \in A \cap C$ (or both, of course)

$$\Rightarrow x \in (A \cap B) \cup (A \cap C)$$

$$\Rightarrow A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \quad \text{.... (1)}$$

Again, $y \in (A \cap B) \cup (A \cap C)$

$$\Rightarrow y \in A \cap B \quad \text{or} \quad y \in A \cap C$$

$$\Rightarrow y \in A \text{ and } B \quad \text{or} \quad y \in A \text{ and } C$$

$$\Rightarrow y \in A \text{ and } y \in B \text{ or } C$$

$$\Rightarrow y \in A \text{ and } y \in B \cup C$$

$$\Rightarrow y \in A \cap (B \cup C)$$

$$\Rightarrow (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \quad \text{.... (2)}$$

(1) and (2) give us the result.

Theorem 2 : (*DeMorgan's laws*). *For sets A, B in a set X,*

(*i*) $X - (A \cup B) = (X - A) \cap (X - B)$ *or* $(A \cup B)' = A' \cap B'$

(*ii*) $X - (A \cup B) = (X - A) \cup (X - B)$ *or* $(A \cap B)' = A' \cup B'$.

Proof : (*i*) Let $x \in X - (A \cup B)$ be any element.

Then $x \in X, \quad x \notin A \cup B$

$$\Rightarrow x \in X, \quad x \notin A, \quad x \notin B$$

$$\Rightarrow x \in X - A, \; x \in X - B$$

$$\Rightarrow x \in (X - A) \cap (X - B)$$

$$\Rightarrow X - (A \cup B) \subseteq (X - A) \cap (X - B) \quad \text{.... (1)}$$

Again $y \in (X - A) \cap (X - B)$

$$\Rightarrow y \in X - A, \quad \text{and} \quad y \in X - B$$

$$\Rightarrow y \in X, \quad y \notin A \quad \text{and} \quad y \in X, \quad y \notin B$$

$$\Rightarrow y \in X \quad \text{and} \quad y \notin A \cup B$$

$$\Rightarrow y \in X - (A \cup B)$$

$$\Rightarrow (X - A) \cap (X - B) \subseteq X - (A \cup B). \quad \text{.... (2)}$$

(1) & (2) give us the result.

(*ii*) Prove similarly.

Definition : Given two elements a, b of a set of X, we define the ordered pair (a, b) to be the set $\{\{a\}, \{a, b\}\}$. a is called the first component (or first co-ordinate) and b is called the second component (or second co-ordinate).

We show $(a, b) = (c, d) \Leftrightarrow a = c, \quad b = d$

If $a = c$, $b = d$ then the result is obvious.

Conversely, $(a, b) = (c, d)$

$$\Rightarrow \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$$

Since, the two sets are equal, they contain same elements.

Thus, $\{a\} = \{c\}$ or $\{a\} = \{c, d\}$

If $\{a\} = \{c\}$, then $\{a, b\} = \{c, d\}$

$$\Rightarrow a = c \text{ and } b = d \quad (\text{as } a = c)$$

Again, if $\{a\} = \{c, d\}$ then $\{a, b\} = \{c\}$

$$\Rightarrow a = c, a = d, a = c, b = c$$

$$\Rightarrow a = c = b = d$$

$$\Rightarrow a = c, b = d$$

Hence the result follows.

We thus notice, the order in which the elements are written is important in as much as (a, b) is not same as (b, a) unless $a = b$, whereas, of course, the two sets $\{a, b\}$ and $\{b, a\}$ are same.

Relations

Definition : Given two sets A and B, the cartesian product $A \times B$ is defined by

$A \times B = \{(a, b) \mid a \in A, b \in B\}$. Thus it is the set of all ordered pairs of elements from A and B.

As an example, if $A = \{1, 2\}$, $B = \{3, 4, 5\}$, then

$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$

Also, then $B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2), (5, 1), (5, 2)\}$

thus $A \times B$ may not equal $B \times A$.

One can, of course, talk of $A \times A$.

Any subset of $A \times B$ is called a (binary) relation from A to B, e.g.,

$R_1 = \{(1, 3), (1, 4), (1, 5)\}$

$R_2 = \{(1, 3)\}$, $R_3 = \{(2, 3), (1, 5)\}$

are all relations from A to B.

A relation from A to A is called a relation in A (or on A).

If R is a relation from A to B and $(a, b) \in R$, then we also express this fact by writing aRb and say a is R-related to b.

If R_1 is a relation from A to B and R_2 is a relation from C to D then R_1 and R_2 are said to be equal if $A = C$, $B = D$ and $aR_1b \Leftrightarrow aR_2b$, $a \in A$, $b \in B$.

Let now, A be a non empty set. A relation R in A is called

Reflexive : if $(a, a) \in R$ for all $a \in A$

Symmetric : if whenever $(a, b) \in R$ then $(b, a) \in R$

Anti-Symmetric : if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$

Transitive : if whenever (a, b), $(b, c) \in R$ then $(a, c) \in R$

A relation R is called an *equivalence relation* if it is reflexive, symmetric and transitive.

A relation R on a set A is called a *partial order* relation, if it is reflexive, anti-symmetric and transitive.

Example 2 : If $A = \{1, 2, 3\}$ then

$R_1 = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$ is reflexive

$R_2 = \{(1, 1), (2, 2)\}$ is not reflexive

$R_3 = \{(1, 2), (2, 1)\}$ is symmetric but not reflexive

$R_4 = \{(1, 1), (1, 2)\}$ is neither reflexive nor symmetric but is transitive.

Example 3 : Let A be the set of all lines in a plane. Let $R \subseteq A \times A$ where $R = \{(l, m) \mid l, m \in A,\ l || m\}$ then R is

Reflexive : as $(l, l) \in R$ for all $l \in A$

as $l || l$ for all $l \in A$

Symmetric : as if $(l, m) \in R$ then $l || m$

$\Rightarrow m || l$

$\Rightarrow (m, l) \in R$

Transitive : as if $(l, m) \in R$, $(m\ n) \in R$

then $l || m,\ m || n$

$\Rightarrow l || n \Rightarrow (l, n) \in R$

Thus relation of parallelism is an equivalence relation.

Example 4 : Let $\mathbf{Z}$ = set of integers then the usual $\leq$ is a partial order relation on $\mathbf{Z}$ as it is

Reflexive : as $a \leq a$ for all $a \in \mathbf{Z}$

Anit-Symmetric : as $a \leq b,\ b \leq a \Rightarrow a = b$

Transitive : as $a \leq b,\ b \leq c \Rightarrow a \leq c$.

Example 5 : Let $R = \{(m, n) \mid m, n \in \mathbf{Z},\ m \mid n\}$

then R is a partial order relation. Verify?

Where by $x \mid y$ (x divides y) we mean, $\exists\ z$, s.t., $y = xz$.

Example 6 : The relation of equality on integers is an equivalence relation.

Example 7 : Let $\mathbf{Z}$ = set of integers. Let $n \neq 0$ be any fixed integer. For any $a, b \in \mathbf{Z}$, we define a relation

$a \equiv b \pmod{n}$ (read as a is congruent to b mod n)

$\Leftrightarrow$ n divides $a - b$

Then this is an equivalence relation as

Reflexivity : $a \equiv a \pmod{n}$

as $a - a$ is divisible by n

as $0 = a - a = 0n$.

Symmetry : Let $a \equiv b \pmod{n}$

Then n divides $a - b$

$\Rightarrow \exists\, c$, s.t., $a - b = nc$

$\Rightarrow b - a = -nc = (-c)n$

$\Rightarrow b \equiv a \pmod{n}$.

Transitivity : Let $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

Then $n \mid a - b,\ n \mid b - c$

$\Rightarrow \exists\, c_1$ & c_2 s.t., $a - b = nc_1$

$b - c = nc_2$

Now, $a - c = (a - b) + (b - c)$

$= nc_1 + nc_2 = n(c_1 + c_2) = nc_3$

$\therefore$ $\exists\, c_3 \in \mathbf{Z}$, s.t., $a - c = nc_3$

$\Rightarrow n$ divides $a - c$

or that $a \equiv c \pmod{n}$.

Equivalence Classes

Let X be a non-empty set and let $\sim$ be an equivalence relation on X. For any $a \in X$, we define equivalence class of a by

$$cl(a) = \{x \in X \mid x \sim a\}$$

i.e., equivalence class of a contains all those members of X, which are related to a under the relation $\sim$. The following theorem gives us certain important properties of equivalence classes.

Theorem 3 : *Let $\sim$ be an equivalence relation on a non-empty set X. Then for any $a, b \in X$*

(*i*) $cl(a) \neq \varphi$

(*ii*) *Either* $cl(a) \cap cl(b) = \varphi$ *or* $cl(a) = cl(b)$

i.e., two equivalence classes are either equal or have no element in common.

(*iii*) $X = \bigcup_{a \in X} cl(a)$.

Proof : (*i*) Since $a \sim a$ by reflexivity

$a \in cl(a)$, $\therefore cl(a) \neq \varphi$.

(*ii*) Let $cl(a) \cap cl(b) \neq \varphi$

Then $\exists$ some $x \in cl(a) \cap cl(b)$

$\Rightarrow x \in cl(a)$ & $x \in cl(b)$

$\Rightarrow x \sim a$ & $x \sim b$

$\Rightarrow a \sim x$ & $x \sim b$

$\Rightarrow a \sim b$.

Now if $y \in cl(a)$ be any element

then $y \sim a$ and as $a \sim b$ we find $y \sim b$

$$\Rightarrow y \in cl\,(b)$$

thus $\quad cl\,(a) \subseteq cl\,(b)$

Similarly $\quad cl\,(b) \subseteq cl\,(a)$

Hence $\quad cl\,(a) = cl\,(b)$.

(*iii*) Clearly any element $x \in X$ will be in at least one class, namely $cl\,(x)$ and hence is a member of $\bigcup_{a \in X} cl\,(a)$.

Again, if $t \in \bigcup_{a \in X} cl\,(a)$ then $t \in cl\,(x)$ for some x and as $cl\,(x) \subseteq X$, $t \in X$

Showing that X equals the union of all equivalence classes of X.

Definition : Let X be a non-empty set. Let K = set of non-empty subsets of X such that every two distinct members of K are disjoint, then K is called a *partition* of X, if X equals the union of all members of K.

In view of this definition, we can say that if X be a non-empty set, with an equivalence relation defined on it, then the set of all equivalence classes of X partitions the set X.

Mappings or Functions

Let A and B be two non-empty sets. A relation f from A to B is called a mapping (or a map or a function) from A to B if for each $a \in A$, $\exists$ a unique $b \in B$ s.t., $(a, b) \in f$ (and in that case we write $b = f(a)$ and b is called image of a under f and a is called pre-image of b under f). We express this by writing $f: A \to B$.

Thus mapping is that relation from A to B in which each member of A is related to some member of B and no member of A is related to more than one member of B, although more than one member of A can be related to the same member of B. A is called the *domain* of f and B is called the *co-domain* of f.

The subset of B which contains only those members which have pre images in A is called *range* of f.

One can, of course, have more than one mapping from A to B.

A mapping $f: A \to B$ is called *one-one* (1-1) *or injective* mapping, if

$$f(x) = f(y) \Rightarrow x = y$$

or if $\quad x \neq y \Rightarrow f(x) \neq f(y)$

Thus under one-one mapping all members of A are related to different members of B.

A mapping $f: A \to B$ is called *onto* or *surjective* mapping, if range of f equals B, i.e., each member of B has a pre-image under f.

A map which is both 1-1 and onto is sometimes referred to as a one-to-one correspondence or a *bijective* map.

To check whether a map $f: A \to B$ is well defined or not, we need verify that $x = y \Rightarrow f(x) = f(y)$.

Example 8 : Let $\mathbf{N}$ = set of natural numbers. Define a map $f: \mathbf{N} \to \mathbf{N}$ s.t., each $a \in \mathbf{N}$ is connected to its square. Since each natural number has a unique square in $\mathbf{N}$ itself, we find f will be a well-defined mapping. We express this by writing.

$$f: \mathbf{N} \to \mathbf{N}, \quad \text{s.t.,}$$
$$f(x) = x^2 \text{ for all } x \in \mathbf{N}$$

We notice that in the notation of our definition

$$f = \{(1, 1), (2, 4), (3, 9), (4, 16), \ldots\ldots\ldots\}$$
$$= \{(x, x^2) \mid x \in \mathbf{N}\}$$

Example 9 : For any set A, the mapping $f: A \to A$, s.t.,

$$f(x) = x \quad \text{for all } x \in A$$

is called the *identity map*. It is trivially a well defined one-one map. It is also onto.

Example 10 : If $\mathbf{Z}$ = set of integers, then the map $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 2x$$

is 1-1 but not onto. $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y$

But $1 \in \mathbf{Z}$ has no pre image.

Example 11 : The map $f: \mathbf{N} \to \{1\}$, s.t.,

$$f(x) = 1 \text{ for all } x \in N$$

where $\mathbf{N}$ = set of naturals is onto map but not 1-1.

Equality of Mappings

Two mapping f and g from A to B *should* be equal if they 'behave' exactly in the same way. We formalise this in

Theorem 4 : *Two maps $f: A \to B$ and $g: A \to B$ are equal iff $f(x) = g(x)$ for all $x \in A$.*

Proof : Let $f = g$.

Let $a \in A$ be any element and let $f(a) = b$.

then $\quad (a, b) \in f \Rightarrow (a, b) \in g$

$$\Rightarrow b = g(a)$$

or that $\quad f(x) = g(x)$ for all x.

Conversely, let $f(a) = g(a)$ for all $a \in A$

Let $x \in f$ be any element, then $x = (a, f(a))$ for some $a \in A$.

Since $\quad f(a) = g(a), \quad x = (a, g(a)) \in g$

i.e., $\quad x \in f \Rightarrow x \in g$

or that $\quad f \subseteq g$

Similarly, $\quad g \subseteq f$

and hence $\quad f = g$.

Definition : Let $f: A \to B$ be a mapping and suppose C and D are subsets

of A and B respectively., s.t., $f(x) \in D$ for all $x \in C$. We say f induces the map $g : C \to D$ where $g(x) = f(x)$ for all $x \in C$ and in that case g is called a *restriction* of f.

Composition of Mappings

Let $f : A \to B$ and $g : B \to C$ be two mappings.

We define a mapping (to be denoted by gof) from A to C by the rule

$$gof(x) = g(f(x)) \text{ for all } x \in A$$

That it is well defined is confirmed by the fact that

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

One can, of course, extend this idea to more than two mappings.

Remark : gof is also denoted by gf.

Theorem 5 : *If $f : A \to B$ and $g : B \to C$ are one-one (onto) mappings then so is gof.*

Proof : Let f and g be one-one

Since $\quad (gof)\,x = (gof)\,y$

$$\begin{aligned} \Rightarrow\ & g(f(x)) = g(f(y)) \\ \Rightarrow\ & f(x) = f(y)) && \text{[as } g \text{ is 1-1]} \\ \Rightarrow\ & x = y && \text{[as } f \text{ is 1-1].} \end{aligned}$$

We find gof is one-one.

Again, if f, g are onto, and $c \in C$ be any element, then $\exists\, b \in B$ s.t., $g(b) = c$ (g being onto). Again, for this $b \in B$, $\exists$ some $a \in A$ s.t.,

$$f(a) = b \text{ as } f \text{ is onto}$$

Now $\quad (gof)\,a = g(f(a)) = g(b) = c$

hence gof is onto.

The converse of the above theorem does not hold (see exercises).

Theorem 6 : *A mapping $f : X \to Y$ is one-one onto iff $\exists$ a mapping $g : Y \to X$ such that gof and fog are identity maps on X and Y respectively.*

Proof : Let $f : X \to Y$ be one-one onto.

Define a mapping $g : Y \to X$, s.t.,

$$g(y) = x \quad \textit{iff} \quad f(x) = y$$

Since f is onto, for any $y \in Y$, $\exists$ an $x \in X$ s.t., $f(x) = y$ and as f is one-one, this x is unique and hence g is well defined.

Now gof is a map from $X \to X$

For any $x \in X$ $\quad$ let $f(x) = y$, then by definition of g

$$g(y) = x$$

Now $\quad (gof)\ x = g(f(x)) = g(y) = x$

Showing thereby that gof is identity map.

Similarly fog will also be identity map.

Conversely, let $f: X \to Y$ be a map for which it is possible to find some $g: Y \to X$ such that fog and gof are identity maps on Y and X respectively.

Let $f(x_1) = f(x_2)$

Then $\quad g(f(x_1)) = g(f(x_2))$ $\quad$ [g is well defined map]

$\Rightarrow (gof)\, x_1 = (gof)\, x_2$

$\Rightarrow x_1 = x_2$ $\quad$ [gof is identity map]

$\Rightarrow f$ is 1-1

Again, let $y \in Y$ be any element

then $\quad y = (fog)\, y$ (fog is identity map)

$= f(g(y))$

thus for $y \in Y$, $\exists\, g(y) \in X$, s.t., $f(g(y)) = y$ i.e., $g(y)$ is pre-image of y, hence f is onto.

Remark : The above mapping g is called inverse of f and is denoted by f^{-1}. It is easy to see that f^{-1} will also be 1-1 onto.

We can restate the above theorem as :-

Theorem 7 : *A map f is invertible iff it is one-one onto.*

Definition : Let $f: A \to B$ be a function. Let $X \subseteq A$ then we define $f(X) = \{f(x) \mid x \in X\}$, which is, of course, a subset of B. it is called image of X.

Again, if $Y \subseteq B$ then $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, which is a subset of A. (f^{-1} here is only a notation and not essentially the inverse function). It is called pre-image of Y.

Theorem 8 : *Let $f: X \to Y$ be a function then*

(*i*) $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$

(*ii*) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

(*iii*) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

(*iv*) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

(*v*) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$

(*vi*) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$

where A_1, A_2 are subsets of X and B_1, B_2 are subsets of Y.

Proof : We leave it for the reader to try.

Theorem 9 : *If $f: A \to B$, $\quad g: B \to C$, $\quad h: C \to D$ be maps then*

(*i*) $ho(gof) = (hog)of$

(*ii*) *If $i: A \to A$, $\quad j: B \to B$ be identity maps then*

$foi = f$ *and* $jof = f$

Proof :(*i*) $ho(gof)$ and $(hog)of$ are both maps from $A \to D$

Since for any $x \in A$

$$[(hog)of]\,x = (hog)(f(x)) = h(g(f(x)))$$
$$[ho(gof)]\,x = h((gof)\,x) = h(g(f(x)))$$
$$h((gof)x) = (ho(gof))x$$

we get result (*i*).

(*ii*) Since foi and f are both maps from $A \to B$ and also for any $x \in A$

$$(foi)\,x = f(i\,(x)) = f(x), \text{ we find } foi = f$$

Again, jof and f are maps from $A \to B$ and for any $x \in A$

$$(jof)\,x = j\,(f(x)) = f(x)$$
$$\Rightarrow jof = f$$

Cor. : If $f: A \to A$ be any mapping and $i: A \to A$ be identity map, then $foi = iof = f$.

Binary Compositions

If a, b are any two natural numbers then we know that $a + b$ is always a natural number and has a definite unique value. Thus + (addition) is an operation that *joins* two elements of **N** the set of naturals to give us a unique element of the same set **N**. This 'joining process' reminds us of the definition of a map. If we define a map

$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \text{ such that}$$
$$f((a,\ b)) = a + b$$

then the definition of mapping is satisfied and it is nothing but what we have mentioned above. Thus addition on natural numbers **N** is a map from $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$. We call such maps *Binary compositions* or *Binary operations*. In general a mapping $f: A \times A \to A$ is called a binary composition or binary operation in A (or on A). One could, of course, have more than one binary composition on the same set. In fact, multiplication is another binary composition on **N** whereas subtraction is not (why?). Subtraction would be binary composition on integers.

The mapping $\quad f: \mathbf{Q} \times \mathbf{Q} \to \mathbf{Q}, \quad$ s.t.,

$$f\,(a,\ b) = \frac{a\,b}{2}$$

where **Q** = rationals is a binary composition on **Q**.

We sometimes express the above by saying that $*$ is a binary composition defined on **Q** by $a * b = \dfrac{a\,b}{2}$. In fact this notation is generally more convenient to use.

A binary composition $*$ is called commutative if

$$a * b = b * a \qquad \text{for all } a,\ b$$

and is called associative if

$$a * (b * c) = (a * b) * c \qquad \text{for all } a,\ b,\ c$$

Addition on natural numbers is both commutative and associative binary composition. If we define $*$ on $\mathbf{N}$ by $a * b = a^2 + b$ then it is easy to see that $*$ is a binary composition on $\mathbf{N}$ but is not associative.

If $*$ is a binary composition on a set X and $a, b \in X$ be any two elements, then $a * b \in X$, by definition. This fact is also sometimes expressed by saying that X is closed under $*$. The name is quite appropriate in as much as when two elements are 'joined' through the composition, the resulting element remains inside the set itself. In other words, the system remains *closed* under the operation. The concept of binary composition is most fundamental in the study of algebra and in fact forms a pedestal for the systems that we shall come across later in the text.

Exercises

1. Prove the following, for sets A, B, C
   (*i*) $A \subseteq B,\ B \subseteq C \Rightarrow A \subseteq C$
   (*ii*) $A \subseteq B \Leftrightarrow A \cup B = B,\ A \subseteq B \Leftrightarrow A \cap B = A$
   (*iii*) If $A \cap B = A \cap C$ and $A \cup B = A \cup C$ then $B = C$
   (*iv*) Show by examples that conclusion in (*iii*) fails if any of the two conditions does not hold.
2. $A \Delta B = (A - B) \cup (B - A)$ is called symmetric difference of two sets A and B. Show that it is equal to $(A \cup B) - (A \cap B)$. Show also that $A \Delta B = B \Delta A$, $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.
3. Prove the results of theorem 1.
4. Let $A = \{1, 2, 3, 4\}$. Give example of a relation in A which is (*i*) equivalence relation, (*ii*) partial order relation, (*iii*) reflexive, not symmetric (*iv*) symmetric, not reflexive, (*v*) reflexive, transitive not symmetric, (*vi*) transitive but not reflexive or symmetric.
5. Show by an example that we can have maps f and g such that fog is one-one (onto) whereas f or g is not one-one (onto).
6. If A be a finite set then show that any one-one map $f: A \to A$ is also onto.
7. Let A and B be two sets with n elements each. Show that the number of one-one onto maps from A to B is $n!$.
8. Let $f: A \to B$ be an invertible mapping. Show that the inverse is unique.
9. Show that the set of all odd integers is not closed under subtraction. What can be said about set of all even integers?
10. Show that matrix addition and matrix multiplication are binary compositions on set of matrices.

Permutations

Let S be a non empty set. Any 1-1, onto mapping $f: S \to S$ is called a permutation (or a non singular transformation) of S. We shall use the notation $A(S)$ to denote the set of all permutations of S. To have some more information about $A(S)$ we first consider

Example 12 : Let $S = \{1, 2, 3\}$

Consider the maps $f: S \to S$, s.t.,

$$f(1) = 2$$
$$f(2) = 3$$
$$f(3) = 1$$

and $g: S \to S$, s.t., $g(1) = 2$, $g(2) = 1$, $g(3) = 3$ then both f, g are permutations on S. Again, the identity map $I: S \to S$, s.t., $I(x) = x$ for all $x \in S$ is also a permutation. It is easy to check that the maps fog, gof and fof are also permutations of X. (In fact, we have already shown that φ, ψ 1–1 onto maps implies $\varphi o \psi$, $\psi o \varphi$ etc. are 1-1 onto in case these maps exist). Hence the set $A(S)$ contains I, f, g, fog, gof, fof. Since the number of ways in which 3 elements can be connected with 3 elements in 1-1 onto way is $3! = 6$, these would be all the members of $A(S)$.

We thus have a non-empty set $A(S)$ having these six members. In view of the results proved earlier we find

$$\varphi o(\psi o \eta) = (\varphi o \psi) o \eta \quad \text{for all } \varphi, \psi, \eta \in A(S)$$
$$\theta o I = I o \theta = \theta \quad \text{for all } \theta \in A(S)$$

Again as each one-one onto map is invertible, we notice each member of $A(S)$ has an inverse, which would also be one-one onto and hence be a member of $A(S)$.

All these properties taken together give us a system called a group, which we shall be discussing in the next chapter.

In fact, this particular $A(S)$ is also denoted by S_3 and is called *symmetric group* of degree 3. We have considered the set S having three elements. If the set S contains n elements, we have a similar situation and get $A(S)$ or S_n, which would finally turn out to be a group (to be called symmetric group of degree n).

One could denote the elements of the set S by x_1, x_2, x_3 etc. instead of 1, 2, 3, but for convenience we use 1, 2, 3.

We now introduce a notation to represent permutations. Consider the above set $A(S) = S_3$.

The mapping f (as defined above) could be written as

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

where first row consists of all members of S and the second row consists of their respective images.

Similarly, $$g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Again since fog will be given by

$$(fog)\ 1 = f(g(1)) = f(2) = 3$$
$$(fog)\ 2 = f(g(2)) = f(1) = 2$$
$$(fog)\ 3 = f(g(3)) = f(3) = 1$$

we can write $fog = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

In fact, the computation as done above could be achieved through the product

$$fog = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

by starting from right bracket towards the first (left) bracket. For instance

$$1 \xrightarrow{g} 2, 2 \xrightarrow{f} 3 \qquad 2 \xrightarrow{g} 1, 1 \xrightarrow{f} 2 \qquad 3 \xrightarrow{g} 3, 3 \xrightarrow{f} 1$$

or that under fog $\quad 1 \to 3,\ 2 \to 2,\ 3 \to 1.$

In this manner we can compute the product of any number of permutations.

We simplify this notation a little further. Since in each representation, the first row is same we omit writing it and simply represent f by (1 2 3), fog by (1 3), g by (1 2) etc.

In f, $\quad 1 \to 2,\ 2 \to 3,\ 3 \to 1.$

In fog, $\quad 1 \to 3,\ 3 \to 1.$ Since 2 is not mentioned it is understood $2 \to 2$.

Again in g, $1 \to 2,\ 2 \to 1$ and 3 remains fixed i.e., $3 \to 3$.

The computation of the product is also done similarly by starting from the right. For instance

$fog = (1\ 2\ 3)\ (1\ 2) = (1\ 3)$

In fact all the members of S_3 in our new notation can be listed as I, (1 2 3), (1 2), (1 3), (2 3), (1 3 2).

Suppose now that $S = \{1, 2, 3, 4, 5, 6\}$

and $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix}$

then in our single row representation f will be written as (1 2 3 5) (4 6).

$1 \to 2,\ 2 \to 3,\ 3 \to 5$ and as $5 \to 1$ and 1 occurs at the first place, so we close the bracket. We start again by considering 4, the element which had not yet figured in the first bracket and find $4 \to 6$ & $6 \to 4$. Thus we get the second bracket (4 6). These brackets (1 2 3 5) and (4 6) are called cycles of the permutation. It is very clear from the example that either a permutation will be a cycle itself or we can write it as a product of cycles, where no element will be common in any two cycles, which will be called disjoint cycles. We formalize these results through the following theorems and definitions.

Theorem 10 : *Let S be a non empty set and f a permutation of S. For $a, b \in S$, define a relation $\sim$ on S by $a \sim b \Leftrightarrow f^n(a) = b$ for some integer n. This relation $\sim$ is an equivalence relation.* [$f^n = fofof$..... *of n times*].

Proof : $a \sim a$ as $f^0(a) = i(a) = a$ where i or I is identity map.

$$a \sim b \Rightarrow \exists\ n, \quad \text{s.t.,} \quad f^n(a) = b$$
$$\Rightarrow a = f^{-n}(b) \Rightarrow b \sim a$$

where f^{-n} the inverse of f^n exists as f is 1-1 onto.

Finally, $a \sim b, \quad b \sim c \Rightarrow \exists$ integers m, n s.t.,

$$f^m(a) = b, \quad f^n(b) = c$$

clearly then

$$f^{m+n}(a) = \left(f^n \circ f^m\right)a = f^n\left(f^m(a)\right) = f^n(b) = c$$
$$\Rightarrow a \sim c$$

hence $\sim$ is an equivalence relation and thus partitions S into disjoint equivalence classes.

Remark : Many a times we write fg in place of fog, for convenience and thus $fof = ff = f^2$ etc.

Definition : The equivalence class of any element $a \in S$ is called *orbit* of a (under f).

Thus
$$cl(a) = \{x \in S \mid x \sim a\}$$
$$= \{f^n(a) \mid n \text{ integer}\} = \text{orbit of } a.$$

Theorem 11 : *If S is a finite set and $f \in A(S)$ then $\exists$ a + ve integer m such that orbit of x is $\{x, f(x), f^2(x), \ldots\ldots, f^{m-1}(x)\}$.*

Proof : Since S is finite, $A(S)$ has finite number of elements.

As $f \in A(S)$, f^2, f^3,..... all are in $A(S)$ and as order of $A(S)$ is finite, after a certain stage some power of f will be identity of $A(S)$. Let m be the smallest +ve integer such that $f^m(x) = x$.

Now $x, f(x), f^2(x), \ldots, f^{m-1}(x)$ will all be distinct as if $f^i(x) = f^j(x)$ for some $i, j, 0 \le i > j \le m-1$.

then $f^{i-j}(x) = x$

But $i - j < m$ leads to a contradiction to the choice of m. Hence $x, f(x), f^2(x), \ldots, f^{m-1}(x)$ are distinct elements of the orbit of x. To show the orbit contains no other elements suppose x' is any other element in the orbit, then $\exists$ some integer n s.t.,

$$f^n(x) = x'$$

But $n = mq + r$ for some integers q, r, where $0 \le r \le m-1$

$$\Rightarrow x' = f^n(x) = f^{mq+r}(x) = f^r . f^{mq}(x) = f^r[f^{mq}(x)]$$
$$= f^r(x), \quad 0 \le r \le m-1$$

$\Rightarrow x'$ is one of the earlier members, proving our theorem.

Cyclic Permutations

Let S be a finite set. A permutation f of S is called a cyclic permutation or a cycle if $\exists$ elements $x_1, x_2, \ldots\ldots, x_n$ in S s.t.,

$$f(x_1) = x_2,\ f(x_2) = x_3, \ldots\ldots f(x_{n-1}) = x_n,\ f(x_n) = x_1$$

and all other elements remain fixed under f i.e., $f(x) = x$ for all other $x \in S$.

We denote f by $(x_1\ x_2\ \ldots x_n)$ in that case and say it is a cycle of length n. It is also called n-cycle. In particular a cycle of length 2 is called a *transposition*.

Cycles of a Permutation

Suppose we have a permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 1 & 7 & 3 & 5 \end{pmatrix}$$

$= (1\ 2\ 4)\ (3\ 6)\ (5\ 7)$ then $(1\ 2\ 4)$, $(3\ 6)$, $(5\ 7)$ are called cycles of the permutation f.

We formalise it in

Definition : Let S be a finite set and $x \in S$. Let $f \in A(S)$. We know $\exists$ a + ve integer m s.t., $x, f(x), f^2(x) \ldots\ldots f^{m-1}(x)$ are all distinct and $f^m(x) = x$. We call $(x f(x) f^2(x) \ldots\ldots f^{m-1}(x))$ a cycle of f.

Example 13 : Consider the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$

here, $f(1) = 8, f^2(1) = f(8) = 3, f^3(1) = 5\ f^4(1) = 6, f^5(1) = 2,$

$$f^6(1) = 7, f^7(1) = 1$$

Thus $(1\ 8\ 3\ 5\ 6\ 2\ 7)$ is a cycle of f.

Again $f(4) = 4, f^2(4) = 4$ etc. So (4) is another cycle of f.

Problem 1 : *Find orbits and cycles of the permutation*

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$$

Solution : Consider 1,

$$f(1) = 6, f^2(1) = 2, f^3(1) = 5, f^4(1) = 1$$

thus $(1\ 6\ 2\ 5)$ is a cycle and $\{1, 6, 2, 5\}$ is orbit of 1, 6, 2, 5

Again, if we consider 3,

$$f(3) = 4,\ f^2(3) = 3$$

thus $(3\ 4)$ is a cycle and $\{3, 4\}$ is orbit of 3 and 4.

Remark : Notice that an orbit is a set, members of which are the constituents of the corresponding cycle.

Theorem 12 : *Let f be a non trivial permutation (i.e., different from identity) of $S = \{1, 2, \ldots\ldots, n\}$. Then f can be represented as product of disjoint cycles each of length greater than or equal to 2. Also the representation is unique except for the order in which the cycles occur.*

Proof : Since f is non trivial there exists at least one orbit with more than one element. Let $O_1, O_2, \ldots\ldots O_k$ be the orbits each with two or more elements. Any orbit we know is of the form $\{a, f(a), f^2(a), \ldots, f^{m-1}(a)\}$ for some $a \in S$, and some $m > 1$. The corresponding cycle of this orbit is

$$(a\ f(a)\ f^2(a) \ldots f^{m-1}(a))$$

Let the corresponding cycles of the orbits $O_1, O_2, \ldots, O_k$ be $f_1, f_2, \ldots, f_k$.

We claim $\qquad f = f_1\ f_2 \ldots f_k$

Let $x \in S$ be any element. If x belongs to a trivial orbit of f then $f(x) = x$ and x will not belong to any of $O_1, O_2, \ldots, O_k$ (orbits are equivalence classes and thus distinct orbits have no elements in common). Thus x remains fixed under $f_1, f_2, \ldots, f_k$ i.e., $(f_1 f_2 \ldots f_k)\, x = x = f(x)$

Suppose now x belongs to one of $O_1, O_2, \ldots, O_k$ say $x \in O_t$ and suppose $O_t = \{a, f(a), f^2(a), \ldots, f^{m-1}(a)\}$

Then $\qquad x = f^p(a)$ for some $p \leq m-1$

$$\Rightarrow f(x) = f(f^p(a)) = f^{p+1}(a)$$

Again $(f_1 f_2 \ldots f_k)\, x = f_t(x)$ as $x \in O_t$ means x remains fixed under every cycle other than f_t (by definition).

But
$$f_t(x) = f_t(f^p(a)) = f^{p+1}(a)$$

Note $\qquad f_t = (a f(a)\ f^2(a) \ldots f^{m-1}(a))$

Thus $\qquad (f_1\ f_2 \ldots f_k)\ x = f^{p+1}(a)$

or that $\qquad (f_1 f_2 \ldots f_k)\, x = f(x) \qquad$ for all x

$$\Rightarrow f = f_1 f_2 \ldots f_k$$

That $f_1, f_2, \ldots, f_k$ are disjoint is clear as the corresponding orbits being equivalence classes are disjoint.

To prove uniquences, suppose f is also equal to $g_1 g_2 \ldots g_m$.

Let $\qquad g_1 = (i_1\ i_2 \ldots i_r), \qquad i_1, i_2, \ldots, i_r \in S$

and $\qquad g = g_2 g_3 \ldots g_m$

Then $\qquad f = g_1 g$

clearly now $i_1, i_2, \ldots i_r$ do not appear in any cycle in g. Thus

$$g(a) = a \qquad \text{if } a = i_1, i_2, \ldots, i_r$$

and $\qquad f(a) = g_1(a) \quad$ if $a = i_1, i_2, \ldots, i_r$

In other words $\{i_1, f(i_1), f^2(i_1), \ldots, f^{r-1}(i_1)\}$

$$= \{i_1, g_1(i_1), g_1^2(i_1), \ldots, g_1^{r-1}(i_1)\}$$

$$= \text{orbit of } f$$

$$\Rightarrow g_1 = f_t \quad \text{for some } t$$

So in this way for each g_i $\exists$ a corresponding f_j s.t., $g_i = f_j$.

Since $f = f_1 f_2 \ldots f_k = g_1 g_2 \ldots g_m$ we can cancel the equal ones on both sides,

resulting into $k = m$ (for otherwise product of some cycles of length ≥ 2 is identity, which not true).

Hence uniqueness follows.

Disjoint Permutations

Two permutations f and g of a set S are called *disjoint* if (*i*) for any $x \in S$, $f(x) \neq x \Rightarrow g(x) = x$ and (*ii*) for any $x \in S$, $g(x) \neq x \Rightarrow f(x) = x$.

For instance, $f = (12)$ and $g = (13)$ are not disjoint in S_3 as $f(1) = 2$ and $g(1) = 3 \neq 1$.

Again in S_5, $f = (1\ 3\ 2)$, $g = (4\ 5)$ are disjoint.

Theorem 13 : *Any two disjoint permutations commute.*

Proof : Let f and g be any two disjoint permutations of set S. We show $fog = gof$.

Let $x \in S$ be any element.

Suppose $f(x) \neq x$ then $g(x) = x$.

Let $f(x) = y$ then $y \neq x$.

Now $(fog)\,x = f(g(x)) = f(x) = y$.

Also $(gof)\,x = g(f(x)) = g(y) = y$

because if $g(y) \neq y$

then $\quad f(y) = y$

$\Rightarrow f(y) = f(x)$

$\Rightarrow y = x \quad$ (f being 1-1), a contradiction.

Hence $fog = gof$ for all $x \in S$ such that $f(x) \neq x$. Again if $x \in S$ be such that $f(x) = x$ then $g(x) \neq x$. Proceeding as above, we again get $fog = gof$ which proves the theorem.

In view of the results that we have proved we find any permutation can be expressed as a product of disjoint cycles. Note for instance,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 2 & 1 & 6 & 5 & 8 & 9 & 7 \end{pmatrix} = (1\ 3\ 2\ 4)\ (5\ 6)\ (7\ 8\ 9)$$

Again any cycle $(1\ 2\ 3\ 4)$ can be written as

$$(14)\,(13)\,(12)$$

i.e., it can be written as a product of transpositions and combining the two results we notice any permutation can be expressed as a product of transpositions (not essentially disjoint). Since $(1\ 2\ 3\ 4)$ can also be written $(4\ 3)\ (4\ 2)\ (4\ 1)$, we find the representation as product of transpositions is not unique.

The above f can be expressed as

$$\begin{aligned} f &= (14)\ (12)\ (13)\ (56)\ (79)\ (89) \\ &= (14)\ (12)\ (13)\ (56)\ (79)\ (89)\ (12)\ (12) \text{ etc.} \end{aligned}$$

Problem 2 : *Show that inverse of* (1 2 3 4) *is* (4 3 2 1).

Solution : Although the result is clear by definition of inverse, we notice, if we multiply (1 2 3 4) with (4 3 2 1) in the way explained above then as

$$(1\ 2\ 3\ 4)\ (4\ 3\ 2\ 1) = I$$

we get $$(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1)$$

In fact for any cycle $(1\ 2\ 3\ \ldots\ n)$

$$(1\ 2\ 3\ \ldots\ n)^{-1} = (n\ \ n{-}1\ \ldots\ 3\ 2\ 1)$$

Problem 3 : *Find different powers of the cycle* (1 2 3 4).

Solution :

$$(1\ 2\ 3\ 4)^2 = (1\ 2\ 3\ 4)\ (1\ 2\ 3\ 4) = (1\ 3)\ (2\ 4)$$
$$(1\ 2\ 3\ 4)^3 = (1\ 2\ 3\ 4)\ (1\ 3)\ (2\ 4) = (1\ 4\ 3\ 2)$$
$$(1\ 2\ 3\ 4)^4 = (1\ 2\ 3\ 4)\ (1\ 4\ 3\ 2) = I.$$

Problem 4 : *Show that* $(ab)^2 = I$ *for any transposition* $(a\ b)$.

Solution : Obvious.

Problem 5 : *Show that nth power of an n-cycle is* I $(n = 1, 2, 3, \ldots\ldots)$.

Solution : One can proceed as in the previous problems.

Problem 6 : *If* $f = (a_1\ b_1)\ (a_2\ b_2)\ (a_3\ b_3)\ (a_4\ b_4)$

then $$f^{-1} = (a_4\ b_4)\ (a_3\ b_3)\ (a_2\ b_2)\ (a_1\ b_1)$$

Solution : Consider the product

$$(a_1\ b_1)\ (a_2\ b_2)\ (a_3\ b_3)\ (a_4\ b_4)\ (a_4\ b_4)\ (a_3\ b_3)\ (a_2\ b_2)\ (a_1\ b_1)$$

which comes out to be I proving our assertion.

Theorem 14 : *Suppose f is a permutation of a finite set S. Then in all expressions of f as product of transpositions, either the number of transpositions is always even or always odd.*

Proof : Suppose there exists a permutation f in S_n for which the theorem does not hold. Then we have two representations of f,

$$f = (a_1\ b_1)\ (a_2\ b_2)\ \ldots\ldots\ldots\ (a_n\ b_n)$$
$$f = (c_1\ d_1)\ (c_2\ d_2)\ \ldots\ldots\ldots\ (c_m\ d_m)$$

where n is even and m is odd.

Since $f^{-1} = (c_m\ d_m)\ (c_{m-1}\ d_{m-1})\ \ldots\ldots\ldots\ (c_2\ d_2)\ (c_1\ d_1)$ we find

$$I = fof^{-1} = (a_1\ b_1)\ \ldots\ldots\ldots\ (a_n\ b_n)\ (c_m\ d_m)\ \ldots\ldots\ldots\ (c_1\ d_1)$$
$$= (x_1\ y_1)\ (x_2\ y_2)\ \ldots\ldots\ldots\ (x_t\ y_t) \text{ (where } t = n + m = \text{odd)}$$

Again as any transposition $(\alpha\beta) = (1\alpha)\ (1\beta)\ (1\alpha)$ the above expression can be written as

$$I = (1x_1)\ (1y_1)\ (1x_1)\ (1x_2)\ (1y_2)\ (1x_2)\ \ldots\ldots\ldots(1x_t)\ (1y_t)\ (1x_t)$$

which would still have odd number of transpositions in the R.H.S.

Consider any $(1\ u)$ in the R.H.S. Since L.H.S. is identity $(1\ u)$ most occur twice (or even number of times) in R.H.S. so as to have 'identity effect' ultimately.

Note $u \to 1$ then $1 \to u$ will give $u \to u$. Thus each transposition in the R.H.S. occurs even number of times meaning that R.H.S. should have even number of transpositions, a contradiction, proving our theorem.

Definition : A permutation is called *even* (*odd*) permutation if it can be expressed as a product of even (odd) number of transpositions.

In view of the previous theorem, we need look for only one representation to identify even or odd permutations.

The following results are rather trivially proved

a) *The product of two even permutations is even* as sum of two even numbers is even.

b) *The product of two odd permutations is even* as sum of two odd numbers is even.

c) *The product of an even and odd permutation is odd* as sum of an even and an odd number is odd.

d) *Inverse of an even* (*odd*) *permutation is even* (*odd*). Indeed

$$f = (a_1\, b_2)\ (a_2\, b_2)\ \ldots\ldots\ (a_n\, b_n).$$

$$\Rightarrow f^{-1} = (a_n\, b_n)\ (a_{n-1}\, b_{n-1})\ \ldots\ldots\ (a_1\, b_1)$$

e) *Identity permutation is always even.*

Example 14 : The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 5 & 6 & 7 & 2 \end{pmatrix}$$

$$= (13)\ (2\ 4\ 5\ 6\ 7)$$

$$= (13)\ (27)\ (26)\ (25)\ (24)$$

is an odd permutation,

whereas the permutation (12) (1 5 7 6) is even as

$$(12)\ (1\ 5\ 7\ 6) = (12)\ (16)\ (17)\ (15).$$

Problem 7 : *Show that a cycle of even length is an odd permutation and a cycle of odd length is an even permutation.*

Solution : Consider the cycle (1 2 3 4) of even length. Since (1 2 3 4) = (14) (13) (12) which is odd permutation, our result is proved for a cycle of length r. It is now trivial that the result is generalised to any cycle. Indeed

$$(1\ 2\ 3\ \ldots\ldots\ n) = (1n)\ (1n{-}1)\ \ldots\ldots\ldots\ (13)\ (12)$$

proves our assertion.

Problem 8 : *Compute* $a^{-1}ba$ *where* $a = (1\ 3\ 5)\ (12)$, $b = (1\ 5\ 7\ 9)$.

Solution : We have $a = (1\ 3\ 5)\ (12)$

$$= (1\ 2\ 3\ 5)$$

$$\Rightarrow \quad a^{-1} = (5\ 3\ 2\ 1)$$

Thus $\quad a^{-1}ba = (5\ 3\ 2\ 1)\ (1\ 5\ 7\ 9)\ (1\ 2\ 3\ 5)$

$$= (3\ 7\ 9\ 5).$$

Theorem 15 : *Let* $\sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k})$ *be a permutation of a finite set S, written as product of disjoint cycles. Let* $o(S) = n$ *and* $n_1 + \ldots\ldots + n_k = n$. *Then*

$$\theta\,\sigma\,\theta^{-1} = (\theta(a_1) \ \ldots\ldots \ (\theta(a_{n_1})) \ldots\ldots \ (\theta(b_1) \ \ldots\ldots \ \theta(b_{n_k}))$$

for all $\theta \in S_n$.

Proof :

Let $$S = \{a_1, \ldots\ldots, a_{n_1}, \ \ldots\ldots, \ b_1, \ \ldots\ldots, b_{n_k}\}$$

Then $$\theta(S) = \{\theta(a_1), \ldots\ldots, \theta(a_{n_1}), \ldots\ldots, \theta(b_1), \ldots\ldots, \theta(b_{n_k})\}$$

Since $\theta : S \to S$ is 1-1, all elements in $\theta(S)$ are distinct. Also θ is onto $\Rightarrow$ $\theta(S) = S$.

Now
$$\begin{aligned}
&(\theta\,\sigma\,\theta^{-1})(\theta\ x_i)\\
&= (\theta\,\sigma)(\theta^{-1}\,\theta\,x_i)\\
&= (\theta\,\sigma)(x_i)\\
&= \theta(\sigma(x_i))\\
&= (\theta(x_{i+1}))
\end{aligned}$$

$\therefore$ $\theta\,\sigma\,\theta^{-1}$ takes any element $\theta(x_i)$ of $\theta(S) = S$ to $\theta(x_{i+1})$ and so does the mapping

$$(\theta a_1 \ \ldots\ldots \ \theta a_{n_1}) \ \ldots\ldots \ (\theta b_1 \ \ldots\ldots \ \theta b_{n_k})$$

$\therefore$ $$\theta \ \sigma \ \theta^{-1} = (\theta a_1 \ \ldots\ldots \ \theta a_{n_1}) \ \ldots\ldots \ (\theta b_1 \ \ldots\ldots \ \theta b_{n_k})$$

Remark : It follows from above that the cycle structure of σ is same as that of $\theta\,\sigma\,\theta^{-1}$ for all $\theta \in S_n$ as σ has k cycles of length $n_1, \ldots\ldots\ldots, n_k$ and same is true for $\theta\,\sigma\,\theta^{-1}$. *Note that* σ *must be written as product of disjoint cycles.*

e.g., take $\theta = (1\ 2\ 3\ 4)$, $\sigma = (1\ 2)\ (2\ 3)$

Then $\theta\,\sigma\,\theta^{-1} = \theta(12)\ (23)\theta^{-1} \neq (\theta 1\ \theta 2)\ (\theta 2\ \theta 3) = (13)\ (34)$

as R.H.S. (13) (34) takes 4 to 1 and $\theta(12)\ (23)\ \theta^{-1}$ takes 4 to 2.

Problem 9 : *Let* $S = \{1, 2, 3, 4\}$. *Find all permutations* θ *of* S *such that* $\theta\ (12)\ (34)\theta^{-1} = (13)\ (24)$.

Solution : Now $\theta(12)\ (34)\theta^{-1}$

$$= (\theta 1\ \theta 2)\ (\theta 3\ \theta 4)$$

$\therefore$ $$(\theta 1\ \theta 2)\ (\theta 3\ \theta 4) = (13)\ (24)$$

Again $$(13)\ (24) = (31)\ (24) = (13)\ (42) = (31)\ (42)$$
$$(24)\ (13) = (24)\ (31) = (42)\ (13) = (42)\ (31)$$

So, θ has 8 choices, namely

$$\theta 1 = 1,\ \theta 2 = 3,\ \theta 3 = 2,\ \theta 4 = 4,\ \textit{i.e.},\ \theta = (23)$$
$$\theta 1 = 3,\ \theta 2 = 1,\ \theta 3 = 2,\ \theta 4 = 4,\ \textit{i.e.},\ \theta = (132)$$

$\theta 1 = 1, \quad \theta 2 = 3, \quad \theta 3 = 4, \quad \theta 4 = 2, \quad$ *i.e.,* $\theta = (2\,3\,4)$

$\theta 1 = 3, \quad \theta 2 = 1, \quad \theta 3 = 4, \quad \theta 4 = 2, \quad$ *i.e.,* $\theta = (1\,3\,4\,2)$

$\theta 1 = 2, \quad \theta 2 = 4, \quad \theta 3 = 1, \quad \theta 4 = 3, \quad$ *i.e.,* $\theta = (1\,2\,4\,3)$

$\theta 1 = 2, \quad \theta 2 = 4, \quad \theta 3 = 3, \quad \theta 4 = 1, \quad$ *i.e.,* $\theta = (1\,2\,4)$

$\theta 1 = 4, \quad \theta 2 = 2, \quad \theta 3 = 1, \quad \theta 4 = 3, \quad$ *i.e.,* $\theta = (1\,4\,3)$

$\theta 1 = 4, \quad \theta 2 = 2, \quad \theta 3 = 3, \quad \theta 4 = 1, \quad$ *i.e.,* $\theta = (1\,4)$

Remark : As in the previous problem, we sometimes take the liberty of writing θx for $\theta(x)$.

Problem 10 : *Show that there does not exist a permutation* θ *of* $S = \{1, 2, \ldots\ldots, 8\}$ *such that*

$$\theta(1\,2\,3)\,\theta^{-1} = (1\,3)\,(5\,7\,8).$$

Solution : Now $\theta(1\,2\,3)\theta^{-1} = (\theta(1)\,\theta(2)\,\theta(3))$ and it does not have cycle of length 2 while (13) (5 7 8) has a cycle of length 2. So, there does not exist θ such that

$$\theta\,(1\,2\,3)\,\theta^{-1} = (13)\,(5\,7\,8).$$

Problem 11 : *Let* $A(S)$ = *set of all permutation on a set S. Show that either all permutations are even or exactly half are even.*

Solution : If all permutations are even there is nothing to prove. Suppose now $A\,(S)$ has odd as well as even permutations and $\exists$ m even and n odd permutations. Then $m + n = o(A(S))$.

Let $e_1, e_2, \ldots\ldots, e_m$ be distinct even permutations. If a be any transposition then $ae_1, ae_2, \ldots\ldots, ae_m$ are odd and will be distinct $[ae_i = ae_j \Rightarrow e_i = e_j]$.

Since $\exists$ in all, n odd permutations

$$m \leq n$$

Similarly interchanging roles of m, n we'll get $n \leq m$ and hence $m = n$.

Remark : Since identity is even permutation, all members of $A(S)$ cannot be odd permutations.

Aliter : Let E and O be the sets of even and odd permutations of $A(S)$ respectively.

Define $\quad \theta : E \to O, \quad$ s.t.,

$$\theta(\sigma) = \sigma(12)$$

Then as σ is even, $\sigma(12)$ will be odd.

Also, $\quad \sigma = \eta \Rightarrow \sigma(12) = \eta(12) \Rightarrow \theta(\sigma) = \theta(\eta)$

Showing that θ is well defined.

Again, $\quad \theta(\sigma) = \theta(\eta) \Rightarrow \sigma(12) = \eta(12)$

$$\Rightarrow \sigma(12)\,(12) = \eta\,(12)\,(12)$$

$$\Rightarrow \sigma = \eta$$

i.e., θ is 1-1.

Also for any $\sigma \in O$, σ will be odd and thus $\sigma(12)$ will be even and $\theta(12) = \sigma(12)\,(12) = \sigma$

Shows θ is onto.

Hence $$o(E) = o(O).$$

Exercises

1. Find the orbits and cycles of the set $S = \{1, 2, 3, 4, 5, 6\}$ under the following permutations

$$(i)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix}, \quad (ii)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}, \quad (iii)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

2. Express the following permutations as product of disjoint cycles
   (*i*) (123) (234) (456) (67)
   (*ii*) (12) (13) (14) (15) (16)
   (*iii*) (24) (26) (28) (13) (15) (17)
3. Find out which of the following are even (odd) permutations
   (*i*) (123) (12)
   (*ii*) (12345) (123) (45)
   (*iii*) (12) (14) (153)
4. Express the following permutations as product of transpositions
   (*i*) (123.....*n*)
   (*ii*) (123) (4576)
   (*iii*) (24) (345)
5. Find the orbits of all elemen ts under the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 6 & 4 & 5 & 9 & 7 & 8 \end{pmatrix} \text{ in } S_9.$$

Some Results From Number Theory

In this section we discuss a few results pertaining to numbers although we do not plan to go through their axiomatic construction.

Definition : A non zero integer a is said to divide an integer b if $b = ac$ for some integer c and we express it as $a \mid b$.

The following results can then be proved

(*i*) $a \mid b,\ b \mid c$ then $a \mid c$

(*ii*) $a \mid b,\ a \mid c$ then $a \mid b + c$

(*iii*) $a \mid 0,\ a \mid a$

We now prove a well known result through :-

Theorem 16 : (Euclid's Algorithm)

Let $k > 0$ be an integer and j be any integer. Then $\exists$ unique integers q and r such that $j = kq + r$, where $0 \le r < k$.

Proof : Let $S = \{j - kq \mid q \text{ is an integer}, j - kq \geq 0\}$.

Then $S \neq \varphi$, as take $q = -|j|$.

Now when $j > 0$, then $j - kq = j + kj > 0 \Rightarrow j - kq \in S$

and if $j < 0$, then $j - kq = j - kj$

$$= j\ (1 - k) \geq 0$$

$$\Rightarrow j - kq \in S$$

$j = 0$, then $j - kq = j - k.0$

$$= j = 0$$

$$\Rightarrow j - kq \in S$$

In any case, $S \neq \varphi$.

By well ordering principle, S has a least element, say $r \in S$.

$r \in S \Rightarrow r = j - kq$ for some integer q

$\Rightarrow j = kq + r$. Also $r \geq 0$

Suppose $r \geq k$

Then $j - kq \geq k$

$\Rightarrow j - k\ (q + 1) \geq 0$

$\Rightarrow j - k\ (q + 1) \in S$

But $j - k\ (q + 1) < j - kq$ as $k > 0$, contradicting $r = j - kq$ is least element of S.

$\therefore \quad 0 \leq r < k$

Uniqueness : Suppose $j = kq + r = kq' + r'$, $0 \leq r$, $r' < k$. Then $k(q - q') = r' - r$. Suppose $r' > r$. Then $r' - r > 0$. But $k \mid r' - r \Rightarrow k \leq r' - r$. Since $r, r' < k$, $r' - r < k$, a contradiction.

$\therefore r' \not> r$. Similarly $r \not> r'$ $\therefore r = r' \Rightarrow kq = kq' \Rightarrow q = q'$.

An important application of this result is the *basis representation theorem.*

Theorem 17 : (Basis Representation Theorem).

Let $b > 0$ be an integer and let $N > 1$ be any integer. Then N can be expressed as

$$N = a_m b^m + a_{m-1} b^{m-1} + \ldots\ldots + a_1 b + a_0,$$

where m and a_is are integers such that $m > 0$ and $0 \leq a_i < b$. Also then these a_is are uniquely determined. (b is called base of representation of N).

Proof : If $N < b$,

then $N = 0b^m + 0b^{m-1} + \ldots\ldots + 0b + N$

is the representation of N as required.

Let $N \geq b > 0$. By Euclid's algorithm $\exists$ integers q, r such that

$$N = bq + r, \quad 0 \leq r < b \leq N$$

Since $N - r > 0$, $bq > 0 \Rightarrow q > 0$ as $b > 0$.

If $q < b$, then $N = bq + r$ is the required representation of n.

If $q \geq b > 0$, then as above by Euclid's algorithm $\exists$ integers q_1, r_1 such that

$$q = bq_1 + r_1, \quad 0 \le r_1 < b \le q$$

Since $q - r_1 > 0$, $bq_1 > 0 \Rightarrow q_1 > 0$ as $b > 0$.

Now $\quad N = bq + r = b\ (bq_1 + r_1) + r$

$$\Rightarrow N = b^2 q_1 + br_1 + r$$

If $q_1 < b$, Then it is the required representation of N. In this way, after finite number of steps, we shall get

$$N = a_m b^m + a_{m-1}\ b^{m-1} + \ .....\ + a_1 b + a_0$$

where a_i's are integers such that

$$0 \le a_i < b \qquad \text{for all } i = 1, \ldots\ldots\ldots, m.$$

Uniqueness of $a_i s$.

Suppose $N = c_m b^m + c_{m-1} b^{m-1} + \ .....\ + c_1 b + c_0$ where each c_i is an integer such that $0 \le c_i < b$. We can choose same m in both the representations of N because if one representation of N has lesser terms we can always insert zero coefficients and thus make the number of terms to be same.

$\therefore \qquad 0 = (a_m - c_m) b^m + \ldots. + (a_1 - c_1)\, b + (a_0 - c_0)$

Let $\qquad a_i - c_i = d_i$.

Then $\qquad d_m b^m + \ldots\ldots + d_1 b + d_0 = 0.$

We have to show that $d_i = 0$ for all i.

Suppose for some i, $d_i \ne 0$. Let k be the least subscript such that $d_k \ne 0$

Then $\qquad d_k b^k + d_{k+1} b^{k+1} + \ldots\ldots + d_m b^m = 0$

$$\Rightarrow d_k b^k = -(d_{k+1} b^{k+1} + \ .....\ + d_m b^m)$$

$$\Rightarrow d_k = -(d_{k+1} b + d_{k+2} b^2 + \ .....\ + d_m b^{m-k})$$

$$= d_k = -b\ (d_{k+1} + d_{k+2} b\ .....\ + d_m b^{m-k-1})$$

$$\Rightarrow b \mid d_k$$

$$\Rightarrow b \mid |d_k|$$

$$\Rightarrow b \le |d_k|$$

But $\qquad a_k, c_k < b \Rightarrow |a_k - c_k| < b$

$$\Rightarrow |d_k| < b,$$

So, we get a contradiction

$\therefore \qquad d_i = 0$ for all $i = 1, \ldots\ldots, m$

$\therefore \qquad a_i = c_i$ for all $i = 1, \ldots\ldots, m$

Note : When the integer N is expressed as

$$N = a_m b^m + \ .....\ + a_1 b + a_0, \quad 0 \le a_i < b,$$

we write

$$N = (a_m a_{m-1}\ .....\ a_1 a_0) b$$

and say that N is $a_m a_{m-1}\ .....\ a_0$ to the base b.

For example,

$$132 = 1.10^2 + 3.10 + 2 \text{ (Here base is 10)}$$

Then as above

$$132 = (132)_{10}$$

So, numbers that we usually write are to the base 10.

Again, if we want to write 132 to the base 2, we first write

$$132 = 2^7 + 2^2 = 2^7 + 0.2^6 + 0.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 0.2 + 0$$

and by basis representation theorem, then

$$132 = (10000100)_2$$

Problem 12 : *If a, b are integers with $b \neq 0$, show that there exist unique integers q and r satisfying $a = bq + r$ where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$.*

Solution : By Euclid's algorithm, there exist unique integers q', r' such that

$$a = q'|b| + r', \quad \text{where } 0 \leq r' < |b|$$

(as $|b| > 0$ when $b \neq 0$).

Case 1 : $0 \leq r' \leq \frac{1}{2}|b|$

Take $\quad r' = r, \; q' = q$ (if $b > 0$), $q' = -q$ (if $b < 0$)

Since $\quad -\frac{1}{2}|b| < 0 \leq r' = r \leq \frac{1}{2}|b|,$

$$-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$$

Also $\quad a = q'|b| + r'$ becomes

$$a = qb + r \qquad \text{if } b > 0$$

and

$$a = (-q)(-b) + r \qquad \text{if } b < 0$$
$$= qb + r$$

where $\quad -\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$

Case 2 : $\frac{1}{2}|b| < r' < |b|$

Take

$$r' = r + |b|$$
$$q' = q - 1 \qquad \text{if } b > 0$$
$$= -q - 1 \qquad \text{if } b < 0$$

Now $\quad \frac{1}{2}|b| < r' = r + |b|$

$$\Rightarrow -\frac{1}{2}|b| < r$$

Also $\quad r' = r + |b| < |b|$

$$\Rightarrow r < 0 < \frac{1}{2}|b|$$

$\therefore \quad -\frac{1}{2}|b| < r < \frac{1}{2}|b|$

Again $\quad a = |b|q' + r'$ becomes

$$a = b\ (q-1) + r + b \qquad \text{when } b > 0$$
$$= bq + r$$

Also, when $b > 0, a = |b|\, q' + r'$ becomes

$$a = -b\,(-q-1) + r - b$$
$$= bq + r$$

where $\quad -\frac{1}{2}|b| < r < \frac{1}{2}|b|.$

The Greatest Common Divisor

A special case in Euclid's algorithm arises when the remainder is zero. We discuss it in this section.

Definition : An integer $d > 0$ is called greatest common divisor (*g.c.d.*) of two integers a, b (non zero) if

(*i*) $d|a,\ d|b$

(*ii*) If $c|a,\ c|b$ then $c|d$

We write d = *g.c.d.* (a, b) or simply $d = (a, b)$.

Remarks :

(*i*) $(a, 0) = |a|,\ (0, b) = |b|$

Clearly, $|a|\,|a,\ |a|\,|0$

If $c|a$, then $c|\,|a| \Rightarrow (a, 0) = |a|$

Similarly $(0, b) = |b|$

(*ii*) If $a|b$, then $(a, b) = |a|$

$|a|\,|a$, and $a|b \Rightarrow |a|\,|b$

If $c|a,\ c|b$, then $c|\,|a|$

$\therefore\ (a, b) = |a|$

(*iii*) *g.c.d.* of a and b does not depend on signs of a and b

i.e. $(a, b) = (-a, b) = (a, -b) = (-a, -b)$

Let $d = (a, b)$. Then $d|a,\ d|b \Rightarrow d|-a,\ d\ |b$

$c|-a,\ c|b \Rightarrow c|a,\ c|b \Rightarrow c|d$

$\therefore\ d = (-a, b)$. Similarly for others.

We now show the existence and uniqueness of g.c.d. of integers a and b.

Theorem 18 : *Let a, b be two integers. Suppose either $a \neq 0$ or $b \neq 0$. Then $\exists$ greatest common divisor d of a, b such that*

$$d = ax + by \text{ for some integers } x, y.$$

d is uniquely determined by a and b.

Proof : Let $S = \{au + bv \mid u,\ v$ are integers and $au + bv > 0\}$.

If $a > 0$, then $a = a.1 + b.0 > 0 \Rightarrow a \in S$.

If $a < 0$, then $-a = a(-1) + b.0 > 0 \Rightarrow -a \in S$.

Similarly, if $b > 0$ then $b \in S$ and if $b < 0$ then $-b \in S$. Since one of a and b is non zero, either $\pm a \in S$ or $\pm b \in S$. In any case $S \neq \varphi$.

By well ordering principle S has a least element, say d.

Now $d \in S \Rightarrow ax + by$ for some integers x and y. Also $d > 0$.

Let $a = dq + r,\ 0 \leq r < d$.

Let $r \neq 0$. Since $r = a - dq$

$$= a - (ax + by)\ q$$

$$= a\ (1 - xq) + b\ (-yq) > 0$$

$$\Rightarrow r \in S.$$

But $r < d$, contradicting the fact that d is least element of S. So, $r = 0$.

Therefore, $a = dq \Rightarrow d \mid a$.

Similarly, $d \mid b$.

Suppose, $c \mid a,\ c \mid b \Rightarrow c \mid ax + by = d$.

So, d is a greatest common divisor of a and b.

If d' is also greatest common divisor of a and b, then $d' \mid a,\ d' \mid b, \Rightarrow d \mid d'$. Similarly, $d \mid a,\ d \mid b \Rightarrow d' \mid d$. Since $d,\ d' > 0,\ d = d'$. So d is uniquely determined by a and b.

Remark : x and y in above theorem need not be unique.

For, $\quad d = ax + by$

$$\Rightarrow d = a\,(x - b) + b\ (a + y)$$

If $x - b = x,\ a + y = y \Rightarrow b = 0 = a$, which is not true. So either $x - b \neq x$ or $a + y \neq y$.

Definition : If *g.c.d.* $(a, b) = 1$, then a and b are said to be *relatively prime* or *co-prime*.

Cor. 1 : Two integers a, b are relatively prime if and only if $\exists$ integers x, y such that $ax + by = 1$.

Proof : Suppose a, b are relatively prime. Then *g.c.d.* $(a, b) = 1$. By above theorem $\exists$ integers x, y such that $ax + by = 1$.

Conversely, let $ax + by = 1$ for some integers x, y Let $d =$ *g.c.d.* (a, b). Then $d \mid a,\ d \mid b \Rightarrow d \mid ax,\ d \mid by \Rightarrow d \mid ax + by = 1 \Rightarrow d = 1$.

So, a, b are relatively prime.

Cor. 2 : If *g.c.d.* $(a, b) = d$, then *g.c.d.* $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Proof : *g.c.d.* $(a, b) = d$

$\Rightarrow \exists$ integers x, y such that

$$d = ax + by$$

$$\Rightarrow 1 = \frac{a}{d}x + \frac{b}{d}y$$

$$\Rightarrow \text{ g.c.d. } \left(\frac{a}{d}, \frac{b}{d}\right) = 1 \qquad \text{by Cor 1.}$$

Cor. 3 : If $a \mid bc$, with *g.c.d.* $(a, b) = 1$, then $a \mid c$

Proof : g.c.d. $(a, b) = 1 \Rightarrow \exists$ integers x, y s.t.

$$ax + by = 1 \Rightarrow acx + bcy = c$$

Now $\quad a \mid ac, a \mid bc \Rightarrow a \mid acx, \; a \mid bcy$

$$\Rightarrow a \mid acx + bcy = c$$

Cor. 4 : If *g.c.d.* $(a, b) = 1$ and *g.c.d.* $(a, c) = 1$, then *g.c.d.* $(a, bc) = 1$.

Proof :Since *g.c.d.* $(a, b) = 1$, $\exists$ integers x, y such that $ax + by = 1$. Also, *g.c.d.* $(a, c) = 1$, $\exists$ integers u, v such that $au + cv = 1$.

$$\therefore \quad 1 = (ax + by)\ (au + cv)$$

$$= a\,(axu + cxv + byu) + bc\,(yv)$$

By Cor. 1, *g.c.d.* $(a, bc) = 1$.

We now give a practical method of finding greatest common divisor of two integers. We first prove the following result.

Lemma : If $a = bq + r$, then *g.c.d.* $(a, b) =$ *g.c.d.* (b, r).

Proof : Let *g.c.d.* $(a, b) = d$.

Then $d \mid a, \; d \mid b \Rightarrow d \mid a, \; d \mid bq \Rightarrow d \mid a - bq = r$. Suppose $c \mid b, \; c \mid r$.

Then $c \mid bq, \; c \mid r \Rightarrow c \mid bq + r \Rightarrow c \mid a, \; c \mid b \Rightarrow c \mid d$. Thus $d =$ *g.c.d.* (b, r).

Let a, b be two integers.

Since *g.c.d.* $(a, b) =$ *g.c.d.* $(|a|, |b|)$, let $a \geq b > 0$.

Let $a = bq_1 + r_1, \; 0 \leq r_1 < b$.

If $r_1 = 0$, Then $b \mid a$ and *g.c.d.* $(a, b) = b$.

Let $r_1 \neq 0$. Divide b by r_1 to get integers q_2 and r_2 s.t.

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then *g.c.d.* $(b, r_1) = r_1$ and so by above lemma, *g.c.d.* $(a, b) = r_1$

If $r_2 \neq 0$, then proceeding as above till we get remainder as zero,

We have

$$a = q_1 b + r_1, \qquad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2$$

.....

$$r_{n-2} = q_n r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1}\ r_n + 0$$

By above lemma,

g.c.d. $(a, b) =$ *g.c.d.* $(b, r_1) = \ldots\ldots =$ *g.c.d.* $(r_n, 0) = r_n$

So, last remainder r_n is *g.c.d* of a and b.

For example, to determine *g.c.d.* (56, 72), we divide 72 by 56 to get,

$$72 = 56 + 16$$
$$56 = 16 \times 3 + 8$$
$$16 = 8 \times 2 + 0$$

Since last non zero remainder is 8, g.c.d. (56, 72) = 8.

Also,
$$\begin{aligned} 8 &= 56-16 \times 3 \\ &= 56-(72-56) \times 3 \\ &= 56 \times (4) + 72\ (-3) \\ &= 56\ x + 72y \quad \text{where } x = 4,\ y = -3 \end{aligned}$$

which shows us the way to find x, y s.t.,

$$g.c.d.\ (a,\ b) = ax + by$$

Theorem 19 : *Let* $k > 0$. *Then* $g.c.d.\ (ka,\ kb) = k\ g.c.d.\ (a,\ b)$.

Proof : Let $\quad g.c.d.\ (a,\ b) = d$

Then $\quad d|a,\ d|b \Rightarrow kd|ka,\ kd|kb$

Also $\exists$ integers x, y s.t.

$$d = ax + by$$
$$\Rightarrow kd = kax + kby$$

Let $\quad c|ka,\ c|kb$ then $c|kax,\ c|kby$

$$\Rightarrow c|kax + kby = kd$$
$$\Rightarrow g.c.d.\ (ka,\ kb) = kd = k\ g.c.d.\ (a, b)$$

(Note, as $k > 0$, $d > 0$ we get $\Rightarrow kd > 0$)

Cor : For any integer $k \neq 0$, $g.c.d.\ (ka,\ kb) = |k|\ g.c.d.\ (a,\ b)$.

Proof : For $k > 0$, result follows from above theorem.

Let $k < 0$. Then $g.c.d.\ (ka,\ kb)$

$$= g.c.d.\ (-ka,\ -kb)$$
$$= -k\ g.c.d.\ (a,\ b) \text{ by above theorem}$$
$$= |k|g.c.d.\ (a,\ b)$$

Definition : The *least common multiple* of two non zero integers a and b, denoted by l.c.m. $(a,\ b)$, is the positive integer m s.t.,

(*i*) $a|m,\ b|m$

(*ii*) if $a|c,\ b|c,$ with $c > 0$, then $m|c$.

Theorem 20 : *For positive integers a and b*

$$g.c.d.\ (a,\ b)\ l.c.m.\ (a,\ b) = ab$$

Proof : Let $\quad d = g.c.d.\ (a,\ b)$

Now $\quad \dfrac{ab}{d} = a.\dfrac{b}{d} \Rightarrow a \left| \dfrac{ab}{d} \right. \quad$ as $\dfrac{b}{d}$ is integer

Also $$\frac{ab}{d} = b.\frac{a}{d} \Rightarrow b \left| \frac{ab}{d} \right. \qquad \text{as } \frac{a}{d} \text{ is integer}$$

Let $a \mid c$, $b \mid c$. Since $(a, b) = d$, $\exists$ integers x, y s.t. $d = ax + by$. Let $m = \dfrac{ab}{d}$.

$$\therefore \qquad \frac{c}{m} = \frac{cd}{ab} = \frac{c\,(ax+by)}{ab} = \left(\frac{c}{b}\right) x + \left(\frac{c}{d}\right) y = \text{integer}$$

$$\Rightarrow m \mid c.$$

Problem 13 : *Let g.c.d.* $(a, b) = 1$.

Show that g.c.d $(a + b,\ a^2 - ab + b^2) = 1$ *or* 3.

Solution : Let $\quad$ g.c.d. $(a + b,\ a^2 - ab + b^2) = d$

Then $\quad d \mid a + b,\ d \mid a^2 - ab + b^2$

$$\Rightarrow d \mid (a+b)^2 = a^2 + b^2 + 2ab, \quad d \mid a^2 - ab + b^2$$

$$\Rightarrow d \mid 3ab$$

Let $\quad$ g.c.d. $(d, a) = e$

Then $\quad e \mid d \mid a + b \Rightarrow e \mid a + b$ and $e \mid a$

$\therefore \quad e \mid (a + b) - a = b$

So, $\quad e \mid$ g.c.d. $(a, b) = 1 \Rightarrow e = 1$

$\therefore \quad$ g.c.d. $(d, a) = 1$

Similarly, $\quad$ g.c.d. $(d, b) = 1$

$\therefore \quad d \mid 3 \Rightarrow d = 1$ or 3.

Problem 14 : *Let g.c.d.* $(a, b) = 1$. *Show that g.c.d.* $(a^n, b^n) = 1$ *for every integer* $n \geq 1$.

Solution : Since g.c.d. $(a, b) = 1$, $\exists$ integers x, y such that $ax + by = 1$.

$$\Rightarrow (ax + by)\ (ax + by) = 1$$

$$\Rightarrow a^2x^2 + 2abxy + by^2 = 1$$

$$\Rightarrow a^2x^2 + b\,(2axy + y^2) = 1$$

$$\Rightarrow \text{g.c.d. } (a^2, b) = 1$$

In this way we will get

$$\text{g.c.d. } (a^n, b) = 1 \quad \text{or} \quad \text{g.c.d. } (b, a^n) = 1$$

Proceeding as above, we get

$$\text{g.c.d. } (b^n, a^n) = 1$$

Definition : By a Linear Diophantine equation we mean an equation $ax + by = c$ in two unknowns x and y, where a, b, c are given integers and one of a, b is not zero., The name is due to the mathematician Diophantus. A natural question arises as to when such an equation would have a solution? The answer is provided by

Theorem 21 : *The linear Diophantine equation $ax + by = c$ has a solution if and only if $d \mid c$ where d = g.c.d. (a, b). If x_0, y_0 is a particular solution, then the other solutions are given by*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

for varying integer t.

Proof : Suppose $ax + by = c$ has a solution.

Let $x = x_0$, $y = y_0$ be a solution.

Then $ax_0 + by_0 = c$. Let d = g.c.d. (a, b).

$$\therefore \qquad d \mid a,\ d \mid b \Rightarrow d \mid ax_0,\ d \mid by_0$$

$$\Rightarrow d \mid ax_0 + by_0 = c$$

Conversely, let $d \mid c$. Let $c = dk$.

Since d = g.c.d (a, b), $\exists$ integers x_0, y_0 s.t.,

$$ax_0 + by_0 = d \Rightarrow a\ (x_0k) + b\ (y_0k) = dk = c$$

$$\Rightarrow ax + by = c \text{ has a solution } x = x_0k,\ y = y_0k.$$

To prove the second assertion, let x_0, y_0 be a given solution of $ax + by = c$.

Let x', y' be any solution of $ax + by = c$.

$$\therefore \qquad ax_0 + by_0 = ax' + by' = c$$

$$\Rightarrow a(x_0 - x') = b(y' - y_0)$$

$$\Rightarrow \frac{a}{d}(x_0 - x') = \frac{b}{d}(y' - y_0), \text{ where } d = \text{g.c.d. } (a, b)$$

$$\Rightarrow \frac{b}{d} \Big| \frac{a}{d}\ (x_0 - x')$$

Since $\qquad$ g.c.d. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$

$$\frac{b}{d} \mid x_0 - x' \Rightarrow \frac{b}{d} \mid x' - x_0$$

$$\Rightarrow x' - x_0 = \frac{b}{d}t, \qquad t \text{ is an integer}$$

$$\Rightarrow x' = x_0 + \frac{b}{d}t \Rightarrow \frac{a}{d}\frac{b}{d}t = \frac{b}{d}(y_0 - y')$$

$$\Rightarrow \frac{a}{d}t = y_0 - y' \Rightarrow y' = y_0 - \frac{a}{d}t$$

It can be easily seen that for all values of t, $x' = x_0 + \frac{b}{d}t$, $y' = y_0 - \frac{a}{d}t$ is a solution of $ax + by = c$ as

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$
$$= ax_0 + by_0 = c.$$

Problem 15 : *Determine all the solutions in the integers of the following Diophantine equation* $56x + 72y = 40$.

Solution : We first find *g.c.d.* (56, 72).

Now $\quad 72 = 56 + 16$

$56 = 3 \times 16 + 8$

$16 = 2 \times 8$

Hence, $\quad$ *g.c.d.* $(56, 72) = 8$.

$8 = 56 - 3 \times 16$

$= 56 - 3 \times (72 - 56)$

$= 4 \times 56 - 3 \times 72$

$\Rightarrow 40 = 56 \times 20 + 72 \times (-15)$

$\Rightarrow x = 20,\ y = -15$, is a solution of $56x + 72y = 40$.

By above theorem any other solution is given by $\left(20 + \frac{72}{8}t, -15 - \frac{56}{8}t\right)$

$= (20 + 9t, -15 - 7t)$ for any integer t.

Prime Numbers

An integer $p > 1$ is called a *prime number* if 1 and p are the only divisors of p.

Theorem 22 : *If a prime under p divides ab, then either p divides a or p divides b.*

Proof : Let $ab = pc$ for some integer c.

Suppose p does not divide a.

Then $\quad$ *g.c.d.* $(a, p) = 1$

$\therefore \quad p \mid ab$ and *g.c.d.* $(a, p) = 1$

$\Rightarrow p \mid b$

We generalise the above result in the following theorem.

Theorem 23 : *If p divides* $a_1 a_2 \ldots\ldots a_n$, *then p divides* a_i *for some i.*

Proof : We prove the result by induction on n.

If $n = 1$, then result is clearly true.

If $n = 2$, the result follows from above.

Let the result be true for naturals less than n.

Suppose $\quad p \mid a_1 \ldots\ldots a_n = (a_1 \ldots\ldots a_{n-1}) a_n$

$$\Rightarrow p \mid a_1 \ldots\ldots a_{n-1} \text{ or } p \mid a_n$$

If p divides $a_1 \ldots\ldots a_{n-1}$, then by induction hypothesis p divides a_i, for some i.

So result is true in this case also.

By induction result is true for all $n > 1$.

Composite Numbers

A composite number is an integer $n > 1$ such that n is not prime.

Problem 16 : *Prove that if $2^n - 1$ is prime, then n is prime.*

Solution : Let $2^n - 1 = p =$ prime.

Let n be not prime.

Then $n = rs$, $1 < r, s < n$

$$\therefore \quad p = 2^n - 1$$

$$= 2^{rs} - 1 = (2^r)^s - 1$$

$$= x^s - 1, \; x = 2^r > 2 \text{ as } r > 1$$

$$= (x-1)(x^{s-1} + x^{s-2} + \ldots\ldots + x + 1)$$

Either $x - 1 = 1$ or $x^{s-1} + \ldots\ldots + x + 1 = 1$

$x - 1 = 1 \Rightarrow x = 2$, which is not true

and $\quad x^{s-1} + \ldots\ldots + x + 1 = 1$

$\Rightarrow x^{s-1} + \ldots\ldots + x = 0$, which is not true

$\therefore \quad n$ is prime.

Problem 17 : *Prove that $n^4 + 4$ is composite if $n > 1$.*

Solution : $\quad n^4 + 4 = (n^2 + 2)^2 - 4n^2$

$$= (n^2 + 2 - 2n)(n^2 + 2 + 2n)$$

$$n > 1 \Rightarrow n \geq 2 \Rightarrow n^2 \geq 2n \Rightarrow n^2 - 2n \geq 0$$

$$\Rightarrow n^2 - 2n + 2 \geq 2$$

Also $\quad n^2 + 2 + 2n > 1$

$\therefore n^4 + 4$ is composite as both $n^2 + 2 + 2n$ and $n^2 + 2 + 2n < n^4 + 4$.

Congruences

Let a, b, c, $(c > 0)$ be integers. We say a is congruent to b modulo c if c divides $a - b$ and write $a \equiv b \pmod{c}$. This relation '$\equiv$' on the set of integers is an equivalence relation as seen earlier.

Addition, subtraction and multiplication in congruences behave naturally.

Let $\quad a \equiv b \pmod{c}$

$$a_1 \equiv b_1 \pmod{c} \Rightarrow c \mid a-b,\ c \mid a_1 - b_1$$
$$\Rightarrow c \mid (a + a_1) - (b + b_1)$$
$$\Rightarrow a + a_1 \equiv b + b_1 \pmod{c}$$

Similarly $a - a_1 \equiv b - b_1 \pmod{c}$

Also $c \mid a-b,\ c \mid a_1 - b_1$

$$\Rightarrow c \mid aa_1 - ba_1,\ c \mid ba_1 - bb_1$$
$$\Rightarrow c \mid (aa_1 - ba_1) + (ba_1 - bb_1)$$
$$\Rightarrow c \mid aa_1 - bb_1$$
$$\Rightarrow aa_1 \equiv bb_1 \pmod{c}$$

We may, however, not be able to achieve the above result in case of division. Indeed $\frac{a}{a_1}$ or $\frac{b}{b_1}$ may not even be integers.

Again, cancellation in congruences in general may not hold.

i.e., $ad \equiv bd \pmod{c}$ need not essentially imply

$a \equiv b \pmod{c}$

For example, $2.2 \equiv 2.1 \pmod{2}$

but $2 \not\equiv 1 \pmod{2}$

However, cancellation holds if $g.c.d.\ (d,\ c) = 1$.

i.e. if $ad \equiv bd \pmod{c}$

and $g.c.d.\ (d,\ c) = 1$

then $a \equiv b \pmod{c}$

Proof : $ad \equiv bd \pmod{c}$

$$\Rightarrow c \mid ad - bd$$
$$\Rightarrow c \mid d\,(a-b)$$
$$\Rightarrow c \mid a-b \text{ as } g.c.d.\ (c\ d) = 1$$
$$\Rightarrow a \equiv b \pmod{c}.$$

Problem 18 : *If $a \equiv b$ (mod n), prove that g.c.d. $(a,\ n)$ = g.c.d. $(b,\ n)$.*

Solution. Let $d = g.c.d.\ (a,\ n)$

Then $d \mid a,\ d \mid n$. But $n \mid a-b$

$\therefore$ $d \mid a-b,\ d \mid a$

$$\Rightarrow d \mid a - (a-b) = b$$

$\therefore$ $d \mid b,\ d \mid n$

Let $c \mid b,\ c \mid n \Rightarrow c \mid b,\ c \mid a-b$ as $n \mid a-b$

$$\Rightarrow c \mid a - b + b = a$$
$$\Rightarrow c \mid a,\ c \mid n$$
$$\Rightarrow c \mid d \text{ as } d = g.c.d.\ (a,\ n)$$

Problem 19 : *Establish that if a is an odd integer, then*

$\therefore$ $$g.c.d.\ (b,\ n) = d$$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}} \text{ for any } n \geq 1.$$

Solution : We prove the result by induction on n.

Let $n = 1$. Then

$$a^{2^n} = a^2$$

and $$2^{n+2} = 2^3 = 8$$

Let $a = 2k + 1$. Then

$$a^2 = 4k^2 + 4k + 1$$
$$= 4k\ (k+1) + 1$$

$\therefore$ $$a^2 - 1 = 4k\ (k+1)$$
$$= \text{multiple of 8 as either } k \text{ is even or } k+1 \text{ is even.}$$

$\therefore$ $$a^2 \equiv 1 \pmod 8$$

So, result is true for $n = 1$.

Assume that the result is true for $n = k$.

Then $$a^{2^k} \equiv 1 \pmod{2^{k+2}}$$

Now $$a^{2^{k+1}} - 1 = (a^{2^k})^2 - 1$$

$$= (a^{2^k} - 1)(a^{2^k} + 1)$$

$$= (\text{multiple of } 2^{k+2})\ (a^{2^k} + 1) \text{ by induction hypothesis.}$$

But $$a = \text{odd} \Rightarrow a^{2^k} = \text{odd} \Rightarrow a^{2^k} + 1 = \text{even}$$

$\therefore$ $$a^{2^{k+1}} - 1 = \text{multiple of } 2^{k+3}$$

$\therefore$ $$a^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$$

So, result is true for $n = k + 1$.

By induction, result is true for all $n \geq 1$.

Problem 20 : *Show that for any integer a,*

$$a^3 \equiv 0,\ 1,\ \text{or } 8 \pmod 9$$

Solution : Let $a = 3k + r,\ 0 \leq r < 3$

If $r = 0$, then $a = 3k$

$$\Rightarrow a^3 = 27k^3 \equiv 0 \pmod 9$$

If $r = 1$, then $a = 3k + 1$

$\therefore$ $$a^3 = 27k^3 + 1 + 9k^2 + 9k$$

$$\Rightarrow a^3 \equiv 1 \pmod 9$$

If $a = 3k+2$, then $a^3 = 27k^3 + 8 + 27k^2 + 36k^2$

$$\Rightarrow a^3 \equiv 8 \pmod 9$$

$\therefore$ $a^3 \equiv 0,\ 1$ or $8 \pmod 9$.

Problem 21 : *If* $ca \equiv cb \pmod n$, *then* $a \equiv b\left(\bmod \frac{n}{d}\right)$, *where* d = *g.c.d.* (c, n).

Solution : d = *g.c.d.* (c, n)

$$\Rightarrow 1 = \text{g.c.d.}\left(\frac{c}{d}, \frac{n}{d}\right)$$

Also $ca \equiv cb \pmod n$

$$\Rightarrow ca - cb = nk \text{ for some integer } k$$

$$\Rightarrow \frac{c}{d}a - \frac{c}{d}b = \frac{n}{d}k$$

$$\Rightarrow \frac{n}{d} \Big| \frac{c}{d}(a-b)$$

$$\Rightarrow \frac{n}{d} \mid a-b \text{ as g.c.d.}\left(\frac{c}{d}, \frac{n}{d}\right) = 1$$

$$\Rightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Problem 22 : *Find the remainder obtained by dividing* $1! + 2! + 3! + 4! + \ldots\ldots + 100!$ *by* 12.

Solution : Each number 4! onwards is a multiple of 12.

$\therefore$ $1! + 2! + 3! + 4! + \ldots\ldots + 100! \equiv 1! + 2! + 3! + 0 + \ldots\ldots + 0 \pmod{12}$

$\Rightarrow 1! + 2! + 3! + 4! + \ldots\ldots + 100! \equiv 9 \pmod{12}$

$\Rightarrow$ 9 is the required remainder.

Problem 23 : *Find the remainder when* 2^{50} *is divided by* 7.

Solution : Now $2^3 \equiv 1 \pmod 7$

$$\Rightarrow (2^3)^{16} \equiv 1^{16} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{48} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{48} \cdot 2^2 \equiv 2^2 \pmod 7$$

$$\Rightarrow 2^{50} \equiv 4 \pmod 7$$

$2^{50} \equiv 4 \pmod 7$

$\therefore$ 4 is the remainder.

Problem 24 : *What is the remainder when the sum* $1^5 + 2^5 + 3^5 + \ldots\ldots + 99^5 + 100^5$ *is divided by* 4.

Solution : Note $1 \equiv 1 \pmod 4 \Rightarrow 1^5 \equiv 1 \pmod 4$

$$2^2 \equiv 0 \pmod 4 \Rightarrow 2^5 \equiv 0 \pmod 4$$

$$3^2 \equiv 1 \pmod 4 \Rightarrow 3^5 \equiv 3 \pmod 4$$

$$\Rightarrow 3^5 \equiv -1 \pmod 4$$

$$4^2 \equiv 0 \pmod 4 \Rightarrow 4^5 \equiv 0 \pmod 4$$

$$\therefore 1^5 + 2^5 + 3^5 + 4^5 \equiv 1 + 0 - 1 + 0 \equiv 0 \pmod 4$$

Any numbers after these will be of the form $2k + 1$, $2k + 2$, $2k + 3$, $2k + 4$, $k > 1$.

Now $(2k + 1)^2 \equiv 1 \pmod 4 \Rightarrow (2k + 1)^5 \equiv 2k + 1 \equiv 1 \pmod 4$

$$(2k + 2)^2 \equiv 0 \pmod 4 \Rightarrow (2k + 2)^5 \equiv 0 \pmod 4$$

$$(2k + 3)^2 \equiv 1 \pmod 4 \Rightarrow (2k + 3)^5 \equiv 2k + 3 \equiv -1 \pmod 4$$

$$(2k + 4)^2 \equiv 0 \pmod 4 \Rightarrow (2k + 4)^5 \equiv 0 \pmod 4$$

$$\therefore \quad 1^5 + 2^5 + 3^5 + 4^5 + \ldots\ldots + 99^5 + 100^5 \equiv 0 \pmod 4$$

So, remainder is 0 when above number is divided by 4.

Before we finish with this chapter we recall the *Well Ordering Principle*, which states that any non empty subset of real numbers which is bounded below has least element. It is sometimes denoted by W.O.P.

Exercises

1. Prove that is a and b are integers with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.
2. Use Euclid's algorithm to establish that
   (*i*) every odd integer is of the form $4k + 1$ or $4k + 3$.
   (*ii*) the square of any integer is either of the form $3k$ or $3k + 1$.
   (*iii*) the cube of any integer is of the form $9k$, $9k + 1$ or $9k + 8$.
3. If $(a, b) = 1$, show that $(a + b, a - b)$ is either 1 or 2.
4. If $(a, b) = 1$, show that
   (i) $(2a + b, a + 2b) = 1$ or 3
   (*ii*) $(a + b, a^2 + b^2) = 1$ or 2
   (*iii*) $(ac, b) = (c, b)$
5. Given x and y, let $m = ax + by$, $n = cx + dy$, where $ad - bc = \pm 1$. Prove that $(m, n) = (x, y)$.
6. Let $\Phi_n = 2^{2^n} + 1$. Prove that if $n < m$, then Φ_n divides $\Phi_m - 2$. (Φ_n is called Fermat number).
7. Prove that if $n \neq m$, $(\Phi_n, \Phi_m) = 1$.
8. Prove that l.c.m. $(ab, ad) = a$ [l.c.m. (b, d)]
9. Prove that if a, b are non zero integers, then g.c.d. $(a, b) \mid$ l.c.m. (a, b).
10. Prove that if $2^n + 1$ is prime, then n is a power of 2.

11. Let $d = (826, 1890)$. Use Euclid's algorithm to compute d and then express d as a linear combination of 826 and 1890.

12. Show that $a^n \mid b^n$ implies $a \mid b$.

13. Determine all solutions in the positive integers of the following Diophantine equation

$$172x + 20y = 100. \qquad (\textit{Ans. } (5, 7))$$

14. Find the remainder when 41^{65} is divided by 7.

15. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.

16. Prove that if $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$ with $g.c.d.\ (b, n) = 1$, then $a \equiv c \pmod{n}$.

17. If $a \equiv b \pmod{n_1}$, and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$ where $n = (n_1, n_2)$.

18. Which of the following congruences hold ?

(*i*) $12, 345, 678, 987, 654, 321 \equiv 0 \pmod{12, 345, 678}$

(*ii*) $12, 345, 678, 987, 654, 321 \equiv 0 \pmod{12, 345, 679}$

19. Prove that if $|a| < \frac{k}{2}, |b| < \frac{k}{2}$ and $a \equiv b \pmod{k}$, then $a = b$.

20. Prove that if $bd \equiv bd' \pmod{p}$ where $p =$ prime and $p \nmid b$ then $d \equiv d' \pmod{p}$.

Chapter 2

Groups

In the previous chapter we studied the notions of relations, maps and in particular binary compositions. We now come to the study of different algebraic structures or algebraic systems, which means a non empty set with one or more binary compositions. We start with groups which occupy a very important seat in the study of abstract algebra.

Definition : A non empty set G, together with a binary composition $*$ (star) is said to form a group, if it satisfies the following postulates

(*i*) *Associativity* : $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$

(*ii*) *Existence of Identity* : $\exists$ an element $e \in G$, s.t.,

$$a * e = e * a = a \text{ for all } a \in G$$

(e is then called *identity*)

(*iii*) *Existence of Inverse* : For every $a \in G$, $\exists$ $a' \in G$ (depending upon a) s.t.,

$$a * a' = a' * a = e$$

(a' is then called inverse of a)

Remarks : (*i*) Since $*$ is a binary composition on G, it is understood that for all $a, b \in G$, $a * b$ is a unique member of G. This property is called *closure property*.

(*ii*) If, in addition to the above postulates, G also satisfies the *commutative law*

$$a * b = b * a \quad \text{for all } a, b \in G$$

then G is called an *abelian group* or a *commutative group*.

(*iii*) Generally, the binary composition for a group is denoted by '.' (dot) which is so convenient to write (and makes the axioms look so natural too).

This binary composition '.' is called product or multiplication (although it may have nothing to do with the usual multiplication, that we are so familiar with). In fact, we even drop '.'and simply write ab in place of $a \,.\, b$.

In future, whenever we say that G is a group it will be understood that there exists a binary composition '.' on G and it satisfies all the axioms in the definition of the group.

If the set G is finite (i.e., has finite number of elements) it is called a *finite group* otherwise, it is called *infinite group*.

We shall always (unless stated otherwise) use the symbols e for identity of a group and a^{-1} for inverse of element a of the group.

Definition : By order of a group, we will mean the number of elements in the group and shall denote it by $o(G)$ or $|G|$.

We now consider a few examples of systems that form groups (or do not form groups).

Example 1 : The set **Z** of integers forms an abelian group w.r.t. the usual addition of integers.

It is easy to verify the postulates in the definition of a group as sum of two integers is a unique integer (thus closure holds). Associativity of addition is known to us. 0 (zero) will be identity and negatives will be the respective inverese elements. Commutativity again being obvious.

Example 2 : One can easily check, as in the previous example, that sets **Q** of rationals, **R** of real numbers would also form abelian groups w.r.t. addition.

Example 3 : Set of integers, w.r.t. usual multiplication does not form a group, although closure, associativity, identity conditions hold.

Note 2 has no inverse w.r.t. multiplication as there does not exist any integer a s.t., $2 . a = a . 2 = 1$.

Example 4 : Let G be the set $\{1, -1\}$. Then it forms an abelian group under multiplication. It is again easy to check the properties.

1 would be identity and each element is its own inverse.

Example 5 : Set of all 2×2 matrices over integers under matrix addition would be another example of an abelian group.

Example 6 : Set of all non zero complex numbers forms a group under multiplication defined by

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

$1 = 1 + i . 0$ will be identity,

$\dfrac{a}{a^2 + b^2} - i\dfrac{b}{a^2 + b^2}$ will be inverse of $a + ib$.

Note $a + ib$ non zero means that not both a & b are zero. Thus $a^2 + b^2 \neq 0$.

Example 7 : The set G of all n^{th} roots of unity, where n is a fixed positive integer forms an abelian group under usual multiplication of complex numbers.

We know that complex number z is an nth root of unity if $z^n = 1$ and also that there exist exactly n distinct roots of unity.

In fact the roots are given by

$$e^{\frac{2\pi ir}{n}}$$

where $r = 1, 2, \ldots, n$ and $e^{ix} = \cos x + i \sin x$

If $a, b \in G$ be any two members, then $a^n = 1$, $b^n = 1$ thus $(ab)^n = a^n\ b^n = 1$.

$$\Rightarrow ab \text{ is an } n^{th} \text{ root of unity}$$

$$\Rightarrow ab \in G \Rightarrow \text{closure holds.}$$

Associativity of multiplication is true in complex numbers.

Again, since $1 \,.\, a = a \,.\, 1 = a$, 1 will be identity.

Also for any $a \in G$, $\dfrac{1}{a}$ will be its inverse as $\left(\dfrac{1}{a}\right)^n = \dfrac{1}{a^n} = 1$.

Commutativity being obvious, we find G is an abelian group.

Example 8 : (*i*) Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

then G forms a group. G is not abelian as $ij \neq ji$.

This is called the ***Quaternion Group***.

(*ii*) If set G consists of the eight matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \text{ where } i = \sqrt{-1}$$

then G forms a non abelian group under matrix multiplication. (Compare with part (i)).

Example 9 : Let $G = \{(a, b) \mid a, b \text{ rationals}, a \neq 0\}$, Define $*$ on G by

$$(a, b) * (c, d) = (ac, ad + b)$$

Closure follows as $a, c \neq 0 \Rightarrow ac \neq 0$

$$[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f)$$
$$= (ace, acf + ad + b)$$
$$(a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d)$$
$$= (ace, acf + ad + b)$$

proves associativity.

(1, 0) will be identity and $\left(1/a, -b/a\right)$ will be inverse of any element (a, b).

G is not abelian as

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$
$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

Example 10 : The set G of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over reals, where $ad - bc \neq 0$, forms a non abelian group under matrix multiplication.

The matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will act as identity and

the matrix $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ will be inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Example 11 : Let $G = \{2^r \mid r = 0, \pm 1, \pm 2, \ldots\ldots\}$

We show G forms a group under usual multiplication.

For any $2^r, 2^s \in G$, $2^r . 2^s = 2^{r+s} \in G$

Thus closure holds.

Associativity is obvious.

Again as $1 \in G$, and $x . 1 = 1 . x = x$ for all $x \in G$

1 is identity.

For any $2^r \in G$, as $2^{-r} \in G$ and $2^r . 2^{-r} = 2^0 = 1$,

we find each element of G has inverse. Commutativity is evidently true.

Example 12 : *Group of Residues* : Let $G = \{0, 1, 2, 3, 4\}$. Define a composition $\oplus_5$ on G by $a \oplus_5 b = c$ where c is the least non -ve integer obtained as remainder when $a + b$ is divided by 5. For example, $3 \oplus_5 4 = 2$, $3 \oplus_5 1 = 4$, etc. Then $\oplus_5$ is a binary composition on G (called addition modulo 5). It is easy to verify that G forms a group under this.

One can generalise this result to

$$G = \{0, 1, 2, \ldots\ldots, n-1\}$$

under addition modulo n when n is any positive integer.

We thus notice

$$a \oplus_n b = \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{if } a+b \geq n \end{cases}$$

Also, in case there is no scope of confusion we drop the sub suffix n and simply write $\oplus$. This group is generally denoted by Z_n.

Example 13 : Let $G = \{x \in \mathbf{Z} \mid 1 \leq x < n,\ x, n \text{ being co-prime}\}$ where $\mathbf{Z}$ = set of integers and x, n being co-prime means H.C.F. of x and n is 1.

We define a binary composition $\otimes$ on G by $a \otimes b = c$ where c is the least + ve remainder obtained when $a.b$ is divided by n. This composition $\otimes$ is called multiplication modulo n.

We show G forms a group under $\otimes$.

Closure : For $a, b \in G$, let $a \otimes b = c$. Then $c \neq 0$, because otherwise $n \mid ab$ which is not possible as a, n and b, n are co-prime.

Thus $c \neq 0$ and also then $1 \leq c < n$.

Now if c, n are not co-prime then $\exists$ some prime no. p s.t., $p \mid c$ and $p \mid n$.

Again as $ab = nq + c$ for some q

We get $p \mid ab$ $\quad [p \mid n \Rightarrow p \mid nq,\ p \mid c \Rightarrow p \mid nq + c]$

$\Rightarrow p \mid a$ or $p \mid b$ (as p is prime)

If $p \mid a$ then as $p \mid n$ it means a, nb are not co–prime.

But a, n are co-prime.

Similarly $p \mid b$ leads to a contradiction.

Hence c, n are co-prime and thus $c \in G$, showing that closure holds.

Associativity : Let $a, b, c \in G$ be any elements.

Let $a \otimes b = r_1$, $(a \otimes b) \otimes c = r_1 \otimes c = r_2$

then r_2 is given by $r_1 c = nq_2 + r_2$

Also $a \otimes b = r_1$ means

$$ab = q_1 n + r_1$$

thus

$$ab - q_1 n = r_1$$

$$\Rightarrow (ab - q_1 n)c = r_1 c = nq_2 + r_2$$

$$\Rightarrow (ab)c = r_2 + nq_2 + nq_1 c = n\ (q_1 c + q_2) + r_2$$

or that r_2 is the least non-negative remainder got by dividing $(ab)c$ by n.

Similary, if $a \otimes (b \otimes c) = r_3$ then we can show that r_3 is the least non-ve remainder got by dividing $a(bc)$ by n.

But since $a(bc) = (ab)c$, $r_2 = r_3$

Hence $a \otimes (b \otimes c) = (a \otimes b) \otimes c$.

Existence of Identity : It is easy to see that

$$a \otimes 1 = 1 \otimes a = a \qquad \text{for all } a \in G$$

or that 1 will act as identity.

Existence of Inverse : Let $a \in G$ be any element then a and n are co-prime and thus we can find integers x and y s.t., $ax + ny = 1$

By division algorithm, we can write

$$x = qn + r, \text{ where } 0 \le r < n$$

$$\Rightarrow ax = aqn + ar$$

$$\Rightarrow ax + ny = aqn + ar + ny$$

$$\Rightarrow 1 = aqn + ar + ny$$

or that

$$ar = 1 + (-aq - y)n$$

i.e., $a \otimes r = 1$. Similarly $r \otimes a = 1$. If r, n are co-prime, r will be inverse of a.

If r, n are not co-prime, we can find a prime number p s.t., $p \mid r$, $p \mid n$

$$\Rightarrow p \mid qn \text{ and } p \mid r$$

$$\Rightarrow p \mid qn + r$$

$$\Rightarrow p \mid x$$
$$\Rightarrow p \mid ax \text{ also } p \mid ny$$
$$\Rightarrow p \mid ax + ny = 1$$

which is not possible. Thus r, n are co-prime and so $r \in G$ and is the required inverse of a.

It is easy to see that G will be abelian. We denote this group by G_n and call it the group of integers under multiplication modulo n.

Remark : Suppose $n = p$, a prime, then since all the integers $1, 2, 3, \ldots\ldots, p-1$ are co-prime to p, these will all be members of G. One can show that $G = \{2, 4, 6, \ldots\ldots, 2\ (p-1)\}$ where $p > 2$ is a prime forms an abelian group under multiplication modulo $2p$.

Example 14 : Let $G = \{0, 1, 2\}$ and define $*$ on G by

$$a * b = |a - b|$$

Then closure is established by taking a look at the composition table

*	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Since $a * 0 = |a - 0| = a = 0 * a$, 0 is identity

and $a * a = |a - a| = 0$ shows each element will be its own inverse.

But the system $(G, *)$ fails to be a group as associativity does not hold.

Indeed $\quad 1 * (1 * 2) = 1 * 1 = 0$

but $\quad (1 * 1) * 2 = 0 * 2 = 2$

Example 15 : Let $S = \{1, 2, 3\}$ and let $S_3 = A(S)$ = set of all permutations of S. We showed in the previous chapter that this set satisfies associativity, existence of identity and existence of inverse conditions in the definition of a group. Also clearly, since f, g permutations on S imply that fog is a permutation on S the closure property is ensured. Hence S_3 forms a group. That it is not abelian follows by the fact that $fog \neq gof$ (see details in previous chapter under permutations). This would, in fact, be the smallest non abelian group and we shall have an occasion to talk about this group again under the section on permutation groups.

Remark : Let X be a non empty set and let $M(X)$ = set of *all* maps from X to X, then $A(X) \subseteq M(X)$. $M(X)$ forms a semi group (see definition ahead) under composition of maps. Identity map also lies in $M(X)$ and as a map is invertible iff it is 1–1, onto i.e., a permutation, we find $A(X)$ the subset of all permutations forms a group, denoted by S_X and is called symmetric group of X. If X is finite with say, n elements then $o(M(X)) = n^n$ and $o(S_X) = \lfloor\underline{n}$ and in that case we use the notation S_n for S_X.

In the definition of a group, we only talked about the existence of identity and inverse of each element. We now show that these elements would also be unique, an elementary but exceedingly useful result. We prove it along with some other results in

Lemma : *In a group G,*

(1) *Identity element is unique.*

(2) *Inverse of each* $a \in G$ *is unique.*

(3) $(a^{-1})^{-1} = a$, *for all* $a \in G$, *where* a^{-1} *stands for inverse of* a.

(4) $(ab)^{-1} = b^{-1} a^{-1}$ *for all* $a, b \in G$

(5) $ab = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$ *for all* $a, b, c \in G$

(called the cancellation laws).

Proof : (1) Suppose e and e' are two elements of G which act as identity. Then, since $e \in G$ and e' is identity,

$$e'e = ee' = e$$

and as $e' \in G$ and e is identity

$$e'e = ee' = e'$$

The two $\Rightarrow e = e'$

which establishes the uniqueness of identity in a group.

(2) Let $a \in G$ be any element and let a' and a'' be two inverse elements of a, then

$$aa' = a'a = e$$

$$aa'' = a''a = e$$

Now $$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

Showing thereby that inverse of an element is unique. We shall denote inverse of a by a^{-1}.

(3) Since a^{-1} is inverse of a

$$aa^{-1} = a^{-1}a = e$$

which also implies a is inverse of a^{-1}

Thus $(a^{-1})^{-1} = a$.

(4) We have to prove that ab is inverse of $b^{-1}a^{-1}$ for which we show

$$(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e.$$

Now $$(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]a^{-1}$$
$$= [a(bb^{-1})]a^{-1}$$
$$= (ae)a^{-1} = aa^{-1} = e$$

Similarly $(b^{-1}a^{-1})(ab) = e$

and thus the result follows.

(5) Let $ab = bc$, then

$$b = eb = (a^{-1}a)b$$
$$= a^{-1}(ab) = a^{-1}(ac)$$

$$= (a^{-1}a)\,c = ec = c$$

Thus $\qquad ab = ac \Rightarrow b = c$

which is called the left cancellation law.

One can similarly, prove the right cancellation law.

Example 16 (*a*) : Let $X = \{1, 2, 3\}$ and let $S_3 = A(X)$ be the group of all permutations on X. Consider $f,\ g,\ h \in A(X)$, defined by

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1$$
$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3$$
$$h(1) = 3, \quad h(2) = 1, \quad h(3) = 2$$

It is easy to then verify that $fog = goh$

But $\qquad f \neq h.$

(*b*) If we consider the group in example 9, we find

$$(1, 2) * (3, 4) = (3, 6) = (3, 0) * (1, 2)$$

But $\qquad (3, 4) \neq (3, 0)$

Hence we notice, cross cancellations *may not* hold in a group.

Theorem 1 : *For elements a, b in a group G, the equations $ax = b$ and $ya = b$ have unique solutions for x and y in G.*

Proof : Now $\qquad ax = b$

$$\Rightarrow \quad a^{-1}(ax) = a^{-1}b$$
$$\Rightarrow \quad ex = a^{-1}b$$
$$\text{or} \quad x = a^{-1}b$$

which is the required solution of the equation $ax = b$.

Suppose $x = x_1$ and $x = x_2$ are two solutions of this equation, then

$$ax_1 = b \text{ and } ax_2 = b$$
$$\Rightarrow ax_1 = ax_2$$
$$\Rightarrow x_1 = x_2 \text{ by left cancellation}$$

Showing that the solution is unique.

Similarly $y = ba^{-1}$ will be unique solution of the equation $ya = b$.

Theorem 2 : *A non empty set G together with a binary composition '.' is a group if and only if*

(1) $a(bc) = (ab)c$ *for all* $a,\ b,\ c \in G$

(2) *For any* $a,\ b \in G$, *the equations* $ax = b$ *and* $ya = b$ *have solutions in G.*

Proof : If G is a group, then (1) and (2) follow by definition and previous theorem.

Conversely, let (1) and (2) hold. To show G is a group, we need prove existence of identity and inverse (for each element).

Let $a \in G$ be any element.

By (2) the equations $ax = a$

$$ya = a$$

have solutions in G.

Let $x = e$ and $y = f$ be the solutions.

Thus $\exists$ $e, f \in G$, s.t., $ae = a$

$$fa = a$$

Let now $b \in G$ be *any* element then again by (2) $\exists$ some x, y in G s.t.,

$$ax = b$$

$$ya = b.$$

Now
$$\begin{aligned} ax = b &\Rightarrow f.(a.x) = f.b \\ &\Rightarrow (f.a).x = f.b \\ &\Rightarrow a.x = f.b \\ &\Rightarrow b = f.b \end{aligned}$$

Again
$$\begin{aligned} y.a = b &\Rightarrow (y.a).e = b.e \\ &\Rightarrow y.(a.e) = b.e \\ &\Rightarrow y.a = be \\ &\Rightarrow b = be \end{aligned}$$

thus we have $\quad b = fb \quad \ldots (i)$

$\quad b = be \quad \ldots (ii)$

for any $\quad b \in G$

Putting $b = e$ in (i) and $b = f$ in (ii) we get

$$e = fe$$

$$f = fe$$

$$\Rightarrow e = f.$$

Hence $\quad ae = a = fa = ea$

i.e., $\exists\, e \in G$, s.t., $ae = ea = a$

$$\Rightarrow e \text{ is identity.}$$

Again, for any $a \in G$, and (the identity) $e \in G$, the equations $ax = e$ and $ya = e$ have solutions.

Let the solutions be $x = a_1$, and $y = a_2$

then $\quad aa_1 = e, \quad a_2a = e$

Now $\quad a_1 = ea_1 = (a_2a)\, a_1 = a_2\, (aa_1) = a_2e = a_2.$

Hence $\quad aa_1 = e = a_1a$ for any $a \in G$

i.e., for any $a \in G$, $\exists$ some $a_1 \in G$ satisfying the above relations $\Rightarrow a$ has an inverse. Thus each element has inverse and, by definition, G forms a group.

Remark : While proving the above theorem we have assumed that equations of the type $ax = b$ and $ya = b$ have solutions in G. The result may fail, if only one type of the above equations has solution. Consider for example :-

G to be a set with at least two elements. Define '.' on G by $a.b = b$ for all $a, b \in G$

then $$a.(b.c) = a.c = c$$
$$(a.b).c = b.c = c$$
shows associativity holds.

Again as $ab = b$, the equation $ax = b$ has a solution for any $a, b \in G$.

We notice that G is not a group, as cancellation laws do not hold in G.

As let $a, b \in G$ be any two distinct members, then
$$ab = b$$
$$bb = b \Rightarrow ab = bb$$
But $$a \neq b.$$

Definition : A non empty set G together with a binary composition '.' is called a *semi-group* if
$$a.(b.c) = (a.b).c \qquad \text{for all } a, b, c \in G$$

Obviously then every group is a semi-group. That the converse is not true follows by considering the set **N** of natural numbers under addition.

The set G in example 14 is not a semi group.

Theorem 3 : *Cancellation laws may not hold in a semi-group.*

Proof : Consider M the set of all 2×2 matrices over integers under matrix multiplication, which forms a semi-group.

If we take $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}, C = \begin{bmatrix} 0 & 0 \\ 3 & 0 \end{bmatrix}$

then clearly $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

But $B \neq C$.

Set of natural numbers under addition is an example of a semi-group in which cancellation laws hold.

Theorem 4 : *A finite semi-group in which cancellation laws hold is a group.*

Proof : Let $G = \{a_1, a_2, \ldots\ldots, a_n\}$ be a finite semi-group in which cancellation laws hold.

Let $a \in G$ be any element, then by closure property
$$aa_1, aa_2, \ldots\ldots, aa_n$$
are all in G.

Suppose any two of these elements are equal

say, $aa_i = aa_j$ for some $i \neq j$

then $a_i = a_j$ by cancellation

But $a_i \neq a_j$ as $i \neq j$

Hence no two of $aa_1, aa_2, \ldots\ldots, aa_n$ can be equal.

These being n in number, will be distinct members of G (Note $o(G) = n$).

Thus if $b \in G$ be any element then

$$b = aa_i \quad \text{for some } i$$

i.e., for $a, b \in G$ the equation $ax = b$ has a solution $(x = a_i)$ in G.

Similarly, the equation $ya = b$ will have a solution in G.

G being a semi-group, associativity holds in G.

Hence G is a group (by theorem 2).

Remark : The above theorem holds only in finite groups. The semi-group of natural numbers under addition being an example where cancellation laws hold but which is not a group.

Theorem 5 : *A finite semi-group is a group if and only if it satisfies cancellation laws.*

Proof : Follows by previous theorem.

When we defined a group, we insisted that $\exists$ an element e which acts both as a right as well as a left identity and each element has both sided inverse. We show now that it is not really essential and only one sided identity and the *same* sided inverse for each element could also make the system a group.

Theorem 6 : *A system* $< G, . >$ *forms a group if and only if*

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(*ii*) $\exists\, e \in G$, *s.t.,* $ae = a$ *for all* $a \in G$

(*iii*) *for all* $a \in G$, $\exists\, a' \in G$, *s.t.,* $aa' = e$.

Proof : If G is a group, we have nothing to prove as the result follows by definition.

Conversely, let the given conditions hold.

All we need show is that $ea = a$ for all $a \in G$

and $a'a = a$ for any $a \in G$

Let $a \in G$ be any element.

By (*iii*) $\exists\, a' \in G$, s.t., $aa' = e$

$\therefore$ For $a' \in G$, $\exists\, a'' \in G$, s.t., $a'a'' = e$ (using (*iii*))

Now $a'a = a'(ae) = (a'a)e = (a'a)\,(a'a'')$

$= a'(aa')a'' = a'(e)\,a'' = (a'e)\,a'' = a'a'' = e.$

Thus for any $a \in G$, $\exists\, a' \in G$, s.t., $aa' = a'a = e$

Again $ea = (aa')a = a(a'a) = ae = a$

$\therefore\ ae = ea = a$ for all $a \in G$

i.e., e is identity of G.

Hence G is a group.

(See Problem 6 for another proof).

It would now be a routine exercise to prove

Theorem 7 : *A system* $< G, . >$ *forms a group if and only if*

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(*ii*) $\exists\, e \in G$, *s.t.*, $ea = a$ *for all* $a \in G$

(*iii*) *for all* $a \in G$, $\exists$ *some* $a' \in G$, *s.t.*, $a'a = e$.

A natural question to crop up at this stage would be what happens, when one sided identity and the other sided inverse exists. Would such a system also form a group? The answer to which is provided by

Example 17 : Let G be a finite set having at least two elements. Define '.' on G by

$$ab = b \qquad \text{for all } a, b \in G$$

then clearly associativity holds in G.

Let $e \in G$ by any fixed element.

Then as $\qquad ea = a \qquad$ for all $a \in G$

e will act as left identity.

Again $a \,.\, e = e$ for all $a \in G$

$\Rightarrow$ e is right inverse for any element $a \in G$.

But we know G is not a group (cancellation laws do not hold in it).

Hence for a system $< G, . >$ to form a group it is essential that the same sided identity and inverse exist.

A Notation : Let G be a group with binary composition '.'. If $a \in G$ be any element then by closure property $a \,.\, a \in G$. Similarly $(a \,.\, a) \,.\, a \in G$ and so on.

It would be very convenient (and natural!) to denote $a \,.\, a$ by a^2 and $a \,.\, (a \,.\, a)$ or $(a \,.\, a) \,.\, a$ by a^3 and so on. Again $a^{-1} \,.\, a^{-1}$ would be denoted by a^{-2}. And since $a \,.\, a^{-1} = e$, it would not be wrong to denote $e = a^0$. It is now a simple matter to understand that under our notation

$$a^m \,.\, a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

where m, n are integers.

In case the binary composition of the group is denoted by +, we will talk of sums and multiples in place of products and powers. Thus here $2a = a + a$, and $na = a + a + \ldots + a$ (n times), if n is $a +$ ve integer. In case n is –ve integer then $n = -m$, where m is +ve and we define $na = -ma = (-a) + (-a) + \ldots + (-a)$ m times].

Problem 1 : *If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \le r \le n$, s.t. $a^r = e$.*

Solution : Since $o(G) = n$, G has n elements.

Let $a \in G$ be any element. By closure property a^2, a^3,..... all belong to G.

Consider $e, a, a^2, \ldots\ldots, a^n$

these are $n + 1$ elements (all in G). But G contains only n elements.

$\Rightarrow$ at least two of these elements are equal. If any of a, a^2 ,....., a^n equals e, our result is proved. If not, then $a^i = a^j$ for some i, j, $1 \le i, j \le n$. Without any loss of generality, we can take $i > j$

then $\qquad a^i = a^j$

$$\Rightarrow a^i . a^{-j} = a^j . a^{-j}$$
$$\Rightarrow a^{i-j} = e \qquad \text{where } 1 \le i - j \le n$$

Putting $i - j = r$ gives us the required result.

Problem 2 : *Show that a finite semi-group in which cross cancellation holds is an abelian group.*

Solution : Let G be the given finite semi-group. Let $a, b \in G$ be any elements. Since G is a semi-group, by associativity

$$a(ba) = (ab)a$$

By cross cancellation then $ba = ab \Rightarrow G$ is abelian.

Since G is abelian, cross cancellation laws become the cancellation laws. Hence G is a finite semi-group in which cancellation laws hold.

Thus G is a group.

Problem 3 : *If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i and any a, b in G, then G is abelian.*

Solution : Let $n, n+1, n+2$ be three consecutive integers for which the given condition holds. Then for any $a, b \in G$,

$$(ab)^n = a^n b^n \qquad \text{.....(1)}$$
$$(ab)^{n+1} = a^{n+1} b^{n+1} \qquad \text{.....(2)}$$
$$(ab)^{n+2} = a^{n+2} b^{n+2} \qquad \text{.....(3)}$$

Now $\quad (ab)^{n+2} = a^{n+2} b^{n+2}$

$$\Rightarrow (ab)(ab)^{n+1} = a^{n+2} b^{n+2}$$
$$\Rightarrow (ab)(a^{n+1} b^{n+1}) = a^{n+2} b^{n+2}$$
$$\Rightarrow ba^{n+1} = a^{n+1} b \text{ (using cancellation)} \qquad \text{.....(4)}$$

Similarly $\quad (ab)^{n+1} = a^{n+1} b^{n+1}$

gives $\quad (ab)(ab)^n = a^{n+1} b^{n+1}$

i.e., $\quad (ab)(a^n b^n) = a^{n+1} b^{n+1}$

$$\Rightarrow ba^n = a^n b$$
$$\Rightarrow ba^{n+1} = a^n ba$$
$$\Rightarrow a^{n+1} b = a^n ba \text{ using (4)}$$
$$\Rightarrow ab = ba.$$

Hence G is abelian.

Remark : Conclusion of the above result may not follow if the given result holds only for two consecutive integers.

Consider, for example, the Quaternion group. One can check that $(ab)^i = a^i b^i$ for $i = 4, 5$ but the group is not abelian.

Problem 4 : *Suppose $(ab)^n = a^n b^n$ for all $a, b \in G$ where $n > 1$ is a fixed integer.*

Show that (*i*) $(ab)^{n-1} = b^{n-1} a^{n-1}$

(*ii*) $a^n b^{n-1} = b^{n-1} a^n$

(*iii*) $(aba^{-1} b^{-1})^{n(n-1)} = e \qquad$ for all $a, b \in G$

Solution : (*i*) We have

$$[b^{-1}\ (ba)\ b]^n = b^{-1}\ (ba)^n\ b$$

and $$[b^{-1}\ (ba)\ b]^n = (ab)^n$$

$$(ab)^n = b^{-1}\ (ba)^n\ b$$

$$\Rightarrow (ab)^{n-1}ab = b^{-1}\ (b^n a^n)b$$

$$\Rightarrow (ab)^{n-1} = b^{n-1}a^{n-1} \qquad \text{for all } a,\ b \in G$$

(*ii*) Now $$(a^{-1}b^{-1}ab)^n = a^{-n}\ b^{-n}\ a^n b^n$$

and $$(a^{-1}b^{-1}ab)^n = a^{-n}\ (b^{-1}ab)^n$$

$$= a^{-n}\ b^{-1}a^n b$$

$\therefore$ $$a^{-n}\ b^{-n}\ a^n b^n = a^{-n}\ b^{-1}a^n b$$

$$\Rightarrow a^n b^{n-1} = b^{n-1}\ a^n \qquad \text{for all } a,\ b \in G$$

(*iii*) Consider $(aba^{-1}\ b^{-1})^{n(n-1)}$

$$= [(aba^{-1}\ b^{-1})^{n-1}]^n$$

$$= [(ba^{-1}\ b^{-1})^{n-1}\ a^{n-1}]^n \text{ by } (i)$$

$$= [ba^{-(n-1)}\ b^{-1}a^{n-1}]^n = [b\ (a^{-(n-1)}\ b^{-1}\ a^{n-1})]^n$$

$$= b^n\ (a^{-(n-1)}\ b^{-1}\ a^{n-1})^n = b^n a^{-(n-1)}\ b^{-n}\ a^{n-1}$$

$$= a^{-(n-1)}\ b^n b^{-n}\ a^{n-1} \text{ by } (ii)$$

$$= e \qquad \text{for all } a,\ b \in G.$$

Problem 5 : *Let G be a group and suppose there exist two relatively prime positive integers m and n such that $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a,\ b \in G$. Show that G is abelian.*

Solution : Since $m,\ n$ are relatively prime, there exist integers x and y such that $mx + ny = 1$.

For any $a,\ b$, we have

$$(a^m b^n)^{mx} = (a^m b^n)\ (a^m b^n).....(a^m b^n) \qquad mx \text{ times}$$

$$= a^m\ (b^n a^m b^n.....b^n a^m)b^n$$

$$= a^m\ (b^n a^m)^{mx-1}\ b^n$$

$$= a^m\ (b^n a^m)^{mx}\ \ (b^n a^m)^{-1} b^n$$

$$= a^m c^m\ (b^n a^m)^{-1}\ b^n \qquad \text{where } c = (b^n a^m)^x$$

$$= c^m\ a^m\ (b^n a^m)^{-1} b^n$$

$$= c^m\ a^m a^{-m} b^{-n}\ b^n = c^m = (b^n a^m)^{mx}$$

Similarly $$(a^m b^n)^{ny} = (b^n a^m)^{ny}$$

giving $$(a^m b^n)^{mx+ny} = (b^n a^m)^{mx+ny}$$

$$\Rightarrow a^m b^n = b^n a^m \qquad \text{for all } a,\ b \in G \qquad \text{..... (1)}$$

Now $$ab = a^{mx+ny}\ b^{mx+ny}$$

$$= a^{mx}.(a^{ny}\ b^{mx})b^{ny}$$

$$= a^{mx}(d^n\ k^m)\, b^{ny} \text{ where } d = a^y,\ k = b^x$$
$$= a^{mx}(k^m\ d^n)\, b^{ny} \text{ by } (1)$$
$$= a^{mx} . b^{mx} . a^{ny} . b^{ny}$$
$$= (a^x)^m . (b^x)^m . (a^y)^n . (b^y)^n$$
$$= (b^x)^m . (a^x)^m . (b^y)^n . (a^y)^n$$
$$= b^{mx}(a^{mx} . b^{ny}) . a^{ny} = b^{mx}(b^{ny} . a^{mx}) . a^{ny}$$
$$= b^{mx+ny} . a^{mx+ny} = ba.$$

Hence G is abelian.

Remark : In the following problem we give another proof to theorem 6 done earlier.

Problem 6 : *Let G be a semi-group. Suppose $\exists\, e \in G$, s.t., $ae = a$ for all $a \in G$ and for each $a \in G$, $\exists\, a' \in G$, s.t., $aa' = e$. Show that G is a group.*

Solution : We first show that G satisfies the right cancellation law.

Let $ac = bc.$

As given $\exists\, c' \in G$, s.t., $cc' = e$

$\therefore$ $(ac)\, c' = (bc)\, c'$

$\Rightarrow a(cc') = b(cc')$

$\Rightarrow ae = be \Rightarrow a = b.$

We now show that e is left identity.

Consider, $(ea)\, a' = e(aa') = e . e = e$

Also $aa' = e$

$\therefore aa' = (ea) = a'$

By right cancellation law,

$a = ea$ for all $a \in G$

$\therefore$ e is also left identify of G.

Again $(a'a)\ a' = a'\ (aa') = a'e = a'$

and $ea' = a'$

$\Rightarrow (a'a)\ a' = ea'$

$\Rightarrow a'a = e$ by right cancellation law

$\Rightarrow a'$ is also left inverse of a

So, G is a group.

Problem 7 : *If in a semi group S, $x^2y = y = yx^2$ $\forall x, y$, then show that S is abelian.*

Solution : $x^2y = y \Rightarrow x^2y^2 = y^2$

$yx^2 = y \quad \forall\, x,\ y \in S$

$\Rightarrow xy^2 = x \quad \forall\, x,\ y \in S$

$\Rightarrow x^2y^2 = x^2$

So $\quad x^2 = y^2 \quad \forall\, x,\ y \in S$

Now $\quad x^2y = y \Rightarrow y^2y = y \Rightarrow y^3 = y \quad \forall\, y \in S$

Also $\quad yx^2y = y^2$ ... (i)

Now $\quad xy^2 = x \Rightarrow xy^2x = x^2$ ...(ii)

By (*i*) and (*ii*), $xy^2x = yx^2y$

Since $\quad y = y^3 \quad \forall\, y \in S$, we get

$$\begin{aligned} xy &= (xy)^3 = xy\ xy\ xy \\ &= xy\,xy\,x^3y = x(yx)^2x(xy) \\ &= (yx)x^2(yx)\,(xy) \\ &= yx^3\,yx^2y = yxy\,x^2y \\ &= (yx)xy^2x = (yx)^3xy^2x \\ &= y(x(yx)^2x)y^2x \\ &= y((yx)\,x^2\,(yx))y^2x \\ &= y^2x^3\,yx\,y^2x = y^2x\,yx\,y^2x \\ &= y(yx^2)y(yx) = (yx)y^2(yx)\,(yx) \\ &= (yx)y^3x\,(yx) = (yx)\,(yx)\,(yx) \\ &= (yx)^3 = yx \quad \forall\, x, y \in S \end{aligned}$$

Hence S is abelian.

Problem 8 : *If G is a semi-group such that given $a \in G$, $\exists$ unique $a' \in G$ such that $aa'a = a$, then show that G is a group.*

Solution : Let e, f be idempotents in G, i.e., $e^2 = e$, $f^2 = f$. (See exercise 5 below). We show $(ef)^2 = ef$.

Now $ef \in G \Rightarrow \exists\, g \in G$, s.t.,

$$(ef)\,g\,(ef) = ef \qquad ....(i)$$

Also $ef(gefg)\ ef = (efgef)\,gef = (ef)\ gef = ef$

$$\Rightarrow g = gefg \qquad ...(ii)$$

Again, $(ef)\,(ge)\,(ef) = efgef = ef$

$$\Rightarrow ge = g \qquad ... (iii)$$

Also, $ef(fg)\ ef = efgef = ef$

$$\Rightarrow fg = g \qquad ...(iv)$$

Now $g^2 = (ge)\ (fg)$ by (*iii*) and (*iv*)

$= g\,(ef) = g$ by (*ii*)

i.e., g is an idempotent.

Also, $g^3 = g^2g = gg = g \Rightarrow ggg = g$

But $g\,(ef)\ g = g$ and so $g = ef$ and

Thus ef is an idempotent, i.e. $(ef)^2 = ef$

Now $(ef)\,f\,(ef) = (ef)\,(ef) = ef$

and $(ef)\ e\ (ef) = ef$

$\Rightarrow f = e$ showing thereby that G has unique idempotent, say e.

Now $aa'a = a \Rightarrow (a'a)^2 = a'a \Rightarrow a'a$ is an idempotent.

$$\Rightarrow a'a = e.$$

Similarly $\quad aa' = e$

Now $\quad a = aa'a = ae$

$$a = aa'a = ea$$

$$\Rightarrow ae = ea = a \qquad \forall\ a \in G$$

$\Rightarrow e$ is identity of G.

Also given $a \in G$, $aa' = e = a'a$ showing that a' is inverse of a.

Hence G is a group.

Exercises

1. Check whether the following systems form a group (a semi-group) or not

   (*a*) G = set of rational numbers under composition $*$ defined by

   $$a * b = \frac{ab}{2}, \qquad a, b \in G$$

   (*b*) $G = \{\pm 1, \pm i\}$, where $i = \sqrt{-1}$ under multiplication.

   (*c*) $G = \{1, w, w^2\}$ where w is cube root of unity under multiplication.

   (*d*) Set of all 2×2 matrices over integers under matrix multiplication.

   (*e*) Set of all matrices of the form $\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$ $\theta \in \mathbf{R}$, under matrix multiplication.

   (*f*) Q = set of all rational numbers under $*$ where $a * b = a + b - ab$.

   (*g*) $G = \{2, 4, 6, 8\}$ under multiplication modulo 10.

2. Let $M = \left\{ \begin{bmatrix} a & a \\ b & b \end{bmatrix} \middle| \ a, b \text{ reals}, a + b \neq 0 \right\}$. Show that M is a semi-group under matrix multiplication and has a right identity and a left inverse for each element. Show that M does not form a group.

3. Show that a group G is abelian iff $(ab)^2 = a^2b^2$.

4. Prove that a group in which every element is its own inverse is abelian.

5. In a group G, an element a is called *Idempotent* if $a^2 = a$. Show that a is idempotent iff $a = e$.

6. Show that if G be a group of even order then it has at least one element $(\neq e)$ which is its own inverse.

7 (*i*) Show that the power set of a finite set X is a finite semi group under intersection, has identity and all elements are idempotent.

(*ii*) Show that a finite semi-group G with identity is a group iff G contains only one idempotent.

8. For any a, x in a group, show that $(x^{-1}\ ax)^n = x^{-1}\ a^n x$ where n is a positive integer.

9. If in a semi group S, $x^{k+1} = x$ for some $k \geq 1$ and $xy^k x = yx^k y \quad \forall\, x, y \in S$ then show that S is abelian.

Subgroups

We have seen that **R**, the set of real numbers, forms a group under addition, and **Z**, the set of integers, also forms a group under addition. Also **Z** is a subset of **R**. It is one of the many situations which prompts us to make

Definition : A non empty subset H of a group G is said to be a *subgroup* of G, if H forms a group under the binary composition of G.

Obviously, if H is a subgroup of G and K is a subgroup of H, then K is subgroup of G.

If G is a group with identity element e then the subset $\{e\}$ and G are trivially subgroups of G and we call them the *trivial* subgroups. All other subgroups will be called non-trivial (or proper subgroups).

We sometimes use the notation $H \leq G$ to signify that H is a subgroup of G and $H < G$ to mean that H is a proper subgroup of G.

It may be a little cumbersome at times to check whether a given subset H of a group G is a subgroup or not by having to check all the axioms in the definition of a group. The following two theorems (especially the second one) go a long way in simplifying this exercise.

Theorem 8 : *A non empty subset H of a group G is a subgroup of G iff*

(*i*) $a, b \in H \Rightarrow ab \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$.

Proof : Let H be a subgroup of G then by definition it follows that (*i*) and (*ii*) hold.

Conversely, let the given conditions hold in H.

Closure holds in H by (*i*).

Again $\qquad a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a(bc) = (ab)c$

Hence associativity holds in H.

Also for any $a \in H$, $a^{-1} \in H$ and so by (*i*)

$$aa^{-1} \in H \Rightarrow e \in H$$

thus H has identity.

Inverse of each element of H is in H by (*ii*).

Hence H satisfies all conditions in the definition of a group and thus it forms a group and therefore a subgroup of G.

Theorem 9 : *A non void subset H of a group G is a subgroup of G iff* $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof : If H is a subgroup of G then, $a, b \in H \Rightarrow ab^{-1} \in H$ (follows easily by using definition).

Conversely, let the given condition hold in H.

That associativity holds in H follows as in previous theorem.

Let $a \in H$ be any element $(H \neq \varphi)$

then $a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

So H has identity.

Again, for any $a \in H$, as $e \in H$

$ea^{-1} \in H \Rightarrow a^{-1} \in H$

i.e., H has inverse of each element.

Finally, for any $a, b \in H$,

$$a, b^{-1} \in H$$
$$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$$

i.e., H is closed under multiplication.

Hence H forms a group and therefore a subgroup of G. Proved.

Remark : If the binary composition of the group is denoted by +, the above condition would read as $a, b \in H \Rightarrow a - b \in H$. Note also that e is always in H.

The following theorem may not prove to be very useful in as much as it confines itself to finite subsets only but nevertheless it has its importance.

Theorem 10 : *A non empty finite subset H of a group G is a subgroup of G iff H is closed under multiplication.*

Proof : If H is a subgroup of G then it is closed under multiplication by definition, so there is nothing to prove.

Conversely, let H be a finite subset s.t.,

$$a, b \in H \Rightarrow ab \in H$$

Now $\quad a, b, c \in H \Rightarrow a, b, c \in G$

$$\Rightarrow a(bc) = (ab)c$$

$\therefore$ Associativity holds in H.

$\Rightarrow H$ is a semi-group.

Again, trivially the cancellation laws hold in H (as they hold in G) and thus H is a finite semi-group in which cancellation laws hold. Hence H forms a group.

Definition : Let G be a group. Let

$$Z(G) = \{x \in G \mid xg = gx \quad \text{for all } g \in G\}$$

then $Z(G)$ is called *centre* of the group G.

Theorem 11 : *Centre of a group G is a subgroup of G.*

Proof : Let $Z(G)$ be the centre of the group G.

Then $Z(G) \neq \varphi$ as $e \in Z(G)$

Again, $\quad x, y \in Z(G) \Rightarrow xg = gx$

$$yg = gy \quad \text{for all } g \in G$$

$$\Rightarrow g^{-1}\ x^{-1} = x^{-1}\ g^{-1}$$

$$g^{-1}\ y^{-1} = y^{-1}\ g^{-1} \qquad \text{for all } g \in G$$

Now $\quad g(xy^{-1}) = (gx)\,y^{-1} = (xg)y^{-1}$

$$= (xg)y^{-1}\,(g^{-1}g) \qquad (\because g^{-1}g = I)$$

$$= xg(y^{-1}\ g^{-1})g = xg(g^{-1}\ y^{-1})g$$

$$= x(gg^{-1})\,y^{-1}g$$

$$= (xy^{-1})g \text{ for all } g \in G$$

$\Rightarrow \quad xy^{-1} \in Z(G)$

Hence $Z(G)$ is a subgroup.

Remark : Obviously, G is abelian iff $Z(G) = G$.

Definition : Let G be a group. $a \in G$ be any element. The subset $N(a) = \{x \in G \mid xa = ax\}$ is called *normalizer* or *centralizer* of a in G.

It is easy to see that normalizer is a subgroup of G.

Problem 9 : *Find centre of* S_3.

Solution : We have $S_3 = \{I, (12), (13), (23), (123), (132)\}$

Centre of S_3 $\quad Z(S_3) = \{\sigma \in S_3 \mid \sigma\theta = \theta\sigma \quad \text{for all } \theta \in S_3\}$.

Since $\quad (12)\,(13) = (132)$

$(13)\,(12) = (123)$

We find (12), (13) do not commute.

$\Rightarrow$ (12) & (13) do not belong to $Z(S_3)$

Again, $\quad (23)\,(132) = (12)$

$(132)\,(23) = (13)$

$\Rightarrow$ (23), (132) do not belong to $Z(S_3)$

Also, $\quad (123)\,(12) = (13)$

$(12)\,(123) = (23)$

Shows $\quad (123) \notin Z(S_3)$

Hence $Z(S_3)$ contains only I.

Problem 10 : *Let G be the group of all 2×2 non singular matrices over the reals. Find centre of G.*

Solution : If $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be any element of the centre $Z(G)$ of G then it should commute with all members of G. In particular we should have

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

$$\Rightarrow b = c,\ a = d$$

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

$$\begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$$\Rightarrow a+b = a, \quad b = c = 0$$

Hence any member $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ of $Z(G)$ turns out to be of the type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

In other words, members of the centre $Z(G)$ are the 2×2 scalar matrices of G.

Problem 11 : *Let G be a group in which*

$(ab)^3 = a^3b^3$

$(ab)^5 = a^5b^5$, *for all* $a, b \in G$

Show that G is abelian.

Solution : We first show that $b^2 \in Z(G)$ for all $b \in G$.

We know $(a^{-1}ba)^3 = a^{-1}b^3a$

By given condition $(a^{-1}ba)^3 = a^{-3}(ba)^3 = a^{-3}b^3a^3$

$$\Rightarrow a^{-1}b^3a = a^{-3}b^3a^3$$

$$\Rightarrow a^2b^3 = b^3a^2 \quad \text{for all } a, b \in G$$

Similarly, $(a^{-1}ba)^5 = a^{-1}b^5a$

$$(a^{-1}ba)^5 = a^{-5}b^5a^5$$

$$\Rightarrow a^{-1}b^5a = a^{-5}b^5a^5$$

$$\Rightarrow a^4b^5 = b^5a^4 \Rightarrow a^4b^3b^2 = b^5a^4$$

$$\Rightarrow (a^2)^2b^3b^2 = b^5a^4 \Rightarrow b^3a^4b^2 = b^5a^4$$

$$\Rightarrow a^4b^2 = b^2a^4 \Rightarrow aa^3b^2 = b^2a^4$$

$$\Rightarrow ab^2a^3 = b^2a^4$$

$$\Rightarrow ab^2 = b^2a \quad \text{for all } a, b \in G$$

$\therefore$ $b^2 \in Z(G)$ for all $b \in G$

Now $(ab)^4 = (ab)^5(ab)^{-1} = a^5b^5b^{-1}a^{-1}$

$$= a^5b^4a^{-1} = a^5a^{-1}b^4, \text{ as } b^2 \in Z(G)$$

$$= a^4b^4$$

$\therefore$ $(ab)^i = a^ib^i$ for three consecutive integers $i = 3, 4, 5$

So, $ab = ba$ for all $a, b \in G$, by problem done earlier.

Hence G is abelian.

Problem 12 : *Show that $N(x^{-1}ax) = x^{-1}N(a)x$ for all $a, x \in G$.*

Solution : Let $y \in N(x^{-1}ax)$

then $(x^{-1}ax)y = y(x^{-1}ax)$

$$\Rightarrow y^{-1}\ x^{-1}\ axy = x^{-1}\ ax$$
$$\Rightarrow xy^{-1}\ x^{-1}\ a = axy^{-1}\ x^{-1}$$
$$\Rightarrow xy^{-1}\ x^{-1} \in N(a)$$
$$\Rightarrow xy^{-1}\ x^{-1} = b \in N(a)$$
$$y^{-1} = x^{-1}\ bx$$
$$\Rightarrow y = x^{-1}\ b^{-1}\ x,\quad b^{-1} \in N(a) \text{ as } b \in N(a)$$
$$\Rightarrow y \in x^{-1}\ N(a)\ x$$

$\therefore$ $$N(x^{-1}\ ax) \subseteq x^{-1}\ N(a)\, x$$

Let $$z \in x^{-1}\ N(a)\ x \Rightarrow z = x^{-1}\ cx,\ c \in N(a)$$

$\therefore$ $$\begin{aligned} z(x^{-1}\, ax) &= (x^{-1}\, cx)\ (x^{-1}\, ax) \\ &= x^{-1}\, cax \\ &= x^{-1}\ acx \qquad \text{as } c \in N(a) \\ &= (x^{-1}\, ax)\ (x^{-1}\, cx) \\ &= (x^{-1}\, ax)\, z \end{aligned}$$
$$\Rightarrow z \in N(x^{-1}\, ax)$$
$$\Rightarrow x^{-1}\, N(a)\ x \subseteq N(x^{-1}\, ax)$$
$$\Rightarrow x^{-1}\ N(a)\ x = N(x^{-1}\, ax) \qquad \text{for all } a,\ x \in G.$$

It would be an easy exercise to show that intersection of two subgroups will be a subgroup. In fact, one can prove that if $\{H_i \mid i \in I\}$ be any set of subgroups of a group G then $\bigcap_{i \in I} H_i$ will be a subgroup of G.

Problem 13 : *Show that union of two subgroups may not be a subgroup.*

Solution : Let $H_2 = \{2n \mid n \in \mathbf{Z}\}$

$H_3 = \{3n \mid n \in \mathbf{Z}\}$

where $(\mathbf{Z}, +)$ is the group of integers. H_2 and H_3 will be subgroups of $\mathbf{Z}$. Indeed

$$2n - 2m = 2(n - m) \in H_2$$

Now $H_2 \cup H_3$ is not a subgroup as $2,\ 3 \in H_2 \cup H_3$

but $$2 - 3 = -1 \notin H_2 \cup H_3$$

Can union of two subgroups be a subgroup? The answer is provided by

Theorem 12 : *Union of two subgroups is a subgroup iff one of them is contained in the other.*

Proof : Let H, K be two subgroups of a group G and suppose $H \subseteq K$ then $H \cup K = K$ which is a subgroup of G.

Conversely, let H, K be two subgroups of G s.t., $H \cup K$ is also subgroup of G. We show one of them must be contained in the other. Suppose it is not true i.e.,

$$H \not\subseteq K,\ K \not\subseteq H$$

Then $$\exists\, x \in H \text{ s.t., } x \notin K$$

$$\exists\ y \in K \text{ s.t., } y \notin H$$

Also then $x, y \in H \cup K$ and since $H \cup K$ is a subgroup, $xy \in H \cup K$

$$\Rightarrow xy \in H \text{ or } xy \in K$$

If $xy \in H$, then as $x \in H$, $x^{-1}(xy) \in H \Rightarrow y \in H$, which is not true

Again, if $xy \in K$, then as $y \in K$, $(xy)y^{-1} \in K \Rightarrow x \in K$ which is not true

i.e., either way we land up with a contradiction.

Hence our supposition that $H \not\subseteq K$ and $K \not\subseteq H$ is wrong.

Thus one of the two is contained in the other. (See exercises also).

Definition : Let H be a subgroup of a group G. For $a, b \in G$, we say a is *congruent* to b *mod* H if $ab^{-1} \in H$.

In notational form, we write $a \equiv b \bmod H$.

It is easy to prove that this relation is an equivalence relation. Corresponding to this equivalence relation, we get equivalence classes. For any $a \in G$, the equivalence class of a, we know will be given by

$$cl(a) = \{x \in G \mid x \equiv a \bmod H\}.$$

Definition : Let H be a subgroup of G and let $a \in G$ be any element. Then $Ha = \{ha \mid h \in H\}$ is called a *right coset* of H in G.

We show in the following theorem that any right coset of H in G is an equivalence class. To be exact we state :

Theorem 13 : $Ha = \{x \in G \mid x \equiv a \text{ mod } H\} = cl(a)$ *for any* $a \in G$.

Proof : Let $x \in Ha$

Then $x = ha$ for some $h \in H$

$$\Rightarrow xa^{-1} = h$$

$$\Rightarrow xa^{-1} \in H$$

$$\Rightarrow x \equiv a \bmod H$$

$$\Rightarrow x \in cl(a)$$

thus $Ha \subseteq cl(a)$.

Again let $x \in cl(a)$ be any element.

Then $x \equiv a \bmod H$

$$\Rightarrow xa^{-1} \in H$$

$$\Rightarrow xa^{-1} = h \text{ for some } h \in H$$

$$\Rightarrow x = ha \in Ha$$

thus $cl(a) \subseteq Ha$

and hence $Ha = cl(a)$.

Having established that right cosets are equivalence classes, we are free to use the results that we know about equivalence classes. We can, therefore, say now that *any two right cosets are either equal or have no element in common* and also that *union of all the right cosets of H in G will equal G.*

Remark : Note that a coset is not essentially a subgroup. If G be the Quaternion

group then $H = \{1, -1\}$ is a subgroup of G. Take $a = i$, then $Ha = \{i, -i\}$ which is not a subgroup of G. (it doesn't contain identity). See theorem 15 ahead.

Lemma : *There is always a 1-1 onto mapping between any two right cosets of H in G.*

Proof : Let Ha, Hb be any two right cosets of H in G.

Define a mapping $f: Ha \to Hb$, s.t.,

$$f(ha) = hb$$

Then
$$h_1a = h_2a \Rightarrow h_1 = h_2 \Rightarrow h_1b = h_2b$$
$$\Rightarrow f(h_1a) = f(h_2a)$$

i.e., f is well defined.

$$f(h_1a) = f(h_2a) \Rightarrow h_1b = h_2b \Rightarrow h_1 = h_2 \Rightarrow h_1a = h_2a$$

Showing f is 1-1.

That f is onto, is easily seen, as for any $hb \in Hb$, ha would be its pre image.

The immediate utility of this lemma is seen, if the group G happens to be finite, because in that case the lemma asserts that any two right cosets of H in G have the same number of elements. Since $H = He$ is also a right coset of H in G, this leads us to state that all right cosets of H in G have the *same* number of elements as are in H (G, being, of course, finite). We are now ready to prove

Theorem 14 (Lagrange's) : *If G is a finite group and H is a subgroup of G then $o(H)$ divides $o(G)$.*

Proof : Let $o(G) = n$.

Since corresponding to each element in G, we can define a right coset of H in G, the number of distinct right cosets of H in G is less than or equal to n.

Using the properties of equivalence classes we know

$$G = Ha_1 \cup Ha_2 \cup \ldots\ldots \cup Ha_t$$

where t = no. of distinct right cosets of H in G.

$$\Rightarrow o(G) = o(Ha_1) + o(Ha_2) + \ldots\ldots + o(Ha_t)$$

(reminding ourselves that two right cosets are either equal or have no element in common).

$$\Rightarrow o(G) = \underbrace{o(H) + o(H) + \ldots\ldots + o(H)}_{t \text{ times}} \text{ using the above lemma}$$

$$\Rightarrow o(G) = t \,.\, o(H)$$

or that $o(H) \mid o(G)$

and we have proved a very important theorem.

But a word of caution here. Converse of Lagrange's theorem does not hold. See under permutation groups.

We have been talking about *right cosets* of H in G all this time. Are there left cosets also? The answer would be an obvious yes. After all we can similarly talk of

$$aH = \{ah \mid h \in H\}, \text{ for any } a \in G$$

which would be called a *left coset*. One can by defining similarly an equivalence relation ($a \equiv b \bmod H \Leftrightarrow a^{-1} b \in H$) prove all similar results for left cosets. It would indeed be an interesting 'brushing up' for the reader, by proving these results independently.

We now come to a simple but very important

Theorem 15 : *Let H be a subgroup of G then*

(*i*) $Ha = H \Leftrightarrow a \in H$; $aH = H \Leftrightarrow a \in H$

(*ii*) $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $aH = bH \Leftrightarrow a^{-1} b \in H$

(*iii*) Ha (*or* aH) *is a subgroup of* G *iff* $a \in H$.

Proof : (*i*) Let $Ha = H$

Since $e \in H$, $ea \in Ha \Rightarrow ea \in H \Rightarrow a \in H$.

Let $a \in H$, we show $Ha = H$.

Let $x \in Ha \Rightarrow x = ha$ for some $h \in H$

Now $h \in H$, $a \in H \Rightarrow ha \in H \Rightarrow x \in H \Rightarrow Ha \subseteq H$

Again, let $y \in H$, since $a \in H$

$ya^{-1} \in H$

$\Rightarrow ya^{-1} = h$ for some $h \in H$

$\Rightarrow y = ha \in Ha$

$\Rightarrow H \subseteq Ha$

Hence $Ha = H$.

(*ii*) $Ha = Hb$

$\Leftrightarrow (Ha)b^{-1} = (Hb)b^{-1}$

$\Leftrightarrow Hab^{-1} = He$

$\Leftrightarrow Hab^{-1} = H$

$\Leftrightarrow ab^{-1} \in H$ using (*i*)

(*iii*) If $a \in H$ then $Ha = H$ which is a subgroup. Conversely, if Ha is a subgroup of G then $e \in Ha$ and thus the right cosets Ha and He have one element e in common and hence $Ha = He = H \Rightarrow a \in H$ by (*i*).

Corresponding results for left cosets can be tackled similarly.

Definition : Let G be a group and H, a subgroup of G. Then *index* of H in G is the number of distinct right (left) cosets of H in G. It is denoted by $i_G(H)$ or $[G:H]$. (See Problem 15).

A look at the proof of Lagrange's theorem suggests that if G is a finite group, then $i_G(H) = \dfrac{o(G)}{o(H)}$.

It is, of course, possible for an infinite group G to have a subgroup $H (\neq G)$ with finite index.

Consider

Example 18 : Let $< \mathbf{Z}, + >$ be the group of integers under addition.

Let $H = \{3n \mid n \in \mathbf{Z}\}$ then H is a subgroup of $\mathbf{Z}$. We show H has only three right cosets in $\mathbf{Z}$ namely H, $H+1$, $H+2$.

If $a \in \mathbf{Z}$ be any element ($\neq 0, 1, 2$) then we can write (by division algorithm).

$$a = 3n + r, \qquad 0 \leq r < 3$$

which gives

$$H + a = H + (3n + r) = (H + 3n) + r = H + r$$

where $\qquad 0 \leq r < 3$

Hence H has only 3 right cosets in $\mathbf{Z}$ and thus has index 3.

Notice, $H - 1 = (H + 3) - 1 = H + (3 - 1) = H + 2$ etc.

Definition : Let H be a subgroup of a group G, we define $C(H) = \{x \in G \mid xh = hx \text{ for all } h \in H\}$ then $C(H)$ is called *centralizer* of H in G.

Also the set

$$N(H) = \{x \in G \mid xH = Hx\}$$
$$= \{x \in G \mid xHx^{-1} = H\}$$

is called *normalizer* of H in G.

It is an easy exercise to see that both $C(H)$ and $N(H)$ are subgroups of G. See problems ahead.

Again as $\quad x \in C(H) \Rightarrow xh = hx \quad$ for all $h \in H$

$$\Rightarrow xH = Hx$$
$$\Rightarrow x \in N(H)$$

we notice $C(H) \subseteq N(H)$.

However, $C(H)$ need not be equal to $N(H)$ as consider the Quaternion group $G = \{\pm 1, \pm i, \pm j, \pm k\}$ and let $H = \{\pm 1, \pm i\}$.

Then $N(H) = G$ and $C(H) = \{\pm 1, \pm i\}$.

Showing that $C(H) \neq N(H)$

Remark : One can define $C(H)$ or $N(H)$ in the same way even if H happens to be only a non empty *subset* of G.

Problem 14 : *Show that* $C(H) = G \Leftrightarrow H \subseteq Z(G)$.

Solution : Let $C(H) = G$. Let $h \in H$ be any element. Then $x \in G \Rightarrow x \in C(H)$ $\Rightarrow xh = hx \Rightarrow$ any element h in H commutes with all elements of $G \Rightarrow h \in Z(G)$ $\Rightarrow H \subseteq Z(G)$.

Conversely, let $H \subseteq Z(G)$. Let $x \in G$. Since $H \subseteq Z(G)$ each element of H commutes with every element of G.

$$\Rightarrow xh = hx \qquad \text{for all } h \in H$$
$$\Rightarrow x \in C(H) \Rightarrow G \subseteq C(H) \Rightarrow G = C(H).$$

Problem 15 : *Show that there exists a one-one onto map between the set of all left cosets of H in G and the set of all right cosets of H in G where H is a subgroup of a group G.*

Solution : Let $\mathfrak{I}$ = set of all left cosets of H in G.

$$\mathfrak{R} = \text{set of all right cosets of } H \text{ in } G.$$

Define a mapping $\theta : \mathfrak{I} \to \mathfrak{R}$, s.t.,

$$\theta(aH) = Ha^{-1} \quad a \in G$$

θ is well defined as $aH = bH$

$$\Rightarrow a^{-1} b \in H$$
$$\Rightarrow Ha^{-1} = Hb^{-1}$$
$$\Rightarrow \theta(aH) = \theta(bH)$$

Taking the steps backwards, we find θ is 1-1. Again, for any $Ha \in \mathfrak{R}$, $a^{-1}H$ is the required pre-image under θ proving that θ is onto.

If G is finite, then the above result reduces to saying that number of left cosets of H in G is same as the number of right cosets of H in G.

Problem 16 : *Let H be a subgroup of a group G and $N(H) = \{a \in G \mid aHa^{-1} = H\}$. Prove that $N(H)$ is a subgroup of G which contains H.*

Solution : $N(H) \neq \varphi$ subset of G as

$$eHe^{-1} = H \Rightarrow e \in N(H)$$

Let now $a, b \in N(H)$ be any two elements, then

$$aHa^{-1} = H$$
$$bHb^{-1} = H$$

then $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1})b = b^{-1}Hb$

$$\Rightarrow (b^{-1}b)Hb^{-1}b = b^{-1}Hb$$
$$\Rightarrow H = b^{-1}Hb$$
$$\Rightarrow aHa^{-1} = a(b^{-1} Hb)a^{-1}$$
$$\Rightarrow aHa^{-1} = ab^{-1}Hba^{-1}$$
$$\Rightarrow H = (ab^{-1})\, H\, (ab^{-1})^{-1}$$
$$\Rightarrow ab^{-1} \in N(H) \text{ i.e., } N(H) \text{ is a subgroup of } G$$

Since $h \in H \Rightarrow hHh^{-1} = H \quad (Ha = H \Leftrightarrow a \in H \text{ etc.})$

we find $h \in N(H)$ showing that $H \subseteq N(H)$.

Problem 17 : *Suppoe that H is a subgroup of a group G such that whenever $Ha \neq Hb$ then $aH \neq bH$. Prove that $gHg^{-1} \subseteq H$ for all $g \in G$.*

Solution : It is given that if $Ha \neq Hb$ then $aH \neq bH$

thus if $aH = bH$ then $Ha = Hb$. .... (1)

Let now $g \in G$, $h \in H$ be any elements, then

$$(g^{-1} h)H = g^{-1}(hH) = g^{-1}H \quad (h \in H)$$

$\therefore$ By (1) $\quad H(g^{-1} h) = Hg^{-1}$

$$\Rightarrow (g^{-1} h)(g^{-1})^{-1} \in H \quad (Ha = Hb \Rightarrow ab^{-1} \in H)$$
$$\Rightarrow g^{-1}hg \in H \quad \text{for all } h \in H$$
$$\Rightarrow g^{-1} Hg \subseteq H.$$

Problem 18 : *If $G = S_3$ and $H = \{I, (13)\}$, write all the left cosets of H in G.*

Solution : $(12)\ H = \{(12)\ I,\ (12)(13)\} = \{(12),\ (132)\}$

$= (123)\ H$ (Show!)

$(23)\,H = \{(23)\ I,\ (23)(13)\} = \{(23),\ (132)\} = (132)\,H$

$(13)\,H = H$ as $(13) \in H$

$I\ H = H$

are all the left cosets of H in G.

Definition : Let H and K be two subgroups of a group G. We define $HK = \{hk \mid h \in H,\ k \in K\}$ then HK will be a non empty subset of G. Will it form a subgroup? The answer is provided by

Theorem 16 : *HK is a subgroup of G iff $HK = KH$.*

Proof : Let HK be a subgroup of G. We show $HK = KH$.

Let $x \in HK$ be any element

Then $x^{-1} \in HK$ (as HK is a subgroup)

$\Rightarrow x^{-1} = hk$ for some $h \in H,\ k \in K$

$\Rightarrow x = (hk)^{-1} = k^{-1}\ h^{-1} \in KH$

thus $HK \subseteq KH$

Again let $y \in KH$ be any element

Then $y = kh$ for some $k \in K,\ h \in H$

$\Rightarrow y^{-1} = h^{-1}\ k^{-1} \in HK$

$\Rightarrow y \in HK$ (as HK is a subgroup)

$\Rightarrow KH \subseteq HK$

Hence $HK = KH.$

Conversely, let $HK = KH.$

Let $a,\ b \in HK$ be any two elements, we show $ab^{-1} \in HK$.

$a,\ b \in HK \Rightarrow a = h_1k_1$ for some $h_1,\ h_2 \in H$

$b = h_2k_2$ $k_1,\ k_2 \in K$

Then $ab^{-1} = (h_1k_1)\,(h_2k_2)^{-1} = (h_1k_1)\,(k_2^{-1}\ h_2^{-1})$

$= h_1\,(k_1k_2^{-1})\,h_2^{-1}$

Now $(k_1k_2^{-1})\ h_2^{-1} \in KH = HK$

thus $(k_1k_2^{-1})\ h_2^{-1} = hk$ for some $h \in H,\ k \in K$

Then $ab^{-1} = h_1\ (hk) = (h_1h)\ k \in HK$

Hence HK is a subgroup.

(See another proof later in Problem 21).

Remarks : (*i*) $HK = KH$ does not mean that each element of H commutes with every element of K. It only means that for each $h \in H,\ k \in K,\ hk = k_1h_1$ for some $k_1 \in K$ and $h_1 \in H$.

(*ii*) If G has binary composition $+$, we define

$$H + K = \{h + k \mid h \in H,\ k \in K\}.$$

Theorem 17 : *If H and K are finite subgroups of a group G then*

$$o(HK) = \frac{o(H).o(K)}{o(H \cap K)}.$$

Proof : Let $D = H \cap K$ then D is a subgroup of K and as in the proof of Lagrange's theorem, $\exists$ a decomposition of K into disjoint right cosets of D in K and

$$K = Dk_1 \cup Dk_2 \cup \ldots\ldots \cup Dk_t$$

and also $$t = \frac{o(K)}{o(D)}$$

Again $HK = H\ (\bigcup_{i=1}^{t} Dk_i)$ and since $D \subseteq H$, $HD = H$

Thus $$HK = \bigcup_{i=1}^{t} Hk_t = Hk_1 \cup Hk_2 \cup \ldots\ldots \cup Hk_t$$

Now no two of $Hk_1, Hk_2, \ldots\ldots, Hk_t$ can be equal as if $Hk_i = Hk_j$ for i, j then $k_i k_j^{-1} \in H \Rightarrow k_i k_j^{-1} \in H \cap K \Rightarrow k_i k_j^{-1} \in D \Rightarrow Dk_i = Dk_j$ which is not true.

Hence
$$\begin{aligned} o(HK) &= o(Hk_1) + (Hk_2) + \ldots\ldots + o(Hk_t) \\ &= o(H) + o(H) + \ldots\ldots + o(H) \\ &= t.\ o(H) \\ &= \frac{o(H).o(K)}{o(H \cap K)} \end{aligned}$$

which proves the result.

Aliter : We have $HK = \{hk \mid h \in H,\ k \in K\}$.

Let $H \cap K = \{x_1, x_2, \ldots\ldots, x_n\}$ and suppose $o(H) = r$, $o(K) = s$

Now $hk = (hx_i)\ (x_i^{-1}k) \in HK \qquad \forall\, i = 1, 2, \ldots\ldots, n$

Also $\qquad hx_i \in H,\ x_i^{-1}k \in K$ as $x_i \in H$ & K

Thus $\qquad hk = (hx_i)\ (x_i^{-1}k) \in HK \qquad \forall\, i = 1, 2, \ldots\ldots, n$

or that hk can be written in at least n different ways. We show these are the only n ways that hk can be expressed as an element of HK.

Suppose $\qquad hk = h_1 k_1$

$$\Rightarrow h^{-1}h_1 = kk_1^{-1} \in H \cap K$$

$$\Rightarrow h^{-1}\ h_1 = x_i$$

and $\qquad kk_1^{-1} = x_i \qquad$ for some $i = 1, 2, \ldots\ldots, n$

or that $\qquad h_1 = hx_i$

$$k_1 = x_i^{-1}k$$

and thus $hk = h_1k_1 = (hx_i)\ (x_i^{-1}\ k)$

Hence each hk can be written in exactly n different ways.

Since h can be chosen in r ways, k can be chosen in s ways, we find hk can be chosen in $\frac{rs}{n}$ ways.

Thus $$o(HK) = \frac{rs}{n} = \frac{o(H).o(K)}{o(H \cap K)}.$$

Note $o(H \cap K) \geq 1$ as $H \cap K \neq \varphi$ as $e \in H \cap K$.

Cor. : If H and K are subgroups of a finite group G such that $o(H) > \sqrt{o(G)}$, $o(K) > \sqrt{o(G)}$ then $o(H \cap K) > 1$.

Proof : We have

$$o(G) \geq o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} > \frac{\sqrt{o(G)}\,.\sqrt{o(G)}}{o(H \cap K)} = \frac{o(G)}{o(H \cap K)}$$

$$\Rightarrow o(H \cap K) > 1.$$

Problem 19 : *Suppose G is a finite group of order pq, where p, q are primes and $p > q$. Show that G has at most one subgroup of order p.*

Solution : Suppose H, K are two subgroups of order p.

By above cor.

$o(H \cap K) > 1$ as $o(K) = o(H) = p > \sqrt{o(G)}$

as $p > q$ $\Rightarrow p^2 > pq$ as $p > q$

$\Rightarrow p^2 > o(G)$

$\Rightarrow p > \sqrt{o(G)}$.

Now $o(H \cap K) \mid o(H) \Rightarrow o(H \cap K) = 1$ or p,

as it cannot be 1, $o(H \cap K) = p = o(H)$

and $H \cap K \subseteq H$

$\Rightarrow H \cap K = H$

Similarly $H \cap K = K$

$\Rightarrow K = H.$

Later, we will show that there exists at least one subgroup of order p.

Remark : We have defined the product HK of two subgroups H and K. The same definition can be used for the product, even if H, K happen to be subsets of G. We will be using this a little later when we come to product of two cosets.

Problem 20 : *Let H be a non empty subset of a group G. Define* $H^{-1} = \{h^{-1} \in G \mid h \in H\}$. *Show that*

(*i*) *If* $HH^{-1} \subseteq H$ *then* H *is a subgroup of* G.

(*ii*) *If* $HH \subseteq H$ *and* $H^{-1} \subseteq H$ *then* H *is a subgroup of* G.

(*iii*) *If* H *is a subgroup of* G *then* $HH = H$, $H = H^{-1}$ *and* $HH^{-1} = H$.

(*iv*) *If* H, K *are subgroups of* G *then* $(HK)^{-1} = K^{-1} H^{-1}$.

Solution : (*i*) Let $a, b \in H \Rightarrow a \in H,\ b^{-1} \in H^{-1}$

$$\Rightarrow ab^{-1} \in HH^{-1} \subseteq H \Rightarrow H \text{ is a subgroup of } G.$$

(*ii*) Let $a,\ b \in H \Rightarrow ab \in HH \subseteq H$

Again $a \in H \Rightarrow a^{-1} \in H^{-1} \subseteq H \Rightarrow H$ is a subgroup of G.

(*iii*) Let $x \in HH \Rightarrow x = ab,\ a \in H,\ b \in H$

H being a subgroup,

$a,\ b \in H \Rightarrow ab \in H \Rightarrow x \in H \Rightarrow HH \subseteq H$

Again $h \in H \Rightarrow h = he \in HH \Rightarrow H \subseteq HH$, hence $HH = H$.

Now, $x \in H \Rightarrow x^{-1} \in H \Rightarrow (x^{-1})^{-1} \in H^{-1} \Rightarrow x \in H^{-1} \Rightarrow H \subseteq H^{-1}$

and $a \in H^{-1} \Rightarrow a = b^{-1},\ b \in H,$

but $b \in H \Rightarrow b^{-1} \in H \Rightarrow a \in H$

$$\Rightarrow H^{-1} \subseteq H \text{ and hence } H = H^{-1}$$

it, therefore, follows that $HH^{-1} = H$.

(*iv*) Let $x \in (HK)^{-1} \Rightarrow x = y^{-1}$ where $y \in HK$

$y \in HK \Rightarrow y = hk,\quad h \in H,\ k \in K$

$\Rightarrow y^{-1} = k^{-1} h^{-1} \in K^{-1} H^{-1}$

$\Rightarrow x \in K^{-1} H^{-1}$ or that $(HK)^{-1} \subseteq K^{-1} H^{-1}$

Again, $x \in K^{-1} H^{-1} \Rightarrow x = ab,\quad a \in K^{-1},\ b \in H^{-1}$

$\Rightarrow a = k^{-1},\ b = h^{-1} \quad k \in K,\ h \in H$

$\therefore\ x \in k^{-1} h^{-1} = (hk)^{-1} = y^{-1}$

where $y = hk \in HK \Rightarrow y^{-1} \in (HK)^{-1} \Rightarrow x \in (HK)^{-1}$

$\Rightarrow K^{-1} H^{-1} \subseteq (HK)^{-1}$. Hence $HK = K^{-1} H^{-1}$

We give a different proof of theorem 16 done earlier in

Problem 21: *Let* H, K *be subgroups of* G. *Show that* HK *is a subgroup of* G *if and only if* $HK = KH$.

Solution : Suppose HK is a subgroup of G.

Then $\quad HK = (HK)^{-1} = K^{-1} H^{-1} = KH$

using previous problem.

Conversely, let $\quad HK = KH$

Then
$$\begin{aligned}(HK)(HK)^{-1} &= (HK)(K^{-1} H^{-1}) \\ &= (HK)(KH) = H(KK)H \\ &= H(KH) = H(HK) \\ &= (HH)K = HK\end{aligned}$$

By previous problem then, HK is a subgroup of G.

Exercises

1. Show that intersection of two subgroups of a group G is a subgroup of G.
2. Let G be the Quaternion group. Find centre of G. Find also the normalizer of i in G.
3. Show that a group cannot be written as union of two (proper) subgroups, although it is possible to express it as union of three subgroups.
4. If H is a subgroup of G, show that
$$g^{-1}Hg \mp \{g^{-1}hg \mid h \in H\} \text{ is a subgroup of } G.$$
5. If G is a group of order 91, show that it cannot have two subgroups of order 13.
6. If $H \subseteq K$ are two subgroups of a finite group G then show that $i_G(H) = i_G(K) \quad i_K(H)$.
7. Show that normalizer of an element a in a group G is a subgroup of G.
8. If H and K are subgroups whose orders are relatively prime then show that $H \cap K = \{e\}$.
9. If H and K are two subgroups of finite indices in G then show that $H \cap K$ is also of finite index in G.
10. If $N(H)$ be the normalizer of H in a group G then show that $Z(G) \subseteq N(H)$, where $H \leq G$.
11. Show that for a group G, $Z(G) = \bigcap_{a \in G} N(a)$.
12. Show that the centralizer $C(H)$ of a subgroup H of a group G is a subgroup of G.
13. Prove (without using the result from equivalence classes) that two right cosets are either equal or have no element in common.
14. If $o(G) = 6$ and $H \neq K$ are subgroups of G each of order 2 then show that HK cannot be a subgroup of G.

Cyclic Groups

Definition : Order of an element : Let G be a group and $a \in G$ be any element. We say a is of *order* (or period) n if n is the least +ve integer s.t., $a^n = e$. If binary composition of G is denoted by +, this would read as $na = 0$, where 0 is identity of G.

If it is not possible to find such n, we say a has infinite order. Order of a will be denoted by $o(a)$. It is obvious that $o(a) = 1$ iff $a = e$.

Cyclic Group : A group G is called a *cyclic* group if $\exists$ an element $a \in G$, such that every element of G can be expressed as a power of a. In that case a is called *generator* of G. We express this fact by writing $G = \langle a \rangle$ or $G = (a)$.

Note we are not saying that generator is unique. Indeed if a is generator so would be a^{-1}. We shall come a little later to the question of number of generators that a cyclic group has. A simple example of a cyclic group is the group of integers under addition, 1 being its generator.

Again the group $G = \{1, -1, i, -i\}$ under multiplication is cyclic as we can express its members as i, i^2, i^3, i^4. Thus i (or $-i$) is a generator of this group.

Theorem 18 : *Order of a cyclic group is equal to the order of its generator.*

Proof : Let $G = \langle a \rangle$ i.e., G is a cyclic group generated by a.

Case (*i*) : $o(a)$ is finite, say n, then n is the least +ve integer s.t., $a^n = e$.

Consider the elements $a^0 = e, a, a^2, \ldots\ldots, a^{n-1}$

these are all elements of G and are n in number.

Suppose any two of the above elements are equal

say $\qquad a^i = a^j$ with $i > j$

then $\qquad a^i . a^{-j} = e \Rightarrow a^{i-j} = e$

But $0 < i-j \leq n-1 < n$, thus $\exists$ a + ve integer $i-j$, s.t. $a^{i-j} = e$ and $i-j < n$, which is a contradiction to the fact that $o(a) = n$.

Thus no two of the above n elements can be equal i.e., G contains at least n elements. We show it does not contain any other element. Let $x \in G$ be any element. Since G is cyclic, generated by a, x will be some power of a.

Let $\qquad x = a^m$

By division algorithm, we can write

$$m = nq + r \text{ where } 0 \leq r < n$$

Now $\qquad a^m = a^{nq+r} = (a^n)^q . a^r = e^q . a^r = a^r$

$$\Rightarrow x = a^r \quad \text{where } 0 \leq r < n$$

i.e., x is one of $a^0 = e, a, a^2, \ldots\ldots, a^{n-1}$

or G contains precisely n elements

$$\Rightarrow o(G) = n = o(a)$$

Case (ii) : $o(a)$ is infinite.

In this case no two powers of a can be equal as if $a^n = a^m$ $(n > m)$ then $a^{n-m} = e$, i.e., it is possible to find a + ve integer $n-m$ s.t., $a^{n-m} = e$ meaning thereby that a has finite order.

Hence no two powrs of a can be equal. In other words G would contain infinite number of elements.

Problem 22 : *If $a \in G$ be of finite order n and also $a^m = e$ then show that $n \mid m$.*

Solution : Let $o(a) = n$, then by definition n is the least +ve integer s.t., $a^n = e$.

Suppose $\qquad a^m = e \qquad$ for some m

By division algorithm, $m = nq + r$, where $0 \leq r < n$

$\therefore \qquad a^m = a^{nq+r}$

$$\Rightarrow e = a^{nq} . a^r = (a^n)^q . a^r = e^q . a^r = a^r$$

where $0 \leq r < n$

Since n is such least +ve integer, we must have $r = 0$

i.e., $m = nq$ or that $u \mid m$.

Problem 23 : *If G is a finite abelian group then show that o(ab) is a divisor of l.c.m. of o(a), o(b).*

Solution : Let $o(a) = n$, $o(b) = m$, $o(ab) = k$.

Let $l = l.c.m. (m, n)$

then $m \mid l$, $n \mid l$, $\Rightarrow l = mr_1$, $l = nr_2$

Now $(ab)^l = a^l b^l$ (G is abelian)

$$= a^{nr_2} b^{mr_1} = e . e = e$$

$$\Rightarrow o(ab) \mid l$$

$$\Rightarrow k \mid l.$$

Problem 24 : *If in a group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$ then show that $o(b) = 31$.*

Solution : We have $b^2 = aba^{-1}$

$$\Rightarrow b^4 = (aba^{-1})(aba^{-1})$$

$$= ab(a^{-1}a)ba^{-1} = ab^2a^{-1}$$

$$= a(aba^{-1})a^{-1}$$

$$\Rightarrow b^4 = a^2ba^{-2}$$

$$\Rightarrow b^8 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b^2a^{-2}$$

$$= a^2(aba^{-1})a^{-2} = a^3ba^{-3}$$

$$\Rightarrow b^{16} = a^4ba^{-4} \text{ (as above)}$$

$$\Rightarrow b^{32} = a^5ba^{-5} = b \text{ as } a^5 = e$$

$$\Rightarrow b^{31} = e \Rightarrow 31 \text{ is a multiple of } o(b)$$

Since 31 is a prime number, it is the least +ve integer such that b^{31}.

$$\Rightarrow o(b) = 31.$$

We are, of course, taking $b \neq e$.

Theorem 19 : *A subgroup of a cylic group is cyclic.*

Proof : Let $G = \langle a \rangle$ and let H be a subgroup of G. If $H = \{e\}$, there is nothing to prove. Let $H \neq \{e\}$. Members of H will be powers of a. Let m be the least +ve integer s.t., $a^m \in H$. We claim $H = \langle a^m \rangle$.

Let $x \in H$ be any element. Then $x = a^k$ for some k. By division algorithm, $k = mq + r$ where $0 \leq r < m$

$$\Rightarrow r = k - mq$$

$$\Rightarrow a^r = a^k . a^{-mq} = x . (a^m)^{-q} \in H$$

But m is the least +ve integer s.t., $a^m \in H$, meaning thereby that $r = 0$.

Thus $k = mq$

or that $x = a^k = (a^m)^q$

i.e., any member of H is a power of a^m.

or that H is cyclic, generated by a^m.

Remark : Any subgroup of $<\mathbf{Z}, +>$ will, therefore, be of the type $n\mathbf{Z}$ = set of multiples of n, where n is an integer (≥ 0). We write $n\mathbf{Z} = <n>$.

Example 19 : Let $H = <a> = \{an \mid n \in \mathbf{Z}\} = a\mathbf{Z}$

$$K = <b> = \{bm \mid m \in \mathbf{Z}\} = b\mathbf{Z}$$

be two subgroups of $<\mathbf{Z}, +>$, then $\mathbf{Z}$ being abelian, $H + K = K + H \Rightarrow H + K$ is a subgroup of $\mathbf{Z}$.

[Note here $HK = H + K$]

We show $H + K = <d> = d\mathbf{Z}$, where d = g.c.d. (a, b)

Now $x \in H + K$

$\Rightarrow$ $x \in <a> + <b>$

$\Rightarrow$ $x = an + bm, \quad n, m \in \mathbf{Z}$

$\Rightarrow$ $x \in <d>$ [as $d \mid a,\ d \mid b \Rightarrow d \mid an + bm \Rightarrow d \mid x$]

Thus $H + K \subseteq <d>$.

Again, $y \in <d> \Rightarrow y = td$

$\Rightarrow y = t\ (ax + by) = atx + bty \in H + K$

Hence $H + K = <d>$

i.e., $a\mathbf{Z} + b\mathbf{Z} = (a, b)\,\mathbf{Z}$.

Theorem 20 : *A cyclic group is abelian.*

Proof : Let $G = <a>$. If $x, y \in G$ be any elements then $x = a^n$, $y = a^m$ for some integers m, n.

Now $xy = a^n . a^m = a^{n+m} = a^{m+n} = a^m . a^n = y . x$

Hence G is abelian.

Remark : In view of the above result, all non abelian groups are non-cyclic. $<\mathbf{Q}, +>$ the group of rationals under addition serves as an example of an abelian group which is not cyclic. For, suppose $\frac{m}{n} \in \mathbf{Q}$ is a generator of $\mathbf{Q}$, then any element of $\mathbf{Q}$ should be a multiple of $\frac{m}{n}$. Now $\frac{1}{3n} \in \mathbf{Q}$, and if $\frac{m}{n}$ is a generator, we should be able to write $\frac{1}{3n} = k\ \frac{m}{n}$, for some k

$$\Rightarrow \frac{1}{3} = km$$

Which is not possible as k, m are integers, whereas $\frac{1}{3}$ is not. Hence no element can act as generator of $\mathbf{Q}$.

Theorem 21 : *If G is a finite group, then order of any element of G divides order of G.*

Proof : Let $a \in G$ be any element.

Let $H = \{a^n \mid n \text{ an integer}\}$

then H is a cyclic subgroup of G, generated by a, as

$$x, y \in H \Rightarrow x = a^n, \; y = a^m$$

$$\therefore \qquad xy^{-1} = a^n . a^{-m} = a^{n-m} \in H$$

By Lagrange's theorem $o(H) \mid o(G)$. But $o(H) = o(a)$

$$\therefore \qquad o(a) \mid o(G)$$

Cor : If G is a finite group then for any $a \in G$

$$a^{o(G)} = e$$

Proof : $o(a) \mid o(G) \Rightarrow o(G) = o(a)k$ for some k

Now $a^{o(G)} = a^{o(a)k} = (a^{o(a)})^k = e^k = e$

Thus any element of a finite group, has finite order. Converse is, however, not true. See page 99.

Example 20 : The group $<\mathbf{Z}, +>$ of integers is an example of a group in which each non identity element is of infinite order.

As another example consider $G = \{2^r : r = 0, \pm 1, ...\}$

then we know G forms a group under multiplication (see examples of groups). No non identity element in G has finite order as

$$(2^r)^n = 1 \text{ iff } 2^{rn} = 1$$

$$\text{iff } r = 0 \text{ or } n = 0.$$

Remark : If G is a finite group of order n and $\exists$ an element $a \in G$, s.t., $o(a) = n$ then G is cyclic, generated by a. Clearly $o(a) = n$ gives $a^n = e$, and lesser powers not equal to e and thus $G = \{a, a^2, ..., a^n = e\}$.

Problem 25 : *Let G be a finite group whose order is not divisible by 3. Suppose $(ab)^3 = a^3b^3$ for all $a, b \in G$, then show that G is abelian.*

Solution : Let $a, b \in G$ be any elements.

Then as $\qquad (ab)^3 = a^3b^3$

we get $\qquad ababab = a^3b^3$

$$\Rightarrow baba = a^2b^2 \text{ (cancellation)}$$

$$\Rightarrow (ba)^2 = a^2b^2 \qquad \ldots (1)$$

Again as $\qquad (ba)^3 = b^3a^3$

we get $\qquad (ba)(ba)^2 = b^3a^3$

$$\Rightarrow (ba)\, a^2b^2 = b^3a^3 \text{ using (1)}$$

$$\Rightarrow a^3b^2 = b^2a^3 \qquad \ldots (2)$$

Consider now
$$(a^{-1}b^{-2}ab^2)^3 = (a^{-1})^3 (b^{-2}ab^2)^3 = a^{-3} (b^{-2}ab^2)^3$$
$$= a^{-3} (b^{-2}a^3b^2)$$
$$= a^{-3} (b^{-2}b^2a^3) \text{ from (2)}$$
$$= a^{-3} a^3 = e$$
$$\Rightarrow o(a^{-1}b^{-2}ab^2) \mid 3$$
$$\Rightarrow o(a^{-1}b^{-2}ab^2) = 1 \text{ or } 3$$

If $o(a^{-1}b^{-2}ab^2) = 3$ then $3 \mid o(G)$ which is not true.

Hence
$$o(a^{-1}b^{-2}ab2) = 1$$
$$\Rightarrow a^{-1}b^{-2}ba^2 = e$$
$$\Rightarrow ab^2 = b^2a \qquad \ldots (3)$$

Again from (1)
$$(ba)^2 = a^2b^2 = a(ab^2) = a(b^2a) \text{ using (3)}$$
$$\Rightarrow (ba)(ba) = ab^2a$$
$$\Rightarrow bab = ab^2 \Rightarrow ba = ab$$

or that G is abelian.

The result that we are going to prove now might raise doubts in the minds of the reader as to the validity of the assertion we made earlier that converse of Lagrange's theorem does not hold. But we promise to prove that little later. For now we prove

Theorem 22 : *Converse of Lagrange's theorem holds in finite cyclic groups.*

Proof : Let $G = \langle a \rangle$ be a finite cyclic group of order n.

Then $o(G) = o(a) = n$

Suppose $m \mid n$. We show $\exists$ a subgroup of G having order m.

Since $m \mid n$, $\exists$ k s.t., $n = mk$

Let H be the cyclic group generated by a^k

then H is a subgroup of G and $o(H) = o(a^k)$

We show $\quad o(a^k) = m$

Now $\quad (a^k)^m = a^{km} = a^n = e, \qquad$ as $o(a) = n$

Suppose now, that $\quad (a^k)^t = e$

Then $\quad a^{kt} = e$
$$\Rightarrow o(a) \mid kt \Rightarrow n \mid kt$$
$$\Rightarrow km \mid kt \Rightarrow m \mid t$$

thus $\quad o(a^k) = m$

which proves the result.

Remark : One can go a step further here and show that such a subgroup (as taken above) would also be unique. Suppose H' is another subgroup of G s.t., $o(H') = m$. Since H' is a subgroup of a cyclic group $G = \langle a \rangle$, H' will be generated by some power of a.

Let $\quad H' = \langle a^p \rangle$

By division algorithm,

$$p = kq + r \qquad 0 \le r < k$$

$$\Rightarrow mp = mkq + mr \qquad 0 \le mr < mk$$

$$\Rightarrow a^{mp} = a^{mkq + mr} = (a^{mk})^q \cdot a^{mr}$$

$$= a^{mr} \qquad (o(a) = n = mk)$$

Now $\quad o(H') = o(a^p) = m$

$$\Rightarrow (a^p)^m = e$$

thus $\quad a^{mr} = e \qquad$ where $0 \le mr < n$

But this $\quad \Rightarrow mr = 0 \;$ (as $o(a) = n$)

$$\Rightarrow r = 0 \text{ as } m \ne 0$$

hence $\quad p = kq$

Thus $\quad H' = \langle a^p \rangle = \langle a^{kq} \rangle \subseteq \langle a^k \rangle = H$

But $\quad o(H') = o(H)$

$$\Rightarrow H = H'.$$

We thus conclude :

If G is a finite cyclic group of order n then the number of distinct subgroups of G is the number of distinct divisors of n, and there is at most one subgroup of G of any given order.

So subgroups of G are of the type $\langle a^k \rangle$ where k is a divisor of n and $\langle a^{n/m} \rangle$ is the unique subgroup of order m. As a particular case, suppose $G = \langle a \rangle$ has order 30. Since divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30, $\exists$ eight subgroups of G, namely

$$\langle a \rangle = \{e, a, a^2, \ldots\ldots, a^{29}\}$$

$$\langle a^2 \rangle = \{e, a^2, a^4, \ldots\ldots, a^{28}\}$$

$$\langle a^3 \rangle = \{e, a^3, a^6, \ldots\ldots, a^{27}\}$$

$\langle a^5 \rangle, \langle a^6 \rangle, \langle a^{10} \rangle, \langle a^{15} \rangle$ and $\langle a^{30} \rangle = \{e\}$ having order 30, 15, 10, 6, 5, 3, 2, 1.

Theorem 23 : *A group G of prime order must be cyclic and every element of G other than identity can be taken as its generator.*

Proof : Let $o(G) = p$, a prime

Take any $a \in G$, $a \ne e$

and let $H = \{a^n \mid n \text{ an integer}\}$ then H is a cyclic subgroup of G.

$\therefore \qquad o(H) \mid o(G) \Rightarrow o(H) = 1$ or p

But $\qquad o(H) \ne 1$ as $a \in H$, $a \ne e$,

Thus $o(H) = p \Rightarrow H = G$, i.e., G is a cyclic group generated by a. Since a was taken as any element (other than e), any element of G can act as its generator.

(See also theorem 29 later)

Cor : A group of prime order is abelian.

Theorem 24 : *A group G of prime order cannot have any non trivial subgroups.*

Proof : If H is any subgroup of G then as $o(H) \mid o(G) = p$, a prime

we find $\quad o(H) = 1$ or p

i.e., $\quad H = \{e\}$ or $H = G$.

Theorem 25 : *A group of finite composite order has at least one non-trivial subgroup.*

Proof : Let $o(G) = n = rs$ where $1 < r, s < n$

Since $n > 1$, $\exists\ e \neq a \in G$. Consider a^r.

Case (i) : $\quad a^r = e$

then $\quad o(a) \leq r$, let $o(a) = k$

then $\quad 1 < k \leq r < n \quad (k > 1$, as $a \neq e)$

Let $\quad H = \{a, a^2, a^3, \ldots\ldots, a^k = e\}$

then H is a non empty finite subset of G and it is closed under multiplication, thus H is a subgroup of G. Since $o(H) = k < n$, we have proved the result.

Case (ii) : $a^r \neq e$, then since $(a^r)^s = a^{rs} = a^n = a^{o(G)} = e$

$o(a^r) \leq s$. Let $o(a^r) = t$ then $1 < t \leq s < n$.

If we take $K = \{a^r, a^{2r}, \ldots\ldots, a^{tr} = e\}$ then K is a non empty finite subset of G, closed under multiplication and is therefore a subgroup of G. Its order being less than n, it is the required subgroup.

Theorem 26 : *If G is a group having no non-trivial subgroups then G must be finite having prime order.*

Proof : Suppose G has infinite order.

Then we can find $a \in G$, s.t., $a \neq e$.

Let $H = \langle a \rangle$, then H is a cyclic subgroup of G and $H \neq \{e\}$. But G has no non-trivial subgroups.

Thus $\quad H = G$

$\Rightarrow G = \langle a \rangle$

Consider now the subgroup $K = \langle a^2 \rangle$

Now $a \notin \langle a^2 \rangle$, because if $a \in \langle a^2 \rangle$ then $a = a^{2t}$ for some integer t

$$\Rightarrow a^{2t-1} = e \Rightarrow o(a) \leq 2t-1$$

meaning thereby that $o(a)$ if finite, which is not true. Thus $a \notin \langle a^2 \rangle$.

Again $\langle a^2 \rangle \neq \{e\}$, because then $a^2 = e$ would again mean that $o(a)$ is finite (≤ 2).

Thus $\langle a^2 \rangle$ is a non-trivial subgroup of G which is not possible. Hence $o(G)$ cannot be infinite.

So $o(G)$ is finite and as it cannot be composite by previous theorem, it must be prime.

Summing up, what we have done above proves

Theorem 27 : *The only groups which have no non-trivial subgroups are the cyclic groups of prime order and the group $\{e\}$.*

All this time we have been talking about cyclic groups and their generators without being very sure as to how many generators a cyclic group could have. To resolve this, we consider the following

Theorem 28 : *An infinite cyclic group has precisely two generators.*

Proof : Let $G = \langle a \rangle$ be an infinite cyclic group.

As mentioned earlier, if a is a generator of G then so would be a^{-1}.

Let now b be any generator of G,

then as $b \in G$, a generates G, we get $b = a^n$ for some integer n

again as $a \in G$, b generates G, we get $a = b^m$ for some integer m

$$\Rightarrow a = b^m = (a^n)^m = a^{nm}$$

$$\Rightarrow a^{nm-1} = e \Rightarrow o(a) \text{ is finite and } \leq nm - 1$$

Since $o(G) = o(a)$ is infinite, the above can hold only if

$$nm - 1 = 0 \Rightarrow nm = 1$$

$$\Rightarrow m = \frac{1}{n} \text{ or } n = \pm 1 \text{ as } m, n \text{ are integers.}$$

i.e., $$b = a \text{ or } a^{-1}$$

In other words, a and a^{-1} are precisely the generators of G.

Question to be answered now is how many generators a finite cyclic group would have. Before we come to the answer we first define what is popularly known as the ***Euler's φ function*** (or Euler's totient function)

For any integer n, we define $\varphi(1) = 1$ and for $n > 1$, $\varphi(n)$ to be the number of +ve integers less than n and relatively prime to n. As an example $\varphi(6) = 2$, $\varphi(10) = 4$ etc.

Note 1, 5 are less than 6 and relatively prime to 6 and 1, 3, 7, 9 (four in number) are less than 10 and relatively prime to 10 etc. Obviously, $\varphi(p) = p-1$, if p is a prime. The following two results can be helpful at times.

(*i*) If $p_1, p_2, \ldots\ldots, p_n$ are distinct prime factors of n (>1), then

$$\varphi(n) = n(1-\frac{1}{p_1}) \quad (1-\frac{1}{p_2}) \ \ldots\ldots \ (1-\frac{1}{p_k})$$

(*ii*) If m, n are co-prime then

$$\varphi(mn) = \varphi(m)\ \varphi(n), \ (m, n \geq 1)$$

We are now ready to prove

Theorem 29 : *Number of generators of a finite cyclic group of order n is* $\varphi(n)$.

Proof : Let $G = \langle a \rangle$ be a cyclic group of order n

then $$o(a) = o(G) = n$$

We claim a^m is generator of G iff $(m, n) = 1$, i.e., m, n are relatively prime.

[For instance, if $n = 8$, then $\varphi(8) = 4$ will be number of generators as we

will show a, a^3, a^5, a^7 will generate G and no other element can generate G. So here m can have values 1, 3, 5, 7].

Let now a^m be a generator of G for some m

Since $a \in G$, $a = (a^m)^i$ for some i

$$\Rightarrow a^{mi-1} = e \Rightarrow o(a) \mid mi-1$$

$$\Rightarrow n \mid mi-1$$

$$\Rightarrow mi-1 = nj \quad \text{for some integer } j$$

i.e.,

$$mi-nj = 1$$

$$\Rightarrow (m, n) = 1.$$

Conversely, let $(m, n) = 1$

Then $\exists$ integers x and y s.t.,

$$mx + ny = 1$$

$$\Rightarrow a^{mx+ny} = a$$

$$\Rightarrow a^{mx} . a^{ny} = a$$

$$\Rightarrow a^{mx} (a^n)^y = a$$

$$\Rightarrow a^{mx} = a \text{ as } \quad o(a) = n$$

$$\Rightarrow a = (a^m)^x$$

Since every element of G is a power of a and a itself is a power of a^m we find a^m generates G, which proves our result.

Theorem (Euler's) 30 : *Let a, n $(n \geq 1)$ be any integers such that g.c.d. $(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof : Let $G_n = \{x \mid x \text{ is an integer}, (x, n) = 1, 1 \leq x < n\}$

Then G_n is a group under multiplication modulo n. By definition of Euler's φ–function,

$$o(G_n) = \varphi(n).$$

If $n = 1$, then $\varphi(n) = \varphi(1) = 1$ and $a^{\varphi(n)} = a^1 \equiv 1 \pmod{1}$ (as 1 divides $a-1$)

Let $\quad n > 1$

Now by Euclid's algorithm

$a = nq + r$, for some integers q, r where $0 \leq r < n$.

If $r = 0$, then $a = nq \Rightarrow n \mid a \Rightarrow (a, n) = n > 1$, a contradiction

$\therefore \quad 1 \leq r < n$

Also $\quad (r, n) = d \Rightarrow d \mid r,\ d \mid n \Rightarrow d \mid a-nq,\ d \mid nq$

$$\Rightarrow d \mid a;\ d \mid n$$

$$\Rightarrow d \mid (a, n) = 1$$

$$\Rightarrow d = 1$$

$\therefore \quad (r, n) = 1$ and $1 \leq r < n$

$$\Rightarrow r \in G_n$$

Also $\quad a = nq + r \Rightarrow a \equiv r \pmod{n}$

It follows from Lagrange's theorem that,

$$r \otimes r \otimes \ldots\ldots \otimes r = \text{identity of } G_n = 1 \qquad [a^{o(G)} = e]$$

where $\otimes$ is composition multiplication modulo n in G_n and $\varphi(n)$ is order of group G_n.

$\therefore \quad r^{\varphi(n)} - nq_1 = 1$, for some integer q_1

$$\Rightarrow r^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

so $a \equiv r \pmod{n} \Rightarrow a^{\varphi(n)} \equiv r^{\varphi(n)} \pmod{n}$.

Theorem (Fermat's) 31 : *For any integer a and prime p,*

$$a^p \equiv a \pmod{p}.$$

Proof : If $(a, p) = 1$, then by Euler's theorem

$$a^{\varphi(p)} \equiv 1 \pmod{p}$$

$$\Rightarrow a^{p-1} \equiv 1 \pmod{p} \qquad \text{as } \varphi(p) = p-1$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

If $(a, p) = p$, then $p \mid a \Rightarrow p \mid a^p$

$\therefore \; p \mid a^p - a$

$$\Rightarrow a^p \equiv a \pmod{p}.$$

(Note $(a, p) = 1$ or p as 1 and p are only divisors of p).

Problem 26 : *Show that if G is a group of order* 10 *then it must have a subgroup of order* 5.

Solution : By Lagrange's theorem such a subgroup can exist.

We first claim that all elements of G cannot be of oder 2. Suppose it is so.

Let $a, b \in G$ be two different elements with order 2.

Let $H = \langle a \rangle$, $K = \langle b \rangle$ be the cyclic subgroups generated by a and b

then $\quad o(H) = 2, \; o(K) = 2$

Since all elements of G are of order 2, it must be abelian (see exercises).

$\therefore \quad HK = KH \Rightarrow HK$ is a subgroup of G

and as $\quad o(HK) = \dfrac{o(H).o(K)}{o(H \cap K)} = \dfrac{2 \times 2}{1} = 4$

[Note $H \cap K = \{e\}$ as $a \neq b$]

By Lagrange's theorem $o(HK)$ should divide $o(G)$

i.e., $4 \mid 10$ which is not true hence our assumption is wrong and thus all elements of G cannot have order 2.

Again since G is finite $o(a) \mid o(G)$ for all $a \in G$

$\Rightarrow \exists$ at least one element $a \in G$, s.t., $o(a) = 5$ or 10.

If $o(a) = 5$, then $H = <a>$ is a subgroup of order 5.

If $o(a) = 10$, then $H = <a^2>$ is a subgroup of order 5.

In any case our result is proved.

Problem 27 : *Let G be a group such that intersection of all its subgroups which are different from $\{e\}$ is a subgroup different from $\{e\}$. Prove that every element of G has finite order.*

Solution : Let $a \in G$ be any element.

If $a = e$, $o(a) = 1$

Let $a \neq e$ and suppose $o(a)$ is not finite.

Consider the cyclic subgroups $<a>$, $<a^2>$, $<a^3>$,.....

Since each $<a^i> \neq \{e\}$ as $o(a)$ is not finite

$<a> \cap <a^2> \cap <a^3> \cap \ldots\ldots \neq \{e\}$ by given condition.

As intersection of cyclic subgroups is cyclic subgroup

$$\bigcap_i <a^i> = <a^m> \text{ for some integer } m$$

Again, $<a^m> \subseteq <a^i>$ for all i

In particular, $<a^m> \subseteq <a^{2m}>$

But $<a^{2m}> \subseteq <a^m>$

(multiples of $2m$ are multiples of m)

$$\Rightarrow <a^m> = <a^{2m}>$$

Thus $a^m \in <a^m> \Rightarrow a^m \in <a^{2m}>$

$$\Rightarrow a^m = (a^{2m})^k$$

$$\Rightarrow a^m\ (^{2k-1}) = e$$

$\Rightarrow o(a)$ is finite, a contradiction.

Hence the result follows.

Theorem 32 : *If G is a finite group of order n and for every divisor d of n $\exists$ unique subgroup of order d, then G is cyclic.*

Proof : Let $d|n$.

Define $A(d) = \{x \in G | o(x) = d\}$

Suppose $A(d) \neq \varphi$ Then $\exists\ x \in G$ s.t. $o(x) = d$.

Let $H = <x>$. Then $o(x) = o(H) = d$. This gives $\varphi(d)$ generators of H or $\varphi(d)$ elements of order d in H. If $\exists\ y \in G$, $y \notin H$ s.t. $o(y) = d$, then $K = <y>$ is a subgroup of order d. It is given that G has unique subgroup of order d. So, $K = H \Rightarrow y \in H$, a contradiction. Thus, the number of elements in G of order d is $\varphi(d)$.

So, $o(A(d)) = \varphi(d)$ if $A(d) \neq \varphi$

and $o(A(d)) = 0$ if $A(d) = \varphi$ for all $d|n$

Clearly, $G = \bigcup_{d|n} A(d)$

Let $d_1, \ldots\ldots, d_s$ be all divisors of n.

Suppose $\quad A(d_1) = \varphi, \ldots\ldots, A(d_i) = \varphi$

and $\quad A(d_{i+1}) \neq \varphi, \ldots\ldots, A(d_s) \neq \varphi$

(Note, if $A(d) = \varphi$ for all $d \mid n$, then $o(G) = 0$, a contradiction. So, $A(d) \neq \varphi$ for some $d \mid n$)

$\therefore \quad o(A(d_1)) = \ldots\ldots = \rho(A(d_i)) = 0$

and $\quad o(A(d_{i+1})) = \varphi(d_{i+1}), \ldots\ldots, o(A(d_s)) = \varphi(d_s)$

Now $\quad G = \bigcup_{d \mid n} A(d) \Rightarrow o(G) = \sum_{d \mid n} o(A(d))$

$$\Rightarrow n = \varphi(d_{i+1}) + \ldots\ldots + \varphi(d_s)$$

By problem 26, $\quad n = \sum_{d \mid n} \varphi(d)$

$\Rightarrow \varphi(d_1) + \ldots. + \varphi(d_i) + \varphi(d_{i+1}) + \ldots.. + \varphi(d_s) = \varphi(d_{i+1}) + \ldots\ldots. + \varphi(d_s)$

$\Rightarrow \varphi(d_1) + \ldots.. + \varphi(d_i) = 0$, a contradiction

So, $A(d) \neq \varphi$ for all $d \mid n$. In particular

$A(n) \neq \varphi \Rightarrow \exists\, x \in A(n) \Rightarrow \exists\, x \in G$ s.t. $o(x) = n = o(G) \Rightarrow G$ is a cyclic group.

Problem 28 : *Show that in a cyclic group of order n, $\exists\ \varphi(m)$ elements of order m for every divisor m of n. Deduce that $n = \sum_{d \mid n} \varphi(d)$.*

Solution : Let m divide n. Then $\exists$ a unique subgroup H of G s.t. $o(H) = m$.

Let $\quad H = \langle b \rangle$

Then $\quad m = o(H) = o(b)$

The number of elements of order m in H equals the number of generators of H. But the number of generators of H is $\varphi(m)$. So, the number of elements of order m in H is $\varphi(m)$. If $k \in G$ s.t. $o(k) = m$, then $K = \langle k \rangle$ has order m. Since G, has unique subgroup of order m, $K = H$.

$\therefore\ k \in H$. So, all elements of order m belong to H.

This gives total number of elements of order m in G to be $\varphi(m)$.

Let $a \in G$ s.t. $o(a) = d$. Then $d \mid o(G) = n$.

From above $\exists\ \varphi(d)$ elements of order d in G. In this way, count all elements of G to get $n = \sum_{d \mid n} \varphi(d)$.

Problem 29 : *Let G be a group.*

Show that $o(a^n) = \dfrac{o(a)}{(o(a), n)}$ *for all* $a \in G$

where n is an integer and $(o(a), n) = g.c.d.\ (o(a), n)$.

Solution : Let $o(a) = m$.

Let $\quad d = (m, n) \Rightarrow \frac{m}{d}, \frac{n}{d}$ are integers

$\therefore \quad (a^n)^{m/d} = (a^m)^{n/d} = e^{n/d} = e$

Let $\quad (a^n)^r = e \Rightarrow a^{nr} = e$

$$\Rightarrow o(a) \mid nr$$

$$\Rightarrow m \mid nr$$

$$\Rightarrow \frac{m}{d} \Big| \frac{n}{d} r$$

$$\Rightarrow \frac{m}{d} \Big| r \quad \text{as} \left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

$$\Rightarrow r \geq \frac{m}{d}$$

$$\therefore \quad o(a^n) = \frac{m}{d} = \frac{o(a)}{(o(a), n)}.$$

Problem 30 : *Let G be a group. Suppose $a, b \in G$, s.t.,*

(*i*) $ab = ba$

(*ii*) $(o(a), o(b)) = 1$.

Show that $o(ab) = o(a)\ o(b)$.

Solution : Let $o(a) = m$, $o(b) = n$

Then $\quad (ab)^{mn} = a^{mn} b^{mn}$ as $ab = ba$

$$= (a^m)^n\ (b^n)^m$$

$$= e$$

Let $\quad (ab)^r = e \Rightarrow a^r b^r = e$

$$\Rightarrow a^r = b^{-r}$$

$$\Rightarrow (a^r)^n = (b^{-r})^n = (b^n)^{-r} = e$$

$$\Rightarrow o(a) \mid rn$$

$$\Rightarrow m \mid rn$$

$$\Rightarrow m \mid r \quad \text{as } (m, n) = 1$$

Similarly, $\quad n \mid r$

$$\Rightarrow l.c.m. \text{ of } (m \ \&\ n) \mid r$$

$$\Rightarrow mn \mid r \Rightarrow mn \leq r$$

$$\therefore \quad o(ab) = mn.$$

Problem 31 : *If a group has finite number of subgroups, then show that it is a finite group.*

Solution : Let G be a group which has n finite number of subgroups. Let $e \neq a \in G$. We show $o(a)$ = finite.

Since G has finite number of subgroups, $< a^i > = < a^j >$ for some integers i, j $i \neq j$.

$$\Rightarrow a^i = (a^j)^r \Rightarrow a^{i-jr} = e$$

$$\Rightarrow i - jr = 0 \text{ or } o(a) = \text{finite}$$

$$\Rightarrow j \text{ divides } i \text{ or } o(a) = \text{finite}$$

If $o(a)$ is not finite, then j divides i and similarly we'll get that i divides j and so $i = j$, a contradiction.

Hence $o(a)$ = finite for all $a \in G$

Consider $< a >$. If $G = < a >$ then $o(G)$ = finite.

If $G \neq < a >$, let $H_1 = < a >$. Then $o(H_1)$ = finite.

Let $a_2 \in G$ s.t., $a_2 \notin H_1$. Let $H_2 = < a_2 >$.

Then $o(H_2)$ = finite.

If $G = H_1 \cup H_2$ then G is finite.

If $G \neq H_1 \cup H_2$ then $\exists\ a_3 \in G$, s.t., $a_3 \notin H_1 \cup H_2$.

Let $H_3 = < a_3 >$, then H_3 is finite. Suppose in this way, we get $H_1, H_2, \ldots\ldots\ldots, H_{n-1}$ to be finite number of subgroups of G.

If $G = H_1 \cup H_2 \cup \ldots\ldots \cup H_{n-1}$, thus $\exists\ a_n \in G$, $a_n \notin H_i\ \forall\ i = 1, 2, \ldots, n-1$. Thus $< a_n > \neq H_i\ \forall\ i = 1, 2, \ldots\ldots, n-1$.

Then $H_n = < a_n >$ is finite.

Thus each subgroup of G is finite and hence G is finite.

Problem 32 : *Show that the number of elements of prime order p in a finite group G is a multiple of $p-1$.*

Solution : Let $x \in G$ s.t. $o(x) = p$. Let $H = < x >$. This gives $\varphi(p) = p - 1$ elements of order p, namely generators of H. If these are the only elements of order p, then we are done, otherwise $\exists\ y \in G$, $y \notin H$, $o(y) = p$. Let $K = < y >$.

Then $H \cap K = \{e\}$ as $o(H \cap K)$ divides $o(H)$ and $o(K)$, $\Rightarrow o(H \cap K) = 1$ or p.

If $o(H \cap K) = p = o(H) = o(K)$ then $H \cap K = H = K \Rightarrow y \in H$, a contradiction.

So, $o(H \cap K) = 1 \Rightarrow H \cap K = \{e\}$. So, $K = < y >$ gives another $\varphi(p) = p - 1$ elements of order p not in H. In this way, since G is finite, we shall have multiple of $p - 1$ elements of order p.

Exercises

1. Show that a group having five or less elements is abelian.
2. For elements a, b, x in a group G. Show that

   (*i*) $o(a) = o(a^{-1})$

(*ii*) $o(a) = o(x^{-1}ax)$.

(*iii*) $o(ab) = o(ba)$

If $a \in G$ be the only element of order n then show that $a \in Z(G)$, the centre of G.

3. If a finite group possesses an element of order 2, show that it possesses an odd number of such elements.
4. If G is a group of order $2n$ and there are n elements in G which have order 2 and the other n elements form a subgroup H of G, then show that $o(H)$ is odd.
5. Show that a subgroup ($\neq \{e\}$) of an infinite cyclic group is infinite.
6. Show that elements of finite order in any abelian group form a subgroup.
7. If G is a cyclic group of order p, a prime then show that any non identity element of G is of order p.
8. Prove that an element of a group G has order n iff the set $\{a^r \mid r = 1, 2, \ldots\}$ consists of precisely n elements. In other words, show that a group of order n is cycle iff it has an element of order n.
9. Let G be a cyclic group of order 6 generated by a. Let H, K be the subgroups generated by a^2, a^3 respectively. Prove that $o(H) = 3$, $o(K) = 2$, $G = HK$ and $H \cap K = \{e\}$.
10. Find order of each element in the group $G = \{\pm 1, \pm i\}$ under multiplication.
11. Find all the subgroups of the quaternion group G and show that $\exists$ no two non-trivial subgroups H, K of G s.t., $H \cap K$ is identity only.
12. Let $A(\mathbf{R})$ be the group of all permutations on $\mathbf{R}$, where $\mathbf{R}$ = set of reals. Let $f: \mathbf{R} \to \mathbf{R}$ s.t., $f(x) = -x$ and $g: \mathbf{R} \to \mathbf{R}$ s.t., $g(x) = 1-x$. Show that f and g are both elements of order 2.
13. Show that $\mathbf{Q} - \{0\}$ under multiplication is not cyclic.

Chapter 3

Normal Subgroups, Homomorphisms, Permutation Groups

The subgroups which have the property that all their right cosets equal the corresponding left cosets play a very significant role in the study of groups. In fact they lead us to the formation of another class of groups that are known as quotient groups. We single out such subgroups and call them normal subgroups.

Definition : A subgroup H of a group G is called a *normal subgroup* of G if $Ha = aH$ for all $a \in G$.

A normal subgroup is also called *invariant* or *self conjugate* subgroup.

Clearly G and $\{e\}$ are normal subgroups of G and are referred to as the trivial normal subgroups. A group not having any non–trivial normal subgroup is called a **simple group**.

It is easy to see that if H is a normal subgroup of G and K is a subgroup of G s.t., $H \subseteq K \subseteq G$ then H is normal in K. Again, if G is abelian, all its subgroups will be normal.

Example 1 : $H = \{1, -1\}$ is a normal subgroup of the Quaternion group G. Indeed $Ha = \{a, -a\} = aH$ for any $a \in G$.

The following two theorems give us equivalent conditions under which a subgroup of a group is normal. So one could also take any one of these as definition of a normal subgroup.

Theorem 1 : *A subgroup H of a group G is normal in G iff $g^{-1}Hg = H$ for all $g \in G$.*

Proof : Let H be normal in G

then $\quad Hg = gH$ for all $g \in G$

$$\Rightarrow g^{-1}Hg = g^{-1}(gH) = (g^{-1}g)H = H.$$

Conversely, let $\quad g^{-1}Hg = H \quad$ for all $g \in G$

Then $\quad g(g^{-1}Hg) = gH$

$$\Rightarrow (gg^{-1})Hg = gH$$

$$\Rightarrow Hg = gH.$$

Hence H is normal.

Theorem 2 : *A subgroup H of a group G is normal in G iff $g^{-1}hg \in H$ for all $h \in H$, $g \in G$.*

Proof : Let H be normal in G,

then $$Ha = aH \quad \text{for all } a \in G.$$

Let $h \in H$, $g \in G$ be any elements,

then $$hg \in Hg = gH$$
$$\Rightarrow hg = gh_1 \text{ for some } h_1 \in H$$
$$\Rightarrow g^{-1}hg = h_1 \in H$$

which proves the result.

Conversely, let $a \in G$ be any element,

then $$a^{-1}ha \in H \quad \text{for all } h \in H$$
$$\Rightarrow a(a^{-1}ha) \in aH \quad \text{for all } h \in H$$
$$\Rightarrow ha \in aH \quad \text{for all } h \in H$$
$$\Rightarrow Ha \subseteq aH$$

Taking $b = a^{-1}$, we note, as $b \in G$

$$b^{-1} hb \in H \quad h \in H$$
$$\Rightarrow aha^{-1} \in H \quad \text{for all } h \in H$$
$$\Rightarrow (aha^{-1})\, a \in Ha \quad \text{for all } h \in H$$
$$\Rightarrow ah \in Ha \quad \text{for all } h \in H$$
$$\Rightarrow aH \subseteq Ha$$

Hence $Ha = aH$, showing H is normal.

Remark : Evidently, it makes no difference in the argument if the above condition is read as $ghg^{-1} \in H$ for all $h \in H$, $g \in G$.

The next theorem also gives us an equivalent condition for a subgroup to be normal, but the importance of this theorem is much more in as much as it helps us to form what would be known as Quotient groups. The very statement of the theorem suggests the presence of a binary composition. (We would also remind the reader here that we *did* talk about the product of two subsets of a group in a remark earlier).

Theorem 3 : *A subgroup H of a group G is normal subgroup of G iff product of two right cosets of H in G is again a right coset of H in G.*

Proof : Let H be a normal subgroup of G.

Let Ha and Hb be any two right cosets of H in G.

then $$\begin{aligned}(Ha)(Hb) &= H(aH)b \\ &= H(Ha)b \\ &= HHab \\ &= Hab \quad ab \in G\end{aligned}$$

Conversely, we are given that product of any two right cosets of H in G is again a right coset.

To show H is normal, let $g \in G$ be any element.

Then Hg and Hg^{-1} are two right cosets of H in G. Thus $HgHg^{-1}$ is also a right coset of H in G.

We claim $\quad HgHg^{-1} = He$

Now $\quad egeg^{-1} \in HgHg^{-1}$

$$\Rightarrow e \in HgHg^{-1}$$

Also $\quad e \in H$

thus H and $HgHg^{-1}$ are two right cosets having one element common. Recalling the properties of equivalence classes we know that two right cosets are either equal or have no element in common. Thus, (as e is common element)

$$H = HgHg^{-1}$$

Now $\quad hgh_1g^{-1} \in HgHg^{-1} \qquad$ for all $h, h_1 \in H, g \in G$

$$\Rightarrow hgh_1g^{-1} \in H \qquad \text{for all } h, h_1 \in H, g \in G$$

$$\Rightarrow h^{-1}(hgh_1g^{-1}) \in h^{-1}H$$

$$\Rightarrow gh_1g^{-1} \in H \qquad \text{for all } h_1 \in H, g \in G$$

$$\Rightarrow H \text{ is normal in } G.$$

Hence the result.

Let H be a subgroup of a group G. Define

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$$

then as seen earlier (see exercises, page 71) $g^{-1}Hg$ forms a subgroup of G.

Again, if we define a mapping $f: H \to g^{-1}Hg$, by

$$f(h) = g^{-1}hg$$

then f will be a 1-1 onto mapping.

In case G is finite, this would mean that both H and $g^{-1}Hg$ (for any $g \in G$) will have same number of elements.

Using this result we have thus proved that *if H be a subgroup of a finite group G s.t., there is no other subgroup of G having the same number of elements as H has, then H is normal in G.* After all, H and $g^{-1}Hg$ (for any $g \in G$) have same number of elements would mean (by given condition) that they are equal and $H = g^{-1}Hg$ means H is normal.

Problem 1 : *Prove that a non empty subset H of a group G is normal subgroup of $G \Leftrightarrow$ for all $x, y \in H$, $g \in G$, $(gx)(gy)^{-1} \in H$.*

Solution : Let H be normal subgroup of G.

Let $x, y \in H$, $g \in G$ be any elements,

then $\quad (gx)(gy)^{-1} = (gx)(y^{-1}g^{-1}) = g(xy^{-1})g^{-1} \in H$

as $xy^{-1} \in H$, $g \in G$, H is normal in G.

Conversely, we show H is normal subgroup of G.

Let $x, y \in H$ be any elements,

then $$xy^{-1} = exy^{-1}e = (ex)(ey)^{-1} \in H \text{ as } e \in G$$

i.e., H is a subgroup of G.

Again, let $h \in H$, $g \in G$ be any elements

then as $$(gh)(ge)^{-1} \in H$$

we get $$(gh)(eg^{-1}) \in H$$

$$\Rightarrow ghg^{-1} \in H$$

$$\Rightarrow H \text{ is normal.}$$

Problem 2 : *If N is a normal subgroup of order 2, of a group G then show that $N \subseteq Z(G)$, the centre of G.*

Solution : Let $N = \{a, e\}$.

Since $e \in Z(G)$ (centre being a subgroup contains e) all that we want to show is that $a \in Z(G)$

i.e., $$ag = ga \quad \text{for all } g \in G$$

or $$g^{-1}ag = a \quad \text{for all } g \in G$$

Let $g \in G$ be any element then as $a \in N$ and N is normal, $g^{-1}ag \in N = \{a, e\}$

$$\Rightarrow g^{-1}ag = a \text{ or } g^{-1}ag = e$$

Since $g^{-1}ag = e \Rightarrow ag = ge \Rightarrow ag = eg \Rightarrow a = e$, which is not true

we get $g^{-1}ag = a \Rightarrow a \in Z(G)$

or $$N \subseteq Z(G).$$

Problem 3 : *Show that a subgroup of index 2 in a group G is a normal subgroup of G.*

Solution : Let H be a subgroup of G, with index 2 then number of distinct right (left) cosets of H in G is 2 and also then G is union of these two right (left) cosets.

Let $g \in G$ be arbitrary.

Case (i) : $g \in H$, then $Hg = gH$ $(=H)$

Hence H is normal.

Case (ii) : $g \notin H$ then $gH \neq H$, $Hg \neq H$.

Thus Hg and $H = He$ are the two distinct right cosets of H in G and

$$G = Hg \cup H$$

Similarly, $$G = gH \cup H$$

$$\Rightarrow Hg \cup H = gH \cup H$$

$$\Rightarrow Hg = gH \quad (\text{as } Hg \cap H = gH \cap H = \varphi)$$

$$\Rightarrow H \text{ is normal in } G.$$

Problem 4 : *If H is a subgroup of a group G such that $(aH)(Hb)$ for any $a, b \in G$ is either a left or a right coset of H in G then H is normal.*

Solution : Let $a \in G$ be any element.

Now $$e = aeea^{-1} = (ae)(ea^{-1}) \in aHHa^{-1}.$$

Also $\qquad e \in H = He = eH$

Thus $(aH)(Ha^{-1})$ and H are two right (left) cosets of H in G and contain a common element e.

$$\Rightarrow aHHa^{-1} = H$$

$$\Rightarrow aHa^{-1} = H \Rightarrow H \text{ is normal.}$$

Problem 5 : *If a cyclic subgroup K of G is normal in G then every subgroup of K is normal in G.*

Solution : Suppose K is generated by a.

Let H be any subgroup of K. We show H is normal in G. Since H is a subgroup of a cyclic group, H will be cyclic.

Let a^m be generator of H.

Let $g \in G$ and $h \in H$ be any elements.

Then $h = (a^m)^n$ for some integer n

therefore, $g^{-1}hg = g^{-1}(a^m)^n g = g^{-1}(a^n)^m g = (g^{-1}a^n g)^m$.

As $K = \langle a \rangle$, $a^n \in K$ and as K is normal in G

we get $\qquad g^{-1}a^n g \in K = \langle a \rangle$.

Thus $\qquad g^{-1}a^n g = a^t$ for some t

$\therefore \qquad g^{-1}hg = (a^t)^m = (a^m)^t \in H$

Hence H is normal in G.

Problem 6 : *Show that the only abelian simple groups are groups of prime order.*

Solution : Let G be a group of prime order, then G is cyclic and therefore, abelian. Also then it contains no non-trivial subgroups. Hence it is simple.

Again, if G be abelian and simple, then each subgroup of G is normal (as G is abelian) it being simple, it contains no non-trivial normal subgroups. Hence G contains only trivial subgroups i.e., G is finite of prime order.

Problem 7 : *If H and K are two normal subgroups of a group G s.t., $H \cap K = \{e\}$ then show that $hk = kh$ for all $h \in H$, $k \in K$*

Solution : Let $h \in H$, $k \in K$ be any elements,

then $h \in H$, $k \in K \subseteq G$, H is normal in G

gives $\qquad k^{-1}hk \in H \Rightarrow k^{-1}hkh^{-1} \in H$

Again $\qquad h^{-1} \in H \subseteq G$, $k \in K$, K is normal in G

gives $\qquad (h^{-1})^{-1}kh^{-1} \in K \Rightarrow hkh^{-1} \in K \Rightarrow k^{-1}hkh^{-1} \in K$

i.e., $\qquad k^{-1}hkh^{-1} \in H \cap K = (e)$

$$\Rightarrow k^{-1}hkh^{-1} = e$$

$$\Rightarrow hk = kh.$$

Remark : If G is the quaternion group then all its subgroups are normal (see exercises).

If $H = \{\pm 1, \pm i\}$, $K = \{\pm 1, \pm j\}$

then $ij \neq ji$. Note here $H \cap K \neq \{e\}$.

Problem 8 : *If G is the union of proper normal subgroups s.t., any two of them have only e in common, then G is abelian.*

Solution : Let $G = H_1 \cup H_2 \cup \ldots\ldots \cup H_k$

Let $x, y \in G$ be any elements, then $x \in H_i$, $y \in H_j$ for some i, j.

Case (i) : If $i \neq j$ then $xy = yx$ using previous problem.

Case (ii) : $i = j$, then $x, y \in H_i$.

Now since H_i is a proper subgroup of G, $\exists$ some $g \in G$ s.t., $g \notin H_i$ (and $g \in H_t$ for some $t \neq i$)

Thus again by previous problem, g commutes with both x and y

i.e., $xg = gx$ and $yg = gy$

Now $g \notin H_i \Rightarrow gx \notin H_i$

$\therefore$ gx also commutes with x, y and $xy \in H_i$

Also
$$\begin{aligned}(xy)g &= g(xy)\\ &= (gx)y = y(gx)\\ &= y(xg) = (yx)g\\ \Rightarrow xy &= yx \text{ (cancellation)}\end{aligned}$$

Hence G is abelian.

Problem 9 : *Show that a subgroup N of G is normal iff $xy \in N \Rightarrow yx \in N$.*

Solution : Let N be normal in G and let $xy \in N$.

Since $$yx = y\,(xy)\,y^{-1}$$

and $xy \in N$, $y \in G$, N is normal in G we find
$$y\,(xy)\,y^{-1} \in N \Rightarrow yx \in N.$$

Conversely, let $n \in N$, $g \in G$ be any elements

then
$$\begin{aligned}n \in N &\Rightarrow (ng)\,g^{-1} \in N\\ &\Rightarrow g^{-1}(ng) \in N \text{ (given condition)}\\ &\Rightarrow N \text{ is normal in } G.\end{aligned}$$

Problem 10 : *Let H be a subgroup of G and let $N = \bigcap_{x \in G} xHx^{-1}$ then show that N is a normal subgroup of G.*

Solution : We know that intersection of subgroups is a subgroup and also subsets of the type xHx^{-1} are subgroups.

Hence $\bigcap_{x \in G} xHx^{-1}$ is a subgroup of G.

Let $g \in G$ be any element, then

$gNg^{-1} = g\,(\cap xHx^{-1})\,g^{-1} = \cap\,(gxHx^{-1}g^{-1}) = \cap\,(yHy^{-1}) = N$

showing thereby that N is normal.

We have used above the result $g\,(H \cap K) = gH \cap gK$ for subgroups H, K and $g \in G$. It is true as

$$x \in g(H \cap K) \Rightarrow x = ga,\ a \in H \cap K$$
$$a \in H \Rightarrow ga \in gH \Rightarrow x \in gH \Rightarrow x \in gH \cap gK$$
$$a \in K \Rightarrow ga \in gK \Rightarrow x \in gK$$

Also $\quad y \in gH \cap gK \Rightarrow y \in gH,\ y \in gK$

$$\Rightarrow y = gh,\ y = gk \qquad h \in H,\ k \in K$$
$$\Rightarrow gh = gk$$
$$\Rightarrow h = k \Rightarrow h,\ k \in H \cap K$$

$\therefore\ y = gh \in g\ (H \cap K)$ proving the result.

Problem 11 : *Let H be a subset of a group G. Let $N(H) = \{x \in G \mid Hx = xH\}$ be the normalizer of H in G.*

We have already shown that $N(H)$ is a subgroup of G. Show

(*i*) *If H is a subgroup of G then $N(H)$ is the largest subgroup of G in which H is normal.*

(*ii*) *If H is a subgroup of G then H is normal in G iff $N(H) = G$.*

(*iii*) *Show by an example, the converse of (ii) fails if H is only a subset of G.*

(*iv*) *If H is a subgroup of G and K is a subgroup of $N(H)$ then H is normal subgroup of HK.*

Solution : (*i*) We Show H is normal in $N(H)$.

Since $Hh = hH$ for all $h \in H$, we find

$h \in N(H)$ for all $h \in H$.

Thus $H \leq N(H)$.

Again by definition of $N(H)$, $Hx = xH$ for all $x \in N(H)$

$\Rightarrow H$ is normal in $N(H)$.

To show that $N(H)$ is the largest subgroup of G in which H is normal suppose K is any subgroup of G such that H is normal in K.

then $k^{-1}Hk = H$ for all $k \in K$

$$\Rightarrow Hk = kH \quad \text{for all } k \in K$$
$$\Rightarrow k \in N(H) \quad \text{for all } k \in K$$
$$\Rightarrow K \subseteq N(H).$$

(*ii*) Let H be a normal subgroup of G

then $N(H) \subseteq G$ (by definition)

Let $x \in G$ be any element,

then $xH = Hx$ as H normal in G.

$$\Rightarrow x \in N(H) \Rightarrow G \subseteq N(H)$$

hence $\quad G = N(H)$.

Conversely, let $G = N(H)$

H is a subgroup of G (given)

Let $h \in H$, $g \in G$ be any elements

Then $\quad g \in N(H)$ as $N(H) = G$

$\Rightarrow gH = Hg$

$\Rightarrow H$ is normal in G.

(*iii*) Consider $G = \langle a \rangle = \{e, a, a^2, a^3\}$

then G being cyclic is abelian group.

Take $H = \{a\}$

then H is a subset and not a subgroup of $G\,(e \notin H)$

Also $N(H) = G$ as G is abelian.

(*iv*) Let K be a subgroup of $N(H)$

then $k \in K \Rightarrow k \in N(H) \Rightarrow Hk = kH$

i.e., $\quad Hk = kH \quad$ for all $k \in K$

$\Rightarrow HK = KH$

$\Rightarrow HK$ is subgroup of $N(H)$

Note, $\quad h \in H \Rightarrow Hh = hH\,(=H)$

$\Rightarrow H \subseteq N(H)$ Also $K \subseteq N(H)$

Again $H \subseteq HK \subseteq N(H)$

hence H is a subgroup of HK

$\Rightarrow H$ is normal subgroup of HK

$[a \in HK \Rightarrow a \in N(H) \Rightarrow Ha = aH]$.

Problem 12 : *Let H be normal in G such that o (H) and* $\dfrac{o(G)}{o(H)}$ *are co prime. Show that H is unique subgroup of G of given order.*

Solution : Let $o(H) = m$, $\dfrac{o(G)}{o(H)} = n$. Suppose K is a subgroup of G of order m.

Then $o(HK) = \dfrac{m.m}{d}$, where $d = o(H \cap K)$

Since H is normal, $HK \leq G$

Thus $\quad o(HK) \mid o(G)$

$$\Rightarrow \quad m \cdot \frac{m}{d} \mid m \cdot n \Rightarrow \frac{m}{d} \mid n$$

$$\Rightarrow \quad d\,\frac{m}{d} \mid dn \Rightarrow m \mid dn$$

$$\Rightarrow \quad m \mid d \text{ as } (m, n) = 1$$

But $d \mid m$ as $H \cap K \leq H$

Thus $d = m$ and hence

$$o(H \cap K) = o(H) = o(K)$$
$$\Rightarrow H = K.$$

Quotient Groups

Let G be a group and N a normal subgroup of G. Let us collect all the right cosets of N in G and form a set to be denoted by $\frac{G}{N}$ or G/N. Since N is normal in G, product of any two right cosets of N will again be a right coset of N in G, i.e., we have a binary composition on $\frac{G}{N}$. We now show formally that this set $\frac{G}{N}$ forms a group under this product as its binary composition.

For $$Na,\ Nb \in \frac{G}{N},\ NaNb = Nab \in \frac{G}{N}$$

If $Na,\ Nb,\ Nc \in \frac{G}{N}$ be any members, then

$Na\,(NbNc) = Na\,(Nbc) = Na(bc) = N(ab)c = NabNc = (NaNb)\,Nc.$

Again $Ne \in \frac{G}{N}$ will act as identity of $\frac{G}{N}$ and for any $Na \in \frac{G}{N}$, Na^{-1} will be the inverse of Na. Thus $\frac{G}{N}$ forms a group, called the *Quotient group* or the *factor group* of G by N.

It is easy to see that if G is abelian then so would be any of its quotient groups as

$$NaNb = Nab = Nba = NbNa.$$

Converse of this result may not hold. See example later.

Remarks : (*i*) In $\frac{G}{N}$, as N is normal, it is immaterial whether we use the word right cosets or left cosets, as $Na = aN$ for all a.

(*ii*) It would indeed be interesting to see what $\frac{G}{\{e\}}$ and $\frac{G}{G}$ are equal to.

Are these G and $\{e\}$ respectively? Well not really but 'almost' so. We will take it up when we come to isomorphisms.

Theorem 4 : *If G is a finite group and N is a normal subgroup of G then*

$$o\left(\frac{G}{N}\right) = \frac{o(G)}{o(N)}.$$

Proof : Since G is finite, using Lagrange's theorem

$$\frac{o(G)}{o(N)} = \text{number of distinct right cosets of } N \text{ in } G$$

$$= o\left(\frac{G}{N}\right).$$

Theorem 5 : *Every quotient group of a cyclic group is cyclic.*

Proof : Let $G = \langle a \rangle$ be a cyclic group.

Then G is abelian, so every subgroup of G is normal. Let H be any subgroup of G. We show $\frac{G}{H}$ is cyclic. In fact we claim $\frac{G}{H}$ is generated by Ha.

Let $Hx \in \frac{G}{H}$ be any element.

Then $x \in G = \langle a \rangle$, i.e., x will be some power of a

Let $\quad x = a^m$

Then $\quad Hx = Ha^m = Ha\,a.....a$ (m times)

$= Ha\,Ha.....Ha$ (m times)

$= (Ha)^m$

i.e., any element Hx of $\frac{G}{H}$ is a power of $Ha \Rightarrow Ha$ generates $\frac{G}{H}$

or that $\frac{G}{H}$ is cyclic.

Remark : The above result is proved for $m > 0$. In case $m \leq 0$, the proof follows similarly. Notice $a^m = a^{-n} = (a^{-1})^n$ where $n > 0$.

Converse of this result is not true. See under permutation groups, page 127.

Example 2 : Let G be the set of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$. Then it is easy to see that G will form a group under matrix multiplication. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ will be identity, $\begin{bmatrix} 1/a & -b/ad \\ 0 & 1/d \end{bmatrix}$ will be inverse of any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$. Also G is not abelian.

Let N be the subset containing members of the type $\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Then N is a subgroup of G. (Prove!) Also it is normal as the product of the type

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} 1 & akd + bd - b/d \\ 0 & 1 \end{bmatrix} \in N$$

So we get the quotient group $\frac{G}{N}$. We show $\frac{G}{N}$ is abelian.

Let $Nx,\ Ny \in \frac{G}{N}$ be any elements, then $x,\ y \in G$.

Let $x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$

$\frac{G}{N}$ will be abelian iff $NxNy = NyNx$

$$\Leftrightarrow Nxy = Nyx$$
$$\Leftrightarrow xy\,(yx)^{-1} \in N$$
$$\Leftrightarrow xyx^{-1}y^{-1} \in N$$

All we need check now is that the product

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} c & e \\ 0 & f \end{bmatrix}\begin{bmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}\begin{bmatrix} \frac{1}{c} & -\frac{e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix} \text{ is a matrix of the type } \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

Thus we can have an abelian quotient group, without the 'parent' group being abelian.

Example 3 : Let $<\mathbf{Z}, +>$ be the group of integers and let $N = \{3n \mid n \in \mathbf{Z}\}$ then N is a normal subgroup of $\mathbf{Z}$.

$\frac{\mathbf{Z}}{N}$ will consist of members of the type $N + a,\ a \in \mathbf{Z}$

We show $\frac{\mathbf{Z}}{N}$ contains only three elements. Let $a \in \mathbf{Z}$ be any element, where $a \neq 0, 1, 2$ then we can write, by division algorithm,

$$a = 3q + r \text{ where } 0 \leq r \leq 2$$
$$\Rightarrow N + a = N + (3q + r) = (N + 3q) + r = N + r \text{ as } 3q \in N.$$

but r can take values 0, 1, 2.

Hence $N + a$ will be one of

$$N,\ N+1,\ N+2$$

or that $\frac{\mathbf{Z}}{N}$ contains only these three members.

Remarks : (*i*) This example also tells us that in case of cosets, $Ha = Hb$ may not necessarily mean $a = b$.

(*ii*) This serves as an example of an infinite group which has a subgroup N having finite index in G. (See page 79 also).

Problem 13 : *Let N be a normal subgroup of a group G. Show that $o(Na) \mid o(a)$ for any $a \in G$.*

Solution : Let $o(a) = n$

then n is the least +ve integer s.t., $a^n = e$.

This gives $\quad Na^n = Ne$

$$\Rightarrow \underset{(n\ times)}{Na.a.....a} = N$$

$$\Rightarrow \underset{(n\ times)}{Na.Na.....Na} = N$$

$$\Rightarrow (Na)^n = N,\ Na \in \frac{G}{N} \text{ and } N \text{ is identity of } \frac{G}{N}$$

$$\Rightarrow o(Na) \mid n \text{ or } o(Na) \mid o(a).$$

Problem 14 : *If G is a group such that $\dfrac{G}{Z(G)}$ is cyclic, where $Z(G)$ is centre of G then show that G is abelian.*

Solution : Let us write $Z(G) = N$. Then $\dfrac{G}{N}$ is cyclic. Suppose it is generated by Ng.

Let $a, b \in G$ be any two elements.

then $\quad Na,\ Nb \in \dfrac{G}{N}$

$$\Rightarrow Na = (Ng)^n,\ Nb = (Ng)^m \text{ for some } n,\ m$$

$$\Rightarrow Na = Ng\,.\,Ng.....Ng = Ng^n$$

$$Nb = Ng^m$$

$$\Rightarrow ag^{-n} \in N,\ bg^{-m} \in N$$

$$\Rightarrow ag^{-n} = x,\ bg^{-m} = y \text{ for some } x, y \in N$$

$$\Rightarrow a = xg^n,\ b = yg^m$$

$$\Rightarrow ab = (xg^n)(yg^m) = x(g^n y)g^m$$

$$= x(yg^n)g^m \text{ as } y \in N = Z(G)$$

$$= xyg^n g^m$$

$$= xyg^{n+m}$$

Similarly, $\quad ba = (yg^m)(xg^n) = y(g^m x)g^n = y(xg^m)g^n$

$$= (yx)g^{m+n}$$

$$\Rightarrow ab = ba \text{ as } xy = yx \text{ as } x, y \in Z(G)$$

Showing that G is abelian.

Remarks (*i*) : We are talking about $\frac{G}{Z(G)}$ assuming, therefore, that $Z(G)$ is a normal subgroup of G, a result which is easily seen to be true. See exercises.

(*ii*) One can, moving on same lines as in the above solution prove that if G/H is cyclic, where H is a subgroup of $Z(G)$ then G is abelian.

(*iii*) If G is a non abelian group then $G/Z(G)$ is not cyclic.

Problem 15 : *Give an example of an infinite group in which every element is of finite order.*

Solution : Let $<\mathbf{Z}, +>$ be the group of integers under addition.

$$\text{Let } G = \left\{\mathbf{Z} + \frac{m}{p^n} \middle| \; \underset{n \geq 0}{m}, n \text{ are integers}, p = \text{fixed prime}\right\}$$

Then G is a subgroup of $\frac{\mathbf{Q}}{\mathbf{Z}}$ where $<\mathbf{Q}, +>$ is the group of rationals under addition.

$$\text{Now} \quad p^n\left(\mathbf{Z} + \frac{m}{p^n}\right) = \mathbf{Z} + \frac{m}{p^n}\, p^n = \mathbf{Z} + m = \mathbf{Z} = \text{zero of } G$$

$$\Rightarrow \text{ order of } \mathbf{Z} + \frac{m}{p^n} \text{ divides } p^n$$

$$\Rightarrow \text{ order of } \mathbf{Z} + \frac{m}{p^n} \text{ is } p^r,\ r \leq n$$

$$\Rightarrow \text{ order of every element in } G \text{ is finite.}$$

Here G is an infinite group.

In fact, one can also show that every subgroup $H \neq G$ is of finite order. So, this also gives an example of an infinite group in which every proper subgroup is of finite order.

Again this group provides us with an example of an infinite p-group. See chapter 5 ahead.

Exercises

1. Show that every subgroup of a cyclic group is normal.
2. Show that intersection of two normal subgroups is a normal subgroup.
3. If H, K are two subgroups of G such that one of them is normal then prove that HK is a subgroup of G. Show further that if both H and K are normal then so is HK.
4. If H and N are two subgroups of G such that N is normal in G then show that $H \cap N$ is a normal subgroup of H. Show by an example that $H \cap N$ may not be normal in G.
5. Every subgroup of an abelian group is normal. Prove that converse is not true. (Consider Quaternion group).

6. Let H be a subgroup of G such that $x^2 \in H$ for all $x \in G$. Show that H is normal in G.
7. Prove that centre of a group is a normal subgroup.
8. Show that $C(H)$ is a normal subgroup of $N(H)$, where $H \leq G$.
9. If A, B, C are normal subgroup of a group G where $B \subseteq A$ then show that
$$A \cap BC = B(A \cap C).$$
10. If H be a normal subgroup of G and $i_G(H) = m$ then show that for any $x \in G$, $x^m \in H$.
11. Show that if every cyclic subgroup of G is normal then every subgroup of G is normal.
12. Prove that if p is a prime number, then any group G of order $2p$ has a normal subgroup of order p.
13. Let N be a normal subgroup of G then show that $\frac{G}{N}$ is abelian iff $xyx^{-1}y^{-1} \in N$, for all $x, y \in G$.
14. Let N be a normal subgroup of a finite group G such that $o(N)$ and $o\left(\frac{G}{N}\right)$ are co-prime. Show that N is unique subgroup of G of order $o(N)$ and that if $x \in G$ be an element such that $x^{o(N)} = e$ then $x \in N$.
15. Give example of a group in which there exist elements a, b such that $o(a)$, $o(b)$ are finite but $o(ab)$ is not finite.
16. Let H and K be two normal subgroups of a group G such that $o(H)$ and $o(K)$ are relatively prime. Prove that $hk = kh$ for all $h \in H$, $k \in K$.
17. Show that a subgroup H of a group G is normal in G iff the set $\frac{G}{H}$ of all its right cosets is closed under multiplication.
18. Let N be a normal subgroup of G such that $o(G/N) = m$ and H is a subgroup of G s.t., $o(H) = n$ and $(m, n) = 1$ then show that $H \subseteq N$.

Homomorphisms - Isomorphisms

In this section we introduce the reader to the idea of an isomorphism which could also be termed as an 'indirect' equality in algebraic systems. Indeed, if two systems have the same number of elements and *behave* exactly in the same manner, nothing much is lost in calling them equal, although at times the idea of equality may look little uncomfortable, especially in case of infinite sets.

Definition : Let $< G, * >$ and $< G', o >$ be two groups.

A mapping $f: G \to G'$ is called a homomorphism if
$$f(a * b) = f(a) \, o \, f(b) \qquad a, b \in G$$

As *agreed* earlier, and when there is no scope of confusion, we shall use the same symbol '.' for both the binary compositions.

With that as notation we find a map

$$f: G \to G' \text{ is a homomorphism if}$$
$$f(ab) = f(a)\, f(b)$$

If, in addition, f happens to be one-one, onto, we say f is an *isomorphism* and in that case write $G \cong G'$.

An onto homomorphism is called *epimorphism.*

A one - one homomorphism is called *monomorphism.*

A homomorphism from a group G to itself is called an *endomorphism* of G.

An isomorphism from a group G to itself is called *automorphism* of G.

If $f: G \to G'$ is onto homomorphism, then G' is called *homomorphic image* of G.

Example 4 : Let $< \mathbf{Z}, + >$ and $< \mathbf{E}, + >$ be the groups of integers and even integers. Define a map $f: \mathbf{Z} \to \mathbf{E}$, s.t.,

$$f(x) = 2x \text{ for all } x \in \mathbf{Z}$$

then f is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$

that f is 1-1 is clear by taking the steps backwards.

f is a homomorphism as

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$$

Also f is onto as any even integer $2x$ would have x as its pre - image.

Hence f is an isomorphism.

In fact this example shows that a subset can be isomorphic to its superset. See Cor. on page 113 also.

Example 5 : Let f be a mapping from $< \mathbf{Z}, + >$ the group of integers to the group $G = \{1, -1\}$ under multiplication defined as

$$f: \mathbf{Z} \to G, \text{ s.t.,}$$
$$f(x) = 1 \text{ if } x \text{ is even}$$
$$= -1 \text{ if } x \text{ is odd}$$

then f is clearly well defined. We check, if it is a homomorphism.

Let $x, y \in \mathbf{Z}$ be any elements.

Case (i) : x, y are both even, then $x + y$ is even and as

$$f(x + y) = 1,\ f(x) = 1,\ f(y) = 1$$

we notice $\quad f(x + y) = 1 = 1 . 1 = f(x) \,.\, f(y)$

Case (ii) : x, y are both odd, then $x + y$ is even and

$$f(x + y) = +1 = (-1)\,(-1) = f(x)\, f(y)$$

Case (iii) : x is odd, y is even, then $x + y$ is odd and

$$f(x + y) = -1 = (-1)\,(1) = f(x)\, f(y)$$

thus in all cases $f(x + y) = f(x)\, f(y)$

Department of Mathematics
8380
LIBRARY

Showing thereby that f is a homomorphism. Is it an isomorphism?

Ontoness is obvious, but f is not 1-1 as $f(x) = f(y)$ does not necessarily mean $x = y$. Indeed $f(2) = f(4)$ but $2 \neq 4$.

Example 6 : *Let G be a group and N, a normal subgroup of G. Define a map*

$$f: G \to \frac{G}{N} \text{ s.t.,}$$

$$f(x) = Nx, \; x \in G$$

then f is clearly well defined. Again

$$f(xy) = Nxy = NxNy = f(x)\, f(y)$$

shows f is a homomorphism.

It is sometimes called the *natural (or canonical) homomorphism*. That f is onto, hardly needs any comment.

The relation of isomorphism in groups is an equivalence relation. (See exercises). Thus whenever a group G is isomorphic to another group G', G' will be isomorphic to G. So we shall simply say that G and G' are isomorphic and denote it by $G \cong G'$.

In most of the theorems and definitions that follow we shall be using G, G' etc., for groups.

Theorem 6 : *If $f: G \to G'$ is a homomorphism then*

(*i*) $f(e) = e'$

(*ii*) $f(x^{-1}) = (f(x))^{-1}$

(*iii*) $f(x^n) = [f(x)]^n$, *n an integer.*

where e, e' are identity elements of G & G' respectively.

Proof : (*i*) We have

$$e \,.\, e = e$$

$$\Rightarrow f(e \,.\, e) = f(e)$$

$$\Rightarrow f(e) \,.\, f(e) = f(e)$$

$$\Rightarrow f(e) \,.\, f(e) = f(e) \,.\, e'$$

$$\Rightarrow f(e) = e' \quad \text{(cancellation)}$$

(*ii*) Again $xx^{-1} = e = x^{-1}x$

$$\Rightarrow f(xx^{-1}) = f(e) = f(x^{-1}x)$$

$$\Rightarrow f(x)\, f(x^{-1}) = e' = f(x^{-1})\, f(x)$$

$$\Rightarrow (f(x))^{-1} = f(x^{-1}).$$

(*iii*) Let n be a +ve integer.

$$f(x^n) = f(\underbrace{x \,.\, x \ldots\ldots x}_{(n \text{ times})})$$

$$= f(x) \,.\, f(x) \;\ldots\ldots f(x) \qquad (n \text{ times})$$

$$= (f(x))^n.$$

If $n = 0$, we have the result by (*i*). In case n is –ve integer, result follows by using (*ii*).

Problem 16 : *Show that* $< \mathbf{Q}, + >$ *cannot be isomorphic to* $< \mathbf{Q}^*, \cdot >$, *where* $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ *and* $\mathbf{Q}$ = *rationals.*

Solution : Suppose f is an isomorphism from $\mathbf{Q}$ to $\mathbf{Q}^*$. Then as $2 \in \mathbf{Q}^*$, f is onto, $\exists\ \alpha \in < \mathbf{Q}, + >$, s.t., $f(\alpha) = 2$.

$$\Rightarrow f(\alpha/2 + \alpha/2) = 2$$

$$\text{or } f(\alpha/2)\ f(\alpha/2) = 2$$

$$\Rightarrow x^2 = 2 \text{ where } x = f(\alpha/2) \in \mathbf{Q}^*$$

But that is a contradiction as there is no rational no. x s.t., $x^2 = 2$.

Hence the result follows.

Problem 17 : *Show that the only homomorphism from the group* $< \mathbf{Q}^*, \cdot >$ *to* $< \mathbf{Z}, + >$ *is the zero homomorphism, where* $\mathbf{Q}^* = \mathbf{Q} - \{0\}$.

Solution : By zero homomorphism f, we mean $f(x) = 0\ \forall\ x$.

Let now $0 \neq f$ be a homomorphism from $< \mathbf{Q}^*, \cdot >$ to $< \mathbf{Z}, + >$.

Let $f(1) = n \in \mathbf{Z}$, Suppose $f(1) = 0$.

Then $f(x) = f\ (\underbrace{1 + 1 + .. + 1}_{(x\ times)})$ if $x > 0$, $x \in \mathbf{Z}$

$$= x\ f(1) = 0$$

Also $0 = f(x) = f(-1 \times (-x)) = f(-1) + f(-x)$

$$\Rightarrow f(-1) = -1\ f(-x)$$

Thus $f(-x) = f(-1 \times x) = f(-1) + f(x) = f(-1) + 0 = -f(-x)$

$\Rightarrow 2f(-x) = 0 \Rightarrow f(-x) = 0 \qquad \forall\, x \in \mathbf{Z},\ x > 0$

Hence $0 = f(1) = f(x \cdot \frac{1}{x}) = f(x) + f(\frac{1}{x}) = f(\frac{1}{x})\ \forall\, x \in \mathbf{Z},\ x \neq 0$

So, $f(r/s) = f(r) + f(1/s)\,(1/s) = 0$

$$\Rightarrow f = 0, \text{ a contradiction}$$

and hence $f(1) \neq 0$

Now $n = f(1) = f(2n \cdot \frac{1}{2n}) = f(\underbrace{\frac{1}{2n} \cdot \frac{1}{2n} \cdots\cdots \frac{1}{2}}_{2n\ times}) = 2n\ f(\frac{1}{2n})$

$$\Rightarrow 1 = 2f\ (\frac{1}{2n}) \text{ which is not true.}$$

Hence zero is the only homomorphism from $\mathbf{Q}^*$ to $\mathbf{Z}$.

Definition : Let $f: G \to G'$ be a homomorphism. The **Kernel** of f, (denoted by Ker$f$) is defined by

$$\text{Ker} f = \{x \in G \mid f(x) = e'\}$$

where e' is identity of G'.

Theorem 7 : *If $f : G \to G'$ be a homomorphism, then Ker f is a normal subgroup of G.*

Proof : Since $f(e) = e'$, $e \in \text{Ker } f$, thus Ker $f \neq \varphi$. Again,

$$x, y \in \text{Ker} f \Rightarrow f(x) = e'$$
$$f(y) = e'$$

Now $\quad f(xy^{-1}) = f(x)\ f(y^{-1}) = f(x)\ (f(y))^{-1} = e'.\ e'^{-1} = e'$

$$\Rightarrow xy^{-1} \in \text{Ker} f$$

Hence it is a subgroup of G.

Again, for any $g \in G$, $x \in \text{Ker} f$

$$f(g^{-1}xg) = f(g^{-1})\ f(x)\ f(g)$$
$$= (f(g))^{-1} f(x) f(g) = (f(g))^{-1}\ e'\ f(g)$$
$$= (f(g))^{-1}\ f(g) = e'$$

$$\Rightarrow g^{-1}\, xg \in \text{Ker} f$$

or that it is a normal subgroup of G.

Theorem 8 : *A homomorphism $f: G \to G'$ is one - one iff Ker $f = \{e\}$.*

Proof : Let $f: G \to G'$ be one - one.

Let $x \in \text{Ker} f$ be any element

then $\quad f(x) = e'$ and as $f(e) = e'$

$$f(x) = f(e) \Rightarrow x = e \text{ as } f \text{ is 1-1}$$

Hence $\quad \text{Ker} f = \{e\}$.

Conversely, let Ker$f$ contain only the identity element.

Let $\quad f(x) = f(y)$

Then $\quad f(x)\ (f(y))^{-1} = e'$

$$\Rightarrow f(xy^{-1}) = e'$$
$$\Rightarrow xy^{-1} \in \text{Ker} f = \{e\}$$
$$\Rightarrow xy^{-1} = e$$
$$\Rightarrow x = y \text{ or that } f \text{ is one - one.}$$

Problem 18 : *Let $f: G \to G'$ be a homomorphism. Let $a \in G$ be such that $o(a) = n$ and $o(f(a)) = m$. Show that $o(f(a)) \mid o(a)$ and f is 1-1 iff $m = n$.*

Solution : Since $\quad o(a) = n$

we find $\quad a^n = e \Rightarrow f(a^n) = f(e)$

$$\Rightarrow f(a\,.\,a.....a) = f(e)$$

$$\Rightarrow (f(a))^n = e$$
$$\Rightarrow o(f(a)) \mid n = o(a)$$

Again, let f be 1-1.

Since $\quad o(f(a)) = m$

we find $\quad (f(a))^m = e'$

$$\Rightarrow f(a) . f(a) .....f(a) = e'$$
$$\Rightarrow f(a . a.....a) = e'$$
$$\Rightarrow f(a^m) = e' = f(e)$$
$$\Rightarrow a^m = e \qquad (f \text{ is } 1\text{-}1)$$

i.e., $o(a) \mid m$ or $n \mid m$, but already $m \mid n$

Hence $\quad m = n.$

Conversely, let $\quad o(a) = o(f(a)).$

Then $\quad f(x) = f(y)$

$$\Rightarrow f(x)\ (f(y))^{-1} = e'$$
$$\Rightarrow f(xy^{-1}) = e'$$
$$\Rightarrow o(f(xy^{-1})) = 1$$
$$\Rightarrow o(xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y$$
$$\Rightarrow f \text{ is } 1\text{-}1.$$

Problem 19 : *Let G be a group and $f: G \to G$ s.t., $f(x) = x^{-1}$ be a homomorphism. Show that G is abelian.*

Solution : Let $x, y \in G$ be any elements.

$$xy = (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1})$$
$$= f(y^{-1})\, f(x^{-1})$$
$$= yx, \text{ hence } G \text{ is abelian.}$$

Theorem 9 : (Fundamental theorem of group homomorphism).

If $f: G \to G'$ be an onto homomorphism with $K = Ker f$, then $\dfrac{G}{K} \cong G'$.

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G.

Proof : Define a map $\varphi : \dfrac{G}{K} \to G'$, s.t.,

$$\varphi(Ka) = f(a),\ a \in G$$

We show φ is an isomorphism.

That φ is well defined follows by

$$Ka = Kb$$
$$\Rightarrow ab^{-1} \in K = \text{Ker } f$$
$$\Rightarrow f(ab^{-1}) = e'$$

$$\Rightarrow f(a)\ (f(b))^{-1} = e'$$
$$\Rightarrow f(a) = f(b)$$
$$\Rightarrow \varphi(Ka) = \varphi(Kb)$$

By retracting the steps backwards, we will prove that φ is 1-1.

Again as $\varphi(KaKb) = \varphi(Kab) = f(ab) = f(a)\ f(b)$

$$= \varphi(Ka)\ \varphi(Kb)$$

we find φ is a homomorphism.

To check that φ is onto, let $g' \in G'$ be any element. Since $f: G \to G'$ is onto, $\exists\, g \in G$, s.t.,

$$f(g) = g'$$

Now $\qquad \varphi(Kg) = f(g) = g'$

Showing thereby that Kg is the required pre-image of g' under φ.

Hence φ is an isomorphism.

Remark : The above theorem is also called first theorem of isomorphism.

Theorem 10 : (Second theorem of Isomorphism). *Let H and K be two subgroups of a group G, where H is normal in G, then*

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

Proof : It is easy to see that $H \cap K$ will be a normal subgroup of K and as $H \subseteq HK \subseteq G$, H will be normal in HK.

Define a map $\quad f: K \to \dfrac{HK}{H}$ s.t.,

$$f(k) = Hk$$

then as $k_1 = k_2 \Rightarrow Hk_1 = Hk_2 \Rightarrow f(k_1) = f(k_2)$

we find f is well defined.

Again $f(k_1 k_2) = Hk_1k_2 = Hk_1\, Hk_2 = f(k_1)\ f(k_2)$

shows f is a homomorphism.

That f is onto is obvious and thus using Fundamental theorem, we find

$$\frac{HK}{H} \cong \frac{K}{\text{Ker}\, f}$$

Since $\qquad k \in \text{Ker} f \Leftrightarrow f(k) = H$

$$\Leftrightarrow Hk = H$$
$$\Leftrightarrow k \in H$$
$$\Leftrightarrow k \in H \cap K \qquad (k \in K \text{ as } \text{Ker} f \subseteq K)$$

We find $\qquad \text{Ker} f = H \cap K$

and our theorem is proved.

Lemma : *If H and K are two normal subgroups of a group G such that $H \subseteq K$, then $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$, and conversely.*

Proof : $\frac{K}{H}$ is a non empty subset of $\frac{G}{H}$, by definition.

For any $Hk_1, Hk_2 \in \frac{K}{H}$

$$(Hk_1)\ (Hk_2)^{-1} = (Hk_1)\ (Hk_2{}^{-1}) = Hk_1k_2^{-1} \in \frac{K}{H}$$

i.e. $\frac{K}{H}$ is a subgroup.

Again, for any $Hk \in \frac{K}{H}$ and $Hg \in \frac{G}{H}$, we notice,

$$(Hg)^{-1}\ (Hk)\ (Hg) = Hg^{-1}\ HkHg$$

$$= Hg^{-1}\ kg \in \frac{K}{H}$$

as $g \in G$, $k \in K$, K is normal in G gives $g^{-1}\ kg \in K$.

We leave the converse as an exercise for the reader.

Theorem 11 : (Third theorem of isomorphism) :

If H and K are two normal subgroups of G such that $H \subseteq K$, then

$$\frac{G}{K} \cong \frac{G/H}{K/H}.$$

Proof : The above lemma ensures that $\frac{K}{H}$ is a normal subgroup of $\frac{G}{H}$ and, therefore, we can talk of $\frac{G/H}{K/H}$.

Define a map $\quad f : \frac{G}{H} \to \frac{G}{K}$ s.t.,

$$f(Ha) = Ka,\ a \in G$$

f is well defined as

$$Ha = Hb$$

$$\Rightarrow ab^{-1} \in H \subseteq K$$

$$\Rightarrow Ka = Kb$$

$$\Rightarrow f(Ha) = f(Hb)$$

f is a homomorphism as

$f(HaHb) = f(Hab) = Kab = KaKb = f(Ha)\, f(Hb)$.

Ontoness of f is obvious.

Using Fundamental theorem of group homomorphism we can say

$$\frac{G}{K} \cong \frac{G/H}{\text{Ker } f}$$

We claim $\text{Ker} f = K/H$

A member of $\text{Ker} f$ will be some member of $\dfrac{G}{H}$.

Now
$$\begin{aligned} Ha \in \text{Ker} f &\Leftrightarrow f(Ha) = K \text{ (identity of } G/K) \\ &\Leftrightarrow Ka = K \\ &\Leftrightarrow a \in K \\ &\Leftrightarrow Ha \in K/H \end{aligned}$$

Hence we find
$$G/K \cong \frac{G/H}{K/H}$$

which proves our result. It is also called *Freshman's theorem.*

Remark : Since $\dfrac{K}{H} = \text{Ker} f$, we notice that $\dfrac{K}{H}$ is a normal subgroup of $\dfrac{G}{H}$ and hence we can talk of $\dfrac{G/H}{K/H}$. Thus we need not prove separately that $\dfrac{K}{H}$ is a normal subgroup of $\dfrac{G}{H}$.

Theorem 12 : *Let $f: G \to G'$ be an onto homomorphism with Ker $f = K$. For H' a subgroup of G', define*

$$H = \{x \in G \mid f(x) \in H'\}$$

Then

(*i*) *H is a subgroup of G and $K \subseteq H$.*

(*ii*) *H' is normal subgroup of G' iff H is normal in G.*

(*iii*) *If H' is normal in G' then* $\dfrac{G'}{H'} \cong \dfrac{G}{H}$.

(*iv*) *This association gives a one - one onto mapping from the family $\boldsymbol{S'}$ of all subgroups of G' onto the family $\boldsymbol{S}$ of all subgroups of G, that contain K.*

Proof : (*i*) $H \neq \varphi$ as $f(e) = e' \in H'$ shows $e \in H$

Again, $x, y \in H \Rightarrow f(x), f(y) \in H'$

$\Rightarrow f(x)\ (f(y))^{-1} \in H'$.

$$\Rightarrow f(xy^{-1}) \in H' \Rightarrow xy^{-1} \in H$$

Thus H is a subgroup.

Since $x \in \text{Ker} f = K \Rightarrow f(x) = e' \in H'$

we find $x \in H \Rightarrow K \subseteq H$.

(*ii*) Let H be normal in G.

Let $g' \in G'$, $h' \in H'$ be any elements. Since f is onto $\exists\, g \in G$, $h \in G$ such that $f(g) = g'$, $f(h) = h'$. Since $h' \in H$, $h \in H$

Now

$$g'^{-1} h'g' = (f(g))^{-1} f(h) f(g)$$
$$= f(g^{-1}) f(h) f(g) = f(g^{-1}hg) \in H'$$

as $g \in G$, $h \in H$, H is normal in G means $g^{-1}hg \in H$

Thus H' is normal in G'.

Conversely, let H' be normal in G'.

For any elements $h \in H$, $g \in G$,

$$f(g^{-1}hg) = (f(g))^{-1} f(h) f(g) \in H'$$

as $f(h) \in H'$, $f(g) \in G'$, H' is normal in G'

$\Rightarrow g^{-1}hg \in H$ or that H is normal in G.

(*iii*) Define a mapping $\varphi : G \to \dfrac{G'}{H'}$ s.t.,

$$\varphi(g) = H'f(g)$$

then φ is well defined as $g_1 = g_2$

$$\Rightarrow f(g_1) = f(g_2)$$
$$\Rightarrow H'f(g_1) = H'f(g_2)$$
$$\Rightarrow \varphi(g_1) = \varphi(g_2)$$

φ will be a homomorphism as

$$\varphi(g_1 g_2) = H'f(g_1 g_2) = H'f(g_1) f(g_2) = H'f(g_1) H'f(g_2)$$
$$= \varphi(g_1)\varphi(g_2)$$

Again, for any $H'g' \in \dfrac{G'}{H'}$ since $g' \in G'$ and is f onto $\exists\, g \in G$, s.t.,

$f(g) = g'$

or that $\varphi(g) = H'f(g) = H'g'$ showing that φ is onto.

By fundamental theorem then

$$\frac{G'}{H'} \cong \frac{G}{\text{Ker}\,\varphi}$$

Now $\qquad x \in \text{Ker}\,\varphi \Leftrightarrow \varphi(x) = H'$

$$\Leftrightarrow H'f(x) = H'$$

$$\Leftrightarrow f(x) \in H' \Leftrightarrow x \in H$$

Hence $\qquad \text{Ker } \varphi = H.$

(*iv*) Define a mapping $\psi : \boldsymbol{S}' \to \boldsymbol{S}$, s.t.,

$$\psi(H') = H$$

where, of course, H is $\{x \in G \mid f(x) \in H'\}$ for any H' in $\boldsymbol{S}'$ By (*i*) we know that it is subgroup of G, containing K and is thus a member of $\boldsymbol{S}$. ψ is, therefore, a well defined mapping.

Let now $\psi(H') = \psi(T')$ where $H', T' \in \boldsymbol{S}'$

then $H = T$ where

$$H = \{x \in G \mid f(x) \in H'\}$$

$$T = \{x \in G \mid f(x) \in T'\}$$

Now for any $h' \in H' \subseteq G'$, since $f: G \to G'$ is onto, we can find $h \in G$, s.t., $f(h) = h' \in H'$

But this shows $h \in H = T$

$$\Rightarrow f(h) \in T'$$

$$\Rightarrow h' \in T' \Rightarrow H' \subseteq T'$$

Similarly $T' \subseteq H'$

i.e., $H' = T'$ or that ψ is one - one.

We show now ψ is onto.

Let $H \in \boldsymbol{S}$ be any member, then H is a subgroup of G and $K \subseteq H$.

Consider $f(H) = \{f(h) \mid h \in H\}$

then $f(H) \neq \varphi$ as $e \in H \Rightarrow f(e) = e' \in f(H)$

Again, for any $f(h_1), f(h_2) \in f(H)$, $h_1, h_2 \in H$

and $(f(h_1))\,(f(h_2)^{-1} = f(h_1 h_2^{-1}) \in f(H)$

i.e., $f(H)$ is a subgroup of G'.

We show $f(H) = H'$ is the required pre - image of H under ψ,

i.e., we show $\psi(H') = H$,

For that we need show $H = \{x \in G \mid f(x) \in H'\}$

Let $x \in H$ then $f(x) \in f(H) = H'$

$$\Rightarrow x \in \{x \in G \mid f(x) \in H'\}$$

or that $H \subseteq \{x \in G \mid f(x) \in H'\}$

Again, if $x \in \{x \in G \mid f(x) \in H'\}$

then $f(x) \in H' = f(H)$

$\exists\, h \in H$, s.t., $f(x) = f(h)$

$$\Rightarrow f(xh^{-1}) = e'$$

$$\Rightarrow xh^{-1} \in \text{Ker} f = K$$

$$\Rightarrow x \in Kh \subseteq H \ [K \subseteq H]$$

Thus $\{x \in G \mid f(x) \in H'\} \subseteq H$

Hence $H = \{x \in G \mid f(x) \in H'\}$

or that $\psi(H') = H$ and so ψ is onto

which completes the proof.

In the following problems we state and prove a *milder version* of the above theorem and its application.

Problem 20 : *Let $f: G \to G'$ be an onto homomorphism from group G to G'. Let H be a subgroup of G and H', a subgroup of G'. Then*

(*i*) *$f(H)$ is a subgroup of G'.*

(*ii*) *$f^{-1}(H')$ is a subgroup of G containing $K = Ker f$, where by $f^{-1}(H')$ we mean $\{x \in G \mid f(x) \in H'\}$*

(*iii*) *$\exists$ 1–1 correspondence between the set of subgroups of G containing K and the set of subgroups of G'.*

Proof : (*i*) Since e = identity of G belongs to H

we have $f(e) \in f(H)$

$$\Rightarrow f(H) \neq \varphi.$$

Let $x, y \in f(H) \Rightarrow x = f(h_1),\ y = f(h_2)$ where $h_1, h_2 \in H$.

$$\therefore\ xy^{-1} = f(h_1)\,(f(h_2))^{-1}$$
$$= f(h_1)\,f(h_2^{-1})$$
$$= f(h_1h_2^{-1}) \in f(H) \text{ as } h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$$

So, $f(H)$ is a subgroup of G'.

(*ii*) Let $a, b \in f^{-1}(H')$

$$\Rightarrow f(a), f(b), \in H'$$
$$\Rightarrow f(a)\,.\,f(b)^{-1} \in H'$$
$$\Rightarrow f(ab^{-1}) \in H'$$
$$\Rightarrow ab^{-1} \in f^{-1}(H')$$

Also $f(e) = e'$ = identity of $G' \in H'$

$$\Rightarrow e \in f^{-1}(H')$$
$$\Rightarrow f^{-1}(H') \neq \varphi$$

So, $f^{-1}(H')$ is a subgroup of G

Also $k \in K \Rightarrow f(k) = e' \in H$

$$\Rightarrow k \in f^{-1}(H')$$
$$\Rightarrow K \subseteq f^{-1}(H')$$

This proves (*ii*)

(*iii*) Let $\mathfrak{A}$ = set of all subgroups of G containing K.

$\mathfrak{B}$ = set of all subgroups of G'

Define $\theta : \mathbb{A} \to \mathbb{B}$ s.t.,

$$\theta(H) = f(H)$$

θ is well defined as

$$H_1 = H_2 \Rightarrow f(H_1) = f(H_2)$$

Let $H' \in \mathbb{B}$. By (*ii*) $f^{-1}(H')$ is a subgroup of G containing K.

$\therefore f^{-1}(H') \in \mathbb{A}$

and $\theta(f^{-1}(H')) = H'$

$\therefore \theta$ is onto.

Let $\theta(H_1) = \theta(H_2)$

$\Rightarrow f(H_1) = f(H_2)$

$\Rightarrow H_1 = H_2$

(as $h_1 \in H_1 \Rightarrow f(h_1) \in f(H_1)$

$\Rightarrow f(h_1) \in f(H_2)$

$\Rightarrow f(h_1) = f(h_2),\ h_2 \in H_2$

$\Rightarrow f(h_1)\, f(h_2^{-1}) = e'$

$\Rightarrow f(h_1 h_2^{-1}) = e'$

$\Rightarrow h_1 h_2^{-1} \in K \subseteq H_2$

$\Rightarrow h_1 \in H_2$

$\Rightarrow H_1 \subseteq H_2$

Similarly, $H_2 \subseteq H_1 \Rightarrow H_1 = H_2$.

$\therefore f$ is 1-1. This proves (*iii*).

Remarks : (*a*) By (*iii*), it follows that any subgroup of G' if of the form $f(H)$ where H is a subgroup of G containing $K = \text{Ker} f$.

(*b*) Let N be a normal subgroup of G.

Then $\varphi : G \to \dfrac{G}{N}$ s.t.,

$$\varphi(x) = Nx$$

is an onto homomorphism with Ker $\varphi = N$. By remark (*a*), any subgroup of $\dfrac{G}{N}$ is of the form $\varphi(H)$, for some subgroup H of G containing Ker $\varphi = N$.

But $\varphi(H) = \{\varphi(x) \mid x \in H\}$

$= \{Nx \mid x \in H\}$

$= \dfrac{H}{N}$

(Note N is normal in $G \Rightarrow N$ is normal in H).

Problem 21 : *Find all the subgroups of* $\frac{\mathbf{Z}}{(12)}$, *where*

$\mathbf{Z}$ = *group of all integers under addition*

and (12) = *subgroup of* $\mathbf{Z}$ *consisting of all multiples of* 12.

Solution : By remark (*b*) above, any subgroup of $\frac{\mathbf{Z}}{(12)}$ is of the form $\frac{H}{(12)}$ where H is a subgroup of $\mathbf{Z}$ under addition and contains (12). But any subgroup of $\mathbf{Z}$ under addition is (n) = set of all multiples of n, $n \geq 0$.

$\therefore H = (2), (3), (4), (6), (12)$. So subgroups of $\frac{\mathbf{Z}}{(12)}$ are

$$\frac{(2)}{(12)}, \frac{(3)}{(12)}, \frac{(4)}{(12)}, \frac{(6)}{(12)}, \frac{(12)}{(12)}$$

Note $\frac{(2)}{(12)} = \{(12), (12)+2, (12)+4, (12)+6, (12)+8, (12)+10\}$

$$\frac{(3)}{(12)} = \{(12), (12)+3, (12)+6, (12)+9\}$$

$$\frac{(4)}{(12)} = \{(12), (12)+4, (12)+8\}$$

$$\frac{(6)}{(12)} = \{(12), (12)+6\}$$

$$\frac{(12)}{(12)} = \{(12)\}.$$

3

Problem 22 : *Show that any infinite cyclic group is isomorphic to* $<\mathbf{Z}, +>$ *the group of integers.*

Solution : Let $G = <a>$ be any infinite cyclic group.

Define $f : G \to \mathbf{Z}$, s.t.,

$f(a^i) = i \qquad i \in \mathbf{Z}$

Since $G = <a>$ is of infinite order, $a^i \in G$ for all $i \in \mathbf{Z}$ and $a^i = a^j$ for no $i \neq j$.

Thus $a^i = a^j \Rightarrow i = j \Rightarrow f(a^i) = f(a^j)$ or that f is well defined.

Again $f(a^i) = f(a^j) \Rightarrow i = j \Rightarrow a^i = a^j \Rightarrow f$ is 1-1.

$f(a^i \cdot a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$

shows that f is a homomorphism.

f is obviously onto and hence the isomorphism is established.

Cor. : Every subgroup of an infinite cyclic group is an infinite cyclic group which is isomorphic to the group itself.

Problem 23 : *Any finite cyclic group of order n is isomorphic to* $\mathbf{Z}_n$ *the group of integers addition modulo n.*

Solution : Let $G = < a >$ be a cyclic group s.t.,

$$o(G) = o(a) = n$$

then $\quad G = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$, $\mathbf{Z}_n = \{0, 1, 2, \ldots\ldots, n-1\}$

Define $\quad f : G \to \mathbf{Z}_n$ s.t.,

f is clearly well defined 1-1 onto mapping.

Again $f(a^i \,.\, a^j) = f(a^{i \oplus j}) = i \oplus j = f(a^i) \oplus f(a^j)$

Thus f is a homomorphism and hence an isomorphism.

Remark : Any two cyclic groups of same order (finite or infinite) are isomorhpic.

Problem 24 : *Show that any finite cyclic group of order n is isomorphic to the quotient group* $\dfrac{\mathbf{Z}}{N}$, *where* $< \mathbf{Z}, + >$ *is group of integers and* $N = < n >$.

Solution : Let $G = < a >$ be of order n

Define $\quad f : \mathbf{Z} \to G$, s.t.,

$$f(m) = a^m$$

then f is clearly well defined onto map.

Since $\quad f(m + k) = a^{m+k} = a^m \; a^k = f(m) \,.\, f(k)$

f is a homomorphism and therefore, by Fundamental theorem $G \cong \dfrac{\mathbf{Z}}{\text{Ker } f}$

We show $\quad \text{Ker} f = N = < n >$

Now

$$\begin{aligned} m \in \text{Ker} f &\Leftrightarrow f(m) = e \\ &\Leftrightarrow a^m = e \\ &\Leftrightarrow o(a) \mid m \\ &\Leftrightarrow n \mid m \\ &\Leftrightarrow m \in < n > \end{aligned}$$

Hence $\quad G \cong \dfrac{\mathbf{Z}}{< n >}$.

Remark : In view of the above results, we notice

$$\mathbf{Z}_n \cong \frac{\mathbf{Z}}{< n >}.$$

Problem 25 : *If G is the additive group of reals and N is the subgroup of G consisting of integers, prove that* $\dfrac{G}{N}$ *is isomorphic to the group H of all complex numbers of absolute value 1 under multiplication.*

Solution : Define a map

$$f: G \to H, \text{ s.t.}$$
$$f(\alpha) = e^{2\pi i\alpha}$$

where $$|e^{2\pi i\alpha}| = |\cos 2\pi\alpha + i \sin 2\pi\alpha|$$
$$= \sqrt{\cos^2(2\pi\alpha) + \sin^2(2\pi\alpha)} = 1$$

We show f is onto.

Let $h \in H$ be any element, then $h = a + ib$

where $$|a + ib| = 1 = \sqrt{a^2 + b^2}$$

If $$a + ib = r(\cos\theta + i \sin\theta)$$

then $$(a + ib) = 1 \Rightarrow r = 1$$

$\therefore$ $$a + ib = \cos\theta + i \sin\theta = e^{i\theta}$$

then $$f\left(\frac{\theta}{2\pi}\right) = e^{\frac{\theta}{2\pi}.2\pi i} = e^{i\theta}$$

$$\Rightarrow \frac{\theta}{2\pi} \text{ is the required pre-image.}$$

Again f is a homomorphism, as

$$f(\theta_1 + \theta_2) = e^{2\pi(\theta_1+\theta_2)i} = e^{2\pi\theta_1 i}.e^{2\pi\theta_2 i}$$
$$= f(\theta_1)\ f(\theta_2)$$

By fundamental theorem of group homomorphism

$$H \cong \frac{G}{\text{Ker } f}$$

We claim $\text{Ker } f = N$

Now $$\alpha \in \text{Ker} \Leftrightarrow f(\alpha) = 1$$
$$\Leftrightarrow e^{2\pi i\alpha} = 1$$
$$\Leftrightarrow \cos 2\pi\alpha + i \sin 2\pi\alpha = 1 = 1 + i0$$
$$\Leftrightarrow \cos 2\pi\alpha = 1, \sin 2\pi\alpha = 0$$
$$\Leftrightarrow 2\pi\alpha = 2\pi\alpha n \pm 0 \text{ where } n \text{ is an integer}$$
$$\Leftrightarrow \alpha = n$$
$$\Leftrightarrow \in N$$

thus $$\text{Ker} f = N$$

and hence $$H \cong \frac{G}{N}.$$

Problem 26 : *Let G be the group of all non zero complex numbers under multiplication and let G' be the group of all real 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where not both a and b are zero, under matrix multiplication, Show that $G \cong G'$.*

Solution : Define a map

$$\varphi : G \to G', \text{ s.t.,}$$

$$\varphi(a + ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

φ is clearly well-defined.

Also

$$\varphi[(a + ib)(c + id)] = \varphi[(ac - bd) + i(ad + bc)] = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}$$

and

$$\varphi(a + ib)\,\varphi(c + id) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}$$

shows that φ is a homomorphism.

Again for $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, the required pre-image is $(a + ib)$.

Thus φ is onto.

Also, $\varphi(a + ib) = \varphi(c + id)$

$$\Rightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$$

$$\Rightarrow a = c,\ b = d \Rightarrow a + ib = c + id$$

Hence φ is an isomorphism.

Problem 27 : *Suppose G is a group of order p^2, where p is a prime. Let $\varphi : G \to H$ be an onto homomorphism, where H is a group. Then show that either φ is an isomorphism or φ maps each element x of G onto the identity e of H and $H = \{e\}$ or else, for each $y \in H$, $\exists$ exactly p elements x of G such that $\varphi(x) = y$.*

Solution : $\varphi : G \to H$ is an onto homomorphism

$o(G) = p^2$.

Since $\operatorname{Ker}\varphi$ is a subgroup of G, By Lagrange's theorem $o(\operatorname{Ker}\varphi) \mid o(G) = p^2$

$$\Rightarrow o(\operatorname{Ker}\varphi) = 1,\ p \text{ or } p^2$$

Case (i) : $o(\operatorname{Ker}\varphi) = 1 \Rightarrow \operatorname{Ker}\varphi = \{e\}$

$\Rightarrow \varphi$ is 1-1

hence φ is an isomorphism.

Case (*ii*) : $o(\text{Ker}\,\varphi) = p^2$

$\Rightarrow \text{Ker}\,\varphi = G$

$\Rightarrow$ for all $x \in G$, $x \in \text{Ker}\,\varphi \Rightarrow \varphi(x) = e$ for all $x \in G$

Since φ is onto, each element of H has a pre-image, but all members of G are mapped to e.

$\therefore \quad H = \{e\}$.

Case (*iii*) : $o(\text{Ker}\,\varphi) = p$

Let $y \in H$ be any element then as φ is onto, $\exists\, x \in G$, s.t., $\varphi(x) = y$

Let $\text{Ker}\,\varphi = \{a_1 = e, a_2, a_3, \ldots\ldots, a_p\}$

We claim $xa_1, xa_2, \ldots\ldots, xa_p$ are distinct.

Suppose $xa_i = xa_j$, then $a_i = a_j$

which is not true.

Thus $xa_1, xa_2, \ldots\ldots, xa_p$ are distinct members of G.

Now $\varphi(xa_i) = \varphi(x)\varphi(a_i) \quad i = 1, 2, \ldots\ldots, p.$

$= ye = y$ for all i $(a_i \in \text{Ker}\,\varphi)$

thus y has p pre-images $x = xa_1, xa_2, \ldots\ldots, xa_p$

To show that y does not have more than p pre-images, let x' be any other pre-image of y under φ

Then $\varphi(x') = y = \varphi(x)$

$\Rightarrow (\varphi(x))^{-1}\,\varphi(x') = e$

$\Rightarrow \varphi(x^{-1}x') = e$

$\Rightarrow x^{-1}x' \in \text{Ker}\,\varphi$

$\Rightarrow x^{-1}x' = a_i$ for some i

$\Rightarrow x' = xa_i$ for some i

i.e., it is one of the p pre-images, we have considered.

Hence y has exactly p pre-images.

5 **Problem 28 :** *Prove that if* $\dfrac{G}{H} \cong \dfrac{G}{K}$ *and G is cyclic then $H = K$. Show by an example that H may not equal K when G is not cyclic.*

Solution : Let $G = \langle a \rangle$ and suppose $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Then n is the smallest +ve integer s.t., $a^n \in H$ (see theorem 19, chapter 2). Thus $H, Ha, \ldots\ldots, Ha^{n-1}$ are distinct right cosets of H in G and no more. So $i_G(H) = n$.

Similarly, $i_G(K) = m$.

Now $\dfrac{G}{H} \cong \dfrac{G}{K} \Rightarrow i_G(H) = i_G(K)$

$\Rightarrow n = m$ or that $H = K$.

For the second part take G to be the quaternion group $\{\pm 1, \pm i, \pm j, \pm k\}$ then G is not cyclic (It is not abelian).

Let $H = \{\pm 1, \pm i\}$, $K = \{\pm 1, \pm j\}$

then H, K are normal subgroups of G and $\frac{G}{H} = \{H, Hj\}$, $\frac{G}{K} = \{K, Ki\}$

The mapping $H \to H$, $Hj \to Ki$ will be an isomorphism, whereas $H \neq K$.

Problem 29 : *Show that the additive group of integers modulo 4 is isomorphic to the multiplicative group of non zero elements of integers modulo 5. State the two isomorphisms.*

Solution : Let $G = \{0, 1, 2, 3\}$ addition mod 4

$G' = \{1, 2, 3, 4\}$ mult. mod 5

Then G, G' are cyclic groups of order 4. Both are generated by 1 and thus $G \cong G'$.

Since $\varphi(4) = 2$, G, G' have two generators each and these are 1, 3.

Define $\theta : G \to G'$, s.t.,

$\theta(1) = 3$.

Then $\theta(2) = \theta(1 \oplus 1) = 3 \otimes 3 = 4$

$\theta(3) = \theta(1 \oplus 1 \oplus 1) = 3 \otimes 3 \otimes 3 = 2$

$\theta(0) = \theta(1 \oplus 1 \oplus 1 \oplus 1) = 3 \otimes 3 \otimes 3 \otimes 3 = 1$

This is one isomorphism.

Again, $\varphi : G \to G'$, s.t.,

$\varphi(3) = 3$

will give $\varphi(2) = \varphi(3 \oplus 3) = 3 \otimes 3 = 4$

$\varphi(1) = 2$, $\varphi(0) = 1$

which is the second isomorphism

One may notice here that under an isomorphism, generator is mapped to a generator.

The Dihedral Group

Let $G = \{x^i y^i \mid i = 0, 1, j = 0, 1, \ldots, n-1, x^2 = e = y^n, xy = y^{-1}x\}$

Then G is a group, called the dihedral group. ($n \geq 3$).

Infact, we can write G also as

$$G = \left\{ \begin{matrix} y, y^2, \ldots\ldots, y^{n-1}, y^n = e \\ xy, xy^2, \ldots\ldots, xy^{n-1}, x \end{matrix} \;\middle|\; x^2 = e = y^n, xy = y^{-1}x \right\}$$

$o(G) = 2n$. We write $G = D_{2n}$

What is the product $(xy)(xy^2)$ in terms of elements of G written as above?

Now $xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1}$

$$\Rightarrow xyx = y^{-1} \text{ as } x^2 = e \Rightarrow x = x^{-1}$$

$\therefore$ $$(xy)(xy^2) = (xyx)y^2$$
$$= y^{-1}y^2 = y$$

Also, how to find yxy^2?

Since $$xy = y^{-1}x \Rightarrow yxy = x$$
$$\Rightarrow yxy^2 = xy$$

In this way, we can compute the product of any two elements of G

We first find $Z(G)$

Consider $y^i \quad (1 \le i \le n)$

Then $$y^i(xy^i) = (y^i xy^i)\, y^{-i+j}$$
$$= xy^{-i+j}$$

Note $$xy = y^{-1}x \Rightarrow xyx^{-1} = y^{-1}$$
$$\Rightarrow (xyx^{-1})^i = y^{-i}$$
$$\Rightarrow xy^i x^{-1} = y^{-i}$$
$$\Rightarrow y^i xy^i = x$$

(This is a very useful relation in D_{2n}).

Also $$(xy^i)\, y^i = xy^{i+j}$$

If $y^i \in Z(G)$, then y^i must commute with xy^j for all j, $1 \le j \le n$.

$\therefore$ $$xy^{-i+j} = xy^{i+j} \text{ for all } j,\ 1 \le j \le n$$
$$\Rightarrow y^{2i} = e$$
$$\Rightarrow o(y) \text{ divides } 2i$$
$$\Rightarrow n \text{ divides } 2i$$

Case 1 : n = odd

Then $$n \mid 2i \text{ and } (n, 2) = 1$$
$$\Rightarrow n \mid i$$
$$\Rightarrow n \le i. \text{ But } i \le n$$

$\therefore$ $$i = n$$

So, $$y^i = y^n = e.$$

Similarly, if $xy^i \in Z(G)$, then $(xy^i)x = x\,(xy^i)$
$$\Rightarrow xy^i x^{-1} = x^2 y^i$$
$$\Rightarrow y^{-i} = x^2 y^i$$
$$\Rightarrow y^{2i} = e \text{ as } x^2 = e$$
$$\Rightarrow o(y) \mid 2i \Rightarrow n \mid 2i \Rightarrow n \mid i \Rightarrow n = i$$

$\therefore$ $$xy^i = xy^n = x$$

But $x \notin Z(G)$ as $xy = y^{-1}x$ (and $x \in Z(G)$ should imply $xy = yx$, i.e., $yx = y^{-1}x \Rightarrow y^2 = e \Rightarrow o(y) = n \mid 2 \Rightarrow n \le 2$, a contradiction as $n \le 3$).

So, $Z(G)$ does not contain any element of the type xy^i. Also if $y^i \in Z(G)$, then $i = n$

$\therefore \qquad Z(G) = \{e\}.$

Case 2 : $\quad n$ = even Let $n = 2m$

Then as above $\quad n \mid 2i$

$$\Rightarrow 2m \mid 2i$$
$$\Rightarrow m \mid i$$
$$\Rightarrow i = m \text{ or } 2m = n$$

i.e., $\quad y^i = y^m$ or $y^{2m} = y^n = e$

Clearly $\quad y^m \in Z(G)$ as $(xy^k)\, y^m = xy^{k+m}$

and $\quad y^m (xy^k) = (y^m xy^m)\, y^{k-m}$

$$= xy^{k-m} = xy^{k+m}$$

as $\quad y^{2m} = e \Rightarrow y^m = y^{-m}$

$\therefore$ only powers i of y s.t., $y^i \in Z(G)$ are $i = m$ and $2m$.

Similarly, as in case 1, if $xy^i \in Z(G)$,

then $n \mid 2i \Rightarrow 2m \mid 2i \Rightarrow m \mid i \Rightarrow i = m$ or $2m$

But $\quad xy^{2m} = xy^n = xe = x \notin Z(G)$

Also $\quad (xy^m)\, y = xy^{m+1}$

and $\quad y(xy^m) = yxy^m$

So, if $xy^m \in Z(G)$, then $xy^{m+1} = yxy^m$

$$\Rightarrow xy = yx$$
$$\Rightarrow y^{-1}x = yx$$
$$\Rightarrow y^2 = e$$
$$\Rightarrow o(y) \text{ divides } 2$$
$$\Rightarrow n \text{ divides } 2$$
$$\Rightarrow n \le 2, \text{ a contradiction}$$

$\therefore \qquad Z(G) = \{e, y^m\}$, where $n = 2m$.

Thus, we have proved the following :–

If n = odd, then $Z(D_{2n}) = \{e\}$ and if n = even = $2m$, then $Z(D_{2n}) = \{e, y^m\}$.

Problem 30 : *Show that* $N = \{y, y^2, \ldots\ldots, y^{n-1}, y^n = e\}$ *is a normal subgroup of* D_{2n}.

Solution : N is a subgroup of D_{2n} generated by y.

Let $\quad g \in D_{2n},\ y^i \in N$

If $g = y^j$, then $gy^i g^{-1} = y^j y^i y^{-j}$

$$= y^i \in N.$$

Let $\quad g = xy^j,\ 1 \le j \le n.$

Then $\quad gy^i g^{-1}$

$$= xy^j y^i (xy^j)^{-1}$$
$$= xy^{i+j} y^{-j}\, x^{-1}$$

$$= xy^i x^{-1}$$
$$= (xyx^{-1})^i$$
$$= y^{-i} \in N \text{ (as } xyx^{-1} = y^{-1})$$

$\therefore$ N is a normal subgroup of G.

Problem 31 : *Show that* $\frac{G}{N}$ *is isomorphic to the multiplicative group* $\{1,-1\}$, *where* $G = D_{2n}$ *and* $N = \{y, y^2, \ldots\ldots, y^{n-1}, y^n = e\}$.

Solution : Define $\theta : G \to W = \{1, -1\}$

$$\theta(y^j) = 1 \text{ for all } j = 1, 2, \ldots\ldots, n$$
$$\theta(xy^j) = -1 \text{ for all } j = 1, 2, \ldots\ldots, n$$

Clearly θ is onto mapping.

Also $\theta(y^j xy^k)$

$$= \theta(y^j xy^j y^{k-j})$$
$$= \theta(xy^{k-j})$$
$$= -1$$

and $\theta(y^j)\ \theta(xy^k) = 1 . (-1) = -1$

$\therefore$ $\theta(y^j xy^k) = \theta(y^j)\ \theta(xy^k)$

Similarly, $\theta(xy^k y^j) = \theta(xy^{k+j}) = -1$

and $\theta(xy^k)\ \theta(y^j) = (-1)(1) = -1$

$\therefore$ $\theta(xy^k y^j) = \theta(xy^k)\,\theta(y^j)$

So, θ is a homomorphism.

$$\therefore \quad \frac{G}{\text{Ker}\,\theta} = W$$

$$\text{Ker}\,\theta = \{g \in G \mid \theta(g) = 1\}$$
$$= \{y^j \mid 1 \le j \le n\}$$
$$= N$$

$$\therefore \quad \frac{G}{N} \cong W.$$

Exercises

1. If $f: G \to G'$ is a homomorphism then show that
$$f(G) = \{f(a) \mid a \in G\}$$
is a subgroup of G'. We also write $f(G) = \text{Im}f$ (Image f). Show further that if H is normal in G then $f(H)$ is normal in $f(G)$, i.e., homomorphic image of a normal subgroup is normal.

2. For a fixed element a in a group G, define
$$f_a : G \to G, \text{ s.t., } f_a(x) = a^{-1}xa, \ x \in G$$

Show that f_a is an isomorphism.

3. Let f, g be homomorphisms from $G \to G'$. Show that $H = \{x \in G \mid f(x) = g(x)\}$ is a subgroup of G.

4. Let G be a finite abelian group. Suppose $o(G)$ and n are co-prime. Show that $\varphi : G \to G$, s.t., $\varphi(x) = x^n$ is an isomorphism.

5. Show that the relation of isomorphism in groups is an equivalence relation.

6. Prove that the group $G = \{1, -1\}$ under multiplication is isomorphic to $G' = \{0, 1\}$ under addition modulo 2.

7. Show that $f : \mathbf{C} \to \mathbf{C}$, s.t. $f(z) = \bar{z}$ is an automorphism where $\mathbf{C}$ = complex numbers.

8. Let G be the group of 2×2 matrices over reals of the type $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ s.t., $ad - bc \neq 0$, under matrix multiplication and G' be the group of non zero real numbers under multiplication. Show that the map $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to ad - bc$ is an onto homomorphism.

9. Show that homomorphic image of
   (*a*) an abelian group is abelian.
   (*b*) a cyclic group is cyclic.
   (*c*) a finite group is finite.

10. Show that converse does not hold in all the cases of the previous problem. (See example 8, page 126).

11. Let $\mathbf{R}$ be the set of real numbers. For $a, b \in \mathbf{R}$, $(a \neq 0)$ define $T_{ab} : \mathbf{R} \to \mathbf{R}$, s.t., $T_{ab}(x) = ax + b$.
    Let G be set of all such maps and let $N = \{T_{1b} \in G\}$. Show that G is a group and N is a normal subgroup of G and that $\frac{G}{N}$ is isomorphic to the group of non zero real numbers under multiplication.

12. If φ is a homomorphism of a group G onto $\overline{G}$ with Kernel K and $\overline{N}$ is a normal subgroup of $\overline{G}$

$$N = \{x \in G \mid \varphi(x) \in \overline{N}\}$$

then prove that $\frac{G}{N} \cong \frac{\overline{G}}{\overline{N}}$ and $\frac{G}{N} \cong \frac{G/K}{N/K}$.

13. Let G be the group of non zero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1. Show that $\frac{G}{N}$ is isomorphic to the group of all positive real numbers under multiplication.

14. For any group G, show that $\frac{G}{\{e\}} \cong G$ and $\frac{G}{G} \cong \{e\}$.
15. Show that a simple group has no non-trivial homomorphic image.
16. Show that a subgroup N of G is normal in G if and only if $\exists$ a group H and a homomorphism $\theta : G \to H$ s.t., $\operatorname{Ker} \theta = N$.
17. If G is a cyclic group of order n and $p \mid n$, prove that there exists a homomorphism of G onto a cyclic group of order p. Find its Kernel.

Permutation Groups

In chapter 1 we discussed permutations, and in chapter 2 we gave an example of permutation groups. We continue the discussion starting with

Theorem (Cayley's) 13 : *Every group G is isomorphic to a permutation group.*

Proof : Let G be the given group and $A(G)$ be the group of all permutations of the set G.

For any $a \in G$, define a map $f_a : G \to G$, s.t.,

$$f_a(x) = ax$$

then as $x = y \Rightarrow ax = ay \Rightarrow f_a(x) = f_a(y)$

f_a is well defined.

Again,
$$\begin{aligned} f_a(x) &= f_a(y) \\ &\Rightarrow ax = ay \\ &\Rightarrow x = y \text{ (cancellation in group } G) \\ &\Rightarrow f_a \text{ is 1-1.} \end{aligned}$$

Also, for any $y \in G$, since $f_a(a^{-1}y) = a(a^{-1}y) = y$, we find $a^{-1}y$ is pre image of y or that f_a is onto and hence a permutation on G.

Thus $f_a \in A(G)$.

Let K be the set of all such permutations. We show K is a subgroup of $A(G)$. $K \neq \varphi$ as $f_e \in K$.

Let $f_a, f_b \in K$ be any members

then since $f_b \circ f_{b^{-1}}(x) = f_b(f_{b^{-1}}(x)) = f_b(b^{-1}x) = b(b^{-1}x)$

$$= ex = f_e(x) \text{ for all } x$$

we find $f_{b^{-1}} = (f_b)^{-1}$ (Note $f_e = I$, identity of $A(G)$).

Also as $(f_a \circ f_b)x = f_a(bx) = a(bx) = (ab)x = f_{ab}(x)$ for all x

we find $\quad f_{ab} = f_a \circ f_b$

Now $\quad f_a \circ (f_b)^{-1} = f_a \circ f_{b^{-1}} = f_{ab^{-1}} \in K$

Showing that K is a subgroup of $A(G)$.

Define now a mapping $\varphi : G \to K$, s.t.,

$$\varphi(a) = f_a$$

then φ is well defined, 1-1 map as

$$\begin{aligned} & a = b \\ \Leftrightarrow\ & ax = bx \\ \Leftrightarrow\ & f_a(x) = f_b(x) \quad \forall x \\ \Leftrightarrow\ & f_a = f_b \\ \Leftrightarrow\ & \varphi(a) = \varphi(b) \end{aligned}$$

φ is obviously onto, and since

$$\varphi(ab) = f_{ab} = f_a o f_b = \varphi(a)\ \varphi(b)$$

φ is a homomorphism and hence an isomorphism which proves our assertion. Note K being a subgroup of a permutation group is a permutation group.

Remark : In particular, if G is a finite group of order n then G is isomorphic to a subgroup of S_n.

Theorem 14 : *Order of any permutation f in S_n is equal to the l.c.m. of the orders of the disjoint cycles in f.*

Proof : Let $f = f_1 f_2 \ldots\ldots f_n$

be the representation of f as product of disjoint cycles $f_1, f_2, \ldots\ldots, f_n$

Let $\qquad o(f_i) = r_i \qquad i = 1, 2, \ldots\ldots\ldots, n$

then $f_i^{r_i} = I$ (identity of S_n)

Let $\qquad r = l.c.m.\ (r_1, r_2, \ldots\ldots, r_n)$

Now $f^r = (f_1 f_2 \ldots\ldots f_n)^r = f_1^r f_2^r \ldots\ldots f_n^r$ as f_i are disjoint and so commutative.

Since $r_i | r$ for all i, we have $r = r_i k_i \quad i = 1, 2, \ldots\ldots, n$

Thus $f^r = f_1^{r_1 k_1} f_2^{r_2 k_2} \ldots\ldots\ldots f_n^{r_n k_n} = I \,.\, I \ldots\ldots I = I$

Suppose now $\qquad f^t = I$

$$\Rightarrow (f_1 f_2 \ldots\ldots f_n)^t = I$$

$$\Rightarrow f_1^t f_2^t \ldots\ldots f_n^t = I$$

$$\Rightarrow f_1^t = f_2^t = \ldots\ldots = f_n^t = I$$

as $f_1, f_2, \ldots\ldots, f_n$ are disjoint (Note if some $f_i^t \neq I$ then L.H.S. cannot be I).

$$\Rightarrow r_i | t \quad \text{for all } i$$

$$\Rightarrow r | t$$

Hence $\qquad r = o(f)$.

Example 7 : Order of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 6 & 5 & 1 & 3 \end{pmatrix} = (1\,2\,4\,5)\,(3\,6)$$

is *l.c.m.* (4, 2) = 4 as $o(1245) = 4$

$$o(36) = 2.$$

Theorem 15 : *The set A_n of all even permutations of S_n $(n \geq 2)$ is a normal subgroup of S_n and $o(A_n) = \dfrac{o(S_n)}{2}$ and index of A_n in S_n is 2.*

Proof : Since identity permutation is even, A_n is a non empty subset of S_n.

Again, $f, g \in A_n \Rightarrow f, g$ are even permutations

$\Rightarrow f, g^{-1}$ are even permutations

$\Rightarrow fog^{-1}$ is even

$\Rightarrow fog^{-1} \in A_n$

or that A_n is a subgroup of S_n.

If $f \in A_n$ and $g \in S_n$ be any members then $g^{-1} o f o g$ will be even permutation, showing that $g^{-1} o f o g \in A_n$ or that A_n is a normal subgroup of S_n.

Let $G = \{1, -1\}$ be the group under multiplication.

Define a map $\varphi : S_n \to G$, s.t.,

$$\varphi(f) = 1 \text{ if } f \text{ is even permutation}$$
$$= -1 \text{ if } f \text{ is odd permutation}$$

then φ is an onto mapping as S_n $(n \geq 2))$ must contain even as well as odd permutations. (Identity permutation and (12) will be in S_n). To show that φ is a homomorphism, let $f, g \in S_n$ be any members.

Case (i) : Both f, g are even, then fog is even

$$\varphi(fog) = 1 = 1 . 1 = \varphi(f)\ \varphi(g)$$

Case (ii) : Both f, g are odd then fog is even

$$\varphi(fog) = 1 = (-1)(-1) = \varphi(f)\ \varphi(g)$$

Case (iii) : One of f, g is odd, other even.

Suppose f is odd and g is even, then fog is odd

$$\varphi(fog) = -1 = (-1)(1) = \varphi(f)\ \varphi(g)$$

hence φ is an onto homomorphism and thus by Fundamental theorem of homomorphism

$$G \cong \frac{S_n}{\text{Ker } \varphi}$$

Since $\quad f \in \text{Ker } \varphi \Leftrightarrow \varphi(f) = 1$

$$\Leftrightarrow f \text{ is even } \Leftrightarrow f \in A_n$$

we have $\quad \text{Ker } \varphi = A_n$

or that $\quad G \cong \dfrac{S_n}{A_n}$

But $\quad o(G) = 2 \Rightarrow o\left(\dfrac{S_n}{A_n}\right) = 2$

$$\Rightarrow \frac{o(S_n)}{o(A_n)} = 2$$

$$\Rightarrow \frac{o(S_n)}{2} = o(A_n)$$

Also then index of A_n in S_n is 2.

Note : A_n is called the *alternating group* of degree n.

Problem 32 : *Show that if H be any subgroup of S_n ($n \geq 2$) then either all permutations in H are even or exactly half are even. (See Problem 11, Chapter 1 also).*

Solution : Since H is a subgroup, it must contain the identity permutation which is even. So H cannot contain only odd permutations. If all members of H are even, we are done. Suppose it contains both odd as well as even permutations. Let $G = \{1, -1\}$ be the group under multiplication.

Define a map $\varphi : H \to G$, s.t.,

$$\varphi(f) = 1 \text{ if } f \text{ is even}$$
$$= -1 \text{ if } f \text{ is odd}$$

then as in above theorem, φ is an onto homomorphism. Also if K = set of all even permutations of H then $\text{Ker}\,\varphi = K$. By Fundamental theorem then

$$\frac{H}{\text{Ker}\,\varphi} \cong G \quad \text{or} \quad \frac{H}{K} \cong G$$

$$\Rightarrow o\left(\frac{H}{K}\right) = o(G) = 2$$

$$\Rightarrow \frac{o(H)}{2} = o(K)$$

which proves the result.

Remark : If a subgroup H of S_n ($n \geq 2$) contains both even and odd permutations then $o(H)$ cannot be odd.

Example 8 : Consider $S_3 = \{I, (12), (13), (23), (123), (132)\}$

Let A_3 be the alternating group, then

$$A_3 = \{I, (123), (132)\}$$

$$o\left(\frac{S_3}{A_3}\right) = \frac{o(S_3)}{o(A_3)} = \frac{6}{3} = 2$$

In fact $\quad \dfrac{S_3}{A_3} = \{A_3, A_3(1\,2)\}$

Also as $\quad A_3 = (A_3(12))^2$

$$A_3(12) = (A_3(12))^1$$

we find $\frac{S_3}{A_3}$ is a cyclic group generated by $A_3(12)$. Otherwise also a group of prime order is cyclic.

Since S_3 is not abelian, S_3 cannot be cyclic.

We recall the following results that we proved earlier

1. Quotient group of a cyclic group is cyclic
2. Quotient group of an abelian group is abelian.
3. Homomorphic image of an abelian group is abelian.
4. Homomorphic image of a cyclic group is cyclic.

That the converse of all these results is not true follows by considering the above example. Notice, we have the natural onto homomorphism from $S_3 \to S_3/A_3$ and S_3/A_3 is abelian.

Problem 33 : *Show that for $n \geq 3$, the subgroup generated by 3-cycles is A_n.*

Solution : Let H be a subgroup generated by 3-cycles, then every element of H is a product of finite number of 3-cycles and as each 3-cycle is even permutation, every element of H will be even permutation or that $H \subseteq A_n$. Again if $f \in A_n$ then f is product of even number of transpositions.

Since product of any two distinct transpositions can be written as a product of three cycles $[(ab)\,(cd) = (abc)\,(bcd),\ (ab)\,(bc) = (abc)]$ we find f can be expressed as a product of 3-cycles $\Rightarrow f \in H$ and hence $H = A_n$.

Problem 34 : *Show that the smallest subgroup of S_n, containing* (12) *and* (1 2 3 ..... n) *is S_n.*

Solution : Let H be the smallest subgroup of S_n, containing (12) and (1 2 3 .....n). We need show $S_n \subseteq H$.

If $f \in S_n$ be any element, then f can be expressed as a product of transpositions and as any transposition $(ab) = (1a)\,(1b)\,(1a)$, f can be expressed as a product of transpositions of the type $(1x)$. We show all transpositions (12), (13), (14) ,....., $(1n)$ are in H, which will imply that f is in H, as f is nothing but product of some such members.

Now $(1n) = (n\ n-1\ .....\ 321)\ (12)\ (123\ .....\ n) \in H$

$\Rightarrow (n\ n-1) = (n\ n-1\ .....\ 321)\ (1n)\ (123\ .....\ n) \in H$

$(n-1\ n-2) = (n\ n-1\ .....\ 321)\ (n\ n-1)\ (123\ ....\ n) \in H$

and so on.

Showing that (43), (32) etc. are in H.

Now $(12) \in H$

$\Rightarrow (13) = (12)\ (23)\ (12) \in H$

$\Rightarrow (14) = (13)\ (34)\ (13) \in H$

.....

$(1n) \in H$

Hence $H = S_n$.

Problem 35 : *Give an example of two subgroups H, K which are not normal, but HK is a subgroup.*

Solution : Let $H = \{I, (12)\}$

$K = \{I, (123), (132)\}$

be two subgroups of S_4 (that these are subgroups can be verified).

Here $HK = \{ I, (12), (123), (132), (12)(123), (12)(132)\}$

$= \{ I, (12), (123), (132), (23), (13)\}$

$KH = \{ I, (123), (132), (12), (123)(12), (132)(12)\}$

$= \{ I, (12), (123), (132), (23), (13)\}$

Thus $HK = KH \Rightarrow HK$ is a subgroup

Now $H(123) = \{(123), (12)(123)\} = \{(123), (23)\}$

$(123)H = \{(123), (13)\}$

or that $H(123) \neq (123)H$

i.e., $Ha \neq aH$ for some $a \in S_4$

$\Rightarrow H$ is not normal in S_4

Similarly one can check that $K(14) \neq (14)K$

or that K is not normal in S_4.

Problem 36 : *Show that* $Z(S_n) = \{I\}$, $(n \geq 3)$.

Solution : Let $\sigma \in Z(S_n)$ be any member and suppose $\sigma \neq I$. We can express

$$\sigma = f_1 f_2 \ldots\ldots f_k$$

as product of disjoint cycles.

Case (i) : f_1 is of length 2, say, $f_1 = (a_1 a_2)$

then as $n \geq 3$, $\exists$ at least one a_3 $(\neq a_1, a_2)$.

Since $\sigma \in Z(S_n)$, $\sigma(a_1 a_2 a_3) = (a_1 a_2 a_3)\sigma$

$\Rightarrow f_1 f_2 \ldots\ldots f_k \ (a_1 a_2 a_3) = (a_1 a_2 a_3) \ f_1 f_2 \ldots\ldots f_k$

$\Rightarrow (a_1 a_2) \ f_2 f_3 \ldots\ldots f_k \ (a_1 a_2 a_3) = (a_1 a_2 a_3) \ (a_1 a_2) \ f_2 f_3 \ldots\ldots f_k$

In L.H.S. $a_1 \to a_2 \to a_1$ and in R.H.S. $a_1 \to a_2 \to a_3$ (Note a_1, a_2 do not belong to any of $f_2, f_3 \ldots\ldots f_k$) which is a contradiction.

Case (ii) : f_1 is of length ≥ 3, say $f_1 = (a_1 a_2 \ldots\ldots a_t)$, $t \geq 3$.

Since $\sigma \in Z(S_n)$, $\sigma(a_1 a_2) = (a_1 a_2)\sigma$

$\Rightarrow f_1 f_2 \ldots\ldots f_k \ (a_1 a_2) = (a_1 a_2) \ f_1 f_2 \ldots\ldots f_k$

$\Rightarrow f_1 (a_1 a_2) \ f_2 f_3 \ldots\ldots f_k = (a_1 a_2) \ f_1 f_2 f_3 \ldots\ldots f_k$

$(a_1 a_2 \in f_1$ and thus do not belong to f_i, $i \geq 2)$.

$\Rightarrow f_1 (a_1 a_2) = (a_1 a_2) f_1$

$\Rightarrow (a_1 a_2 \ldots\ldots a_t) \ (a_1 a_2) = (a_1 a_2) \ (a_1 a_2 \ldots\ldots a_t)$

In L.H.S. $a_t \to a_1$ and in R.H.S. $a_t \to a_1 \to a_2$ giving us a contradiction. Hence our supposition that $\sigma \neq I$ is not possible.

Problem 37 : *Show that in S_n the number of distinct cycles of length r is* $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$, $(r \leq n)$.

Solution : Since the number of distinct arrangements of r objects chosen out of n objects is ${}^nP_r = \frac{n!}{(n-r)!}$ and the cycles

$$(a_1 a_2 \ldots\ldots a_r),\ (a_2 a_3 \ldots\ldots a_r a_1),\ (a_3 a_4 \ldots\ldots a_r a_1 a_2),\ \ldots\ldots,\ (a_r a_1 \ldots\ldots a_{r-1})$$

are same, we find the number of distinct r-cycles will be $\frac{1}{r} \cdot \frac{n!}{(n-r)!}$.

Problem 38 : *Show by an example that converse of Lagrange's theorem may not hold.*

Solution : Consider the alternating group A_4.

$$o(A_4) = \frac{o(S_4)}{2} = \frac{\lfloor 4}{2} = 12$$

We show although $6 \mid 12$, A_4 has no subgroup of order 6. Suppose H is a subgroup of A_4 and $o(H) = 6$.

By previous problem the number of distinct 3-cycles in S_4 is $\frac{1}{3} \cdot \frac{4!}{(4-3)!} = \frac{4.3.2.1}{3.1} = 8$.

Again, as each 3-cycle will be even permutation all these 3-cycles are in S_4. Obviously then, at least one 3-cycle, say σ, does not belong to H ($o(H) = 6$).

Now $\sigma \notin H \Rightarrow \sigma^2 \notin H$, because if $\sigma^2 \in H$

then $\sigma^4 \in H$

$\Rightarrow \sigma \in H$

as $\sigma^3 = I$ as $o(\sigma) = 3$.

Let $K = \langle \sigma \rangle = \{I, \sigma, \sigma^2\}$ then $o(K) = 3$ $(= o(\sigma))$

and $H \cap K = \{I\}$ $(\sigma, \sigma^2 \notin H)$

$\Rightarrow o(HK) = \frac{o(H).o(K)}{o(H \cap K)} = \frac{6.3}{1} = 18$, not possible as $HK \subseteq A_4$ and $o(A_4) = 12$.

Problem 39 : *A_4 is the only subgroup of order 12 in S_4.*

Solution : Let H be any subgroup of order 12 in S_4. Let $H \neq A_4$. Then H contains an odd permutation.

Thus H has 6 odd and 6 even permutations.

$\Rightarrow H \cap A_4$ is a subgroup of A_4 of order 6

$\Rightarrow A_4$ has subgroup of order 6

But that is not possible by above problem. Hence the result.

Problem 40 : *Show that* (123) *is not the cube of any member of* S_n.

Solution : We first show that if $(\alpha_1 \alpha_2 \ldots\ldots \alpha_9)$ is any cycle

then $(\alpha_1 \alpha_2 \ldots\ldots \alpha_9)^3 = (\alpha_1 \alpha_4 \alpha_7)\ (\alpha_2 \alpha_5 \alpha_8)\ (\alpha_3 \alpha_6 \alpha_9)$

Since $(\alpha_1 \alpha_2 \ldots\ldots \alpha_9)^2 = (\alpha_1 \alpha_2 \ldots\ldots \alpha_9)\ (\alpha_1 \alpha_2 \ldots\ldots \alpha_9)$

$$= (\alpha_1 \alpha_3 \alpha_5 \alpha_7 \alpha_9 \alpha_2 \alpha_4\ \alpha_6 \alpha_8)$$

$$(\alpha_1 \alpha_2 \ldots\ldots \alpha_9)^3 = (\alpha_1 \alpha_2 \ldots\ldots \alpha_9)\ (\alpha_1 \alpha_3 \alpha_5 \alpha_7 \alpha_9 \alpha_2 \alpha_4\ \alpha_6 \alpha_8)$$

$$= (\alpha_1 \alpha_4 \alpha_7)\ (\alpha_2 \alpha_5 \alpha_8)\ (\alpha_3 \alpha_6 \alpha_9)$$

Suppose now $(1\ 2\ 3) = \alpha^3$ for some $\alpha \in S_n$, then as α can be expressed as product of disjoint cycles

Let $\alpha = \sigma_1 \sigma_2 \ldots\ldots \sigma_k$ where σ_i are disjoint cycles

Then $\alpha^3 = \sigma_1^3 \sigma_2^3 \ldots\ldots \sigma_k^3$ (as disjoint cycles commute)

Also $\alpha^3 = (123)$

$$\Rightarrow \alpha^9 = (123)^3 = I \Rightarrow o(\alpha) = 9$$

thus each σ_i will be of length 3 or 9 as order of a permutation is the l.c.m. of the orders (lengths) of its disjoint cycles.

Again there is at least one σ_i whose length is 9 otherwise if all have length 3 then l.c.m. will be 3 implying $o(\alpha) = 3$ which is not true.

Without loss of generality take length of σ_i to be 9.

Now if length of any σ_i is 3 then $\sigma_i^3 = I$.

So $\alpha^3 = (123) = \sigma_1^3 \sigma_2^3 \ldots\ldots \sigma_k^3$

$$= \sigma_1^3 \times \text{other cubes of cycles of length 9}$$

Let $\sigma_1 = (\alpha_1 \alpha_2 \ldots\ldots \alpha_9)$

$\Rightarrow \sigma_1^3 = (\alpha_1 \alpha_4 \alpha_7)\ (\alpha_2 \alpha_5 \alpha_8)\ (\alpha_3 \alpha_6 \alpha_9)$

$\Rightarrow (123) = (\alpha_1 \alpha_4 \alpha_7)\ (\alpha_2 \alpha_5 \alpha_8)\ (\alpha_3 \alpha_6 \alpha_9) \times$ other cycles which do not contain $\alpha_1, \alpha_2 \ldots\ldots, \alpha_9$

(as all are disjoint) which will be a contradiction as each α_i is different and so if $\alpha_1 = 1$, $\alpha_2 = 2$, $\alpha_3 = 3$ then α_4 is such that it is fixed in L.H.S. but in R.H.S. $\alpha_4 \to \alpha_7$. Hence the result.

Example 9 : Consider $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$

Let us denote these elements by e, x, y, z then the following table gives us the respective products

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

which also shows that closure holds in K_4 and thus K_4 forms a group. It is called **Klein's four group** which is a subgroup of S_4.

Remarks (*i*) : We could also take the elements e, x, y, z to be the matrices

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ under matrix multiplication.

(*ii*) : We may further notice that any non cyclic abelian group of order 4 is of the type $G = \{e, a, b, ab\}$. Here each element (except e) will have order 2. [$x \in G \Rightarrow o(x) \mid o(G) \Rightarrow o(x) = 1$, 2 or 4. But $o(x) = 4$ gives $x^4 = e$ and then G will be cyclic]

Thus $o(a) = o(b) = o(ab) = 2$

i.e., $a^2 = b^2 = (ab)^2 = e$

Clearly this group G is isomorphic to the Klein's four group [$e \to I$, $a \to (12)(34)$, $b \to (13)(24)$, $ab \to (14)(23)$]. Hence every non cyclic (abelian) group of order 4 is isomorphic to the Klein's four group.

Problem 41 : *Show by an example that we can find three groups $E \subseteq F \subseteq G$ such that E is normal in F, F is normal in G whereas E is not normal in G.*

Solution : Let $E = \{I, (12)(34)\}$

$$F = K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$$

$$G = A_4$$

then E is not normal in G as

$$E(123) = \{I(123), (12)(34)(123)\} = \{(123), \quad (243)\}$$

$$(123)E = \{(123)\ I, (123)(12)(34)\} = \{(123), \quad (134)\}$$

Showing that $E(123) \neq (123)E \qquad (123) \in A_4 = G$.

E would be normal in F as index of E in F is 2.

Also F is normal in G as

Let $\theta \in A_4$ and $(ab)(cd) \in K_4$ be any elements.

(a, b, c, d being any of $1, 2, 3, 4$)

then $\theta(ab)(cd)\theta^{-1} = (\theta(a)\theta(b))(\theta(c)\theta(d)) \in K_4$ as all permutations with this cycle structure are in K_4.

$$\Rightarrow K_4 \text{ is normal in } A_4.$$

Note that all elements in K_4 are even permutations and so belong to A_4.

Theorem 16 : *Let H be a subgroup of G and $\mathcal{L} = \{aH \mid a \in G\}$ then $\exists$ a homomorphism $\theta : G \to A(\mathcal{L})$ s.t., $Ker\,\theta$ is the largest normal subgroup of G contained in H.*

Proof : Define $\theta : G \to A(\mathcal{L})$, s.t.,

$$\theta(g) = f_g$$

where $f_g : \mathcal{L} \to \mathcal{L}$, s.t.,

$$f_g(aH) = gaH$$

To show that θ is well defined, we need prove that $f_g \in A(\mathcal{L})$

Now $f_g(aH) = f_g(bH)$

$\Rightarrow gaH = gbH$

$\Rightarrow aH = bH \quad \Rightarrow f_g$ is 1-1

Again for any $aH \in \mathcal{L}$,

$$fg(g^{-1}aH) = aH, \text{ showing that}$$

f_g is onto and thus $f_g \in A(\mathcal{L})$

We have $\theta(gH) = f_{gh}$, $\theta(g)\ \theta(h) = f_g\ f_h$

and since $f_{gh}(aH) = ghaH$

$f_g f_h(aH) = f_g(f_h(aH) = f_g(haH) = ghaH$

we thus find $f_{gh} = f_g f_h$

or that θ is a homomorphism.

Since Kernel of a homomorphism is normal subgroup, we have Ker θ, a normal subgroup of G.

Again, if $g \in \text{Ker}\,\theta$ then

$$\theta(g) = I = \text{Identity of } A(\mathcal{L})$$

$\Rightarrow f_g = I$

$\Rightarrow f_g(aH) = aH \quad \forall\, aH \in h$

In particular,

$$f_g(eH) = eH \Rightarrow geH = eH \Rightarrow gH = H$$
$$\Rightarrow g \in H$$

$\Rightarrow \text{Ker}\,\theta \subseteq H$

Let now K be any normal subgroup of G, contained in H. Let $k \in K$ be any element. We want to show that $k \in \text{Ker}\,\theta$ or that $\theta(k) = I$

or that $f_k = I$

or that $f_k(aH) = aH \quad \forall\, aH$

Now $f_k(aH) = kaH = a(a^{-1}\ ka)H = ahH = aH$

[Note $a^{-1}ka \in K \subseteq H$]

Hence $K \subseteq \text{Ker}\,\theta$ which proves the theorem.

Cor. : *If $H \neq G$ is a subgroup of a finite group G, s.t., $o(G)$ does not divide $i_G(H)!$ then G has a non trivial normal subgroup. (i.e., G is not simple).*

Proof : By above theorem, we find Ker θ is a normal subgroup of G.

Since $\text{Ker}\,\theta \subseteq H \neq G$, $\text{Ker}\,\theta \neq G$

If $\operatorname{Ker}\theta = \{e\}$, then θ is 1-1 and thus $\theta : G \to A(\mathcal{L})$ is 1-1 homomorphism i.e., G is isomorphic to a subgroup T of $A(\mathcal{L})$.

$\Rightarrow o(G) = o(T)$

But $o(T) \mid o(A(\mathcal{L})) \Rightarrow o(G) \mid o(A(\mathcal{L})) = i_G(H)$! a contradiction and so $\operatorname{Ker}\theta \neq \{e\}$ and is the required non trivial normal subgroup.

Remark : If $H = \{e\}$, the above theorem is nothing but Cayley's theorem, as then $\operatorname{Ker}\theta = \{e\} \Rightarrow \theta$ is 1-1.

Exercises

1. In S_3, show that we can find elements, a, b s.t., $(ab)^2 \neq a^2 b^2$. Also show that there exist four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.
2. Find order of all elements in S_3 and list all its subgroups.
3. Show that S_4 has no element of order greater than or equal to 4.
4. Show that A_4 has no subgroup of order 6.
5. Let $H = \{I, (123), (132)\}$, $K = \{I, (12)\}$ be two subgroups of S_3. Write all the left and right cosets of H and K in S_3. Hence show that H is normal whereas K is not normal in S_3.

Generators of a Subgroup

Let S be a non empty subset of a group G. Let

$$H = \{x_1 x_2 \ldots\ldots x_n \mid n \text{ is finite but not fixed, } x_i \text{ or } \underset{\text{for all } i}{x_i^{-1}} \in S\}$$

then H is a subgroup of G and contains S. $S \neq \varphi \Rightarrow H \neq \varphi$

Again, $x, y \in H \Rightarrow x = x_1 x_2 \ldots\ldots x_n \quad x_i \text{ or } x_i^{-1} \in S$

$$y = y_1 y_2 \ldots\ldots y_m \qquad y_j \text{ or } y_j^{-1} \in S$$

$\Rightarrow xy^{-1} = x_1 x_2 \ldots\ldots x_n . y_m^{-1} y_{m-1}^{-1} \ldots\ldots\ldots y_2^{-1} . y_1^{-1} \in H$

Showing that H is a subgroup of G.

$S \subseteq H$ follows by definition of H.

This subgroup H is called the subgroup of G, generated by S and we write $H = \langle S \rangle$.

Indeed if $S = \{a\}$, $H = \langle a \rangle$, the subgroup we've been talking about earlier.

Theorem 17 : *$H = \langle S \rangle$ is the smallest subgroup of G containing S.*

Proof : Suppose K is a subgroup of G containing S

$$x \in H \Rightarrow x = x_1 x_2 \ldots\ldots\ldots x_n, \qquad x_i \text{ or } x_i^{-1} \in S$$

if $x_i \in S$ then $x_i \in K$ as $S \subseteq K$

if $x_i^{-1} \in S$ then $x_i^{-1} \in K \Rightarrow x_i \in K$ (as K is a subgroup)

i.e., $x_i \in K$ for all i

$\Rightarrow x \in K \Rightarrow H \subseteq K$

or that H is the smallest subgroup containing S.

Remark : $H = <S>$ will be the intersection of all subgroups of G containing S.

Example 10 : Let $G = S_3$, $S = \{(12), (13)\}$

$$(13)\ (12) = (231) = (123) \in H$$
$$(12)\ (13) = (132) \in H$$
$$(12)\ (123) = (2\ 3) \in H$$
$$(12)\ (12) = I \in H$$

we find all members of S_3 are in $H = <S>$

i.e., $<S> = S_3$.

Note $(12), (13) \in S \subseteq H$.

Problem 42 : *Show that every finitely generated subgroup of* $<\mathbf{Q}, +>$ *is cyclic. Hence show that* $<\mathbf{Q}, +>$ *is not finitely generated.*

Solution : Let H be a subgroup of $<\mathbf{Q}, +>$ such that H is generated by

$$\left\{\frac{m_1}{n_1}, \frac{m_2}{n_2}, \ldots\ldots, \frac{m_r}{n_r}\right\}$$

We claim H is generated by $\dfrac{1}{n_1\, n_2 \ldots\ldots n_r}$.

Since $\dfrac{m_i}{n_i} = m_i \dfrac{n_1\, n_2 \ldots\ldots n_{i-1}\, n_{i+1} \ldots n_r}{n_1\, n_2 \ldots\ldots n_{i-1}\, n_i\, n_{i+1} \ldots n_r}$ for all $i = 1, 2, \ldots\ldots, r$

each $\dfrac{m_i}{n_i}$ is a multiple of $\dfrac{1}{n_1\, n_2 \ldots\ldots n_r}$

Now if $x \in H$ be any element then

$$x = \alpha_1 \frac{m_1}{n_1} + \alpha_2 \frac{m_2}{n_2} + \ldots\ldots + \alpha_r \frac{m_r}{n_r} \qquad \alpha_i \text{ integers}$$

$$= \text{multiple of } \frac{1}{n_1\, n_2 \ldots\ldots n_r}$$

or that H is cyclic generated by $\dfrac{1}{n_1\, n_2 \ldots\ldots n_r}$

If we take $H = \mathbf{Q}$ then $<\mathbf{Q}, +>$ is cyclic which is not true (See remark on page 74).

Hence $<\mathbf{Q}, +>$ is not finitely generated.

Commutator

Let $a, b \in G$, G a group. Then $a^{-1} b^{-1} ab$ is called a *commutator* of a and b, or simply a commutator in G. Let S denote the set of all commutators in G and let G' denote the subgroup of G generated by S then G' is called *commutator* subgroup of G *or derived group* of G.

Theorem 18 : *Let G' be the commutator subgroup of a group G then*

(*i*) *G' is normal in G.*

(*ii*) $\dfrac{G}{G'}$ *is abelian and*

(*iii*) *G' is the smallest subgroup of G such that* $\dfrac{G}{G'}$ *is abelian.*

Proof : Let $g \in G,\ x \in G'$

$$x \in G' \Rightarrow x = c_1 \ldots\ldots c_n,\ c_i \text{ or } c_i^{-1} \in S$$

$$c_i \in S \Rightarrow c_i \text{ is a commutator}$$

$$\Rightarrow c_i = a_i^{-1} b_i^{-1} a_i b_i, \text{ for some } a_i, b_i \in G$$

$$c_i^{-1} \in S \Rightarrow c_i^{-1} \text{ is a commutator}$$

$$\Rightarrow c_i^{-1} = \alpha_i^{-1} \beta_i^{-1} \alpha_i \beta_i \text{ for some } \alpha_i, \beta_i \in G$$

$$\Rightarrow c_i = \beta_i^{-1} \alpha_i^{-1} \beta_i \alpha_i$$

$$\Rightarrow c_i \text{ is a commutator}$$

$\therefore$ for each i, c_i is a commutator

Now, $$g^{-1}xg = g^{-1} (c_1 \ldots\ldots c_n) g$$
$$= (g^{-1} c_1 g)(g^{-1} c_2 g) \ldots\ldots (g^{-1} c_n g)$$

but $$g^{-1} c_i g = g^{-1} (a_i^{-1} b_i^{-1} a_i b_i) g$$
$$= (g^{-1} a_i g)^{-1} (g^{-1} b_i g)(g^{-1} a_i g)^{-1} (g^{-1} b_i g)$$
$$= \alpha_i^{-1} \beta_i^{-1} \alpha_i \beta_i \quad \text{where } \alpha_i = g^{-1} a_i g$$
$$\beta_i = g^{-1} b_i g$$

$\therefore$ $g^{-1} c_i g \in S$ for all i

$\therefore$ $g^{-1} x g \in G'$

So, G' is a normal subgroup of G. Consider $G'x\, G'y$. Then

$$G'x\, G'y = G'y\, G'x$$
$$\Leftrightarrow G'xy = G'yx$$
$$\Leftrightarrow (xy)(yx)^{-1} \in G'$$
$$\Leftrightarrow xyx^{-1} y^{-1} \in G'$$

which is true as G' contains all commutators of G.

$\therefore \quad \dfrac{G}{G'}$ is abelian.

Suppose $\dfrac{G}{K}$ is abelian. We show that $G' \subseteq K$.

Since $\dfrac{G}{K}$ is abelian,

$$\begin{aligned} Kx\,Ky &= Ky\,Kx && \text{for all } x, y \in G \\ \Leftrightarrow\ Kxy &= Kyx && \text{for all } x, y \in G \\ \Leftrightarrow\ xyx^{-1}y^{-1} &\in K && \text{for all } x,\ y \in G \end{aligned}$$

$\Rightarrow K$ contains S, the set of all commutators of G.

But G' is the smallest subgroup of G containing S

$\therefore \qquad G' \subseteq K$

Cor. : *G is abelian $\Rightarrow G' = \{e\}$*

Proof : Let G be abelian,. Let $K = \{e\}$

Then $\dfrac{G}{K} = \dfrac{G}{\{e\}}$ is abelian.

$\therefore \qquad G' \subseteq K = \{e\}$, but $\{e\} = K \subseteq G'$

$\therefore \qquad G' = \{e\}$.

Conversely, let $G' = \{e\}$. Now $\dfrac{G}{G'}$ is abelian $\Rightarrow \dfrac{G}{\{e\}}$ is abelian. But $\dfrac{G}{\{e\}} \cong G$

$\Rightarrow G$ is abelian.

Problem 43 : *For $G = S_3$, prove that $G' = A_3$.*

Solution : $o(G')$ divides $o(G) = 6$

$\Rightarrow o(G') = 1, 2, 3,$ or 6

$o(G') = 1 \Rightarrow G' = \{I\} \Rightarrow G$ is abelian, a contradiction.

$o(G') = 6 = o(G) \Rightarrow G' = G$. But $\dfrac{G}{A_3}$ is abelian being of order 2

$\Rightarrow G' = G \subseteq A_3$, a contradiction.

If $o(G') = 2$, then $\dfrac{G}{A_3}$ is abelian

$\Rightarrow G' \subseteq A_3 \Rightarrow o(G') = 2$ divides $o(A_3) = 3$, a contradiction.

$\therefore \qquad o(G') = 3$

But A_3 is only subgroup of order 3 in S_3.

$\therefore \qquad G' = A_3$.

Problem 44 : *If N is a normal subgroup of G and $N \cap G' = \{e\}$, show that $N \subseteq Z(G)$.*

Solution : Let $n \in N$, $x \in G$

Then $x^{-1} n^{-1} xn \in G'$

But $x^{-1} n^{-1} xn = (x^{-1} n^{-1} x) n \in N$ as N is a normal subgroup of G.

$\therefore$ $x^{-1} n^{-1} xn \in G' \cap N = \{e\}$

$\Rightarrow x^{-1} n^{-1} xn = e$

$\Rightarrow xn = nx$ for all $x \in G$

$\Rightarrow n \in Z(G)$ for all $n \in N$

$\Rightarrow N \subseteq Z(G)$.

Exercises

1. Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$, the group of quaternions. Let $S = \{i, j\}$. Show that S generates G.
2. Let $G = S_n$, S = set of all transpositions in G. Show that S generates G.
3. Show that the set $\{1\}$ generates the group $\mathbf{Z}$ of integers under addition.
4. Prove that the alternating group $A_n (n \geq 3)$ may be generated by $(n-2)$, 3-cycles of the form (123), (124),.....,(12n).
5. If H, K are subgroups of G, show that $H \subseteq K \Rightarrow H' \subseteq K'$.
6. Let G be a simple non abelian group. Show that $G = G'$.

Chapter 4

Automorphisms and Conjugate Elements

We start by recalling that by automorphism we mean an isomorphism of a group G to itself. Also under permutation groups we noticed that set of all permutations (1-1 onto maps) forms a group. We show now that set of all automorphisms also forms a group, the two being closely related. We intend studying a few results pertaining to these groups. To begin with we take examples of automorphisms.

Example 1: Let G be a group, then the identity map $I: G \to G$, s.t., $I(x) = x$ is trivially an automorphism of G. In fact, it is sometimes called trivial automorphism of G.

Example 2: Let $\mathbf{Z}$ = group of integers under addition

then $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(n) = -n$$

is an automorphism as $f(n) = f(m) \Rightarrow -n = -m \Rightarrow n = m \Rightarrow f$ is 1-1.

Again, since for any $n \in \mathbf{Z}$, $f(-n) = n$ we find f is onto.

Now $f(n+m) = -(n+m) = -n-m = f(n) + f(m)$

shows f is a homomorphism and hence an automorphism.

Example 3 : If G be an abelian group and $f: G \to G$ be such that $f(x) = x^{-1}$ then as $f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$,

f is a homomorphism.

Again $\quad f(x) = f(y) \Rightarrow x^{-1} = y^{-1}$

$$\Rightarrow x = y \Rightarrow f \text{ is 1-1.}$$

f is clearly onto and hence an automorphism.

Example 4: If G be a non abelian group, then the above defined map $f: G \to G$ s.t., $f(x) = x^{-1}$ is not an automorphism.

Since G is non abelian, $\exists\ x, y \in G$ s.t., $xy \neq yx$

Now if $\quad f(xy) = f(x)f(y)$

then $$(xy)^{-1} = x^{-1} y^{-1}$$
$$\Rightarrow (xy)^{-1} = (yx)^{-1}$$
$$\Rightarrow xy = yx, \text{ a contradiction.}$$

Hence f is not an automorphism.

We notice then $f: G \to G$, s.t., $f(x) = x^{-1}$ is an automorphism iff G is abelian.

Example 5: Let G be a finite abelian group of order n (n = odd >1). We show G has a non trivial automorphism.

Define $$f: G \to G \text{ ,s.t.,}$$
$$f(x) = x^{-1}$$

then f is an automorphism (as seen above).

Now if $$f = I$$

Then $$f(x) = x \quad \text{for all } x \in G$$
$$\Rightarrow x^{-1} = x \quad \text{for all } x \in G$$
$$\Rightarrow x^2 = e \quad \text{for all } x \in G$$
$$\Rightarrow o(x) \mid 2 \quad \text{for all } x \in G$$
$$\Rightarrow o(x) = 1 \text{ or } 2 \quad \text{for all } x \in G$$

If $x \neq e$ then $o(x) = 2$ and as $o(x) \mid o(G)$
$$2 \mid o(G) \Rightarrow o(G) \text{ is even, not true}$$

Hence $$f \neq I$$

which proves the result.

Let G be a group and let Aut G denote the set of all automorphisms of G. One can in the routine way show (and we urge the reader to try) that Aut G forms a group under the composition of mappings. We, however, prove this result through the following theorem which gives us little more information about Aut G.

Theorem 1 : *Let G be a group. Let Aut G denote the set of all automorphisms of G and $A(G)$ be the group of all permutations of G. Then Aut G is a subgroup of $A(G)$.*

Proof : Since $I \in$ Aut G. Aut $G \neq \varphi$

Let $T \in$ Aut G. Then T is 1-1 onto from G to G.

$\therefore$ T is a permutation of G.

$\therefore$ $T \in A(G)$. So, Aut $G \subseteq A(G)$.

Let $T_1, T_2 \in$ Aut G.

Then $$(T_1 T_2)(xy)$$
$$= T_1(T_2(xy))$$
$$= T_1(T_2(x) T_2(y)) \text{ as } T_2 \text{ is a homomorphism}$$
$$= T_1(T_2(x)) T_1(T_2(y)) \text{ as } T_1 \text{ is a homomorphism}$$
$$= (T_1 T_1)(x) \cdot (T_1 T_2)(y) \text{ for all } x, y \in G$$

$\therefore$ $T_1 T_2$ is a homomorphism from G into G.

Again, $(T_1 T_2)(x) = (T_1 T_2)(y)$

$\Rightarrow T_1(T_2(x)) = (T_1(T_2(y))$

$\Rightarrow T_2(x) = T_2(y)$ as T_1 is 1-1

$\Rightarrow x = y$ as T_2 *is* 1-1

$\therefore$ $T_1 T_2$ is 1-1.

Let $x \in G$. Since $T_1 : G \to G$ is onto $\exists\, y \in G$ s.t. $T_1(y) = x$. Again as $T_2 : G \to G$ is onto, $\exists\, z \in G$ s.t. $y = T_2(z)$

$\Rightarrow T_1(T_2(z)) = x$

$\Rightarrow (T_1 T_2)(z) = x$

$\therefore$ $T_1 T_2$ is also onto.

So, $T_1 T_2 \in \text{Aut}G$.

Let $T \in \text{Aut}\, G$. Then T is 1-1 onto $\Rightarrow$ T is invertible and

$T^{-1} : G \to G$ s.t. $T^{-1}(x) = y \Leftrightarrow T(y) = x$

as $TT^{-1} = I = T^{-1} T$

T^{-1} is 1-1 as $T^{-1}(x_1) = T^{-1}(x_2)$

$\Rightarrow TT^{-1}(x_1) = TT^{-1}(x_2)$

$\Rightarrow I(x_1) = I(x_2)$

$\Rightarrow x_1 = x_2$

Let $x \in G$ then $y = T(x) \in G$

$\therefore$ $T^{-1}(y) = T^{-1}(T(x)) = (T^{-1} T)x = x$

$\therefore$ T^{-1} is onto.

Let $T^{-1}(xy) = z$ then $T(z) = xy$

Let $T^{-1}(x) = x_1$, $T^{-1}(y) = y_1$

Then $x = T(x_1)$, $y = T(y_1)$

$\Rightarrow T(z) = xy = T(x_1)\, T(y_1) = T(x_1 y_1)$

as T is a homomorphism.

$\therefore$ $z = x_1 y_1$ as T is 1-1

So $T^{-1}(xy) = z = x_1 y_1 = T^{-1}(x)\, T^{-1}(y)$ for all $x, y \in G$

$\Rightarrow T^{-1}$ is a homomorphism.

Thus $T^{-1} \in \text{Aut}\, G$

Hence, Aut G is a subgroup of $A(G)$.

(Thus Aut G forms a group).

Inner Automorphism

Let $g \in G$. Define $T_g : G \to G$ s.t.

$T_g(x) = gxg^{-1}$ for all $x \in G$

Then T_g is 1-1 as

$$T_g(x) = T_g(y)$$
$$\Rightarrow gxg^{-1} = gyg^{-1}$$
$$\Rightarrow x = y.$$

Let $x \in G$. Then $g^{-1}xg \in G$

and $\quad T_g(g^{-1}xg) = g(g^{-1}xg)\,g^{-1} = x$

$\therefore \quad T_g$ is onto

Also $\quad T_g(xy) = g(xy)g^{-1}$

$$= (gxg^{-1})\,(gyg^{-1})$$
$$= T_g(x)\;T_g(y) \text{ for all } x, y, \in G$$

Hence T_g is an automorphism of G and it is called an *inner automorphism* of G.

Theorem 2 : *The set $I(G)$ of all inner automorphisms of G is a subgroup of Aut G.*

Proof : $T_e \in I(G)$ where e = identity of G.

$\therefore \quad I(G) \neq \varphi$

Let $\quad T_{g_1}, T_{g_2} \in I(G)$

Then $\quad T_{g_1}T_{g_2}(x) = T_{g_1}(g_2 x g_2^{-1}) = g_1 g_2 x g_2^{-1} g_1^{-1}$

$$= (g_1g_2)\;x\;(g_1g_2)^{-1}$$
$$= T_{g_1g_2}(x) \quad \text{for all } x \in G.$$

$\therefore \quad T_{g_1}T_{g_2} = T_{g_1g_2} \in I(G)$

Let $\quad T_g \in I(G)$

Then $\quad T_gT_{g-1} = T_e = I$ (as $T_e(x) = exe^{-1} = x$ for all $x \in G$)

and $\quad T_{g-1}T_g = I$

$\therefore \quad T_{g-1} = (T_g)^{-1} \Rightarrow (T_g)^{-1} \in I(G)$

$\therefore$ $I(G)$ is a subgroup of Aut G.

In fact, $I(G)$ is normal in Aut G. See exercises.

A question arises, when is $T_{g_1} = T_{g_2}$?

Suppose $\quad T_{g_1} = T_{g_2}$

then $\quad T_{g_1}(x) = T_{g_2}(x)$ for all $x \in G$

$\Leftrightarrow \quad g_1 x g_1^{-1} = g_2 x g_2^{-1}$ for all $x \in G$

$\Leftrightarrow \quad g_2^{-1} g_1 x = x g_2^{-1} g_1$ for all $x \in G$

$\Leftrightarrow \quad g_2^{-1} g_1 \in Z(G)$

$\Leftrightarrow \quad g_1 Z(G) = g_2 Z(G)$

$\therefore \quad T_{g_1} = T_{g_2} \Leftrightarrow g_1 Z(G) = g_2 Z(G)$

In view of this, we have the following

Theorem 3 : $\dfrac{G}{Z(G)} \cong I(G)$.

Proof : Define $\theta : \dfrac{G}{Z(G)} \to I(G)$, s.t.,

$$\theta\,(g\,Z(G)) = T_g$$

θ is well defined as

$$g_1 Z(G) = g_2 Z(G) \Rightarrow g_2^{-1} g_1 \in Z(G)$$

$$\Rightarrow T_{g_1} = T_{g_2} \text{ (from above)}$$

$$\Rightarrow \theta\,(g_1 Z(G)) = \theta\,(g_2 Z(G))$$

θ is 1-1 as

$$\theta\,(g_1 Z(G)) = \theta\,(g_2 Z(G))$$

$$\Rightarrow T_{g_1} = T_{g_2}$$

$$\Rightarrow g_2^{-1}\, g_1 \in Z(G)$$

$$\Rightarrow g_1 Z(G) = g_2 Z(G)$$

θ is onto as

$$T_g \in I(G) \Rightarrow g \in G$$

and

$$g\,Z(G) \in \frac{G}{Z(G)} \text{ s.t., } \theta\,(g\,Z(G)) = T_g$$

Also

$$\theta\,(g_1\,Z(G)\,g_2\,Z(G)) = \theta\,(g_1\,g_2\,Z(G))$$

$$= T_{g_1 g_2}$$

$$= T_{g_1} T_{g_2}$$

$$= \theta\,(g_1\,Z(G))\,\theta\,(g_2\,Z(G))$$

$\therefore$ θ is a homomorphism and hence an isomorphism.

If G is a finite group, then $o(Z(G))$ = finite.

$$\therefore o\left(\frac{G}{Z(G)}\right) = \frac{o(G)}{o(Z(G))}. \quad \text{But } o\left(\frac{G}{Z(G)}\right) = o(I(G))$$

$$\therefore \qquad o(I(G)) = \frac{o(G)}{o(Z(G))}.$$

Note : Theorem 3 can also be proved as follows

Define $\varphi : G \to I(G)$, s.t., $\varphi(g) = T_g$ for all $g \in G$.

Then φ is onto homomorphism. Show that $\operatorname{Ker}\varphi = Z(G)$,

then $\dfrac{G}{\operatorname{Ker}\varphi} \cong I(G)$.

Problem 1 : *Let T be an automorphism of G. Show that $o(Ta) = o(a)$ for $a \in G$. Deduce that $o(bab^{-1}) = o(a)$ for all $a, b \in G$.*

Solution : We refer the reader to problem 18, page 104.

Suppose now $o(a) = n$

Then $(Ta)^n = Ta^n = T(e) = e$

If $(Ta)^m = e$ then $T(a^m) = T(e)$

$\Rightarrow a^m = e \Rightarrow m \geq n$

$\therefore$ $o(Ta) = n = o(a)$

If $o(a)$ = infinite, then $o(Ta)$ is also infinite for

$o(Ta) = n < \infty \Rightarrow (Ta)^n = e$

$\Rightarrow T(a^n) = T(e) \Rightarrow a^n = e \Rightarrow o(a)$ = finite, a contradiction.

$\therefore$ $o(Ta)$ = infinite.

Now $bab^{-1} = T_b(a)$

$\therefore$ $o(T_b(a) = o(a)$

$\Rightarrow o(bab^{-1}) = o(a)$.

Problem 2: *Let G be an infinite cyclic group. Determine Aut G.*

Solution : Let $G = \langle a \rangle$.

Let $T \in \text{Aut } G$

We show that $G = \langle Ta \rangle$

Let $x \in G$

Since T is onto, $\exists\ y \in G$ s.t., $x = T(y)$

$y \in G \Rightarrow y = a^r$ for some integer r

$\therefore$ $x = Ty = Ta^r = (Ta)^r$

$\therefore$ Ta is a generator of G.\

But G has only 2 generators, namely a, a^{-1}.

$\therefore$ $Ta = a$ *or* $Ta = a^{-1}$.

$\therefore$ T has only two choices and thus

$o(\text{Aut } G) \leq 2$

Define $T : G \to G$ s.t.,

$T(x) = x^{-1}$

then $T \in \text{Aut } G$

Also $T \neq I$ as $T = I \Rightarrow T(x) = x$ for all x

$\Rightarrow x^{-1} = x$ for all $x \Rightarrow a^{-1} = a \Rightarrow a^2 = e$

$\Rightarrow o(a)$ is finite, a contradiction

$\therefore$ $T \neq I$. Thus G has at least two automorphisms.

$\therefore$ $o(\text{Aut } G) \geq 2$

$\Rightarrow o(\text{Aut } G) = 2$.

In fact, $\text{Aut } G = \{ I,\ T \mid T(x) = x^{-1} \text{ for all } x \in G \}$

Since $o(\text{Aut } G) = 2$, Aut G is a cyclic group of order 2, and as any cyclic group of order n is isomorphic to Z_n (group under addition module n), Aut $G \cong Z_2$.

(Note : Here Aut G has very small order, while G is of very large order).

Problem 3 : *Let G be a finite cyclic group of order n. Determine Aut G.*

Solution : Let $G = <a>$, $o(G) = o(a) = n$.

Let $\quad T \in \text{Aut } G$

Then as in problem 2,

$$G = < Ta >,$$

But G has only $\varphi(n)$ generators, therefore T has only $\varphi(n)$ choices

$\therefore \quad o(\text{Aut } G) \leq \Rightarrow \varphi(n)$

Define $\quad T_m : G \to G$ s.t.,

$$T_m(x) = x^m, \qquad (m, n) = 1, 1 \leq m < n$$

Then $\quad T_m$ Aut G (Verify)

If $\quad T_r = T_s$, then $T_r(a) = T_s(a)$

$\Rightarrow a^r = a^s$. Let $r > s$

$\Rightarrow a^{r-s} = e$

$\Rightarrow o(a) \mid r-s$

$\Rightarrow n \mid r-s$

$\Rightarrow n \leq r-s < n$, a contradiction

$\therefore \quad T_r \neq T_s$ for all r, s $(r \neq s)$, $1 \leq r, s \leq m$

where $\quad (r, n) = (s, n)$

This gives at least $\varphi(n)$ automorphisms of G.

$\therefore \quad o(\text{Aut } G) \geq \varphi(n)$

$\Rightarrow o(\text{Aut } G) = \varphi(n)$

Infact, $\quad \text{Aut } G = \{T_m \mid T_m(x) = x^m, \ (m, n) = 1\}_{1 \leq m < n}$

We thus find $\quad o(\text{Aut } G) = \varphi(n)$

We show that Aut $G \cong G_n$ the group of integers multiplication modulo n.

Define $\quad \theta : \text{Aut } G \to G_n$ s.t.

$$\theta(T_m) = m, \qquad 1 \leq m < n, \ (m, n) = 1$$

Then $\quad \theta(T_r) = \theta(T_s)$

$\Rightarrow r = s$

$\Rightarrow T_r = T_s \Rightarrow \theta$ is 1-1

Given $m \in G_n$, $1 \leq m < n$, $(m, n) = 1$,

$$\exists \ T_m \in \text{Aut } G \text{ s.t. } \theta(T_m) = m$$

$\therefore \ \theta$ is onto.

To show that θ is a homomorphism, we prove $\theta(T_r T_s) = \theta(T_r) \otimes \theta(T_s)$

Now for $1 \le r, s < n$, $(r, n) = 1 = (s, n)$,

$$T_r T_s(x) = T_r(x^s) = (x^s)^r = x^{r \otimes s} = T_{r \otimes s}(x)$$

$$\Rightarrow T_r T_r = T_{r \otimes s}$$

$$\Rightarrow \theta(T_r T_s) = \theta(T_{r \otimes s})$$

$$= r \otimes s = \theta(T_r) \otimes \theta(T_s).$$

$\therefore$ θ is a homomorphism and so an isomorphism.

Hence $\quad \text{Aut}\, G \cong G_n$

This completely determines Aut G.

(**Note** : By problems 2 and 3, cyclic groups of order 3 and 4 and infinite cyclic groups have automorphism groups of order 2 which are isomorphic. But groups themselves are non- isomorphic. Also, Aut G is abelian, whenever G is cyclic).

Problem 4 : *If* $f: G \to G$ *s.t.,*

$$f(a) = a^n$$

is an automorphism, show that

$$a^{n-1} \in Z(G) \text{ for all } a \in G.$$

Solution : Consider $f(a^{-n} x a^n) = (a^{-n} x a^n)^n$

$$= a^{-n} x^n a^n$$

$$= f(a^{-1})\, f(x)\, f(a)$$

$$= f(a^{-1} x a)$$

$\therefore \quad a^{-n} x\, a^n = a^{-1}\, xa$ as $f \in \text{Aut}\, G$

$\therefore \quad xa^{n-1} = a^{n-1}\, x$ for all $x, a \in G$

Thus $a^{n-1} \in Z(G) \quad \forall\, a \in G.$

Problem 5 : *Let* $f: G \to G$ *be a homomorphism (i.e.* f *is endomorphism of* G*). Suppose* f *commutes with every inner automorphism of* G*. Show that*

(*i*) $K = \{x \in G \mid f^2(x) = f(x)\}$ *is a normal subgroup of* G.

(*ii*) G/K *is abelian.*

Solution : (*i*) $\quad f^2(e) = f(f(e)) = f(e) \Rightarrow e \in K$

$\therefore \quad K \ne \varphi$ (Where e is identity of G)

Let $x, y \in K \therefore f(x) = f^2(x)$

$$f(y) = f^2(y)$$

Then

$$f^2(xy^{-1}) = f(f(xy^{-1}))$$

$$= f(f(x) f(y^{-1})) = f(f(x) f(y)^{-1})$$

$$= f^2(x) f(fy))^{-1}$$

$$= f^2(x) f^2(y))^{-1}$$

$$= f(x) f(y^{-1})$$

$$= f(xy^{-1})$$

$\Rightarrow xy^{-1} \in K.$

Thus K is a subgroup of G.

Let $g \in G$, $x \in K$. Consider

$$\begin{aligned} f^2(gxg^{-1}) &= f(f(gxg^{-1})) \\ &= f(f T_g(x)) \\ &= f(T_g\, f(x)) \text{ as } f\, T_g = T_g\, f \\ &= f(g)\, f^2(x)\, f(g^{-1}) \\ &= f(g)\, f(x)\, f(g^{-1}) \text{ as } x \in K \Rightarrow f(x) = f^2(x) \\ &= f(gxg^{-1}) \end{aligned}$$

$\therefore$ $gxg^{-1} \in K$ for all $x \in K$, $g \in G$

$\therefore$ K is a normal subgroup of G.

(*ii*) $\dfrac{G}{K}$ is abelian

$$\begin{aligned} &\Leftrightarrow KxKy = KyKx \text{ for all } x, y \in G \\ &\Leftrightarrow Kxy = Kyx \text{ for all } x, y \in G \\ &\Leftrightarrow xyx^{-1}y^{-1} \text{ for all } x, y \in G \end{aligned}$$

Now,

$$\begin{aligned} f^2(xyx^{-1}y^{-1}) &= f(f(xyx^{-1}y^{-1})) \\ &= f(f(T_x yy^{-1})) = f(f\, T_x y))\, f(y^{-1})) \\ &= f(T_x f(y))\, f(y)^{-1}) = f(x)\, f(y)\, x^{-1})\, f(y)^{-1}) \\ &= f(x\, T_{f(y)}\, x^{-1}) = f(x)\, f\, T_{f(y)}\, x^{-1} \\ &= f(x)\, T_{f(y)}\, f(x^{-1}) = f(x)\, f(y)\, f(x^{-1})\, f(y)^{-1} \\ &= f(x)\, f(y)\, f(x^{-1})\, f(y^{-1}) \\ &= f(xyx^{-1}y^{-1}) \end{aligned}$$

$\therefore$ $xyx^{-1}\, y^{-1} \in K$

$\Rightarrow \dfrac{G}{K}$ is abelian.

Problem 6 : *For any integer $a > 1$, $n > 0$ show that* $n \mid \varphi(a^n - 1)$.

Solution : Let $G = \langle b \rangle$ s.t. $o(G) = o(b) = a^n - 1$

Define $T : G \to G$ s.t.,

$T(x) = x^a$

Since $(a \,.\, a^n - 1) = 1$, $T \in \text{Aut}\, G$

by exercise 1 (*iii*)

Also $T^2(x) = T(T(x))$

$$= T(x^a) = (x^a)^a = x^{a^2}$$

In general, $T^r(x) = x^{a^r}$

$\therefore \quad T^n(x) = x^{a^n} = x$ for all $x \in G$

(as $x^{o(G)} = e \Rightarrow x^{a^n-1} = e \Rightarrow x^{a^n} = x$)

$\therefore \quad T^n = 1$

If $\quad T^m = 1$, then $T^m(b) = b$

$\Rightarrow b^{a^m} = b \Rightarrow b^{a^m-1} = e$

$\Rightarrow o(b) \mid (a^m-1)$

$\Rightarrow a^n-1 \mid (a^m-1) \Rightarrow a^n-1 \leq (a^m-1)$

$\Rightarrow a^n \leq a^m \Rightarrow n \leq m$

$\therefore \quad o(T) = n$

Also $\quad o(\text{Aut } G) = \varphi(a^n-1)$, by problem 3

$\therefore \quad T \in \text{Aut } G \Rightarrow o(T) \mid o(\text{Aut } G)$

$\Rightarrow n \mid \varphi(a^n-1)$.

Characteristic Subgroups

A subgroup H of G is called a *characteristic subgroup* of G if

$$T(H) \subseteq H \quad \text{for all } T \in \text{Aut } G.$$

Example 6 : Let G be a cyclic group of order 4

$$G = \{e, a\ a^2, a^3\}$$

Then $\text{Aut } G = \{I, T\}$, where $T(x) = x^3$ for all $x \in G$ by problem 3.

Let $\quad H = \{e, a^2\} \leq G$

$\therefore \quad I(H) = \{I(e), I(a^2)\} = H$

$T(H) = \{T(e), T(a^2)\} = \{e, a^6 = a^2\} = H$

$\therefore$ H is a characteristic subgroup of G. (See exercise 20)

Problem 7 : *Show that a characteristic subgroup of a group G is a normal subgroup of G. Is the converse true?*

Solution : Let H be a characteristic subgroup of G. Let $g \in G$, $h \in H$.

Now $T(H) \subseteq H$, $\forall\, T \in \text{Aut } G$

In particular, $T_g(H) \subseteq H$, T_g being inner automorphism

Thus $ghg^{-1} = T_g(h) \in T_g(H) \subseteq H$

$\therefore$ H is a normal subgroup of G.

Converse, however is not true.

Let G be an abelian group of order 4.

Then $\quad G = \{e, a, b, ab \mid a^2 = e = b^2 = (ab)^2, ab = ba\}$

Let $H = \{e, a\} \leq G$

Then H is normal subgroup of G as index of H in G is 2.

Let $T: G \to G$ s.t $T(a) = b$, $T(b) = a$, $T(ab) = ab$, $T(e) = e$

Then $T \in \text{Aut}\, G$

But $T(a) = b \notin H \Rightarrow H$ is not characteristic subgroup of G.

Problem 8 : *If $o(Aut\, G) > 1$, then $o(G) > 2$.*

Solution : Suppose $o(G) \leq 2$.

If $o(G) = 1$ then G has only one automorphism, namely identity map I, contradicting $o(\text{Aut}\, G) > 1$.

If $o(G) = 2$, then $G = \{e, a \mid a^2 = e, a \neq e\}$.

Since $o(\text{Aut}\, G) > 1$, $\exists\ T \in \text{Aut}\, G$ s.t. $T \neq 1$

$\therefore\ \exists\ x \in G$ s.t., $T(x) \neq x$. But $T(e) = e$.

$\therefore\ T(a)$ must be a, contradicting that $\exists\ x$ s.t. $T(x) \neq x$.

$\therefore\quad o(G) \neq 2$

Hence $o(G) > 2$.

Problem 9 : *If G is any group in which $g^2 \neq e$ for some $g \in G$, then G has a non-trivial automorphism.*

Solution : If G is abelian, then $T: G \to G$ s.t., $T(x) = x^{-1}$ for all $x \in G$ is an automorphism of G by Example 3. If $T = I$, then $T(g) = I(g) \Rightarrow g^{-1} = g \Rightarrow g^2 = e$, a contradiction.

If G is non abelian, then some inner automorphism of G is non-trivial as

$$\begin{aligned} T_x = I \text{ for all } x \in G &\Rightarrow T_x(y) = y && \text{for all } x, y \in G \\ &\Rightarrow xyx^{-1} = y && \text{for all } x, y \in G \\ &\Rightarrow xy = yx && \text{for all } x, y \in G \\ &\Rightarrow G \text{ is abelian, a contradiction.} \end{aligned}$$

In any case, G has non trivial automorphism (see example 5 also).

The reader may go through the following problem only after acquainting himself (herself) with vector spaces.

Problem 10 : *A finite group having more than two elements has a non trivial automorphism.*

Solution : If $\exists\ g \in G$ s.t., $g^2 \neq e$, then result follows by problem 9.

Let $g^2 = e$ for all $g \in G$.

Then G is abelian. G can be regarded as a vector space V over Z_2, the field $\{0, 1\}$mod 2, by defining $g_1 + g_2 = g_1 g_2$ for all $g_1, g_2 \in G$ and $\alpha g = e$ if $\alpha = 0$ and $\alpha g = g$ if $\alpha = 1$. Then any invertible linear map $V \to V$ is an automorphism of G and conversely.

(Note : e is zero of V and $-g$ is negative of g in V). If V is finite dimensional, then $T: V \to V$ s.t. $T(\alpha_1 e_1 + \ldots + \alpha_n e_n) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \ldots \alpha_n e_n$ is 1-1 onto linear map. $(T \neq 1)$

Here $\{e_1 \ldots, e_n\}$ is a basis of V.

If G is finite, then dim V is finite $= n > 1$ and $o(V) = 2^n = o(G)$. If $o(G) = 4$ and $g^2 = e$ for $g \in G$ then

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

are all invertible linear maps from V into V. So $o(\text{Aut } G) = 6$ and Aut G is non-abelian.

Problem 11 : *If $G = S_3$, then show that Aut $G \cong S_3$.*

Solution : By exercise 7, $G \cong I(G)$

Let $S = \{(12), (13), (23)\}$

$=$ Set of all elements of order 2 in G.

Let $T \in \text{Aut } G$. By problem 1, $o(Ta) = o(a) = 2$ for all $a \in S$.

$\therefore$ T Takes elements of S into elements of S.

Thus $T : S \to S$, (i.e. T can be restricted to S. We write it as $T|S$). Also $T : G \to G$ is 1-1. So is $T|S$

Since S is finite and $T : S \to S$ is 1-1, $T|S$ is also onto.

$\therefore$ $T|S$ is a permutation of S.

$\therefore$ $T|S \in A(S)$

Define $\theta : \text{Aut } G \to A(S)$ s.t.,

$\theta(T) = T|S$

θ is well defined as $T_1 = T_2 \Rightarrow T_1, T_2$ agree on each element of G

$\Rightarrow T_1, T_2$ agree on elements of S

$\Rightarrow T_1|S = T_2|S \Rightarrow \theta(T_1) = \theta(T_2)$

Let $\theta(T_1) = \theta(T_2) \Rightarrow T_1|S = T_2|S$

$$\begin{aligned} \Rightarrow T_1[(123)] &= T_1\ [(13)(12)] \\ &= T_1(13)\ T_1(12) \\ &= T_2(13)\, T_2(12) \\ &= T_2[(13)(12)] \\ &= T_2[(123)] \end{aligned}$$

Also $T_2[(132)] = T_2[(132)]$

and $T_1(I) = T_2(I)$

$\Rightarrow T_1, T_2$ agree on all elements of G

$\Rightarrow T_1 = T_2$

$\therefore$ θ is 1-1.

Also θ is onto from Aut G to $\theta(\text{Aut } G)$

$\therefore$ $o(\text{Aut } G) = o(\theta(\text{Aut } G)$

But $\theta(\text{Aut } G) \subseteq A(S)$

$$\Rightarrow o(\theta(\text{Aut } G)) \leq o(A(S)) = 3! = 6$$

$$\Rightarrow o(\text{Aut } G) \leq 6$$

But $\quad G \cong I(G) \Rightarrow o(I(G)) = o(G) = 6$

Also $\quad I(G) \leq \text{Aut } G$

$$\Rightarrow o(I(G)) \leq o(\text{Aut } G)$$

$$\Rightarrow o(\text{Aut } G) \geq 6$$

$\therefore \quad o(\text{Aut } G) = 6 = o(I(G))$

$$\Rightarrow I(G) = \text{Aut } G$$

$$\Rightarrow \text{Aut } G \cong G = S_3.$$

Exercises

1. Show that the following maps are automorphisms

   (*i*) G = cyclic group of order 6, $f: G \to G$, s.t. $f(x) = x^5$.

   (*ii*) G = group of positive real numbers under multiplication

   $f: G \to G$, s,t $f(x) = x^2$.

   (*iii*) G = finite abelian group of order n. $f: G \to G$, *s,t.*,

   $f(x) = x^m$, $1 \leq m < n$, $(m, n) = 1$.

2. Let H be a subgroup of G. Show that $T(H)$ is subgroup of G for all $T \in \text{Aut } G$

3. If H is normal in G, show that $T(H)$ is also normal in G for all $T \in \text{Aut } G$.

4. Show that $I(G)$ is a normal subgroup of Aut G.

5. Show that $I(G) = \{I\}$ if and only if G is abelian.

6. If $\dfrac{G}{Z(G)}$ is cyclic then (show that) G is abelian (See page 98). Deduce that G is abelian if Aut G is cyclic.

7. Show that $G \cong I(G)$ if $G = S_3$.

8. Show that the commutator subgroup of a group G is a characteristic subgroup of G.

9. If $G_1 \cong G_2$, show that $I(G_1) \cong I(G_2)$ and $\text{Aut } G_1 \cong \text{Aut } G_2$.

10. If G is (non cyclic) abelian group of order 4, then shown that $\text{Aut } G \cong S_3$.

    (By solved problem 11 and this exercise it follows that two non isomorphic groups may have isomorphic automorphism groups).

11. If G is a finite group and $T \in \text{Aut}\, G$ s.t. $T(x) = x$ if and only if $x = e$ (such an automorphism is called a fixed point free automorphism). Show that $g \in G$ can be written as $x^{-1}\ T(x)$ for some $x \in G$.

12. Further in exercise 11, if $T^2 = I$, show that G is abelian and $o(G) =$ odd.

13. Let $o(G) = 2n$. Let H be a subgroup of G consisting of only those elements of G whose order is not 2. Suppose $o(H) = n$. Show that n is odd and H is abelian.

14. If H is a characteristic subgroup of G, show that $T(H) = H$ for all $T \in \text{Aut}\, G$.

15. (*i*) If H is a characteristic subgroup of K and K is normal in G, show that H is normal in G.

    (*ii*) Show if H is characteristic subgroup of K and K is characteristic subgroup of G then H is characteristic subgroup of G, i,e., the characteristic property is transitive.

16. Give an example to show that H is normal in K and K is normal in G, need not imply H is normal in G. (see problem 41. page 131).

17. If K is a characteristic subgroup of G and $T \in \text{Aut}\, G$, show that

$$T' : \frac{G}{K} \to \frac{G}{K} \quad \text{s.t. } T'(Kg) = K(Tg) \text{ for all } g \in G$$

is an automorphism. Further, show that the map $T \to T'$ is a homomorphism of $\text{Aut}\, G$ into $\text{Aut}\,(G/K)$.

18. Let G be an abelian group. Let $H = \{x \in G \mid x^n = e,\ n = \text{fixed integer}\}$. Show that H is a characteristic subgroup of G.

19. If H is a unique subgroup of order m in G, show that H is characteristic subgroup of G.

20. Show that every subgroup of a finite cyclic group is characteristic subgroup.

21. Prove that automorphism group of a finite group is finite.

22. Let G be the group of all $n \times n$ non singular matrices over a field F. Let y' denote the transpose of matrix y. Define

$$\theta : G \to G \text{ s.t.}$$
$$\theta(x) = (x^{-1})'$$

Show that $\theta \in \text{Aut}\, G$ and θ is an outer automorphism of G unless either $F = Z_2$ and $n \leq 2$ or $F = Z_3$ and $n = 1$. (An automorphism of G is called an *outer automorphism* of G if it is not an inner automorphism).

23. Let f be an endomorphism of a group G, which commutes with every inner automorphism of G. Let H be the set of all elements x of G s.t., $f^2(x) = f(x)$. Show that H is normal subgroup of G and G/H is abelian.

Conjugate Elements

Definition : Let G be a group, $a, b \in G$. Define a relation $\sim$ on G as follows :

$$a \sim b \Leftrightarrow \exists\, c \in G \text{ s.t. } a = c^{-1} bc$$

It is not difficult to see that $\sim$ is an equivalence relation on G. *If $a \sim b$ we say a is conjugate to b (or a, b are conjugates and relation $\sim$ is called conjugate relation on G).*

Let $cl(a)$ denote the equivalence class of a in G then $cl(a)$ is called *conjugate class* of a in G. Since $\sim$ is an equivalence relation on G, it divides G into disjoint equivalence classes.

$$\therefore \qquad G = \bigcup_{a \in G} cl(a), \text{ where}$$

$$\begin{aligned} cl(a) &= \{x \in G \mid x \sim a\} \\ &= \{x \in G \mid x = y^{-1}ay,\ y \in G\} \\ &= \{y^{-1} ay \mid y \in G\} \\ &= \text{set of all conjugates of } a \text{ in } G. \end{aligned}$$

Remarks : (*i*) $cl(a) = \{a\} \Leftrightarrow a \in Z(G)$

Suppose $cl(a) = \{a\}$. Then $y^{-1} ay = a$ for all $y \in G$.

$$\therefore \qquad ya = ay \text{ for all } y \in G$$

$$\therefore \qquad a \in Z(G)$$

Conversely, let $a \in Z(G)$. Let $x \in cl(a)$ be any element, then $x = y^{-1}ay$ for some $y \in G$

$$\Rightarrow x = ay^{-1}y \text{ (as } a \in Z(G)$$

$$\Rightarrow x = a \Rightarrow cl(a) = \{a\}.$$

(*ii*) G is abelian $\Leftrightarrow cl(a) = \{a\}$ for all $a \in G$

$$\begin{aligned} G \text{ is abelian} &\Leftrightarrow G = Z(G) \\ &\Leftrightarrow a \in Z(G) \text{ for all } a \in G \\ &\Leftrightarrow cl(a) = \{a\} \text{ for all } a \in G. \end{aligned}$$

We shall denote by $k(G)$ or k, the number of conjugate classes in G. It follows by remark (*ii*) that $o(G) = k \Leftrightarrow G$ is abelian.

Normalizer of an element $a \in G$ was defined to be the set $N(a) = \{x \in G \mid xa = ax \text{ for all } x \in G\}$. Also $N(a) \leq G$. It can be shown that $N(a) = G \Leftrightarrow a \in Z(G)$

$$\begin{aligned} N(a) = G &\Leftrightarrow gN(a) \text{ for all } g \in G \\ &\Leftrightarrow ga = ag \text{ for all } g \in G \\ &\Leftrightarrow a \in Z(G). \end{aligned}$$

So, by remark (*i*) it follows that

$$N(a) = G \Leftrightarrow cl(a) = \{a\}.$$

Problem 12 : *Suppose $a \in G$ has only two conjugates in G then show that $N(a)$ is a normal subgroup of G.*

Solution : Let a, $g^{-1}ag$ be two conjugates of a in G. We show

$$G = N(a) \cup N(a)\ g$$

Let $x \in G$. Consider $x^{-1}\ ax$. Then $x^{-1}ax = a$ or $g^{-1}ag$.

If $x^{-1}ax = a$, then $xa = ax \Rightarrow x \in N(a)$

If $x^{-1}ax = g^{-1}ag$, then $xg^{-1}a = axg^{-1}$

$$\Rightarrow xg^{-1} \in N(a)$$

$$\Rightarrow x \in N(a)\,g$$

$$\therefore \qquad G = N(a) \cup N(a)\,g$$

and thus index of $N(a)$ in G is 2, showing thereby that $N(a)$ is a normal subgroup of G.

Problem 13 : *Let G be a finite group and x, y be conjugate elements of G. Show that the number of distinct elements $g \in G$ s.t. $g^{-1}\ xg = y$ is $o(N(x))$.*

Solution : Let $g = g_1, g_2 \ldots\ldots, g_n$ be distinct elements of G s.t., $g_i^{-1}xg_i = y$

Let $\qquad S = \{g = g_1,\ g_2 \ldots\ldots,\ g_n\}$

We show that $S = N(x)g$

Suppose $s \in S$ then $s = g_i$ for some i, $\qquad 1 \le i \le n$

If $s = g_1 = g$, then $s = g = eg \in N(x)g$

If $s \neq g_1$, then $s = g_i\ i \neq 1$

and $\qquad g^{-1}xg = g_i^{-1}xg_i$

$$\Rightarrow g_ig^{-1}x = xg_ig^{-1}$$

$$\Rightarrow g_ig^{-1} \in N(x)$$

$$\Rightarrow g_i \in N(x)$$

$$\Rightarrow s \in N(x)g$$

or that $\qquad S \subseteq N(x)g$

Again $\qquad z \in N(x)g \Rightarrow z = hg,\ h \in N(x)$

$$\Rightarrow z^{-1}\ xz = g^{-1}\ h^{-1}\ xhg$$

$$\Rightarrow z^{-1}\ xz = g^{-1}\ xg \text{ as } xh = hx$$

$$\Rightarrow z^{-1}\ xg = y$$

$$\Rightarrow z = g_i \text{ for some } i$$

$$\Rightarrow z \in S$$

$$\Rightarrow N(x)g \subseteq S$$

Hence $\qquad S = N(x)g$

and thus $\qquad o(S) = o(N(x)g) = o(N(x))$

(**Note :** As $\qquad gg_i^{-1}\ x = xgg_i^{-1}$ for all $i = 1, \ldots, n$

$gg_i^{-1} \in N(x)$ for all i

$\Rightarrow N(x)g = N(x)g_i$ for all i)

Problem 14 : *Suppose X is a conjugate class of non trivial elements of G. Let $T \in Aut\, G$. Show that $T(X) = \{T(x) \mid x \in X\}$ is a conjugate class of elements of G.*

Solution : Let $X = cl(a),\ a \neq e$

We show that $T(X) = cl(Ta)$

Let $y \in T(X) \Rightarrow y = Tx,\ x \in X = cl(a)$

$= T(g^{-1} ag),\ g \in G$

$= T(g)^{-1}\ T(a)\ T(g) \in cl(T(a))$

$\therefore$ $T(X) \subseteq cl(Ta)$

again $z \in cl(Ta) \Rightarrow z = h^{-1}\, T(a)\ h,\ h \in G$

$= (Th_1)^{-1}\ Ta\ Th$

(as T is onto $\Rightarrow h = Th_1,\ h_1 \in G$)

$= Th_1^{-1}\ Ta\ Th$

$= T(h^{-1}\ ah)$

$\in T(cl\, a) = T(X)$

$T(X) = cl(Ta)$

Hence $T(X)$ is a conjugate class of G.

The following theorem helps us to determine the order of conjugate class of an element.

Theorem 4 : *Let G be a finite group, $a \in G$.*

Then $$o(cl(a)) = \frac{o(G)}{o(N(a))}.$$

Proof : Since $N(a) \leq G$, G can be written as union of disjoint right cosets of $N(a)$ in G.

Let $G = \bigcup_{i=1}^{t} N(a)x_i \quad [t \leq n = o(G)]$

Let $S = \{x_1^{-1}\ ax_1, \ldots\ldots, x_i^{-1}\ ax_i\}$

Suppose $x_i^{-1} ax_i = x_j^{-1} ax_j$ for $i \neq j$

Then $x_i x_j^{-1} a = ax_i x_j^{-1}$

$\Rightarrow x_i\, x_j^{-1} \in N(a)$

$\Rightarrow N(a)\, x_i = N(a)\, x_j$, a contradiction

$\therefore$ all elements in S are distinct i,e,

$o(S) = t$

Also $o(G) = t.\ o(N(a))$

$$\therefore \qquad \frac{o(G)}{o(N(a))} = t = o(S).$$

We show that $S = cl(a)$

Let $s \in S$ then $s = x_i^{-1} a x_i$, for some i, $1 \le i \le n$

$\Rightarrow s$ is conjugate of a

$\Rightarrow s \in cl(a) \Rightarrow S \subseteq cl(a)$

Again $x \in cl(a) \Rightarrow x = g^{-1}ag$, $g \in G$

$g \in G \Rightarrow g \in N(a)\ x_i$ for some i, $1 \le i \le n$

$\Rightarrow g = yx_i$, $y \in N(a)$

Thus $x = x_i^{-1} y^{-1} ayx_i$

$= x_i^{-1} ax_i$ as $ya = ay$

$\Rightarrow x \in S$

$\therefore \quad cl(a) \subseteq S \Rightarrow S = cl(a)$

or that $$o(cl(a)) = o(S) = \frac{o(G)}{o(N(a))}$$

Remark : Since $G = \bigcup_{a \in G} (cl(a))$

$$o(G) = \sum_{a \in G} o(cl(a))$$

$$= \sum_{a \in Z(G)} o(cl(a)) + \sum_{a \notin Z(G)} o(cl(a))$$

$$= Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

(By remark (*i*) earlier $o(cl(a)) = 1 \Leftrightarrow a \in Z(G)$).

$$\therefore \qquad o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$

i.e., $$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

This equation is called *class equation* of G.

Problem 15 : *Let G be a finite group and $x \in G$ then show that*

$$o(N(x)) \ge o\left(\frac{G}{G'}\right)$$

Solution : We show that $cl(x) \subseteq G'x$

Let $\quad y \in cl(x) \Rightarrow y = g^{-1}xg, \; g \in G$

$$= (g^{-1}xg)\,(x^{-1}x)$$
$$= (g^{-1}xg^{-1}x^{-1})x$$
$$\in G'x$$

$\therefore \quad cl(x) \subseteq G'(x)$

$\therefore \quad o(cl(x)) \leq o(G'x)$

$$\therefore \quad \frac{o(G)}{o(N(x))} \leq o(G'x) = o(G')$$

$$\therefore \quad \frac{o(G)}{o(G')} \leq o(N(x)).$$

Problem 16 : *Let G be a group of order p^n, p = prime, n = + ve integer. Show that $o(Z(G)) > 1$.*

Solution : If $G = Z(G)$, $o(Z(G)) = o(G) > 1$.

If $G \neq Z(G)$, then $\exists$ some $a \in G$, s.t., $a \notin Z(G)$ Then $N(a) < G$ [as $a \notin Z(G)$ $\Rightarrow$ $at \neq ta$ for some $t \in G$, i.e., $t \notin N(a)$, $t \in G$].

$\therefore \quad o(N(a)) = p^m, \; m < n$

i.e., $\quad \dfrac{o(G)}{o(N(a))} = p^{n-m}, \; n - m > 0$

i.e. $\quad o(cl(a)) = p^{n-m}$ = multiple of p

$\therefore \quad \sum_{a \notin Z(G)} o(cl(a))$ = multiple of $p = kp$, (say)

By class equation of G

$$p^n = o(G) = o(Z(G)) + \sum_{a \notin Z(G)} o(cl(a))$$
$$\Rightarrow o(Z(G)) = p^n - kp = p(p^{n-1} - k)$$
$$\Rightarrow p \mid o(Z(G)) \Rightarrow o(Z(G) > 1.$$

Remark : If follows from above problem that if G is a finite non abelian simple group then $o(G)$ is divisible by at least two distinct primes. Since G is simple, it has no non trivial normal subgroups. Now $Z(G)$ is a normal subgroup of G. $Z(G) = G \Rightarrow G$ is abelian, which is not so. Thus $Z(G) = \{e\}$, which means $o(G)$ cannot be of the type p^n, i,e, it is not divisible by only one prime.

Problem 17 : *A group of order p^2 (p = prime) is abelian.*

Solution : Suppose $o(G) = p^2$ and G is non - abelian.

$\therefore \; Z(G) \neq G$. So $\exists\, a \in G$ s.t. $a \notin Z(G)$. $\Rightarrow N(a) \neq G$

$$Z(G) < N(a)$$

By problem 16, $o(Z(G)) > 1$. $\therefore$ $o(N(a)) > 1$. Since $o(N(a)) \mid p^2 = o(G)$ and $o(N(a) \neq p^2, o(N(a)) = p$. But $1 < o(Z(G)) < o(N(a)) = p$ and $o(Z(G)) \mid p^2$, a contradiction.

$\therefore$ G is abelian.

A question arises whether group of order p^3(p = prime) is abelian? The answer is no as the Quaternion group is non abelian and has order 2^3. Infact, there exist non abelian groups of order p^3 for all primes p.

For example

$$\text{Let } G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \begin{array}{l} a, b, c \text{ are arbitrary} \\ \text{elements of a field } F \end{array} \right\}$$

Then G is a non abelian group of order p^3 if F is a field of order p.

Problem 18 : *Let G be a non abelian group of order p^3. Determine $o(Z(G))$ and k = number of conjugate classes of G.*

Solution : By problem 16, $o(Z(G)) \neq 1$. Since G is non abelian, $o(Z(G)) \neq p^3$.
$\therefore$ $o(Z(G)) = p^2$ or p.

$\exists$ $a \in G$ s.t. $a \notin Z(G)$. Since $Z(G) < N(a)$, $o(Z(G)) < o(N(a))$.

If $o(Z(G)) = p^2$, then $o(N(a)) > p^2$ and $o(N(a)) \mid p^3$

$o(N(a)) \neq p^3$ (as $a \notin Z(G) \Rightarrow N(a) \neq G$). This is not possible.

$\therefore$ $o(Z(G)) = p$. Also, in that case

$$\frac{o(G)}{o(N(a))} = \frac{p^3}{p^2} = p \text{ for all } a \notin Z(G)$$

$$\therefore \qquad o(cl(a)) = p \text{ for all } a \notin Z(G)$$

$\therefore$ every conjugate class has length (order) 1 or p. Those classes which have length 1 are $p = o(Z(G))$ in number. So each of $k-p$ remaining classes have order p.

$\therefore$ $\quad o(G) = p^3 = p + (k-p)p$

i.e., $\quad p^2 = 1 + k - p$

Hence $\quad k = p^2 + p - 1$.

Problem 19 : *Suppose G is a finite group and $k(G)$ = number of conjugate classes of G is 3. Then show that either G is a cyclic group of order 3 or is non abelian group S_3 of order 6 (upto isomorphism).*

Solution : If all three classes of G are of length one, then $o(G) = 3 \Rightarrow G$ is cyclic group of order 3. Suppose G has one class of length > 1. Then G is non abelian. Let C_1, C_2, C_3 be three classes.

Suppose $\quad o(C_3) > 1$.

If $\quad o(C_1) = o(C_2) = 1$

then $\quad o(C_3) = n - 2$

where $\quad n = o(G)$. But $o(C_3) = n - 2 \mid o(G) = n$

Also $\quad n - 2 \mid n - 2$

$\therefore$ $\quad n - 2 \mid n - (n-2) = 2$

$$\Rightarrow n-2 = 1 \text{ or } 2$$
$$\Rightarrow n = 3 \text{ or } 4$$

In either case, G is abelian.

(as $n = 3 \Rightarrow o(G) = 3 = \text{prime} \Rightarrow G$ is cyclic

$\Rightarrow G$ is abelian

$n = 4 \Rightarrow o(G) = p^2 = 2^2 \Rightarrow G$ is abelian)

We are thus left with only one option, that only one class in G is of length 1. Let $o(C_1) = 1$, $o(C_2) > 1$, $o(C_3) > 1$. $o(Z(G)) = 1$.

By class equation,

$$n = o(G) = o(C_1) + o(C_2) + o(C_3)$$
$$= 1 + o(C_2) + o(C_3)$$

But $\quad o(C_3) \mid o(G) = n, \; o(C_3) \mid o(C_3)$

$$\Rightarrow o(C_3) \mid n - o(C_3) = 1 + o(C_2)$$
$$\Rightarrow o(C_3) \le 1 + o(C_2)$$

Similarly, $\quad o(C_2) \le 1 + o(C_3)$

If $o(C_3) < 1 + o(C_2)$ and $o(C_2) < 1 + o(C_3)$

then $o(C_3) \le o(C_2)$, $o(C_2) \le o(C_3)$

$\therefore \quad o(C_2) = o(C_3)$

$\therefore \quad o(C_3) \mid 1 \quad o(C_3) \Rightarrow o(C_3) \; 1 \Rightarrow o(C_3) = 1$

a contradiction.

Thus either $\quad o(C_3) = 1 + o(C_2)$

or $\quad o(C_2) = 1 + o(C_3)$

If $\quad o(C_3) = 1 + o(C_2)$

then $\quad o(G) = 1 + o(C_2) + 1 + o(C_2)$

$$\Rightarrow o(G) - 2 \; o(C_2) = 2$$

But $\quad o(C_2) \mid o(G), \; o(C_2) \mid o(C_2) \Rightarrow o(C_2) \mid 2 \; o(C_2)$

$\therefore \quad o(C_2) \mid o(G) - 2 \; o(C_2) = 2$

$\therefore \quad o(C_2) = 2$ and $o(C_3) = 3$

or that $\quad o(G) = 6$

Similarly, if $o(C_2) = 1 + o(C_3)$, then $o(G) = 6$

$\therefore$ G is non abelian group of order 6 and so, isomorphic to S_3.

Problem 20 : *Let G be a group and $e \ne a \in G$ s.t. $o(a)$ = finite. Suppose G has only two conjugate classes. Then show that G is a finite group of order* 2.

Solution : Let $e \ne b \in G$. Since G has only 2 conjugate classes, namely $\{e\}$ and $cl(a)$. $b \in cl(a) \;\therefore\; b = g^{-1}ag$ for some $g \in G$.

$\therefore \quad o(b) = o(a)$ for all $b \ne e$ in G

Suppose $\quad o(a) = mn, \; m > 1, \; n > 1$

Then $o(a^m) = n$

Since order of all non identity elements in G is same, $o(a^m) = mn$

$\therefore \quad n = mn \Rightarrow m = 1$; a contradiction

$\therefore \quad o(a) = p =$ prime.

$\therefore \quad o(b) = p$ for all $e \neq b \in G$

Suppose $p \neq 2$

then $a^2 \neq e \Rightarrow a^2 \in cl(a)$

$\therefore \quad a^2 = g^{-1} ag$ for some $g \in G$

$$\therefore \quad (a^2)^2 = (g^{-1} ag)^2$$
$$= g^{-1} a^2 g$$
$$= g^{-1} (g^{-1} ag) g$$
$$= g^{-2} ag^2$$

$$\therefore \quad a^{2^2} = g^{-2} ag^2$$

In this way, we get $a^{2^p} = g^{-p} ag^p$

Since $o(g) = o(a) = p$

$$a^{2^p} = eae = a$$

$$\Rightarrow a^{2^p - 1} = e \Rightarrow o(a) = p \mid 2^p - 1$$

By Fermat's Theorem, $p \mid 2^p - 2$

$\therefore \quad p \mid (2^p - 1) - (2^p - 2) = 1$, a contradiction

$\therefore \quad p = 2$

$\Rightarrow o(a) = 2$. So $o(b) = 2$ for all $e \neq b \in G$

$\Rightarrow G$ is abelian.

So, every conjugate class in G is of length one. Since G has only 2 classes, order of G is 2.

(**Note :** $\exists$ infinite groups in which no non trivial element has finite order and group has only 2 conjugate classes. Therefore, it is necessary to assume that $\exists\, e \neq a \in G$ s.t. $o(a) =$ finite, in the above problem).

Problem 21 : *Prove that a group of order* 15 *is abelian. Hence, show that it is cyclic.*

Solution : Suppose G is a group of order 15. Suppose it is non abelian. Then $Z(G) \neq G$

$\therefore \; o(Z(G)) = 1, 3$ or 5 as $o(Z(G)) \mid o(G) = 15$

If $o(Z(G)) = 3$ or 5, then $o\left(\dfrac{G}{Z}\right) = 5$ or $3 =$ prime

$\Rightarrow \dfrac{G}{Z(G)}$ is cyclic $\Rightarrow G$ is abelian, a contradiction.

$\therefore \qquad o(Z(G)) = 1$

Thus there is only one conjugate class of length one. All other classes are of length 3 or 5 as order of class divides $o(G) = 15$. If all other classes are of length 3, then by class equation,

$o(G) = 15 = 1 + 3k$, which is not true.

Therefore, there exists one class C of length 5 and this is the only class of length 5 (by class equation).

Let $x \in C$. Then $C = cl(x)$ and

$$5 = o(C) = o(cl(x)) = \frac{o(G)}{o(N(x))} \Rightarrow o(N(x)) = 3$$

Since $x \neq e$ and $x \in N(x)$, $o(x) \mid o(N(x)) = 3 \Rightarrow o(x) = 3$.

Conversely, let $o(x) = 3$. Since $o(x) \mid o(N(x))$, $o(N(x)) = 3k$ where $k = 1$ or 5 as $o(N(x)) \mid o(G) = 15$.

If $k = 5$, then $o(N(x)) = 15 = o(G) \Rightarrow N(x) = G$

$\Rightarrow x \in Z(G) \Rightarrow x = e$ as $Z(G) = \{e\}$, a contradiction

$\therefore \qquad k = 1 \Rightarrow o(N(x)) = 3$

$$\Rightarrow o(cl(x)) = \frac{o(G)}{o(N(x))} = \frac{15}{3} = 5$$

$$\Rightarrow cl(x) = C$$

as C is the only class of length 5. Since $x \in cl(x)$ we find $x \in C$.

So, the number of elements of order 3 is 5, a contradiction as number of elements of order p (p = prime) is multiple of $p - 1$ (in this case, number of elements of order 3 will be a multiple of 2)

$\therefore$ G must be abelian.

Let $e \neq x \in G$. Since $o(x) \mid o(G) = 15$, $o(x) = 3$ or 5. If all non identity elements in G are of order 3, let $o(x) = 3$, $o(y) = 3$, $H = \langle x \rangle$, $K = \langle y \rangle$ then $o(H) = 3 = o(K)$. Since G is abelian, H is normal in G, K is normal in $G \Rightarrow HK \leq G \Rightarrow o(HK) \mid o(G) = 15$

But $o(HK) = \dfrac{o(H)\,o(K)}{o(H \cap K)} = \dfrac{3 \times 3}{1} = 9$ and $9 \nmid 15$

we get a contradiction

$\therefore$ $\exists$ a $\exists$ G s.t $o(a) = 5$. By the same argument as above $\exists$ $b \in G$, s.t. $o(b) = 3$. Since $ab = ba$, $o(a)$ and $o(b)$ are relatively prime.

$$\begin{aligned} o(ab) &= o(a)\ o(b) \\ &= 3 \times 5 = 15 \\ &= o(G) \end{aligned}$$

$\therefore$ G is cyclic group of order 15.

(**Note** : We shall prove the above result with the help of Sylow's Theorems in the next chapter).

Problem 22 : *Let G be a non trivial finite group. Let p be least prime dividing $o(G)$. Let $k(G) > \frac{o(G)}{p}$. Then show that $Z(G) \neq \{e\}$.*

Solution : Let $Z(G) = \{e\}$. Let $o(G) = p^{\alpha} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ where $p, p_1, p_2, \ldots p_n$ are distinct primes s.t., $p < p_1 < \ldots < p_n$, $a > 0$, $\alpha_i \geq 0$. $k(G) > \frac{o(G)}{p} = p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ and $Z(G) = \{e\} \Rightarrow \exists$ only one class of length one and at least $p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ classes of length $\geq p$ (as order of class divides $o(G)$). This gives one identity element and at least $p\,(p^{\alpha-1} p_1^{\alpha_1} \ldots p_n^{\alpha_n}) = p^{\alpha} p_1^{\alpha_1} \ldots p_n^{\alpha_n} = o(G)$ elements of G which exceed $o(G)$, a contradiction. Hence $Z(G) \neq \{e\}$.

Problem 23 : *Let N be normal in G, a finite group. Show that $k(G/N) \leq k(G) - j + i$,*

where j = number of conjugate classes in G of elements in N.

Solution : $G = \bigcup_{a \in N} cl(a) \bigcup_{a \notin N} cl(a) = N \bigcup_{a \notin N} cl(a)$

(See Exercise 8).

Let r = number of classes $cl(a)$, $a \notin N$

$\therefore \qquad k(G) = j + r$

$$\begin{aligned}
\text{Now } cl(Nx) &= \{(Ng)^{-1} Nx\,(Ng) \mid g \in G\} \\
&= \{Ng^{-1} xg \mid g \in G\} \\
&= \{Ny \mid y = g^{-1} xg,\ g \in G\} \\
&= \{Ny \mid y = g^{-1} xg,\ g \in G\} \\
&= \{Ny \mid y \in cl\,(x)\} \\
&= Ncl\,(x)
\end{aligned}$$

If $x \in N$, then $g^{-1}\ xg \in N$ for all $g \in G$

$$\begin{aligned}
&\Rightarrow cl(x) \subseteq N \\
&\Rightarrow Ncl(x) = N \\
&\Rightarrow cl(Nx) = N
\end{aligned}$$

If $x\, cl(a)$, $a \notin N$, then $cl(x) = cl(a)$

$$\begin{aligned}
&\Rightarrow Ncl(x) = Ncl(a) \\
&\Rightarrow cl(Nx) = Ncl(a)
\end{aligned}$$

But there are r such classes $cl(a)$, $a \notin N$. Therefore, there are at most $r + 1$ classes in $\frac{G}{N}$. (For, two classes $cl(a), cl(b,)\ a, b \notin N$ may give rise to same class in $\frac{G}{N}$).

$$\therefore \qquad k\left(\frac{G}{N}\right) \leq r+1 = k(G) - j + 1.$$

Definition : Let $H \leq G$. Let $g \in G$. Then $g^{-1}Hg$ is called conjugate of H in G. The set $\{g^{-1}Hg \mid g \in G\} = cl(H)$ is called *conjugate class* of H in G. As before, we can determine the order of this conjugate class.

Theorem 5 : *Let $H \leq G$, G = finite group.*

Then $$o(cl(H)) = \frac{o(G)}{o(N(H))}.$$

Proof : Since $N(H) \leq G$

$$G = \bigcup_{i=1}^{t} N(H)\, x_i$$

where $N(H)\ x_i \cap N(H)\, x_i = \varphi$ for some $i \neq j$

Let $S = \{x_1^{-1}\ Hx_1, \ldots\ldots, x_t^{-1}\ Hx_t\}$

We show that $S = cl(H)$

Let $g^{-1}\, Hg \in cl(H), \quad g \in G$

$$g \in G \Rightarrow g \in N(H)\ x_i \text{ for some } i$$

$$\Rightarrow g = yx_i,\ y \in N(H)$$

$$\Rightarrow g^{-1}Hg = x_i^{-1}\ y^{-1}Hyx_i$$

$$= x_i^{-1}\, Hx_i \text{ as } y \in N(H) \Rightarrow y^{-1}\, Hy = H$$

$$\Rightarrow g^{-1}Hg \in S$$

$\therefore$ $cl(H) \subseteq S.$

Clearly, $S \subseteq cl(H)$

$\therefore$ $S = cl(H).$

Also, $x_i^{-1}\ Hx_i = x_j^{-1}\ Hx_j$

$$\Rightarrow x_i\, x_j^{-1} H = Hx_i\, x_j^{-1}$$

$$\Rightarrow x_i\, x_j^{-1} \in N(H)$$

$$\Rightarrow N(H)\, x_i = N(H)\ x_j$$

$$\Rightarrow i = j$$

$\therefore$ $o(S) = t$

$$\Rightarrow o(cl\,(H)) = t = \frac{o(G)}{o(N(H))}.$$

Theorem (Cauchy's) 6 : *Let G be a finite group and suppose p is a prime s.t., $p \mid o(G)$, then $\exists\ x \in G$ s.t., $o(x) = p$.*

Proof : We first prove the result when G is abelian. We prove it by induction on $n = o(G)$. Result is vacuously true when $n = 1$. Assume it to be true for all groups having order less than $o(G)$. If G has non trivial subgroups, then G is cyclic group of prime order. Since $p \mid o(G)$, $o(G) = p$, $G = \langle x \rangle$ s.t. $o(x) = o(G) = p$. So result follows.

Let H be a non trivial subgroup of G i.e. $H \neq \{e\}$, G. Since G is abelian, H is normal in G. If $p \mid o(H)$, then, by induction hypothesis as $o(H) < o(G)$, H is abelian, $\exists\ x \in H$ s.t. $o(x) = p$, $x \in H \Rightarrow x \in G$. So, result is again true.

Let $p \nmid o(H)$.

Since $o(G) = o(G/H).\ o(H)$ and $p \mid o(G)$, we find

$$p \mid o\left(\frac{G}{H}\right).\ o(H)$$

But $p \nmid o(H)$, hence $p \mid o(G/H)$. Also $o\left(\frac{G}{H}\right) < o(G)$ as $H \neq \{e\}$ and G is abelian means $\frac{G}{H}$ is abelian.

So, by induction bypothesis $\frac{G}{H}$ has an element Hy of order p.

$$\begin{aligned}
\therefore \quad & (Hy)^p = H \\
\Rightarrow\ & Hy^p = H \\
\Rightarrow\ & y^p \in H \\
\Rightarrow\ & (y^p)^t = e \text{ where } i = o(H) \\
\Rightarrow\ & (y^t)^p = e \\
\Rightarrow\ & o(y^t) \mid p \\
\Rightarrow\ & o(y^t) = 1 \text{ or } p
\end{aligned}$$

If $\quad y^t = e$ (i.e. $o(y^t) = 1$) then $Hy^t = He = H$

$$\begin{aligned}
\Rightarrow\ & (Hy)^t = H \\
\Rightarrow\ & o(Hy) \mid t \\
\Rightarrow\ & p \mid t = o(H), \text{ a contradiction}
\end{aligned}$$

$\therefore \quad o(y^t) = p,\ y^t \in G$

So result is true in this case.

By induction, result is true for all abelian groups.

Let Now G be any group. We again use induction on $o(G)$. The result is vacuously true for $o(G) = 1$. Assume result is true for all groups with order less then $o(G)$. If $T < G$ and $p \mid o(T)$ then by induction hypothesis $\exists\, x \in T$ s.t. $o(x) = p$. So, result is true in this case. Assume $p \nmid o(T)$ for all $T < G$. Consider class equation of G

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

Now $\quad a \notin Z(G) \Rightarrow N(a) < G$

$$\Rightarrow p \nmid o(N(a))$$

$$\Rightarrow p \mid \frac{o(G)}{o(N(a))} \qquad \left(\text{as } o(G) = \frac{o(G)}{o(N(a))} . o(N(a))\right)$$

$$\Rightarrow \qquad p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

Since $p \mid o(G)$, we have $p \mid o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} = o(Z(G))$

But $\quad p \nmid o(T) \quad \forall\, T < G$

and thus $\quad Z(G) = G \Rightarrow G$ is abelian.

But result is true for abelian groups. Hence, by induction, result is true for all groups.

Problem 24 : *Show that an abelian group of order pq (p, q distinct primes) is cyclic*

Solution : By cauchy's theorem. $\exists\, a, b \in G$ s.t., $o(a) = p$, $o(b) = q$ Also as $(p, q) = 1$, $ab = ba$

$$o(ab) = o(a) . o(b) = pq$$

i.e., G has an element ab of order equal to $o(G)$

Hence G is cyclic.

Remark : In view of above problem, abelian groups of order 6, 10, 15 etc., are all cyclic.

Similar Permutations

Two permutations σ and $\eta \in S_n$ are called similar if they have same cycle structure when decomposed as product of disjoint cycles.

For example, $\quad \sigma = (1\ 2)\ (3\ 4\ 5) \in S_5$

and $\quad \eta = (1\ 2\ 3)\ (4\ 5) \in S_5$

are similar as σ has 1 cycle of length 2 and 1 cycle of length 3 same as η.

However $\sigma = (1\ 2)\ (3\ 4)$, $\eta = (1\ 2\ 3\ 4)$ are not similar in S_4 as σ has 2 cycles of length 2 and η has no cycle of length 2.

Note : We talk of similar permutations only when they have been represented as product of disjoint cycles.

Theorem 7 : *Two permutations $\sigma, \eta \in S_n$ are similar if and only if they are conjugate in S_n.*

Proof : Suppose $\sigma, \eta \in S_n$ are similar

Let $\sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k})$

$\eta = (a_1' \ldots\ldots a'_{n_1}) \ldots\ldots (b_1' \ldots\ldots b'_{n_k})$

where $n_1 + n_2 + \ldots\ldots + n_k = n$

Define

$$\theta = \begin{pmatrix} a_1 & \ldots\ldots & a_{n_1} & \ldots\ldots & b_1 & \ldots\ldots & b_{n_k} \\ a_1' & \ldots\ldots & a'_{n_1} & \ldots\ldots & b_1' & \ldots\ldots & b'_{n_k} \end{pmatrix}$$

Then $\theta \in S_n$

and $\theta\sigma\theta^{-1} = (\theta a_1 \ldots\ldots \theta a_{n_1}) \ldots\ldots (\theta b_1 \ldots\ldots \theta b_{n_k})$

$= (a_1' \ldots\ldots a'_{n_1}) \ldots\ldots (b_1' \ldots\ldots b'_{n_k})$

$= \eta$

$\therefore$ σ η are conjugate in S_n

Conversely, suppose σ η are conjugate in S_n.

Then $\exists\ \theta \in S_n$ *s.t.* $\theta\sigma\theta^{-1} = \eta$

Let $\sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k})$

Then $\eta = \theta\sigma\theta^{-1} = (\theta a_1 \ldots\ldots \theta a_{n_1}) \ldots\ldots (\theta b_1 \ldots\ldots \theta b_{n_k})$

So, σ, η are similar.

Partition of an Integer

Let n be a positive integer. A sequence of positive integers $n_1, n_2, \ldots\ldots\ldots, n_k$, $n_1 \leq n_2 \leq \ldots\ldots \leq n_k$, such that $n = n_1 + n_2 + \ldots\ldots + n_k$ is called a partition of n and $n_1, n_2, \ldots, n_k$ are called parts of the partition.

For example , let $n = 3$ Then $3 = 1 + 1 + 1$, $3 = 1 + 2$, $3 = 3$ are all partitions of $n = 3$. This gives 3 partitions of n. Also $n = 4$ has 5 partitions namely, $4 = 1 + 1 + 1 + 1$, $4 = 1 + 1 + 2$, $4 = 1 + 3$, $4 = 2 + 2$, $4 = 4$.

The number of partitions of n is denoted by $p(n)$. So $p(3) = 3$, $p(4) = 5$.

Theorem 8 : *The number of conjugate classes in S_n is $p(n)$.*

Proof : Let $\mathscr{A}$ = Set of all conjugate classes in S_n.

$\mathscr{B}$ = Set of all partitions on n.

Consider $cl(\sigma)$, $\sigma \in S_n$.

Let $\sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k})$ as product of disjoint cycles. Here $n_1 + \ldots\ldots + n_k = n$. We arrange cycles in such a way that $n_1 \geq \ldots\ldots \geq n_k$. This gives a partition $\{n_1, n_2, \ldots\ldots, n_k\}$ of n.

Define $f : \mathscr{A} \to \mathscr{B}$, s.t.,

$f(cl(\sigma)) = \{n_1, n_2, \ldots\ldots, n_k\}$

f is well defined as $cl(\sigma) = cl(\eta)$

$$\Rightarrow \sigma, \eta \in cl(\sigma)$$

$$\Rightarrow \sigma, \eta \text{ are conjugate in } S_n$$

$$\Rightarrow \sigma, \eta \text{ are similar in } S_n$$

$$\Rightarrow \sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k})$$

and $$\eta = (a_1' \ldots\ldots a_{n_1}') \ldots\ldots (b_1' \ldots\ldots b_{n_k}')$$

$$\Rightarrow f(cl(\sigma)) = \{n_1, \ldots, n_k\} = f(cl(\eta))$$

Suppose $cl(\sigma) \neq cl(\eta)$

Then σ and η are not conjugate and so not similar

$\Rightarrow \sigma, \eta$ have different cycle structure

$\Rightarrow$ the corresponding partitions are different.

i,e $\{n_1, n_2, \ldots\ldots\ldots, n_k\} \neq \{n'_1, n'_2, \ldots\ldots\ldots, n'_r\}$ where, of course, $n = n_1 + n_2 + \ldots\ldots + n_k = n'_1 + n'_2 + \ldots\ldots + n'_r$

$$\Rightarrow f\ (cl(\sigma) \neq f(cl(\eta)$$

$$\Rightarrow f \text{ is 1-1}$$

f is onto for, let $\{n_1, \ldots, n_k\} \in \mathscr{B}$ be a partition of n. Then $n = n_1 + \ldots\ldots + n_k$.

Define $\sigma = (a_1 \ldots\ldots a_{n_1}) \ldots\ldots (b_1 \ldots\ldots b_{n_k}) \in S_n$

Then $cl(\sigma) \in \mathscr{A}$

and $f(cl(\sigma)) = \{n_1, \ldots\ldots, n_k\}$

$\therefore f$ is both 1-1 and onto.

So, $o(\mathscr{A}) = o(\mathscr{B}) = p(n)$

$\Rightarrow$ number of conjugate classes in S_n is $p(n)$.

Problem 25 : *Let* (12) $\in S_n$. *Determine all elements in* S_n *which commute with* (12).

Solution : Let $\sigma \in S_n$ s.t. $\sigma(1) = 1$, $\sigma(2) = 2$.

Then $\sigma(12)\ \sigma^{-1} = (\sigma 1 \sigma 2) = (12)$

$$\Rightarrow \sigma(12) = (12)\ \sigma$$

The number of such $\sigma \in S_n$ is clearly $(n-2)!$ (as $\sigma(1) = 1$, $\sigma(2) = 2$, σ will take remaining $n-2$ letters among themselves and so σ will be a permutation on $n-2$ letters).

Also, $\eta = \sigma(12) \in S_n$

and $\eta(12)\ \eta^{-1} = (\eta 1\ \eta 2) = (21) = (12)$

$$\Rightarrow \eta\ (12) = (12)\ \eta$$

The number of $\eta s \in S_n$ is equal to the number of $\sigma \in S_n$ $(= (n-2)!)$

This gives $2(n-2)!$ distinct permutations in S_n commuting with (12).

Now $$o(cl(12)) = \frac{o(S_n)}{o(N(12))} = \frac{n!}{o(N(12))}$$

But $cl(12)$ is the set of those permutations in S_n which are conjugate (or similar) to (12).

$\therefore$ $o(cl(12))$ = number of cycles of length 2 in S_n.

Since (12) = (21) and the first place can be chosen in n ways, second in $n-1$ ways, we have $n(n-1)$ cycles of length 2 but each such cycle is counted twice, we get $\frac{n(n-1)}{2}$ distinct cycles of length 2.

$$\therefore \qquad o(cl(12)) = \frac{n(n-1)}{2}$$

$$\therefore \qquad o(N(12)) = \frac{2n!}{n(n-1)} = 2\ (n-2)!$$

$$\therefore \qquad N(12) = \{\sigma,\ \sigma(12) \mid \sigma(1) = 1,\ \sigma(2) = 2,\ \sigma \in S_n\}$$

= set of all permutations is S_n commuting with (12).

Problem 26 : *Find all permutations in $S_n\ (n \geq 4)$ which commute with* $\sigma = (12)(34)$.

Solution : $\sigma = (12)(34)$ can be written in 8 ways in S_n as follows

(12)(34), (21)(34), (21)(43)(12)(43)

(34)(12), (34)(21), (43)(21), (43)(12)

The 1st place in σ can be chosen in n ways, 2nd in $n-1$, 3rd in $n-2$ and 4th in $n-3$ ways. This gives $n(n-1)(n-2)(n-3)$ ways in which σ can be chosen. As σ can be written in 8 ways, the number of permutations in S_n similar to σ is equal to $\frac{n(n-1)(n-2)(n-3)}{8} = o(cl(\sigma))$

$$\therefore \qquad o(N(\sigma)) = \frac{o(G)}{o(cl(\sigma))} = \frac{8n!}{n(n-1)(n-2)(n-3)}$$

Let $\tau \in S_n$ s.t. τ fixes 1, 2, 3, 4.

Then $\tau\sigma\tau^{-1} = (\tau 1\ \tau 2)\ (\tau 3\ \tau 4) = (12)\ (34) = \sigma$

$\therefore \qquad \sigma\tau = \tau\sigma$

The number of $\tau \in S_n$ is $(n-4)!$. Clearly $\tau(12)$, $\tau(34)$, $\tau(12)\ (34)\ \tau(13)\ (24)$, $\tau(14)\ (23)\ \tau(1324)$, $\tau(1423)$

Commute with σ and the number of each such permutations

= number of $\tau \in S_n$ $(= (n-4)!)$.

So, we get $8\ (n-4)!$, permutations in S_n which commute with σ. Since $o(N(\sigma)) = 8\ (n-4)!$, these are the only permutations in S_n which commute with σ.

Problem 27 : *Find two permutations in A_5 which are similar but not conjugate in A_5.*

Solution : Let $\sigma = (12345) \in A_5$

$$\eta = (13245) \in A_5$$

Since σ η are cycles of length 5, these are similar permutations.

If σ, η are cycles of length 5, these are similar permutations.

If σ η are conjugate in A_5, then $\exists$ $\theta \in A_5$ s.t. $\theta\sigma\theta^{-1} = \eta$

$\therefore$ $(\theta 1\ \theta 2\ \theta 3\ \theta 4\ \theta 5) = (13245)$

Since (13245) can be written in 5 ways, there are 5 cases.

Case 1 : $\theta 1 = 1,\ \theta 2 = 3,\ \theta 3 = 2,\ \theta 4 = 4,\ \theta 5 = 5$

$\therefore$ $\theta = (23) \notin A_5$

Case 2 : $\theta 1 = 3,\ \theta 2 = 2,\ \theta 3 = 4,\ \theta 4 = 5,\ \theta 5 = 1$

$\therefore$ $\theta = (1345) = (15)\ (14)\ (13) \notin A_5$

Case 3 : $\theta 1 = 2,\ \theta 2 = 4,\ \theta 3 = 5,\ \theta 4 = 1,\ \theta 5 = 3$

$\therefore$ $\theta = (124)\ (35) = (14)\ (12)\ (35) \notin A_5$

Case 4 : $\theta 1 = 4,\ \theta 2 = 5,\ \theta 3 = 1,\ \theta 4 = 3,\ \theta 5 = 2$

$\therefore$ $\theta = (143)\ (25) = (13)\ (14)\ (25) \notin A_5$

Case 5 : $\theta 1 = 5,\ \theta 2 = 1,\ \theta 3 = 3,\ \theta 4 = 2,\ \theta 5 = 4$

$\therefore$ $\theta = (1542) = (12)\ (14)\ (15) \notin A_5$

So in each case we get a contradiction.

Hence σ, η are not conjugate in A_5.

Remark : Two conjugate permutations would always be similar.

Problem 28 : *Find all permutations in A_5 which commute with*

(*i*) $\sigma = (12345)$

(*ii*) $\tau = (123)$

(*iii*) $\eta = (12)\ (34)$

Solution : (*i*) By Exercise 11, σ, σ^2, σ^3, σ^4, $\sigma^5 = I$ are permutations in S_5 commuting with σ. Since $\sigma \in A_5$, all powers of σ belong to A_5.

$\therefore$ $o(N(\sigma)) = 5$ in A_5.

$$\therefore\ o(cl(\sigma)) = \frac{o(A_5)}{o(N(\sigma))} = \frac{60}{5} = 12 \text{ in } A_5$$

$\therefore$ (12345) and (13245) break up into two conjugate classes each of length 12 in A_5.

(*ii*) Let $\theta \in S_5$ s.t. θ fixes 1, 2, 3. Then either $\theta = (45)$ or $\theta = I$. By Exercise 12, $\tau\theta$, $\tau^2\theta$, θ are all permutations in S_5 commuting with τ. Thus τ, τ^2, I are the only permutations in A_5 commuting with τ.

$\therefore$ $o(N(\tau)) = 3$ in A_5

$\therefore$ $o(cl\,(\tau)) = 20$ in A_5

$\therefore$ $cl\,(\tau)$ has all cycles of length 3 in S_5.

(*iii*) By problem 27, there are 8 permutations in S_5 commuting with η. These are

I, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423). Among these I, (12)(34), (13)(24), (14)(23) $\in A_5$.

$\therefore$ these are all permutations in A_5 commuting with η.

$$o(N(\eta)) = 4 \text{ in } A_5$$

So, $$o(cl(\eta)) = 15 \text{ in } A_5 \text{ which is same as } o(cl(\eta)) \text{ in } S_5.$$

$\therefore$ Conjugate class of η remains same in A_5 and S_5.

Problem 29 : *Determine all the conjugate classes of A_5.*

Solution : By problem 28, A_5 has 5 conjugate classes. $cl(I) = \{I\}$, $cl((123))$ = {all 20 cycles of length 3},

$cl((12)(34))$ = {all 15 permutations similar to (12) (34)},

$cl((12345))$ = {12 cycles of length 5},

$cl((13245))$ = {12 cycles of length 5}.

This gives 60 elements in A_5 and so all classes in A_5.

Problem 30 : *Show that A_5 is simple.*

Solution : Let N be normal in A_5, $N \neq \{I\}$, $N \neq A_5$. By Exercise 8, N = union of some conjugate classes in A_5. Since $I \in N$, $o(N)$ can't divide $o(A_5) = 60$. Thus A_5 is simple.

Exercises

1. Let G be non abelian group. Show that for all $x \in G$, $Z(G) < N(x)$.
2. Let X be a conjugate class of elements in G and let $\overline{X} = \{x^{-1} \mid x \in X\}$. Show that $\overline{X}$ is a conjugate class of elements in G.
3. Suppose that G is finite. Prove that if $o(G)$ is odd, then $\{e\}$ is the only conjugate class X such that $X = \overline{X}$. If $o(G)$ is even, show that $\exists$ at least one conjugate class $X \neq \{e\}$ such that $X = \overline{X}$.
4. Prove that if G is a finite group with $k(G)$ even, then $o(G)$ is a even.
5. Let G be a finite group. Show that $k(G) = 2$ if and only if G is cyclic group of order 2.
6. Let G be a finite non abelian group. Show that $k(G) > o(Z(G)) + 1$.
7. Let N be normal in G. Show that either $cl(a) \cap N = \varphi$ or $cl(a) \subseteq N$ for all $a \in G$.
8. Let $N \leq G$. Show that N is normal in G if and only if $N = \bigcup_{a \in N} cl(a)$.
9. Let $o(G) = p^n$, p being a prime and $n > 0$. Let N be normal in G, $(N \neq \{e\})$. Show that $N \cap Z(G) \neq \{e\}$.

10. If G is finite non abelian group such that $\dfrac{G}{Z(G)}$ is abelian, then show that $k(G) \geq o\left(\dfrac{G}{Z(G)}\right) + o(Z(G)) - 1$.

(Hint : Use Problem 23).

11. Show that permutations in S_n commuting with $\sigma = (1\ 2 \ldots\ldots\ldots n)$ are σ, σ^2 σ^{n-1}, $\sigma^n = I$.

12. Show that permutations in S_n commuting with $\sigma = (1\ 2 \ldots\ldots r)$, $1 < r \leq n$, are τ, $\sigma\tau$, $\sigma^2\tau, \ldots, \sigma^{r-1}\tau$ where τ fixes $1, 2, \ldots, r$.

Chapter 5

Sylow Theorems and Direct Products

In this chapter we study groups of order p^n (p = prime) and three theorems due to Sylow called Sylow's theorems. The ideas developed are so useful that plenty can be known about the nature of a group by knowing only its order.

Definition : A p-group is a group in which every element has order p^r where p = prime. Here p is same for all elements and r may vary.

The group $K_4 = \{I, (12)(34), (13)(24), (14)(23)\}$ and the Quaternion group are examples of finite p-groups. Here $p = 2$. For example of an infinite p-group, see problem 15 on page 99.

S_3 is not a p-group.

Since we shall mainly be studying finite groups, the following result will be useful.

Theorem 1 : *Let G be a finite group. Then G is a p-group if and only if $o(G) = p^n$.*

Proof : Suppose G is a p-group. Let q be a prime dividing $o(G)$. By Cauchy's theorem $\exists\ x \in G$ s.t. $o(x) = q$. But $o(x) = p^r$ as G is a p-group.

$\therefore\ q = p^r \Rightarrow q = p$. So, p is the only prime dividing $o(G)$. Thus $o(G) = p^n$.

Conversely, let $o(G) = p^n$ (p = prime).

Let $x \in G$. Then $o(x) \mid o(G) = p^n \Rightarrow o(x) = p^r$.

$\therefore$ every element of G has order which is some power of p. So, G is a p-group.

Problem 1 : *In a finite p-group G, every proper subgroup is a proper subgroup of its normaliser in G. (In other words, if $o(G) = p^n$, $H \leq G$, $H \neq G$, then $\exists\ g \in G$, $g \notin H$, s.t. $gHg^{-1} = H$).*

Solution : We prove the result by induction on n. Let $n = 1$. Then $o(G) = p$. Since $H \neq G$, $o(H) = 1$.

$\therefore\ H = \{e\}$ or $gHg^{-1} = g\{e\}g^{-1} = \{e\} = H$ for all $e \neq g \in G$.

$$g \neq e \Rightarrow g \notin H.$$

Thus result is true for $n = 1$. Assume it to be true for all groups having order less than p^n. Let $o(G) = p^n$. Suppose $H = N(H)$.

Since $\quad Z(G) \subseteq N(H) = H, \; H \neq G$

$\dfrac{H}{Z(G)}$ is a proper subgroup of $\dfrac{G}{Z(G)}$.

Now $$o\left(\frac{G}{Z(G)}\right) = p^m, m < n$$

(as $o(Z(G)) > 1$ by problem 16, page 156)

For convenience, we write $Z(G) = N$, then by induction hypothesis, $\exists\, Ng \in \dfrac{G}{N}$, $Ng \notin \dfrac{H}{N}$, s.t.,

$$Ng\,\frac{H}{N}\,(Ng)^{-1} = \frac{H}{N}$$

$$\Rightarrow Ng\,Nh\,Ng^{-1} \in \frac{H}{N} \qquad \forall\, h \in H$$

$$\Rightarrow Ng\,hg^{-1} \in \frac{H}{N} \qquad \forall\, h \in H$$

$$\Rightarrow Ng\,hg^{-1} = Nh_1 \text{ for some } h_1 \in H$$

$$\Rightarrow gh\,g^{-1}\,h_1^{-1} \in N = Z(G) \subseteq H$$

$$\Rightarrow gh\,g^{-1} \in H \qquad \forall\, h \in H$$

$$\Rightarrow gH\,g^{-1} \subseteq H$$

$$\Rightarrow gH\,g^{-1} = H \text{ as } o(gHg^{-1}) = o(H)$$

Thus $g \in N(H)$ and as $Ng \notin \dfrac{H}{N}$, $g \notin H$, or that $N(H) \neq H$, a contradiction. Hence $H \subset N(H)$.

Thus result is true for n also.

By induction, result is true for all $n \geq 1$.

Problem 2 : *Let $o(G) = p^n$ (p = prime). If $H \leq G$ s.t. $o(H) = p^{n-1}$, show that H is normal in G.*

Solution : Now $H \subseteq N(H) \subseteq G$

Since $\quad o(H) = p^{n-1} \mid o(N(H)) \mid o(G) = p^n$

$o(N(H)) = p^{n-1}$ or p^n

If $\quad o(N(H)) = p^n = o(G)$,

then $\quad N(H) = G$

and so H is normal in G.

If $\quad o(N(H)) = p^{n-1}$,

then $N(H) = H$

Since $Z(G) \subseteq N(H) = H$

$$o\left(\frac{H}{Z(G)}\right) = p^{n-1-m}, \text{ where } o(Z(G)) = p^m,\ m > 0$$

and $$o\left(\frac{G}{Z(G)}\right) = p^{n-m},$$

We now prove the result by induction on n. When $n = 1$, $H = \{e\}$ and so H is normal in G. Assume result to be true for all p-groups with order less than $o(G)$. Here $\frac{G}{Z(G)}$ is a p-group s.t. $o\left(\frac{G}{Z(G)}\right) = p^{n-m}$, $n - m < n$ (as $m > 0$) and $o\left(\frac{H}{Z(G)}\right) = p^{n-m-1}$. By induction hypothesis, $\frac{H}{Z(G)}$ is normal in $\frac{G}{Z(G)} \Rightarrow H$ is normal in G. So $N(H) = G \Rightarrow H = G$, a contradiction. Thus $o(N(H)) \neq p^{n-1}$. So result is true for n also. By induction, result is true for all $n > 0$.

Remark : This problem follows by problem 1 also as

$o(H) \mid o(N(H)) \mid o(G)$ gives

$o(N(H)) = p^{n-1}$ or p^n

$o(N(H)) = p^n \Rightarrow N(H) = G \Rightarrow H$ is normal in G.

$o(N(H)) = p^{n-1}$ is not possible as $H < G$, thus $H < N(H)$ by problem 1.

Problem 3 : *Let G be a finite p-group of order p^m. Show that G has normal subgroups $G_0, G_1, \ldots G_m$ s.t.*

$$\{e\} = G_0 < G_1 < \ldots\ldots < G_{m-1} < G_m = G$$

and $o(G_i) = p^i$ for all $i = 0, 1, \ldots, m$.

Solution : We prove the result by induction on m. The result is clearly true for $m = 0, 1$. Assume it to be true for all p - groups with order less than $o(G)$.

Let $o(G) = p^m$, $m > 1$.

Let $e \neq z \in Z(G)$.

Let $o(z) = p^n$, $n > 0$.

Let $G_1 = < z^{p^{n-1}} > \leq Z(G)$

Then $o(G_1) = p$ and G_1 is normal in G.

Let $\overline{G} = \frac{G}{G_1}$.

Then $o(\overline{G}) = p^{m-1}$.

By induction hypothesis $\overline{G}$ has normal subgroups $\overline{G}_i$ ($i = 0, 1, \ldots, m-1$) s.t.,

$$\{e\} = \overline{G}_0 < \overline{G}_1 < \ldots\ldots < \overline{G}_{m-1} = \overline{G}$$

where $\quad o(\overline{G}_i) = p^i$ for all i

But $\overline{G}_i < \overline{G} \Rightarrow \overline{G}_i = \dfrac{G_{i+1}}{G_1}$ where $G_1 < G_{i+1}$.

Since $\overline{G}_i = \dfrac{G_{i+1}}{G_1}$ is normal in $\overline{G} = \dfrac{G}{G_1}$, G_{i+1} is normal in G for all i.

$\therefore \quad G_1 < G_2 < \ldots\ldots < G_m = G$

and $\quad o(G_{i+1}) = p^{i+1}$

Since $G_0 = \{e\}$, the subgroups $G_0, G_1, \ldots\ldots, G_m$ are the required subgroups. So result is true for m. By induction result is true for all $m \geq 0$.

We now prove the converse of Lagrange's Theorem for finite abelian groups.

Theorem 2 : *Let G be an abelian group of order n. Then for every divisor m of n, G has a subgroup of order m.*

Proof : We prove the result by induction on n. When $n = 1$, $G = \{e\}$ and so result is clearly true for $n = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $o(G) = n$, $m \mid n$, $m > 1$. Let p be a prime dividing m. So, $p \mid n = o(G)$. By Cauchy's Theorem $\exists\ x \in G$ s.t. $o(x) = p$. Let $K = \langle x \rangle$.

Then $o(K) = o(x) = p$. Since G is abelian, K is normal in G. Consider $\dfrac{G}{K}$, $o\left(\dfrac{G}{K}\right) = \dfrac{n}{p} < n$.

Also $\dfrac{G}{K}$ is abelian. Let $m = pm_1$.

Now $$m = pm_1 \mid o(G) = o\left(\frac{G}{K}\right) o(K)$$

$$\Rightarrow m_1 \mid o\left(\frac{G}{K}\right)$$

By induction hypothesis $\exists$ subgroup $\dfrac{H}{K}$ of $\dfrac{G}{K}$ s.t. $o\left(\dfrac{H}{K}\right) = m_1$. $H \leq G$.

$\therefore \quad o(H) = o(K)\, m_1 = pm_1 = m$

So, result is true in this case also. Hence by induction, theorem is proved.

Cor. : Converse of Lagrange's theorem holds in finite cyclic groups. (A result, we proved earlier also)

Sylow p-subgroups

Let p be a prime s.t. p^n divides order of a group G and p^{n+1} does not divide it. Then a subgroup H of G s.t. $o(H) = p^n$ is called a Sylow p-subgroup of G or p-Sylow subgroup of G.

We now discuss three theorems due to Sylow called Sylow's theorems. First theorem shows the existence of a Sylow p-subgroup of G for every prime p dividing $o(G)$ while second theorem shows that any two Sylow p-subgroups of G are conjugate. The third theorem gives the number of Sylow p-subgroups of G.

Theorem 3 (Sylow's First Theorem) : *Let p be a prime and m, a +ve integer s.t. p^m divides $o(G)$. Then $\exists$ a subgroup H of G s.t. $o(H) = p^m$.*

Proof : We prove the theorem by induction on $o(G)$. Result is vacuously true when $o(G) = 1$. Assume it to be true for all groups with order less than $o(G)$. Let $p^m \mid o(G)$. If K is a subgroup of G s.t., $K \neq G$ and $p^m \mid o(K)$, then by induction $\exists\, H \leq K$ s.t., $o(H) = p^m$. $H \leq K \Rightarrow H \leq G$. So result holds in this case. Assume p^m does not divide order of any proper subgroup of G. Consider class equation of G.

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$a \notin Z(G) \Rightarrow N(a) \neq G \Rightarrow p^m \nmid o(N(a))$$

But
$$p^m \mid o(G) \Rightarrow p^m \left| \frac{o(G)}{o(N(a))} \cdot o(N(a)) \right.$$

$$\Rightarrow p \mid \frac{o(G)}{o(N(a))} \quad \text{for all } a \notin Z(G) \text{ as } p^m \nmid o(N(a))$$

$$\Rightarrow p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$\Rightarrow p \mid o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))} = o(Z(G))$$

$$\Rightarrow \exists\ x \in Z(G) \text{ s.t. } o(x) = p$$

Let $\quad K = \langle x \rangle \subseteq Z(G) \quad \Rightarrow K$ is normal in G.

Now $o(G/K) < o(G)$ and $p^m \mid o(G) = o(G/K) \,.\, o(K)$, $p^m \nmid o(K)$ and thus $p^{m-1} \mid p^m \mid o(G/K)$. (Notice in case $m = 1$, the result follows by Cauchy's theorem).

By induction hypothesis $\exists$ a subgroup $\dfrac{H}{K}$ of $\dfrac{G}{K}$ s.t. $o\left(\dfrac{H}{K}\right) = p^{m-1}$.

$\therefore \quad o(H) = p^m,\ H/K \leq G/K \Rightarrow H \leq G$

Thus result is true in this case also.

Hence by induction the theorem follows.

Cor. : If p is a prime s.t. $p^n \mid o(G)$ and $p^{n+1} \nmid o(G)$, then a $\exists$ Sylow p-subgroup of G.

Proof : Take $m = n$ and use the above theorem.

Remark : Sometimes the statement of this corollory is taken as Sylow's first theorem. In fact another (more general) version of the theorem would be

If G is a finite group of order $n = p^k q$ $(k \geq 1)$, where p is a prime and q, a +ve integer, (p, q relatively prime) then for each i, $1 \leq i \leq k$, G has a subgroup of order p^i.

Double Cosets

Definition : Let $H, K \leq G$. Let $a, b \in G$. Define a relation '$\sim$' on G as follows:

$$a \sim b \Leftrightarrow \exists\ h \in H,\ k \in K \text{ s.t. } a = hbk$$

It can be easily shown that '$\sim$' is an equivalence relation on G. So, it divides G into disjoint union of equivalence classes. Equivalence class of $a \in G$ is given by

$$\begin{aligned} cl(a) &= \{x \in G \mid a \sim x\} \\ &= \{hak \mid h \in H,\ k \in K\} \\ &= HaK, \text{ called double coset of } H \text{ and } K \text{ in } G. \end{aligned}$$

$$G = \bigcup_a cl(a) = \bigcup_a Hak$$

Define $\quad f : HaK \to HaKa^{-1}$ s.t.,

$$f(hak) = haka^{-1} \text{ for all } h \in H,\ k \in K$$

Clearly, f is well defined as $hak = h'ak'$

$$\Rightarrow haka^{-1} = h'ak'a^{-1}$$

f is 1–1 as $\quad f(hak) = f(h'ak')$

$$\Rightarrow haka^{-1} = h'ak'\ a^{-1}$$

$$\Rightarrow hak = h'ak'$$

Let $haka^{-1} \in HaKa^{-1} \Rightarrow hak \in Hak$ and

$$f(hak) = haka^{-1}$$

$\therefore \quad f$ is both 1–1 and onto.

Thus, $\quad o(HaK) = o(HaKa^{-1})$, (if H, K are finite)

$$= \frac{o(H)\, o(aKa^{-1})}{o(H \cap aKa^{-1})} = \frac{o(H)\, o(K)}{o(H \cap aKa^{-1})}$$

If G is a finite group, then

$$o(G) = \sum_a o(HaK) = \sum_a \frac{o(H)\, o(K)}{o(H \cap aKa^{-1})}$$

We are now ready to prove Sylow's second theorem.

Theorem 4 (Sylow's Second theorem) : *Any two Sylow p-subgroups of a finite group G are conjugate in G.*

Proof : Let P, Q be Sylow p-subgroups of G. Let $o(P) = p^n = o(Q)$ where $p^{n+1} \nmid o(G)$. Suppose P and Q are not conjugate in G.

i.e., $P \neq gQg^{-1}$ for any $g \in G$

By the discussion done above

$$o(PxQ) = \frac{o(P)\,o(Q)}{o(P \cap xQx^{-1})}$$

Since, $P \cap xQx^{-1} \leq P$

$o(P \cap xQx^{-1}) = p^m, \; m \leq n$

If $m = n$, then $P \cap xQx^{-1} = P$

$\Rightarrow P \subseteq xQx^{-1}$

$\Rightarrow P = xQx^{-1}$ as $o(xQx^{-1}) = o(Q) = o(P)$

which is a contradiction.

$\therefore$ $m < n$ and thus $o\,(PxQ) = p^{2n-m}$, $m < n$ for all $x \in G$

$\Rightarrow o(PxQ) = p^{n+1}\,(p^{n-m+1})$ = multiple of p^{n+1}

Thus $o(G) = \sum_x o(PxQ)$ = multiple of p^{n+1}

$p^{n+1} \mid$ R.H.S $\Rightarrow p^{n+1} \mid o(G)$, a contradiction

$\therefore$ $P = gQg^{-1}$ for some $g \in G$.

Before we prove Sylow's third theorem, we prove

Lemma : *Let P be a Sylow p-subgroup of G. Then the number of Sylow p-subgroups of G is equal to* $\dfrac{o(G)}{o(N(P))}$.

Proof : We know that

$$o(cl\,(P)) = \frac{o(G)}{o(N(P))} \quad \text{(See theorem 5 page 162)}$$

Since $cl\,(P) = \{Q \mid Q \leq G,\; Q = gPg^{-1},\; g \in G\}$

= set of all Sylow p-subgroups of G,

the number of Sylow p-subgroups of G is $\dfrac{o(G)}{o(N(P))}$.

Theorem 5 (Sylow's Third Theorem) : *The number of Sylow p-subgroups of G is of the form $1 + kp$ where $(1 + kp) \mid o(G)$, k being a non negative integer.*

Proof : Let P be a Sylow p-subgroup of G.

Let $o(P) = p^n$. Now $G = \bigcup_x PxP$

$$= \bigcup_{x \in N(P)} PxP \cup \bigcup_{x \notin N(P)} PxP$$

$x \in N(P) \Rightarrow Px = xP \Rightarrow PPx = PxP$

$\Rightarrow Px = PxP$

$$\therefore \qquad \bigcup_{x \in N(P)} PxP = \bigcup_{x \in N(P)} Px = N(P)$$

as $P \leq N(P)$ and union of disjoint right cosets equals the set

$$x \notin N(P) \Rightarrow Px \neq xP \Rightarrow xPx^{-1} \neq P$$

$$\Rightarrow o(P \cap xPx^{-1}) = p^m, \quad m < n$$

(as in Sylow's second theorem)

$$\Rightarrow o(PxP) = p^{2n-m}, \quad m < n$$

$$\therefore \qquad o(G) = o(N(P)) + \sum_{x \notin N(P)} o(PxP)$$

$$= o(N(P)) + \sum_{x \notin N(P)} p^{2n-m}$$

$$\therefore \qquad \frac{o(G)}{o(N(P))} = 1 + \sum \frac{p^{2n-m}}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))}, \quad t = \text{integer}$$

Since L.H.S. = integer, $p^{n+1} \dfrac{t}{o(N(P))} = r =$ integer

$$\therefore \qquad p^{n+1}t = r.o(N(P))$$

Again as $\quad P \leq N(P)$

$$o(P) \mid o(N(P))$$

$$\Rightarrow p^n \mid o(N(P))$$

$$\Rightarrow o(N(P)) = p^n u$$

$$\therefore \qquad p^{n+1}t = r\ o(N(P))$$

$$\Rightarrow pt = r.u$$

$$\Rightarrow p \mid ru$$

If $p \mid u$ then $p^{n+1} \mid o(N(P)) \mid o(G) \Rightarrow p^{n+1} \mid o(G)$, a contradiction.

$\therefore\ p \mid r \Rightarrow \dfrac{r}{p} =$ integer $\Rightarrow \dfrac{t}{u} =$ integer $k = \dfrac{r}{p}$.

$$\therefore \qquad \frac{o(G)}{o(N(P))} = 1 + \frac{p^{n+1}t}{o(N(P))}$$

$$= 1 + p\frac{t}{u} = 1 + kp$$

By above lemma, $\dfrac{o(G)}{o(N(P))}$ = number of Sylow p-subgroups of G.

$\therefore$ The number of Sylow p-subgroups is of the form $1 + kp = \dfrac{o(G)}{o(N(P))}$

$\Rightarrow (1 + kp) \mid o(G)$.

This proves the theorem.

Note : If $o(G) = p^n q$, $(p, q) = 1$ then the number of Sylow p-subgroups is $1 + kp$, where $(1 + kp) \mid p^n q$

$\Rightarrow (1 + kp) \mid q$ as $(1 + kp, p^n) = 1$

Cor. : If P is the only Sylow p-subgroup of G, then P is normal in G and conversely.

Proof : By Sylow's third theorem

$$\frac{o(G)}{o(N(P))} = 1 \Rightarrow o(G) = o(N(P))$$

Since $N(P) \leq G$

$N(P) = G$

$\Rightarrow P$ is normal in G.

Conversely, if Sylow p-subgroup P is normal in G, then

$$N(P) = G \Rightarrow o(N(P)) = o(G)$$

$$\Rightarrow \frac{o(G)}{o(N(P))} = 1$$

$\Rightarrow$ The number of Sylow p-subgroups of G is 1

$\Rightarrow P$ is the only Sylow p-subgroup of G.

Lemma : *Let P be a Sylow p-subgroup of G. Let $x \in N(P)$ s.t. $o(x) = p^i$. Then $x \in P$.*

Proof : Let $o(P) = p^n$, $p^{n+1} \nmid o(G)$

Now $(Px)^{p^i} = Px^{p^i} = Pe = P$

$[P$ is normal in $N(P)$ and $x \in N(P)]$

$\Rightarrow o(Px) \mid p^i$

$\Rightarrow o(Px) = p^j, \quad j \geq o$

Let $j > 0$. $\overline{K} = < Px > \leq \dfrac{N(P)}{P}$ s.t. $o(\overline{K}) = p^j$

Since $(\overline{K}) \leq \dfrac{N(P)}{P}, \overline{K} = \dfrac{K}{P}$ where $K \leq N(P)$

$$p^j = o(\overline{K}) = \frac{o(K)}{o(P)} = \frac{o(K)}{p^n}$$

$\Rightarrow o(K) = p^{n+j}, j > 0$

But $o(K) \mid o(N(P)) \mid o(G)$

$\Rightarrow p^{n+j} \mid o(G), j > 0$, a contradiction

$\therefore j = 0$ $\quad o(Px) = p^j = 1$

$\Rightarrow Px = P \Rightarrow x \in P.$

Theorem 6 : *Every p-subgroup of a finite group G is contained in some Sylow p-subgroup of G.*

Proof : Let $H \leq G$ s.t. $o(H) = p^m$ i.e. H is a p-subgroups of G.

Let S = set of all Sylow p-subgroups of G.

Then $$o(\mathcal{S}) = 1 + kp$$

Define a relation $\sim$ on $\mathcal{S}$ as follows :

For $P_1, P_2 \in \mathcal{S}$, let $P_1 \sim P_2 \Leftrightarrow \exists\, x \in H$ s.t. $P_1 = x\, P_2 x^{-1}$. It can be shown that $\sim$ is an equivalence relation on $\mathcal{S}$. For $P \in \mathcal{S}$ equivalence class of P in $\mathcal{S}$ is given by $cl\,(P) = \{xPx^{-1} \mid x \in H\}$.

If $N_H(P) = \{x \in H \mid xP = Px\}$ then $N_H(P) \leq H$.

Thus $$o(cl(P)) = \frac{o(H)}{o(N_H(P))} = p^s,\ s \geq 0.$$ (See theorem 15 page 162)

Suppose H is not contained in any Sylow p-subgroup of G. Then $H \not\subseteq P$.

$\therefore$ $\exists$ some $x \in H$ s.t. $x \notin P$

If $xPx^{-1} = P$, then $x \in N(P)$ and $o(x) = p^i$ [as $x \in H$, $o(x) \mid o(H)$]

$\Rightarrow x \in P$ by above lemma, which is not true

Hence $$xPx^{-1} \neq P,\ x \in H$$

$\Rightarrow P, xPx^{-1}$ are distinct members of $cl(P) \Rightarrow o(cl(P)) > 1$

$\therefore\ o(cl(P)) = p^s,\ s > 0 \Rightarrow o(cl(P))$ = multiple of p

This is true for all $P \in \mathcal{S}$

Since $$\mathcal{S} = \cup\ cl\,(P)$$

$$o(\mathcal{S}) = \sum o(cl(P)) = \text{a multiple of } p$$

$\Rightarrow 1 + kp$ = a multiple of p, a contradiction.

Hence H is contained in some Sylow p-subgroup of G.

Cor. : Let G be a finite group, and P be a p-subgroup of G then P is a Sylow p-subgroup of G if and only if no p-subgroup of G properly contains P.

Proof : Suppose P is a Sylow p-subgroup of G. Let H be a p-subgroup of G. If $P \subset H$ then $o(H) > o(P) = p^n \Rightarrow o(H) = p^{n+m}$, $m > 0$.

But $$H \leq G \Rightarrow o(H) \mid o(G)$$

$$\Rightarrow p^{n+m} \mid o(G),\ \text{a contradiction as } p^{n+1} \nmid o(G)$$

$\therefore$ no p-subgroup of G contains P properly.

Conversely, since P is a p-subgroup of G, $\exists$ a Sylow p-subgroup Q of G s.t., $P \subseteq Q$. But no p-subgroup contains P properly.

$\therefore$ $$Q = P$$

$\Rightarrow P$ is a Sylow p-subgroup of G.

Remark : In a finite group G, no Sylow p-subgroup can be properly contained in a p-subgroup.

Problem 4 : *Let* $o(G) = 30$. *Show that*

(*i*) *Either Sylow* 3-*subgroup or Sylow* 5-*subgroup is normal in* G.

(*ii*) G *has a normal subgroup of order* 15.

(*iii*) *Both Sylow* 3-*subgroup and Sylow* 5-*subgroup are normal in* G.

Solution : $o(G) = 30 = 2 \times 3 \times 5$

The number of Sylow 3-subgroups is $1 + 3k$ and $(1 + 3k) \mid 10 \Rightarrow k = 0$ or 3

If $k = 0$, then sylow 3-subgroup is normal.

Let $k \neq 0$, then $k = 3$. This gives 10 Sylow 3-subgroups H_i each of order 3 and so we have 20 elements of order 3. [Notice (for $i \neq j$) $o(H_i \cap H_j) \mid o(H_i) = 3 \Rightarrow o(H_i \cap H_j) = 1$ only and so these 20 elements are different. Each H_i has one element e of order 1 and other two of order 3. $a \in H_i \Rightarrow o(a) \mid o(H_i) = 3 \Rightarrow o(a) = 1, 3$].

The number of Sylow 5-subgroups is $1 + 5k'$ and $(1 + 5k') \mid 6 \Rightarrow k' = 0$ or 1.

If $k' = 0$, then Sylow 5-subgroup is normal.

Let $k' \neq 0$. Then $k' = 1$. This gives 6 Sylow 5 subgroups each of order 5 and we get 24 elements of order 5. But we have already counted 20 elements of order 3. Thus we have more than 44 elements in G, a contradiction. So,. either $k = 0$ or $k' = 0$.

i.e., either Sylow 3-subgroup or Sylow 5-subgroup is normal in G.

Which proves (*i*).

Let H be a Sylow 3-subgroup of order 3 and K, a Sylow 5-subgroup of order 5.

By (*i*), either H is normal in G or K is normal in G.

In any case, $HK \leq G$, $o(HK) = 15$ as $o(H \cap K)$ divides $o(H) = 3$ and $o(K) = 5 \Rightarrow o(H \cap K) = 1$. Since index of HK in G is 2, HK is normal in G. This proves (*ii*).

Suppose, H is normal in G, K is not normal in G. By (*i*) G has 6 Sylow 5-subgroups and so 24 elements of order 5. But $o(HK) = 15 \Rightarrow HK$ is cyclic (*See problem* 6 *ahead*) $\Rightarrow HK$ has $\varphi(15) = 8$ elements of order 15. Thus G has $24 + 8 = 32$ elements, a contradiction.

$\therefore$ K is normal in G.

If H is not normal in G, then by (*i*), G has 10 sylow 3-subgroups and so 20 elements of order 3. From above HK has 8 elements of order 15 and K has 4 elements of order 5. This gives $20 + 8 + 4 = 32$ elements in G, a contradiction.

$\therefore$ H is normal in G. So both H and K are normal in G.

This proves (*iii*).

Problem 5 : *Let* G *be group of order* 231. *Show that* 11-*Sylow subgroup of* G *is contained in the centre of* G.

Solution : $o(G) = 231 = 3 \times 7 \times 11$.

The number of Sylow 11-subgroups of G is $1 + 11k$ and $(1 + 11k) \mid 21$. Clearly then $k = 0$.

So, Sylow 11-subgroup H of G is normal in G.

The number of Sylow 7-subgroups of G is $1 + 7k'$ and $(1 + 7k') \mid 33$. So, $k' = 0$.

Thus, Sylow 7-subgroup K of G is normal in G.

$$o(H) = 11, \; o(K) = 7$$

Now $o\left(\frac{G}{K}\right) = 33 = 3 \times 11$ and $3 \nmid (11-1)$, thus $\frac{G}{K}$ is cyclic and so $\frac{G}{K}$ is abelian. (See problem 6)

But G' is smallest subgroup of G such that G/G' is abelian (G' denotes the commutator subgroup of G).

$\therefore \; G' \subseteq K \Rightarrow o(G') = 1$ or 7. If $o(G') = 1$, then

$G' = \{e\} \Rightarrow x^{-1}y^{-1}xy = e \Rightarrow xy = yx$ for all $x, y \in G \Rightarrow G$ is abelian $\Rightarrow G = Z(G) \Rightarrow H \subseteq Z(G)$.

Let $\quad o(G') = 7 \Rightarrow G' = K$

Clearly $H \cap K = \{e\}$ as $o(H \cap K)$ divides $o(H) = 11$ and $o(K) = 7$.

Let $x \in H, \; y \in G$ Then $x^{-1}y^{-1}xy \in G' = K$. Also

$x^{-1}y^{-1}xy = x^{-1}(y^{-1}xy) \in H$ as H is normal in G.

$$\therefore \quad x^{-1}y^{-1}xy \in H \cap K = \{e\}$$

$$\Rightarrow xy = yx \text{ for all } y \in G, \; x \in H$$

$$\Rightarrow H \subseteq Z(G).$$

Problem 6 : *Let $o(G) = pq$, where p q are distinct primes, $p < q$, $p \nmid q$. Show that G is cyclic.*

Solution : The number of Sylow p-subgroups is $1 + kp$ and $(1 + kp) \mid q \Rightarrow 1 + kp = 1$ or q, $1 + kp = 1 \Rightarrow$ Sylow p-subgroup is unique $\Rightarrow$ Sylow p-subgroup H is normal in G.

$1 + kp = q \Rightarrow kp = q - 1 \Rightarrow p \mid q - 1$, a contradiction.

Thus $1 + kp \neq q$ and so Sylow p-subgroup is normal.

The number of Sylow q-subgroups is $1 + k'q$ and $(1 + k'q) \mid p \Rightarrow 1 + k'q = 1$ or p

If $1 + k'q = p$, then $k'q = p - 1 \Rightarrow q \mid p - 1 \Rightarrow q \leq p - 1 < p \Rightarrow q < p$, a contradiction.

$1 + k'q = 1 \Rightarrow$ Sylow q-subgroup K is normal in G.

$o(H) = p, o(K) = q, \; H \cap K = \{e\}$, H is normal in G, K is normal in G.

$[x \in H \cap K \Rightarrow o(x) \mid o(H), o(x) \mid o(K) \Rightarrow o(x) = 1]$

Thus $\quad hk = kh$ for all $h \in H, \; k \in K$

Let $\quad H = \langle a \rangle, K = \langle b \rangle$ (Groups of prime order are cyclic)

$$o(a) = o(H) = p, \; o(b)) = o(K) = q$$

Now $\quad ab = ba, \; (o(a), \; o(b)) = (p, \; q) = 1$

$$\therefore \quad o(ab) = o(a) \cdot o(b) = pq = o(G)$$

$$\Rightarrow G \text{ is cyclic.}$$

Problem 7 : *Let p be a prime dividing $o(G)$ and $(ab)^p = a^p b^p$ for all $a, b \in G$. Show that (i) Sylow p-subgroup P is normal in G.*

(ii) $\exists$ a normal subgroup N of G s.t.

$$P \cap N = \{e\} \text{ and } G = PN$$

(iii) G has non-trivial centre.

Solution : Let $p^n \mid o(G)$, $\quad p^{n+1} \nmid o(G)$.

Let $\qquad H = \{x \in G \mid x^{p^n} = e\}$

$H \neq \varphi$ as $e^{p^n} = e \Rightarrow e \in H$

Let $\qquad x, y \in H \Rightarrow (xy^{-1})^{p^n} = x^{p^n} (y^{-1})^{p^n} = e.e = e$

$\qquad \Rightarrow xy^{-1} \in H$

$\therefore \qquad H \leq G$

Let q be a prime dividing $o(H)$.

Then $\qquad x \in H$ s.t $o(x) = q$

But $\qquad x \in H \Rightarrow o(x) \mid p^n \Rightarrow q \mid p^n \Rightarrow q = p$

$\therefore$ H is a p-group. $o(H) = p^m$, $m \leq n$.

Let P be a Sylow p-subgroup of G.

Then $o(P) = p^n$. Let $x \in P \Rightarrow x^{p^n} = e$

$\Rightarrow x \in H \Rightarrow P \subseteq H \Rightarrow o(P) \mid o(H) \Rightarrow p^n \mid p^m \Rightarrow n \leq m \therefore m = n$

So, $\qquad o(H) = p^n = o(P)$

$\qquad \Rightarrow H = P.$

Thus H is the only Sylow p-subgroup of G and so is normal in G. This proves (*i*)

Define $\qquad \theta : G \to G$ s.t

$\qquad \theta(x) = x^{p^n}$

Then θ is a homomorphism.

$$\Rightarrow \frac{G}{\text{Ker}\,\theta} \cong ImG \text{ is normal in } G \; [\theta(G) = ImG]$$

Since $\qquad x \in \text{Ker}\,\theta \Leftrightarrow \theta(x) = e$

$\qquad \Leftrightarrow x^{p^n} = e$

$\qquad \Leftrightarrow x \in H = P$

$\qquad P = \text{Ker}\,\theta$

Let $\qquad N = ImG$ which is normal in G.

(as $\theta(x) \in N$, $g \in G \Rightarrow g^{-1}\,\theta(x) g = g^{-1}\, x^{p^n}\, g$

$\qquad = (g^{-1}xg)^{p^n} = \because (g^{-1}xg) \in N)$

Let $\quad x \in P \cap N \Rightarrow x \in P, \quad x \in N$

$$\Rightarrow x^{p^n} = e,\ x = \theta(y) = y^{p^n}$$

$$\Rightarrow y^{p^{2n}} = e \Rightarrow o(y) = p^r,\ r \leq n$$

as $p^{n+1} \nmid o(G)$

we get $\quad y^{p^r} = e,\ r \leq n$

$$\Rightarrow y^{p^n} = (y^{p^r})^{p^{n-r}} = e \Rightarrow x = e$$

$$\Rightarrow P \cap N = \{e\}$$

Also $\quad \dfrac{G}{P} \cong N \Rightarrow \dfrac{o(G)}{o(P)} = o(N)$

$$\Rightarrow o(G) = o(P) \,.\, o(N)$$

But $\quad o(PN) = o(P)\ o(N)$

$$\Rightarrow o(G) = o(PN)$$

$$\Rightarrow PN = G$$

This proves (*ii*).

Let $z \in Z(P)$, $z \neq e$. Let $g \in G$.

Since $G = PN$, $g = xy$, $x \in P$, $y \in N$

Also P is normal in G, N is normal in G, $P \cap N = \{e\}$

$$\Rightarrow x'y' = y'x' \text{ for all } x' \in P,\ y' \in N$$

Now $\quad zg = z(xy) = (zx)y$

$$= (xz)y \text{ as } z \in Z(P)$$

$$= x(zy) = x(yz) \text{ as } z \in P,\ y \in N$$

$$= (xy)z = gz \text{ for all } g \in G$$

$\therefore \quad z \in Z(G)$

$\therefore \quad Z(G) \neq \{e\}$

which proves (*iii*).

Problem 8 : *Show that Aut* $S_4 \cong S_4$.

Solution : We know $Z(S_4) = \{I\}$ and thus $S_4 \cong I(S_4)$ (See theorem 3 page 142)

Now the number of Sylow 3-subgroups in S_4 is $1 + 3k$, where $(1 + 3k) \mid 24$ $[o(S_4) = 24 = 2^3 \times 3^1]$

i.e, $k = 0, 1$ are possible values.

$k = 0$ means only one subgroup, but we have more than one Sylow 3-subgroup. In fact S_4 has the following 4 Sylow 3-subgroups

$P_1 = \{I, (123), (132)\}$, $P_2 = \{I, (124), (142)\}$

$P_3 = \{I, (234), (243)\}$, $P_4 = \{I, (134), (143)\}$

[Notice if H be a Sylow 3-subgroup of S_4 then $o(H) = 3$' Also $a \in H$ $\Rightarrow o(a) \mid o(H) = 3 \Rightarrow o(a) = 1, 3$].

Let $\mathscr{A} = \{P_1, P_2, P_3, P_4\}$

Let $T \in \text{Aut}\, G$, $G = S_4$, then $T : G \to G$ is an automorphism

$\therefore\ T(P_i) \leq G\ \forall\ i$

Also $o(T(P_i)) = o(P_i)$ (See problem 1 page 142)

$\Rightarrow o(T(P_i)) = 3$ and $T(P_i) \leq G$

$\Rightarrow T(P_i)$ is a Sylow 3-subgroup of G, $\forall\ i$

$\Rightarrow T(P_i) \in \mathscr{A}\ \forall\ i$

$\Rightarrow T$ is a map from $\mathscr{A} \to \mathscr{A}$ and is 1-1 as it is 1-1 from $G \to G$

Also then T will be onto ($\mathscr{A}$ being finite)

Define θ : Aut $G \to A(\mathscr{A})$, s.t.,

$\theta(T) = T'$ Where T' is restriction of T on $\mathscr{A}$

then by above discussion, θ is well defined.

If $\theta(T_1) = \theta(T_2)$

then $T_1' = T_2'$

$\Rightarrow T_1'(P_i) = T_2'(P_i) \qquad i = 1, 2, 3, 4$

$\Rightarrow (T_2')^{-1}\ T_1'(P_i) = P_i$

$\Rightarrow \varphi\ (P_i) = P_i\ \forall\ i$ Where $\varphi = (T_2')^{-1} T_1'$

$\Rightarrow \varphi$ is identity map on $\mathscr{A}$ and, therefore, on G.

(If $\varphi \neq I$, than φ must not fix some transposition as every element in G is product of transpositions. Suppose $\varphi(12) \neq (12)$. Also $o(\varphi(12)) = o(12) = 2$ and Klein's four group is a characteristic subgroup of S_4, $\varphi(12)$ must be a transposition So, either $\varphi(12)$ is a transposition disjoint from (12) or not. Suppose $\varphi(12) = (34)$ or $\varphi(12) = (23)$. If $\varphi(12) = (34)$, then $\varphi(P_1) \neq P_1$ and if $\varphi(12) = (23)$, than $\varphi(P_2) \neq P_2$. So, $\varphi = I$).

Thus $(T_2')^{-1}\ T_1' = I \Rightarrow T_1 = T_2 \Rightarrow \theta$ is 1–1

$o(\text{Aut}\, G) \leq o(A(\mathscr{A})) = 4! = 24$

But $o(I(G)) = o(G) = 24$

$\Rightarrow o(\text{Aut}\, G) \leq 24 = o(I(G))$

$\Rightarrow o(\text{Aut}\, G) = o(I(G))$ [as $o(I(G)) \leq o(\text{Aut}\, G)$ by def.]

$\Rightarrow I(G) = \text{Aut}\, G \Rightarrow \text{Aut}\, G \cong G$

or that Aut $S_4 \cong S_4$.

Problem 9 : *If G is a finite non abelian simple group and $H \leq G$, show that* $[G : H] \geq 5$.

Solution : Let $[G : H]$ = index of H in $G = n$.

Let $\mathscr{L}$ = set of all left cosets of H in G.

Then $o(\mathcal{L}) = n$.

Define $\theta : G \to A(\mathcal{L}) = S_n$ s.t.,

$\theta(g) = T_g$

where $T_g : \mathcal{L} \to \mathcal{L}$ s.t.,

$T_g(xH) = gxH$

It can be shown that T_g is 1-1 and so onto.

$\therefore$ $T_g \in A(\mathcal{L})$ and θ is a homomorphism.

Let $g \in \text{Ker}\,\theta \Rightarrow \theta(g) = T_g = I$

$\Rightarrow gxh = xH$ for all $x \in G$

$\Rightarrow gH = H \Rightarrow g \in H$

$\therefore$ $\text{Ker}\,\theta \subseteq H$

Since Ker θ is normal in G and G has no non trivial normal subgroup Ker $\theta = \{e\}$ or G. But Ker $\theta = G \Rightarrow H = G$ which is not true. $\therefore$ Ker $\theta = \{e\}$.

Thus, G is isomorphic to a subgroup of S_n.

Let $n = 4$, then G is a subgroup of S_4.

Since G is simple $G \neq S_4$ and $o(G)$ must be divisible by at least two primes (for if $o(G)$ is divisible by one prime only, then G has non trivial centre as normal subgroup).

$\therefore$ $o(G) = 2^2 \times 3$ or $o(G) = 2 \times 3$

If $o(G) = 2^2 \times 3$, then Sylow 3-subgroup or Sylow 2-subgroup is normal. So, $o(G) \neq 2^2 \times 3$. If $o(G) = 2 \times 3$ and G is non abelian then $G \cong S_3$

$\Rightarrow$ G has normal subgroup A_3.

In either case, we get a contradiction. Hence $n \neq 4$.

If $n = 3$, then G is a subgroup of S_3. Since G is simple, $G \neq S_3$. $\therefore$ $G < S_3 \Rightarrow o(G) = 1$, 2 or 3 which is not possible as G is non abelian.

Clearly, $n \neq 1, 2$.

$\therefore$ $n > 4$

$\therefore$ $[G : H] \geq 5$.

Problem 10 : *Show that there is no simple group of order* 144.

Proof : Let G be a group of order $144 = 2^4 \times 3^2$,and suppose G is simple.

The number of Sylow 3-subgroups of G is $1 + 3k$ and $(1 + 3k) \mid 16 \Rightarrow k = 0, 1, 5$. If $k = 0$, then Sylow 3-subgroup is unique and normal, which is not possible.

If $k = 1$, then $\exists$ 4 Sylow 3-subgroups of G and if P is any one of these then as $\dfrac{o(G)}{o(N(P))} = 4$ = number of Sylow 3-subgroups, we find $N(P)$ is a subgroup of G with index 4 which is not possible in view of problem 9 above.

If $k = 5$, then $\exists$ 16 Sylow 3-subgroups each of order 9 in G. Let H_1, H_2, be any Sylow 3-subgroups. Since $H_1 \cap H_2 \leq H_1$, $o(H_1 \cap H_2) \mid 9 \Rightarrow o(H_1 \cap H_2) = 1$, 3 or 9. If $o(H_1 \cap H_2) = 9$, then $o(H_1 \cap H_2) = o(H_1) = o(H_2)$, $\Rightarrow H_1 = H_1 \cap H_2 = H_2$,

a contradiction. If $o(H_1 \cap H_2) = 3$, then $H_1 \cap H_2$ is normal in H_1 and H_2. Since $N(H_1 \cap H_2)$ is the largest subgroup of G in which $H_1 \cap H_2$ is normal.

$$H_1 \subseteq N(H_1 \cap H_2), \quad H_2 \subseteq N(H_1 \cap H_2)$$

$$\Rightarrow \quad H_1 H_2 \subseteq N(H_1 \cap H_2) \subseteq G$$

Again as $$o(H_1 H_2) = \frac{o(H_1)\, o(H_2)}{o(H_1 \cap H_2)} = 27,$$

$o(N(H_1 \cap H_2)) \geq 27$ and divides $o(G) = 144$

$\therefore \quad o(N(H_1 \cap H_2)) = 36, 48, 72$ or 144

But then $[G : N(H_1 \cap H_2)] = 4, 3, 2$ or 1 which is not possible by prob. 9.

$\therefore \quad o(H_1 \cap H_2) = 1$

i.e. any two Sylow 3-subgroups of G intersect trivially. This gives 128 elements of order 3^i ($i = 1$ or 2). Since Sylow 2-subgroup is of order 16 and not normal, there are at least 16 elements of order 2^i ($i = 1, 2, 3$ or 4) and one identity element. So, we get 145 elements in G, a contradiction.

Showing that G is a simple group.

Problem 11 : *Suppose that G is a finite group and p is the smallest prime divisor of $o(G)$. Show that a subgroup H of index p in G is normal in G.*

Solution : Let S = set of all left cosets of H in G.

Then $\quad o(S) = p$

Define $\quad \theta : G \to A(S)$ s.t.,

$\theta(g) = T_g$

where $\quad T_g : S \to S$

$Tg(xH) = gxH$

Then θ is a homorphism s.t. Ker $\theta \subseteq H$.

Let Ker $\theta = K$ then $K \subseteq H$ and K is normal in G.

$\frac{G}{K}$ is isomorphic to a subgroup of $A(S) = S_p$ (Using Fundamental theorem)

$\therefore o\left(\frac{G}{K}\right)$ divides $p!$.

If $m \mid o\left(\frac{G}{K}\right)$ then $m \mid o(G)$ [as $o(G) = o(K)\ [G : K]$].

Since p is the smallest prime dividing $o(G)$, $m = 1$ or p.

$\therefore \ o\left(\frac{G}{K}\right)$ is divisible by 1 or p *only.*

$$\Rightarrow \ o\left(\frac{G}{K}\right) = 1 \text{ or } p$$

But $$o(G/K) = [G:K] = [G:H]\ [H:K]$$
$$= p\,[H:K]$$
$$\geq p$$

$\therefore$ $$o\left(\frac{G}{K}\right) = p \Rightarrow [H:K] = 1$$
$$\Rightarrow H = K$$
$$\Rightarrow H = \text{Ker}\,\theta \text{ is normal in } G.$$

Remark : The result that a subgroup of index 2 is normal now follows from this problem also.

Problem 12 : *Let G be a finite group. Let H be normal in G. If p be a prime dividing $o(G)$ s.t. $([G:H]), p) = 1$, show that H contains every Sylow p-subgroup of G.*

Solution : Let $[G : H] = m$

$\therefore$ $(m, p) = 1 \Rightarrow p \nmid m \Rightarrow p^i \nmid m,\ i > 0$

Let $p^n \mid o(G),\ p^{n+1} \nmid o(G)$

Then $$o(G) = \frac{o(G)}{o(H)} \cdot o(H)$$
$$= [G:H]\ o(H)$$
$$= m \cdot o(H)$$

Since $p^n \mid o(G), p^n \mid m \Rightarrow p^n \mid o(H)$

$\therefore$ By Sylow's first theorem $\exists\, K \leq H$ s.t. $o(K) = p^n$.

$\therefore$ K is Sylow p-subgroup of G.

Let P be any Sylow p-subgroup of G

Then $P = gKg^{-1},\ g \in G$

$\therefore$ $K = g^{-1}Pg$. But $K \subseteq H$

$\therefore$ $g^{-1}Pg \subseteq H$

$\Rightarrow P \subseteq gHg^{-1} = H$ as H is normal in G.

Hence H contains all Sylow p-subgroups of G.

Problem 13 : *Let G be a finite group and $H \leq G$. Suppose p is a prime dividing $o(G)$. Let P be a Sylow p-subgroup of H contained in some Sylow p-subgroup S of G. Show that $P = S \cap H$.*

Solution : Since $P \subseteq S,\ P \subseteq H$

$P \subseteq S \cap H$

Also $S \cap H \leq S \Rightarrow S \cap H$ is a p-subgroup.

Since $S \cap H \leq H$, $S \cap H$ is a p-subgroup of H.

$\therefore$ $P \subseteq S \cap H \subseteq H$

As P is Sylow p-subgroup of H, there is no p-subgroup of H properly containing P.

$\therefore$ $P = S \cap H.$

Problem 14 : *If in above problem, Q is another Sylow p-subgroup of H s.t. $Q \subseteq T$ where T = Sylow p-subgroup of G, then show that $S \neq T$ if $P \neq Q$.*

Solution : By above problem

$$P = S \cap H, \quad Q = T \cap H$$

If $S = T$, then $P = Q$ and the result follows.

Problem 15 : *If G is a finite group and p is a prime dividing $o(H)$ where $H \leq G$, then show that the number of Sylow p-subgroups of H is less than or equal to the number of Sylow p-subgroups of G.*

Solution : If $P_1, \ldots\ldots, P_r$ are Sylow p-subgroups of H, then $\exists$ Sylow p-subgroups $S_1, \ldots\ldots, S_r$ of G s.t. $P_1 \subseteq S_1, \ldots\ldots, P_r \subseteq S_r$. By above problem since $P_1, \ldots\ldots, P_r$ are distinct, so are $S_1, \ldots S_r$.

$\therefore$ The number of Sylow p-subgroups of $G \geq r$ = the number of Sylow p-subgroups of H.

Problem 16 : *Let p be a prime dividing $o(G)$. Show that*

(*i*) *If K is normal in G and P is a Sylow p-subgroup of G, then $P \cap K$ is a Sylow p-subgroup of G.*

(*ii*) $\dfrac{PK}{K}$ *is a Sylow p-subgroup of* $\dfrac{G}{K}$

(*iii*) *Every Sylow p-subgroup of* $\dfrac{G}{K}$ *is of the form* $\dfrac{PK}{K}$ *where P is a Sylow p-subgroup of G.*

Solution : (*i*) Suppose $P \cap K$ is not a Sylow p-subgroup of K. Then $\exists$ Sylow p-subgroup Q of K s.t., $P \cap K \subset Q \subseteq R$ where R = Sylow p-subgroup of G.

Since P and R are Sylow p-subgroups of G,

$$P = xRx^{-1} \text{ for some } x \in G$$

$$\begin{aligned} xQx^{-1} &\subseteq x(K \cap R)x^{-1} \\ &\subseteq (xKx^{-1}) \cap (xRx^{-1}) \\ &= K \cap P \text{ as } K \text{ is normal in } G \\ &\subset Q \end{aligned}$$

But $o(xQx^{-1}) = o(Q) \Rightarrow xQx^{-1} = Q$, a contradiction.

$\therefore$ $P \cap K$ is a Sylow p-subgroup of K.

(*ii*) Let $p^m \mid o(K)$, $p^{m+1} \nmid o(K)$

Then $o(P \cap K) = p^m$ by (*i*)

$$\text{But } o\left(\frac{PK}{K}\right) = \frac{o(P)\,o(K)}{o(P \cap K)\,o(K)} = \frac{o(P)}{o(P \cap K)} = \frac{p^n}{p^m} = p^{n-m}$$

$$\text{Now } p^n \mid o(G),\ p^m \mid o(K) \quad \Rightarrow p^{n-m} \mid o\left(\frac{G}{K}\right)$$

Also $p^{n-m+1} \nmid \left(\frac{G}{K}\right)$

$\therefore \frac{PK}{K}$ is a Sylow p-subgroup of $\frac{G}{K}$.

(*iii*) Let $\frac{H}{K}$ be a Sylow p-subgroup of $\frac{G}{K}$

Let $p^n \mid o(G),\ p^{n+1} \nmid o(G)$

$p^m \mid o(K),\ p^{m+1} \nmid o(K)$

Let $o(K) = p^m v,\ (p,v) = 1$

$o(G) = p^n u,\ (p,u) = 1$

$\therefore p^{n-m} \mid o(G/K),\ p^{n-m+1} \nmid o\left(\frac{G}{K}\right)$

$\Rightarrow$ order of Sylow p-subgroup of $\frac{G}{K}$ is p^{n-m}

$\Rightarrow o\left(\frac{H}{K}\right) = p^{n-m}$

$\Rightarrow o(H) = o(K)\, p^{n-m} = p^n v,\ (p,v) = 1$

Let P be a Sylow p-subgroup of H then P is also a Sylow p-subgroup of G.

Clearly, $PK \subseteq H$ as $P \subseteq H,\ K \subseteq H$

and $o(PK) = \frac{o(P)\, o(K)}{o(P \cap K)} = \frac{p^n p^m v}{p^m}$

(as by (*i*) $P \cap K$ is Sylow p-subgroup of K)

$\therefore o(PK) = p^n v,\ (p,v) = 1$

$= o(H)$

$\therefore H = PK$

$\Rightarrow \frac{H}{K} = \frac{PK}{K}$ where P = Sylow p-subgroup of G

This proves (*iii*).

Problem 17 : *Let G be a group of order pqr, $p < q < r$ being primes. Prove that some Sylow subgroup of G is normal. Hence, show that G is not simple.*

Solution : Suppose that no Sylow subgroup of G is normal.

Then the number of Sylow p-subgroups of G is $1 + kp$ and $(1 + kp) \mid qr$ $\Rightarrow 1 + kp = q,\ r$ or $qr\ (\geq q)$

The number of Sylow q-subgroups of G is $(1 + k'q) \mid pr \Rightarrow 1 + k'q = p,\ r$ or pr.

If $1 + k'q = p$, then $q \mid p - 1 \Rightarrow q < p$, a contradiction.

$\therefore$ The number of Sylow q-subgroups of G is r or pr $(\geq r)$

Also the number of Sylow r-subgroups of G is $(1+k''r) \mid pq \Rightarrow 1+k''r = p, q$ or pq.

If $1+k''r = p$ or q then $r \mid (p-1)$ or $r \mid (q-1)$ $\Rightarrow r < p$ or $r < q$, a contradiction.

$\therefore$ The number of Sylow r-subgroups of G is pq.

Sylow p-subgroups give at least $q\,(p-1)$ elements of order p and Sylow q-subgroups give at least $r(q-1)$ elements of order q and Sylow r-subgroups give $pq\,(r-1)$ elements of order r .

$$\therefore \qquad o(G) = pqr \geq q\,(p-1) + r\,(q-1) + pq\,(r-1) + 1$$

$$\therefore \qquad 0 \geq rq - q - r + 1 = (q-1)\,(r-1)$$

$$\therefore \qquad (q-1)\,(r-1) \leq 0, \text{ a contradiction.}$$

Thus, some Sylow subgroup of G is normal.

Hence G is not a simple group.

Problem 18 : *Let G be a group of order pqr, $p < q < r$ being primes. Prove*

(*i*) *Sylow r-subgroup is normal in G.*

(*ii*) *G has a normal subgroup of order qr.*

(*iii*) *If $q \nmid r-1$ then Sylow q-subgroup is normal in G.*

Solution : (*i*) Suppose that Sylow r-subgroup is not normal in G. Then the number of Sylow r-subgroups is pq (See previous problem). Denote these by $H_1, \ldots\ldots, H_{pq}$. $o(H_i) = r$ for all i. By previous problem, either Sylow p-subgroup or Sylow q-subgroup is normal in G. Let Sylow q-subgroup H be normal in G. Then $HH_1, \ldots\ldots, HH_{pq}$ are subgroups of order qr.

Suppose $HH_i = HH_j$. Then $H_i, H_j \subseteq HH_i = HH_j$

$$\Rightarrow H_iH_j \subseteq HH_i \Rightarrow o(H_iH_j) \leq o(HH_i)$$

$$\Rightarrow r^2 \leq qr$$

$$\Rightarrow r \leq q, \text{ a contradiction}$$

$\therefore$ $HH_1, \ldots\ldots, HH_{pq}$ are distinct subgroups.

Let $\qquad K_i = HH_i$

Then $\qquad K_1 \cap K_2 \leq K_1$.

$$\Rightarrow o(K_1 \cap K_2) = 1,\ q,\ r \text{ or } qr$$

If $o(K_1 \cap K_2) = 1$, then $o(K_1 K_2) = q^2r^2 > pqr$, a contradiction.

If $o(K_1 \cap K_2) = q$, then $o(K_1 K_2) = qr^2 > pqr$, a contradiction.

If $o(K_1 \cap K_2) = r$, then $o(K_1 K_2) = q^2r > pqr$, a contradiction.

If $o(K_1 \cap K_2) = qr = o(K_1)$, then $K_1 = K_1 \cap K_2$.

Also $K_2 = K_1 \cap K_2 \Rightarrow K_1 = K_2$,a contraction.

Thus Sylow q-subgroup is not normal. If Sylow p-subgroup is normal, then $\exists$ $p-1$ elements of order p.

Sylow r-subgroups give $pq(r-1)$ elements of order r.

The number of Sylow q-subgroups is $1 + kq$ and $(1 + kq) \mid pr \Rightarrow 1 + kq = p, r$ or pr.

If $1 + kq = p$, then $q \mid (p - 1) \Rightarrow q < p$, a contradiction.

$\therefore$ $1 + kq = r$ or $pr > p$.

This gives more than $p(q - 1)$ elements of order q.

Thus $o(G) = pqr > pq\ (r - 1) + (p - 1) + p\,(q - 1) + 1$

or that $0 > 0$, a contradiction.

Hence Sylow p-subgroup is normal in G, and we get a contradiction.

$\therefore$ Sylow r-subgroup is normal in G.

(*ii*) Let H be a Sylow r-subgroup.

H is normal in G by (*i*).

Let K be a Sylow q-subgroup, $o(K) = q$

Since H is normal in G, $HK \leq G$ and $o(HK) = qr$.

Also p is smallest prime dividing $o(G)$ and $\dfrac{o(G)}{o(HK)} = p$,

HK is normal in G.

(*iii*) If $q \nmid (r-1)$, then HK is cyclic group of order qr. The number of elements of order qr is $\varphi(qr) = \varphi(q)\,\varphi(r) = (q - 1)\,(r - 1)$. Suppose Sylow q-subgroup is not normal. Then, the number of Sylow q-subgroups is $1 + kq$ and

$$(1 + kq) \mid pr \Rightarrow 1 + kq = p,\ r \text{ or } pr$$
$$\Rightarrow 1 + kq = r \text{ or } pr \text{ as } p < q$$
$$\Rightarrow 1 + kq = pr \text{ as } q \nmid (r - 1)$$

This gives $pr\,(q - 1)$ elements of orders q. Sylow p-subgroup gives $p - 1$ elements of order p.

Also Sylow r-subgroup gives $r - 1$ elements of order r.

Thus $o(G) \geq (r - 1) + (p - 1) + pr\,(q-1) + (q - 1)\,(r - 1) + 1$

$$pqr \geq (r - 1) + (p - 1) + pqr - pr + qr - q - r + 2$$
$$pr + q \geq qr + p$$
$$p\,(r - 1) \geq q\,(r - 1)$$
$$\Rightarrow p \geq q, \text{ a contradiction}$$

Hence, Sylow q - subgroup is normal in G.

Problem 19 : *Let G be a non abelian group of order 12 in which Sylow 3-subgroup is normal. Show that G has an element of order 6.*

Solution : Since Sylow 3-subgroup is normal, it will be unique. Let it be H then $o(H) = 3$, which being a prime shows H is cyclic. Let $H = (a)$. Then $o(a) = o(a^{-1}) = 3$ If $cl\,(a)$ is the conjugate class of a in G then

$$o(cl\,(a)) = \frac{o(G)}{o(N(a))} = 1 \text{ or } 2$$

Notice, $cl(a) = \{g^{-1}ag \mid g \in G\}$ and $o(g^{-1}ag) = o(a) = 3$ and as a, a^{-1} are the only elements of order 3, either $cl(a) = \{a\}$ or $cl(a) = \{a, a^{-1}\}$.

Thus $o(N(a)) = 6$ or 12

$\Rightarrow \exists\, b \in N(a)$, s.t., $o(b) = 2$

$\Rightarrow ab = ba$ and $o(ab) = 6$

i.e., G has an element of order 6.

Problem 20 : *If $\sigma \in Aut\, G$ and $o(\sigma) = p$, then σ must fix at least one Sylow p-subgroup of G.*

Solution : Let P be a Sylow p-subgroup of G. If $\sigma(P) \neq P$ then P, $\sigma(P)$, $\sigma^2(P)$,....., $\sigma^{p-1}(P)$ are p distinct Sylow p-subgroups of G.

Note if $\sigma^i(P) = \sigma^i(P)$, then $\sigma^{i-j}(P) = P$

Since $\theta(\sigma) = P$, $<\sigma> = <\sigma^{i-j}>$

$\Rightarrow \sigma = (\sigma^{i-j})^t$

$\Rightarrow \sigma(P) = (\sigma^{i-j})^t(P) = P$, a contradiction.

In this way, we'll get kp sylow p-subgroups of G. By sylow's third theorem, there are $1 + k'p$ Sylow p-subgroup of G. Thus at least one Sylow p-subgroup of G must be fixed by σ.

Problem 21 : *If H is normal in G and P is a Sylow p-subgroup of H then $G = N_G(P)\, H$.*

Solution : Let $x \in G$. Then $x^{-1}Px$ is a Sylow p-subgroup of H as H is normal in G and $P \subseteq H$.

Thus, $x^{-1}Px = y^{-1}py$ for some $y \in H$

$\Rightarrow yx^{-1}Pxy^{-1} = P$

$\Rightarrow yx^{-1} \in N(P)$

$\Rightarrow x = (xy^{-1})\, y \in N_G(P)\, H.$

$\Rightarrow G = N_G(P)\, H.$

Problem 22 : *If in a finite group G, there are at most d elements of order d for every $d \mid o(G)$, then G is cyclic.*

Solution : Let $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$

Consider Sylow p_1-group Sp_1

Then $o(Sp_1) = p_1^{\alpha_1}$

Suppose Sp_1 is not cyclic. Then the number of elements in Sp_1 of order p_i is less than or equal to p_1

of order p_1^2 is $\leq p_1^2$

of order p_1^3 is $\leq p_1^3$

and so on .....

of order $p_1^{\alpha_1 - 1}$ is $\leq p_1^{\alpha_1 - 1}$

Thus $p_1^{\alpha_1} \le 1 + p_1 + p_1^2 + p_1^3 + \ldots\ldots + p_1^{\alpha_1 - 1} = \dfrac{p_1^{\alpha_1 - 1}}{p_1 - 1}$, a contradiction.

So, Sp_1 is cyclic. Similarly each Sp_i is cyclic.

Since there are $1 + kp$, Sylow p_1-groups, the number of elements of order $p_1^{\alpha_1}$ is

$$(1 + kp_1)\ \varphi(p_1^{\alpha_1}) \le p_1^{\alpha_1}$$

$$\Rightarrow (1 + kp_1)\ (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \le p_1^{\alpha_1}$$

$$\Rightarrow p_1^{\alpha_1} + kp_1^{\alpha_1 + 1} - p_1^{\alpha_1 - 1} - kp_1^{\alpha_1} \le p_1^{\alpha_1}$$

$$\Rightarrow p_1^{\alpha_1 - 1}\ (kp_1^2 - 1 - kp_1) \le 0$$

$$\Rightarrow p_1^{\alpha_1 - 1}(kp_1\ (p_1 - 1) - 1) \le 0 \Rightarrow k = 0.$$

or that Sylow p_1-group is normal.

Similarly, each Sylow p_i-group is normal and cyclic.

Hence G is cyclic.

Suppose p = prime s.t. $p^r | n!$ and $p^{r+1} \nmid n!$. Then $r = \sum_{j=1}^{\infty} \left[\dfrac{n}{p^j}\right]$, where $[x]$ represents greatest integer not greater than x. (This result can be found in any book on Number theory).

In particular, if $n = p^k$, then $r = p^{k-1} + p^{k-2} + \ldots\ldots + 1$ we denote r by $n(k)$ to mean the highest power of p dividing $p^k!$.

We now give a method of constructing Sylow p-groups inductively in symmetric groups Sp^k.

When $k = 1$, then clearly $p | o(S_p) = p!$ and $p^2 \nmid p!$

(as $p^2 | p! \Rightarrow p | (p-1)$ 2.1

$\Rightarrow p | (p - r), 1 \le r \le p - 1$

$\Rightarrow p \le p - r$, a contradiction)

$\therefore$ order of Sylow p-subgroup in S_p is p and group generated by $(1\ 2 \ldots p)$ is a Sylow p-subgroup. So, We have constructed Sylow p-subgroup when $k = 1$. Assume that we have constructed it for $k - 1$. Consider Sp^k.

Divide the set of p^k letters $1, 2, \ldots, p^k$ into p sets each consisting of p^{k-1} letters as follows

$$\{1, 2, \ldots\ldots p^{k-1}\}, \{p^{k-1} + 1, \ldots\ldots, 2p^{k-1}\}, \ldots\ldots$$
$$\ldots\ldots\{(p-1)\}p^{k-1} + 1, \ldots\ldots, p^{k-1}\ p = p^k\}$$

Let

$\sigma = (1p^{k-1} + 1 \ldots (p-1)\ p^{k-1} + 1)\ (2p^{k-1} + 2 \ldots\ldots (p-1)\ p^{k-1} + 2) \ldots\ldots\ldots\ldots$
$(p^{k-1}\ 2p^{k-1} \ldots\ldots p^k)$

= product of p^{k-1} disjoint cycles each of length p.

Note, first cycle in σ consists of first letter from each set, second cycle has second letter from each set and so on.

Clearly $\sigma^p = I$ as disjoint cycles commute.

Let $\quad A = \{\tau \in Sp^k \mid \tau(i) = i \text{ for all } i > p^{k-1}\}$

$\therefore \quad I \in A$ i.e., $A \neq \varphi$

Let $\quad \tau, \tau' \in A \Rightarrow \tau\,\tau'(i) = i$ for all $i > p^{k-1}$

$\Rightarrow \tau\tau' \in A \leq Sp^k$

But $\tau \in A \Rightarrow \tau$ is permutation on p^{k-1} letters, $\therefore A \cong Sp^{k-1}$.

By induction hypothesis Sp^{k-1} has Sylow p-subgroup. $\therefore A$ has Sylow p-subgroup P_1. $o(P_1) = p^{n(k-1)} = 1 + \ldots + P^{k-2}$.

Let $P_2 = \sigma P_1 \sigma^{-1}$, $P_3 = \sigma^2 P_1 \sigma^{-2}, \ldots\ldots P_p = \sigma^{p-1} P_1 \sigma^{-(p-1)}$.

Each $P_i \leq Sp^k$ s.t. $P_i \cong P_1$ (Where $x \in P_1$ is mapped into $\sigma^i x \sigma^{-i}$).

$\therefore o(P_i) = o(P_1) = p^{n(k-1)}$. Also σ takes letters of first set into second set, letters from second set into third set and so on. So, $\tau \in A \Rightarrow \sigma T \sigma^{-1}$ consists of letters from second set as $T \in A$ means $\tau(i) = i$ for all $i > p^{k-1}$. Similarly $\sigma^2 \tau \sigma^{-2}$ will consist of letters from third set on. Therefore, $P_1, P_2, \ldots, P_{p-1}$ will have disjoint permutations and so commute with each other. Hence $T = P_1 P_2 \ldots P_p \leq Sp^k$.

Also
$$\begin{aligned} o(T) &= o(P_1)\ o(P_2)\ \ldots o(P_p) \\ &= o(P_1)\ o(P_1)\ \ldots\ldots o(P_1)\ (p \text{ times}) \\ &= p^{p(n(k-1)} = p^{1+n(k-1)} \end{aligned}$$

Let
$$\begin{aligned} P &= \{\sigma^j t \mid t \in T,\ 0 \leq j \leq p-1\} \\ &= <\sigma> T \end{aligned}$$

Since
$$\begin{aligned} \sigma T \sigma^{-1} &= \sigma(P_1 \ldots P_p)\sigma^{-1} \\ &= (\sigma P_1 \sigma^{-1})\ (\sigma P_2 \sigma^{-1}) \ldots\ldots (\sigma P_p \sigma^{-1}) \\ &= P_2 P_3 \ldots P_p P_1 = P_1 P_2 \ldots P_p = T \\ &\Rightarrow \sigma T = T \sigma \\ &\Rightarrow <\sigma> T = T <\sigma> \\ &\Rightarrow P \leq Sp^k \end{aligned}$$

Also $<\sigma> \cap T = \{I\}$ as σ takes first set into second set while T takes first set into first set.

$\therefore$
$$\begin{aligned} o(P) &= o(<\sigma>)\ o(T) \\ &= pp^{pn}\ (k-1) \\ &= p^{p(n\ (k-1))+1} \\ &= p^{p(1+p+\ldots+p^{k-2})+1} \\ &= p^{1+p+\ldots+p^{k-1}} = p^{n(k)} \end{aligned}$$

So, P is required Sylow p-subgroup of G.

Problem 23 : *Find a Sylow 3-subgroup of S_9.*

Solution : We urge the reader to first go through the discussion on the previous two pages. Let $P_1 = \{I, (123), (132)\}$ be a Sylow 3-subgroup of S_3.

Divide the set $\{1, 2, 3, 4, 5, 6, 7, 8, 9,\}$ into 3 sets as follows

$$\{1, 2, 3\}, \quad \{4, 5, 6\}, \quad \{7, 8, 9\}$$

Let $\sigma = (1\,4\,7)\ (2\,5\,8)\ (3\,6\,9)$

Then $\sigma^3 = I$

Let $P_2 = \sigma\ P_1 \sigma^{-1} = \{I, (456), (465)\}$

$P_3 = \sigma^2\ P_2\, \sigma^{-2} = \{I, (789), (798)\}$

Let $T = P_1 P_2 P_3,\ o(T) = 3^3$

Let $P = <\sigma>\ T$

Then $o(P) = 3^4$

Also $n(2) = 1 + 3 = 4$

$\Rightarrow P$ is a Sylow 3-subgroup of S_9.

Problem 24 : *Let G be the group of $n \times n$ invertible matrices over the integers modulo p, p a prime. Find a p-Sylow subgroup of G.*

Solution : Let A be an $n \times n$ matrix in G. Since A is invertible, rows of A are linearly independent over the field F of integers modulo p. Since first row of A is linearly independent, it is non zero. It can be chosen in $(p^n - 1)$ ways. Second row should not be α $(\alpha \in F)$ times the first row. So, second row can be chosen in $(p^n - p)$ ways. Third row should not be α times first row $+ \beta$ times second row $(\alpha, \beta \in F)$. So, third row can be chosen in $(p^n - p^2)$ ways as α, β can be chosen in p^2 ways. In this way, last nth row can be chosen in $p^n - p^{n-1}$ ways.

$$\begin{aligned} \therefore \qquad o(G) &= (p^n - 1)\ (p^n - p) \ldots\ldots (p^n - p^{n-1}) \\ &= p^{1+2+\ldots+(n-1)}\ ((p^n - 1)\ (p^{n-1} - 1) \ldots\ldots (p - 1)) \\ &= p^{\frac{n(n-1)}{2}}\ ((p^n - 1) \ldots\ldots (p - 1)) \end{aligned}$$

Since $(p, (p^i - 1)) = 1$, order of Sylow p-subgroup of G is $p^{\frac{n(n-1)}{2}}$

$$\text{Let } P = \left\{ \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & \ldots & \end{bmatrix} \{ \mid \text{enteries above diagonal from } F\} \right\}$$

$P \neq \varphi$ as $I \in P$

Also

$$A, B \in P \Rightarrow A = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & \ldots & \ldots & \ldots \\ O & & & 1 & & \ldots \\ & & & & & 1 \end{bmatrix}$$

$$\Rightarrow AB = \begin{bmatrix} 1 & \dots & \dots & \dots & \dots & \dots \\ & 1 & \dots & \dots & \dots & \dots \\ & & 1 & \dots & \dots & \dots \\ O & & & 1 & & \dots \end{bmatrix} \in P$$

$\therefore \qquad P \leq G$

Let $A \in P$. The first row in A can be chosen in p^{n-1} ways, second row in p^{n-2} ways and in this way $(n-1)$th row in p ways and last row is fixed.

So, $\qquad o(P) = p^{n-1}\ p^{n-2} \dots p^1$

$$= p^{1+\dots\dots+(n-1)} = p^{\frac{n(n-1)}{2}}$$

$\therefore$ P is Sylow p-subgroup if G.

In the following problem we discuss non abelian groups of order 6 and 8.

Problem 25 : *Find all non abelian groups of order 8.*

Solution : Let G be a non abelian group of order 8. As $o(a) \mid o(G)$ for all $a \in G$, $o(a) = 1, 2, 4$ or 8. If for some $a \in G$, $o(a) = 8$, G is cyclic. So there is no element in G of order 8. If each non identity element is of order 2, then G is abelian. So, $\exists\, a \in G$ s.t. $o(a) = 4$. Let $H = \langle a \rangle$. $o(H) = o(a) = 4$.

$\therefore$ H is normal in G as index of H in G is 2.

Let $\qquad G = H \cup Hb,\ b \notin H$

Then $b^2 \in H$ as $b^2 \notin H \Rightarrow H, Hb, Hb^2$ are distinct right cosets of H in G, a contradiction.

If $b^2 = a$, then $o(b^2) = \dfrac{o(b)}{(2, o(b))} = \dfrac{o(b)}{2}$

$\Rightarrow o(a) = \dfrac{o(b)}{2} \Rightarrow o(b) = 2\ .\ o(a) = 8$, a contradiction.

Similarly, if $b^2 = a^3$, then $b^2 = a^{-1} \Rightarrow o(b^2) = o(a^{-1}) = 4 \Rightarrow o(b) = 8$.

So, $b^2 = e$ or a^2.

Since H is normal in G, $b^{-1}ab \in H$.

But $\qquad o(b^{-1}ab) = o(a) = 4$

$\qquad \Rightarrow b^{-1}ab = a$ or a^3

If $b^{-1}ab = a$, then $ab = ba$. Since $G = H \cup Hb$, $G = \{e, a, a^2, a^3, ab, a^2b, a^3b, b\}$ and $ab = ba$ would imply G is abelian.

$\therefore \qquad b^{-1}ab = a^3$

Thus, we have two non abelian groups G of order 8, namely

(*i*) G, generated by a, b s.t. $a^4 = e,\ b^2 = e,\ b^{-1}ab = a^3 = a^{-1}$.

(*ii*) G, generated by a, b s.t $a^4 = e,\ -b^2 = a^2,\ b^{-1}ab = a^3 = a^{-1}$.

In fact (*i*) is the Dihedral group of order 8 and (*ii*) is the Quaternion group of order 8.

Remark : Although the Dihedral group and the Quaternion groups have same order 8, they are not isomorphic. In the Quaternion group a^2 is the only element of order 2 whereas in the Dihedral group, there are 5 elements a^2, b, ab, a^2b, a^3b of order 2. Recall if $f: G \to G'$ is an isomorphism then $o(f(a)) = o(a)\ \forall\ a \in G$.

Problem 26 : *Find all non abelian groups of order* 6.

Solution : Let G be a non abelian group of order 6. By Cauchy's theorem, $\exists\ a, b \in G$ s.t. $o(a) = 3$, $o(b) = 2$. Let $H = \langle a \rangle$ then $o(H) = o(a) = 3$. Since index of H in G is 2, H is normal in G. If $b \in H$, then $o(b) \mid o(H) \Rightarrow 2 \mid 3$, a contradiction. $\therefore\ b \notin H$.

$\therefore\ H$ and Hb are distinct right cosets of H in G.

Hence $\qquad G = H \cup Hb = \{e, a, a^2, b, ab\ a^2b\}$

Also H is normal in $G \Rightarrow b^{-1}ab \in H \Rightarrow b^{-1}ab = a$ or a^2.

If $b^{-1}ab = a$, then $ab = ba \Rightarrow G$ is abelian.

$\therefore\ b^{-1}ab = a^2 = a^{-1}$

So, there is only one non abelian group G of order 6, namely

$G = \{e, a, a^2\ b, ab\ a^2b \mid a^3 = e = b^2, b^{-1}ab = a^{-1}\}$

Indeed G is isomorphic to S_3 by the map $\theta : G \to S_3$ s.t. $\theta(e) = I$, $\theta(a) = (1\ 2\ 3)$, $\theta(a^2) = (1\ 3\ 2)$, $\theta(b) = (13)$, $\theta(a^2b) = (23)$.

Remark : Any non abelian group of order 6 is isomorphic to S_3. Also since any abelian group of order 6 is cyclic (see page 164) we find there are only two abstract groups of order 6.

Exercises

1. If N is normal in G and N, $\dfrac{G}{N}$ are both p-groups, show that G is a p-group.
2. If G is a finite non trival p-group, then show that G has a normal subgroup of index p.
3. If a group of order p^n contains exactly one subgroup each of order $p, p^2, \ldots\ldots, p^{n-1}$ show that G is cyclic.
4. Let P be a Sylow p-subgroup of G, prove that $N(N(P)) = (N(P))$.
5. Let P be a Sylow p-subgroup of G and suppose a, b are in the centre of P. Suppose further that $a = xbx^{-1}$ for some $x \in G$. Prove that $\exists\ y \in N(P)$ s.t. $a = yby^{-1}$.

   (Hint : $P \leq N(a)$, $P \leq N(b)$ as $a, b \in Z(P)$

   $$xPx^{-1} \leq xN(b)x^{-1} \leq N(xbx^{-1}) = N(a)$$
6. If $o(G) = p^2q$ where p, q are primes, show that either Sylow p-subgroup or Sylow q-subgroup is normal in G.

7. If G is a group of order 385, show that Sylow 11-subgroup is normal in G and Sylow 7-subgroup is in the centre of G.

8. Let G be group. Prove that $o\left(\frac{G}{Z(G)}\right)$ cannot be 77.

9. Let G be a group of order 255. Show that
   (*i*) Sylow 17-subgroup is normal in G.
   (*ii*) $\exists$ a normal subgroup K of order 85.
   (*iii*) $K \subseteq Z(G)$.
   (*iv*) G is cyclic.

10. If G is a non abelian group of order 231, show that $Z(G)$ is Sylow 11 subgroup of G.

11. Let $o(G) = 108$. Show that either Slow 3-subgroup is normal or there exits a normal subgroup of order 9.

12. If H is a normal subgroup of order p^k of a finite group G, show that H is contained in every Sylow p-subgroup of G.

13. If $o(G) = p^n q$ with $p > q$ primes, show that G contains a unique normal subgroup of index q.

14. Show that groups of order 12, 28, 56 and 200 must contain a normal Sylow subgroup.

15. Show that groups of order 36, 42, 99, 112 and 120 are not simple.

16. Let $o(G) = pq$ where p and q are distinct primes. Prove that G has a proper normal subgroup. Prove further that if neither prime is congruent to 1 modulo the other, then G is abelian.

17. Find a Sylow 2-subgroup of S_4.

18. If p is prime number, give explicit generators for a Sylow p-subgroup of Sp^2.

19. Find a Sylow 2-subgroup and a Sylow 3-subgroup of S_6.

20. Show that 21 is the smallest possible odd integer that can be the order of a non abelian group.

21. Show that there are four groups of order 30.

Direct Products

The reader is well aquainted with the idea of product of two sets as a set of ordered pairs. We explore the possibility of getting a new group through the product of two groups. Let G_1, G_2 be any two groups. Let $G = G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$.

What better way could there be than to define multiplication on G by $(g_1, g_2)\ (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$. That G forms a group under this as its composition should not be a difficult task for the reader. Indeed (e_1, e_2) will be identity of G where e_1, e_2 are identities of G_1 and G_2 are respectively. Also $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

We call $G = G_1 \times G_2$ *direct product or external direct product* (EDP) of G_1, G_2. Again if G_1, G_2 are abelian then so would be $G_1 \times G_2$.

In a similar way, we can define external direct product $G_1 \times G_2 \times \ldots \times G_n$ of arbitrary groups $G_1, G_2 \ldots, G_n$ as

$$G_1 \times \ldots \times G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

where composition is component wise multiplication.

Let $G = G_1 \times \ldots \times G_n$ = direct product of $G_1, \ldots, G_n$.

Define $H_1 = \{g_1, e_2, \ldots, e_n\} \mid g_1 \in G_1,\ e_i$ = identity of $G_i\ \}$

$H_2 = \{(e_1, g_2, e_3 \ldots, e_n) \mid g_2 \in G_2\}$,

.....

$H_n = \{(e_1 \ldots e_{n-1}, g_n) \mid g_n \in G_n\}$

We show that H_1 is normal in G.

$H_1 \neq \varphi$ as $(e_1, e_2, \ldots, e_n) \in H_1$

Let $(g_1, e_2, \ldots, e_n)\ (g'_1, e_2, \ldots e_n) \in H_1$

Then $(g_1, e_2, \ldots, e_n)\ (g'_1, e_2, \ldots, e_n)^{-1}$

$= (g_1, e_2, \ldots, e_n)\ (g_1^{-1}, e_2, \ldots e_n)$

$= (g_1 g_1^{-1}, e_2, \ldots e_n) \in H_1$

Thus $H_1 \leq G$

Let $g = (g_1, \ldots, g_n) \in G$

$x = (x_1, e_2, \ldots, e_n) \in H_1$

Then $gxg^{-1} = (g_1, \ldots, g_n)\ (x_1, e_2 \ldots, e_n)\ (g_1^{-1}, \ldots, g_n^{-1})$

$= (g_1 x_1 g_1^{-1}, e_2, \ldots e_n) \in H_1$

$\therefore H_1$ is normal in G.

Similarly, each H_i is normal in G for all $i = 1, \ldots, n$.

Let $g = (g_1, \ldots, g_n) \in G$

Then $g = (g_1, e_2, \ldots, e_n)\ (e_1, g_2, e_3 \ldots e_n) \ldots (e_1, \ldots, e_{n-1}) \in H_1 H_2 \ldots H_n$

Suppose $g = h_1 h_2 \ldots h_n = h'_1 h'_2, \ldots h'_n,\ h_i,\ h'_i \in H_i$

$\Rightarrow (g_1, e_2, \ldots, e_n) \ldots (e_1, \ldots e_{n-1}, g_n)$

$= (g'_1, \ldots, e_n) \ldots (e_1, \ldots e_{n-1}, g'_n)$

$\Rightarrow (g_1, \ldots g_n) = (g'_1 \ldots g'_n)$

$\Rightarrow g_i = g'_i$ for all $i = 1, \ldots, n$

$\Rightarrow h_i = h'_i$ for all $i = 1, \ldots, n$

So, $g \in G$ can be written uniquely as product of elements from $H_1, \ldots, H_n$.

We summarise this through the following definition.

Let $H_1, \ldots, H_n$ be normal subgroups of G. G is said to be an internal direct product (IDP) of $H_1, \ldots, H_n$ if $G = H_1 H_2 \ldots, H_n$ and each $g \in G$ can be written uniquely as product of elements from $H_1, \ldots, H_n$.

Example 1 : Consider the groups $Z_2 = \{0, 1\}$, $Z_3 = \{0, 1, 2\}$ under addition modulo. Here $Z_2 \times Z_3 = \{(0, 0), (0, 1), (0, 2), (1, 0)\ (1, 1), (1, 2)\}$ will form a group under element wise multiplication (addition). In fact it is a cyclic group generated by $(1, 1)$.

Indeed, $2(1, 1) = (1, 1) + (1, 1) = (1 \oplus_2 1, 1 \oplus_3 1) = (0, 2)$, $3(1, 1) = (1, 1) + (1, 1) + (1, 1) = (1, 0)$ etc.

We further note that since two cyclic groups of same order are isomorphic, (See remark on page 114) we must have $Z_2 \times Z_3 \cong Z_6$.

On the other hand one can show that $Z_2 \times Z_2$ is not isomorphic to Z_4. In fact $Z_2 \times Z_2$ is not cyclic (whereas Z_4 is). If $Z_2 \times Z_2$ is cyclic then it has a generator whose order should be same as $o(Z_2 \times Z_2) = 4$. But no element of $Z_2 \times Z_2$ has order 4. Notice, $2(1, 1) = (0, 0)$ i.e., order of $(1, 1)$ is less than or equal to 2 etc. Hence no element can be generator of $Z_2 \times Z_2$. One can show that $Z_n \times Z_m \cong Z_{nm}$ iff n and m are relatively prime. (See problem 28 on page 203).

Theorem 7 : *Let H_1, H_2 be normal in G. Then G is an IDP of H_1 and H_2 if and only if*

(*i*) $G = H_1H_2$

(*ii*) $H_1 \cup H_2 = \{e\}$.

Proof : Suppose G is an IDP of H_1 and H_2. Let $g \in G$. Then $g = h_1h_2$, $h_1 \in H_1$, $h_2 \in H_2$

Then $\quad G \subseteq H_1H_2$. But $H_1H_2 \subseteq G$

$\Rightarrow \quad G = H_1H_2$

Let $\quad g \in H_1 \cap H_2 \Rightarrow g \in H_1,\ g \in H_2$

$\therefore\ g = ge = eg$ is written in 2 ways as product of elements from H_1 and H_2.

$\therefore \quad g = e \Rightarrow H_1 \cap H_2 = \{e\}$.

Conversely, let $G = H_1H_2$ and $H_1 \cap H_2 = \{e\}$.

Let $g \in G \Rightarrow g \in H_1H_2 \Rightarrow g = h_1h_2,\ h_1 \in H_1,\ h_2 \in H_2$

Let $g = h_1h_2 = h'_1h'_2,\ h_1, h'_1 \in H_1,\ h_2, h'_2 \in H_2$

$$\Rightarrow h_1^{-1}h'_1 = h_2h'^{-1}_2 \in H_1 \cap H_2 = \{e\}$$

$$\Rightarrow h_1 = h'_1,\ h_2 = h'_2$$

$\therefore$ G is an IDP of H_1 and H_2.

Example 2 : Let $G = \langle a \rangle$ be of order 6. Let $H = \{e, a^2, a^4\}$, $K = \{e, a^3\}$ then H and K are normal (G is abelian) subgroups of G. $H \cap K = \{e\}$.

$$HK = \{e,\ ea^3,\ a^2e,\ a^2a^3,\ a^4e,\ a^4a^3\}$$
$$= \{e,\ a^2,\ a^3,\ a^4,\ a^5,\ a\} = G$$

Hence G is IDP of H and K.

Theorem 8 : *Let $H_1, H_2, \ldots\ldots, H_n$ be normal in G. Then G is an IDP of $H_1, H_2, \ldots\ldots, H_n$ if and only if*

(*i*) $G = H_1H_2 \ldots\ldots H_n$

(*ii*) $H_i \cap H_1H_2 \ldots\ldots H_{i-1}H_{i+1} \ldots\ldots H_n = \{e\}$

for all $i = 1, \ldots\ldots, n$

Proof : Suppose G is an IDP of $H_1, \ldots\ldots, H_n$. Then (i) follows from the definition of IDP

Let $\quad g \in H_i \cap H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_n$

Then $\quad g = h_i, \; h_i \in H_i$ and $g = h_1 h_2 \ldots\ldots h_{i-1} h_{i+1} \ldots\ldots h_n \quad h_j \in H_j$

$$\Rightarrow g = ee \ldots\ldots h_i \ldots\ldots e$$

$$g = h_1 h_2 \ldots\ldots h_{i-1} e h_{i+1} \ldots\ldots h_n$$

Since this representation of g should be unique we get $e = h_1, e = h_2, \ldots\ldots, h_i = e, \ldots\ldots$ or that $g = e$, which proves the result.

Conversely, let $g \in G$ then $g \in H_1 \ldots\ldots H_n \Rightarrow g = h_1 \ldots\ldots h_n, \; h_i \in H_i$

We show this representation is unique.

Let $\quad g = h'_1 \ldots\ldots h'_n, \qquad h'_i \in H_i$

$\therefore \quad h_1 \ldots\ldots h_n = h'_1 \ldots\ldots h'_n$

By (ii) $H_i \cap H_j = \{e\}$ for all $i \neq j$ because if $x \in H_i \cap H_j$

Then $x \in H_i, \quad x \in H_j. \; (j \neq i)$

$$x \in H_j \Rightarrow x \in H_1 \ldots\ldots H_j \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_n$$

as $\quad x = e \ldots\ldots x \ldots\ldots e \,.\, e \ldots\ldots e$

$$\Rightarrow x \in H_i \cap H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_n = \{e\}$$

Also H_i is normal in G, H_j is normal in G for all i, j, thus $h_i h_j = h_j h_i$ for all $i \neq j$

$\therefore \quad h_1 \ldots\ldots h_n = h'_1 \ldots\ldots h'_n$

$$h_n = (h_1^{-1} h'_1)(h_2^{-1} h'_2) \ldots\ldots (h_{n-1}^{-1} h'_{n-1}) h'_n$$

$\therefore \; h_n'^{-1} h_n = (h_1^{-1} h'_1) \ldots\ldots (h_{n-1}^{-1} h'_{n-1}) \in H_1 \ldots\ldots H_{n-1} \cap H_n = \{e\}$

$\therefore \quad h_n = h'_n$

Similarly $\quad h_{n-1} = h'_{n-1}, \ldots\ldots, h_1 = h'_1$

$\therefore$ G is an IDP of $H_1, \ldots\ldots, H_n$.

Remark : If G is an IDP of $H_1, H_2, \ldots\ldots, H_n$ then $H_i \cap H_j = \{e\}, \; i \neq j$.

We now show that IDP of subgroups of G is isomorphic to their external direct product (EDP).

Theorem 9 : *Let G be a group and suppose G is IDP of $H_1, \ldots\ldots, H_n$. Let T be EDP of $H_1, \ldots\ldots, H_n$. Then G and T are isomorphic.*

Proof : Define $\quad \theta : T \to G$, s.t.,

$$\theta(h_1, \ldots\ldots, h_n) = h_1 \ldots\ldots h_n, \qquad h_i \in H_i$$

θ is well defined as $(h_1, \ldots\ldots, h_n) = (h'_1, \ldots\ldots, h'_n)$

$$\Rightarrow h_i = h'_i \text{ for all } i$$

$$\Rightarrow h_1 \ldots\ldots h_n = h'_1 \ldots\ldots h'_n$$

$$\Rightarrow \theta(h_1, \ldots\ldots, h_n) = \theta(h'_1, \ldots\ldots, h'_n)$$

θ is homomorphism as

$$\theta(h_1, \ldots\ldots, h_n) \; (h'_1, \ldots\ldots, h'_n)$$

$$= \theta\ (h_1 h'_1, \ldots\ldots, h_n h'_n)$$
$$= (h_1 h'_1) \ldots\ldots (h_n h'_n)$$
$$= (h_1, \ldots\ldots, h_n)\ (h'_1, \ldots\ldots h'_n)$$

as $h_i h_j = h_j h_i$

$h'_i h'_j = h'_j h'_i$ for all $i \neq j$

$$= \theta\,(h_1, \ldots\ldots, h_n)\ \theta\,(h'_1, \ldots\ldots, h'_n)$$

θ is 1-1 as $\theta\,(h_1, \ldots\ldots, h_n) = \theta\,(h'_1, \ldots\ldots, h'_n)$

$\Rightarrow h_1 \ldots\ldots h_n = h'_1 \ldots\ldots h'_n$

$\Rightarrow h_i = h'_i$ for all i by definition of IDP

$\Rightarrow (h_1, \ldots\ldots, h_n) = (h'_1, \ldots\ldots, h'_n)$

θ is onto as $g \in G \Rightarrow g = h_1 \ldots\ldots h_n, \quad h_i \in H_i$

$= \theta\,(h_1, \ldots\ldots, h_n), \quad (h_1, \ldots\ldots, h_n) \in T$

$\therefore$ θ is an isomorphism.

Hence $G \cong T$.

Problem 27 : *Show that a group of order 4 is either cyclic or is an IDP of two cyclic groups of order 2 each.*

Solution : Let G be a non cyclic group of order 4. Then $G \cong K_4$, the Klein's four group. See page 131. Also then $K_4 \cong Z_2 \times Z_2$ see page 201. Hence $G \cong Z_2 \times Z_2$ where Z_2 is cyclic group of order 2. In view of above theorem then G is IDP of two cyclic groups of order 2 each.

Problem 28 : *Let A, B be cyclic groups of order m and n respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.*

Solution : Let $A = \langle a \rangle$, $B = \langle b \rangle$

$$o(A) = o(a) = m,\ o(B) = o(b) = n$$

Suppose $A \times B$ is cyclic.

Let $A \times B = \langle (x, y) \rangle$, $x \in A$, $y \in B$

$$o(A \times B) = mn = o(x, y)$$

Let *g.c.d.* of m and n be d.

$\therefore$ $\dfrac{m}{d}$ and $\dfrac{n}{d}$ are relatively prime integers.

Consider $(x, y)^{\frac{mn}{d}} = \left(x^{\frac{mn}{d}},\ y^{\frac{mn}{d}} \right)$

$$= \left((x^m)^{\frac{n}{d}},\ (y^n)^{\frac{m}{d}} \right)$$

$$= (e_1^{n/d}, e_2^{m/d}),\ e_1 = \text{identity of } A$$

$$e_2 = \text{identity of } B$$

$$= (e_1, e_2)$$
$$= \text{identity of } A \times B$$

$\therefore \quad o(x, y) \mid \frac{mn}{d}$

$\Rightarrow mn \mid \frac{mn}{d}$

$\Rightarrow d.\frac{mn}{d} \mid \frac{mn}{d}$

$\Rightarrow d \mid 1 \Rightarrow d = 1$

$\therefore$ m and n are relatively prime.

Conversely, let m and n be relatively prime. We show $A \times B$ is cyclic, generated by (a, b). For that we prove $o(a, b) = mn = o(A \times B)$.

Consider $\quad (a, b)^{mn} = (a^{mn}, b^{mn})$

$= ((a^m)^n, (b^n)^m)$

$= (e_1, e_2) = \text{identity of } A \times B$

Let $\quad (a, b)^r = (e_1, e_2)$

$\Rightarrow (a^r, b^r) = (e_1, e_2)$

$\Rightarrow a^r = e_1, \; b^r = e_2$

$\Rightarrow o(a) = m \mid r, \; o(b) = n \mid r$

$\Rightarrow mn \mid r$ as m, n are relatively prime.

$\Rightarrow mn \leq r$

$\therefore \quad o(a, b) = mn = o(A \times B)$

Hence $\quad A \times B = <(a, b)> =$ cyclic group generated by (a, b).

Problem 29 : *Show that every group of order p^2, p a prime, is either cyclic or is isomorphic to direct product of two cyclic groups each of order p.*

Solution : Let $o(G) = p^2$. Then G is abelian (Problem 17, page 156) Suppose G is non cyclic. Since $p \mid o(G)$ $\exists$ $a \in G$ s.t. $o(a) = p$. Let $A = <a>$, $o(A) = o(a) = p$.

Now $A \neq G \Rightarrow \exists$ $b \in G$ s.t. $b \notin A$.

Also $o(b) \mid o(G) = p^2 \Rightarrow o(b) = 1, p$ *or* p^2

If $o(b) = p^2$, then G is cyclic.

If $o(b) = 1$, then $b = e \in A$, a contradiction.

$\therefore$ $o(b) = p$. Let $B = <b>$, $o(B) = o(b) = p$

$$A \cap B \leq A \Rightarrow o(A \cap B) \mid o(A) = p$$
$$\Rightarrow o(A \cap B) = 1 \text{ or } p$$

If $o(A \cap B) = p$, then $A = A \cap B \Rightarrow A \subseteq B \Rightarrow A = B$ as $o(A) = o(B)$, a contradiction as $b \in B$, $b \notin A$

$\therefore \quad o(A \cap B) = 1$

$\therefore \quad A \cap B = \{e\}$

Since G is abelian, A is normal in G, B is normal in G.

Also $$o(AB) = \frac{o(A)\,o(B)}{o(A \cap B)} = p^2 = o(G)$$

$\therefore$ $$G = AB$$

By theorem 7, G is an IDP of A and B.

By theorem 9, G is isomorphic to EDP of A and B.

Problem 30 : *Let G be a finite abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.*

Solution : Let $o(G) = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r}$

where $p_1, \ldots\ldots, p_r$ are distinct primes.

Since G is abelian, each Sylow subgroup H_i of G is normal. $o(H_i) = p_i^{\alpha_i}$.

Let $$g \in H_i \cap H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_r$$
$$\Rightarrow g \in H_i,\ g \in H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_r$$

Let $$t = p_1^{\alpha_1} \ldots\ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots\ldots p_r^{\alpha_r}$$
$$g \in H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_r$$
$$\Rightarrow g = h_1 \ldots\ldots h_{i-1} h_{i+1} \ldots\ldots h_r,\ h_j \in H_j$$
$$\Rightarrow g^t = h_1^t \ldots\ldots h_{i-1}^t h_{i+1}^t \ldots\ldots h_r^t = e \text{ as } h_j^t = e \text{ for all } j \neq i$$
$$\Rightarrow o(g) \mid t$$

But $$g \in H_i \Rightarrow o(g) \mid o(H_i) = p_i^{\alpha_i}$$
$$\Rightarrow o(g) = p_i^{\beta_i},\ \beta i \geq 0$$

$\therefore$ $$p_i^{\beta_i} \mid t$$
$$\Rightarrow p_i^{\beta_i} \mid p_1^{\alpha_1} \ldots\ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots\ldots p_r^{\alpha_r}$$
$$\Rightarrow \beta i = 0$$
$$\Rightarrow o(g) = 1 \Rightarrow g = e.$$

$\therefore$ $H_i \cap H_1 \ldots\ldots H_{i-1} H_{i+1} \ldots\ldots H_r = \{e\}$ for all $i = 1, \ldots\ldots, r$

Now $$o(H_1 \ldots\ldots H_r) = \frac{o(H_1)\,o(H_2 \ldots\ldots H_r)}{o(H_1 \cap H_2 \ldots\ldots H_r)} = o(H_1)\ o(H_2 \ldots\ldots H_r)$$

But $x \in H_2 \cap H_3 \ldots\ldots H_r \Rightarrow x \in H_2 \cap H_1 H_3 \ldots\ldots H_r$

as $H_3 \ldots\ldots H_r \subseteq H_1 H_3 \ldots\ldots H_r$

$\Rightarrow x = e$

$\therefore$ $$o(H_2 \ldots\ldots H_r) = o(H_2)\ o(H_3 \ldots\ldots H_r)$$

In this way, we get

$$o(H_1 \ldots\ldots H_r) = o(H_1)\ o(H_2) \ldots\ldots o(H_r) = o(G)$$
$$\Rightarrow G = H_1 \ldots\ldots H_r$$

By theorem 8, G is an IDP of $H_1, \ldots\ldots H_r$ and so isomorphic to EDP of $H_1, \ldots\ldots, H_r$ by theorem 9.

Problem 31 : *Let N be normal in G. If $G = H \times K$ where H, K are subgroups of G, then prove that either N is abelian or N intersects H or K non trivially.*

Solution : Suppose $N \cap H = \{e\}$, $N \cap K = \{e\}$.

Since $G = H \times K$, H is normal in G, K is normal in G. $\therefore$ $nh = hn$ for all $n \in N$, $h \in H$ and $nk = kn$ for all $n \in N$, $k \in K$.

Let $n_1, n_2 \in N$.

$$n_2 \in N \Rightarrow n_2 \in G \Rightarrow n_2 = h_2k_2,\ h_2 \in H_1,\ k_2 \in K$$

$$\begin{aligned} \therefore \quad n_1n_2 &= n_1h_2k_2 \\ &= h_2n_1k_2 \\ &= h_2k_2n_1 \\ &= n_2n_1 \end{aligned}$$

So, N is abelian.

Problem 32 : *Let m and n be relatively prime integers. Let u, v be any integers. Show that $\exists$ an integer t s.t. $t \equiv u \pmod{m}$ and $t \equiv v \pmod{n}$.*

(This is called *Chinese Remainder Theorem*).

Solution : Let Z_m, Z_n denote the groups under addition modulo m, n respectively. Z_m and Z_n are cyclic groups generated by 1. By problem 28, $Z_m \times Z_n$ is cyclic group generated by (1, 1).

Let $\quad u = mq_1 + r, \quad 0 \le r < m$

$\quad v = nq_2 + s, \quad 0 \le s < n$

$\therefore \quad r \in Z_m,\ s \in Z_n$

$\therefore \quad (r, s) \in Z_m \times Z_n$

$\therefore$ $\exists$ integer t s.t., $(r, s) = t\ (1, 1)$

$$\therefore \quad (r, s) = (\underbrace{1 \oplus \ldots\ldots \oplus 1}_{t \text{ times}},\ \underbrace{1 \oplus \ldots\ldots \oplus 1}_{\text{times}})$$

where the composition in first coordinate is under addition modulo m and in second, under addition modulo n.

$\therefore \quad (r, s) = (t - mq_3,\ t - nq_4)$

$\therefore \quad r = t - mq_3,\ s = t - nq_4$

$\therefore \quad u = mq_1 + t - mq_3$

$\quad v = nq_2 + t - nq_4$

$\therefore \quad t \equiv u \pmod{m}$

$\quad t \equiv v \pmod{n}$.

Problem 33 (*a*) : *Show that S_3 can not be written as internal direct product of two non trivial subgroups.*

(*b*) *Show that the quaternion group cannot be written as IDP of its non trivial subgroups.*

Solution : Suppose S_3 is an internal direct product of its subgroups H and K where $H \neq \{I\}$, $K \neq \{I\}$

Then $S_3 = HK$, $H \cap K = \{I\}$

H is normal in S_3, K is normal in S_3

$$\Rightarrow o(S_3) = 6 = o(H)\, o(K)$$

$\Rightarrow$ Either $o(H) = 2$ or $o(K) = 2$

as $o(H)$ and $o(K) > 1$.

In S_3, subgroups of order 2 are $\{I, (12)\}$, $\{I, (13)\}$, $\{I, (23)\}$ and none of these is normal subgroup of S_3.

$\therefore$ S_3 can't be written as IDP of two non trivial subgroups.

Again we know (See exercise 11, page 86) that all the non - trivial subgroups of the quaternion group contain 1 and -1 and thus the condition $H_i \cap H_j = (e)\ \forall\ i \neq j$ does not hold. Hence by remark on page 202, result follows.

Problem 34 : *If H, K are normal subgroups of G, show that $\dfrac{G}{H \cap K}$ is isomorphic to a subgroup of $\dfrac{G}{H} \times \dfrac{G}{K}$.*

Solution : Define $\theta : G \to \dfrac{G}{H} \times \dfrac{G}{K}$ s.t.,

$$\theta(x) = (Hx,\ Kx) \text{ for all } x \in G$$

θ is well defined as $x = y \Rightarrow Hx = Hy,\ Kx = Ky \Rightarrow (Hx,\ Kx) = (Hy,\ Ky)$.

θ is a homomorphism as

$$\begin{aligned}\theta(xy) &= (Hxy,\ Kxy)\\ &= (HxHy,\ KxKy)\\ &= (Hx,\ Kx)\ (Hy,\ Ky)\\ &= \theta(x)\ \theta(y) \text{ for all } x, y \in G\end{aligned}$$

$$\begin{aligned}\operatorname{Ker}\theta &= \{x \in G \mid \theta(x) = \text{identity of } \frac{G}{H} \times \frac{G}{K}\}\\ &= \{x \in G \mid (Hx,\ Kx) = (H, K)\}\\ &= \{x \in G \mid Hx = H,\ Kx = K\}\\ &= \{x \in G \mid x \in H,\ x \in K\}\\ &= \{x \in G \mid x \in H \cap K\}\\ &= H \cap K.\end{aligned}$$

$\therefore \quad \dfrac{G}{\operatorname{Ker}\theta} = \dfrac{G}{H \cap K}$ is isomorphic to $\theta(G)$

(Note θ is onto map from G to $\theta(G)$)

Also, $\theta(G)$ is a subgroup of $\dfrac{G}{H} \times \dfrac{G}{K}$.

$\therefore \quad \dfrac{G}{H \cap K}$ is isomorphic to a subgroup of $\dfrac{G}{H} \times \dfrac{G}{K}$.

In two isomorphic groups the number of elements with a specific order will be same in both. The converse, however, may not hold as is evident by

Example 3 : Let G be the set of matrices of the type $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ where $a, b, c \in F_3$. Here $F_3 = \{0, 1, 2\} \bmod 3$ (See under chapter VII on Rings)

Then one can check that G forms a non abelian group. In fact, it would be a subgroup of the group of all 3×3 non singular matrices over F_3.

Since each of a, b, c have three choices, $o(G) = 3^3$.

Order of each non identity element of G will be 3 as

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} \neq I \text{ as one of } a, b, c \text{ is non zero}$$

and $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

If we consider the group $Z_3 \times Z_3 \times Z_3$, then it is an abelian group of order 27 in which each non identity element is of order 3. Thus both the groups have 26 elements of order 3 (plus one identity) But G and $Z_3 \times Z_3 \times Z_3$ cannot be isomorphic as one is abelian and the other a non abelian group.

Exercises

1. If H, K are subgroups of a group G s.t. $G = H \times K$, show that $\dfrac{G}{H} \cong K, \quad \dfrac{G}{K} \cong H$.
2. Let G_1, G_2, G_3 be groups. Show that
   (*i*) $G_1 \times G_2 \cong G_2 \times G_1$
   (*ii*) $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3 \cong G_1 \times G_2 \times G_3$.

3. Show that a group of order 4 is cyclic or internal direct product of two cyclic groups of order 2 each.
4. Let G be a group. Let $H = \{(g, g) \mid g \in G\}$, Show that $H \leq G \times G$ and H is normal in $G \times G$ if and only if G is abelian.
5. Let $G = G_1 \times \ldots\ldots \times G_n$. Show that
   (*i*) $Z(G) = Z(G_1) \times \ldots\ldots \times Z(G_n)$
   (*ii*) $N(g) = N(g_1) \times \ldots\ldots \times N(g_n)$ where $g = (g_1 \ldots\ldots g_n) \in G$
6. Show that the multiplicative group of non zero real numbers is an internal direct product of two non - trivial subgroups.
7. Prove that the group **Q** of all rational numbers under addition can't be written as direct sum of two non trivial subgroups.
8. If N_1 is normal in G_1 and N_2 is normal in G_2 then show that $N_1 \times N_2$ is normal in $G_1 \times G_2$ and $\dfrac{G_1 \times G_2}{N_1 \times N_2} \cong \dfrac{G_1}{N_1} \times \dfrac{G_2}{N_2}$.

Finite Abelian Groups

Having studied direct products, one would like to know whether groups can be written as direct product of some 'simple looking' groups. Luckily, such a class of groups exists, namely finite abelian groups. The main purpose of this section is to prove that all important theorem called fundamental theorem on finite abelian groups which states that a finite abelian group is a direct product of cyclic groups. This paves the way for us to spell out the method that gives the number of non - isomorphic finite abelian groups of a given order.

We first show that a finite abelian group can be written as a direct product of p - groups. (See problem 30 for different proof).

Theorem 10 : *A finite abelian group is a direct product of its Sylow p-subgroups.*

Proof : Let G be a finite abelian group of order n. Let $n = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r}$ p_i's being distinct primes.

Let $S_1, \ldots\ldots S_r$ be distinct Sylow p_i-subgroups respectively. $o(S_i) = p_i^{\alpha_i}$ for all $i = 1, \ldots\ldots, r$

We show that $G = S_1 \times \ldots\ldots \times S_r$

Since G is abelian, each S_i is a normal subgroup of G.

Let $\quad m = p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$

and $\quad T = \{x \in G \mid x^m = e\}$

Then T is a subgroup of G as G is abelian.

Now $\quad x \in S_1 \cap T \Rightarrow o(x) \mid o(S_1) = p_1^{\alpha_1}$

and $\quad o(x) \mid m$

So, $o(x) \mid (p_1^{\alpha_1}, m) = 1$

$\Rightarrow o(x) = 1$

$\Rightarrow x = e$

$\therefore \quad S_1 \cap T = \{e\}$

As $(p_1^{\alpha_1}, m) = 1$, $\exists$ integers u, v such that

$$up_1^{\alpha_1} + vm = 1$$

Let $x \in G$. Then $x = x^1$

$= x^{up_1^{\alpha_1} + vm}$

$= x^{vm} . x^{up_1^{\alpha_1}}$

$\in S_1 . T$ (as $(x^{vm})^{p_1^{\alpha_1}} = x^{vn} = (x^n)^v = e$

$\Rightarrow o(x^{vm}) \mid p_1^{\alpha_1}$

$\Rightarrow o(x^{vm}) = p_1^{\beta_1}$

$\Rightarrow \langle x^{vm} \rangle$ is a p_1-group

$\Rightarrow \langle x^{vm} \rangle \subseteq S_1$

$\Rightarrow x^{vm} \in S_1$

Also $(x^{up_1^{\alpha_1}})^m = x^{un} = e$

$\Rightarrow x^{up_1^{\alpha_1}} \in T)$

$\therefore \quad G = S_1 T$

Since G is abelian, S_1 and T are normal subgroups of G.

$\therefore \quad G = S_1 \times T$

Also, $o(G) = o(S_1 T)$

$= o(S_1)\ o(T)$

$\Rightarrow n = p_1^{\alpha_1} o(T)$

$\Rightarrow o(T) = p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r} = m$

As above, we can show that

$T = S_2 \times U$, where U is a subgroup of T such that $o(U) = p_3^{\alpha_3} \ldots\ldots p_r^{\alpha_r}$

In this way, we shall have

$$G = S_1 \times S_2 \ldots\ldots S_r$$

Having *broken* G into product of p-subgroups, we prove results on finite abelian p-groups rather than G itself.

Theorem 11 : *Let G be an abelian group of order p^n, p a prime and let $a \in G$ have maximal order of all elements in G. Then $G = A \times Q$ where A is the cyclic subgroup generated by a and $Q \leq G$.*

Proof : We prove the result by induction on n. If $n = 1$, then $o(G) = p$. So, G is cyclic group of order p. Thus G has an element of highest order p.

$\therefore\ o(a) = p = o(G)$ and $G = \langle a \rangle = A$. So, result is true in this case.

Assume that the result is true for all $m < n$. Suppose that $\exists\ b \in G$ s.t., $b \notin A = \langle a \rangle$ and $o(b) = p$. We show that the result is true in this case.

Let $B = \langle b \rangle$. Then $A \cap B \leq B \Rightarrow o(A \cap B) = 1$ or p.

If $o(A \cap B) = p = o(B)$, then $A \cap B = B \Rightarrow B \subseteq A \Rightarrow b \in A$, a contradiction.

$\therefore\ A \cap B = \{e\}$.

Let $\overline{G} = \dfrac{G}{B}$. Let $\bar{a} = Ba$.

Now
$$(\bar{a})^{o(a)} = (Ba)^{o(a)}$$
$$= Ba^{o(a)}$$
$$= B$$
$$\Rightarrow o(\bar{a}) \mid o(a)$$

Now
$$Ba^{o(\bar{a})} = Ba^{o(\bar{a})} = B$$
$$\Rightarrow a^{o(\bar{a})} \in B$$

Also
$$a^{o(\bar{a})} \in A$$
$$\Rightarrow a^{o(\bar{a})} \in A \cap B = \{e\}$$
$$\Rightarrow a^{o(\bar{a})} = \{e\}$$
$$\Rightarrow o(a) \mid o(\bar{a})$$
$$\Rightarrow o(a) = o(\bar{a}).$$

Now $\bar{a}$ is an element of maximal order in $\overline{G}$ for, if $\bar{c} \in \overline{G}$ has order more than $o(\bar{a})$

then
$$o(\bar{c}) \mid o(c) \Rightarrow o(\bar{c}) \leq o(c)$$
$$\Rightarrow o(c) \geq o(\bar{c}) > o(\bar{a}) = o(a)$$
$$\Rightarrow o(c) > o(a)$$

contradicting that a has maximal order in G.

By induction hypothesis, $\overline{G} = \langle \bar{a} \rangle \times T$ for some subgroup T of $\overline{G}$. But T is a subgroup of $\overline{G} \Rightarrow T = \dfrac{Q}{B}$ for some subgroup Q of G. We show that $G = A \times Q$.

Let $x \in A \cap Q$. Then $x \in A \Rightarrow x = a^i$.

But $x \in Q \Rightarrow a^i \in Q \Rightarrow Ba^i \in T \Rightarrow (Ba)^i \in T \Rightarrow a^{-i} \in T$

$\Rightarrow a^{-i} \in <\bar{a}> \cap T \Rightarrow a^{-i} = \bar{e} \Rightarrow Ba^i = Be \Rightarrow a^i \in B$

$\therefore \quad a^i \in A \cap B = \{e\}$

$\Rightarrow a^i = e \Rightarrow x = e \Rightarrow A \cap Q = \{e\}$

Let $x \in G$.

Then $\quad \bar{x} = Bx \in \bar{G} = <\bar{a}> . T$

$\Rightarrow \bar{x} = \bar{a}^{-j}\, \bar{y}, \bar{y} \in T$

$\Rightarrow xy^{-1} a^{-j} \in B \subseteq Q$

$\Rightarrow x = a^j z,\ z \in Q$

$x \in <a> . Q$

$\Rightarrow G = AQ$

$\therefore\ G = A \times Q$ and so result follows.

Suppose that there is no element $b \in G$, $b \notin A$ s.t., $o(b) = p$. We show that in this case $G = A$. Assume that $G \neq A$. Let $x \in G$, $x \notin A$. Assume x has smallest possible order.

Now $\quad o(x^p) = \dfrac{o(x)}{(p, o(x))} = \dfrac{p^i}{(p, p^i)} = \dfrac{p^i}{p} = p^{i-1}$

$\Rightarrow o(x^p) < o(x)$

$\Rightarrow x^p \in A$

$\Rightarrow x^p = a^j.$

Suppose $p \nmid j$

Let $\quad o(a) = m = p^s$

Now $\quad c \in G \Rightarrow o(c) = p^r$

$\Rightarrow p^r \leq o(a) = p^s$ as a has maximal order

$\Rightarrow r \leq s$

$\Rightarrow o(c) \mid o(a) = m$

$\Rightarrow c^m = e$ for all $c \in G$

$p \nmid j \Rightarrow m \nmid \dfrac{jm}{p}$

and so, $\quad (a)^{\frac{jm}{p}} \neq e$

$\therefore \quad x^m = (x^p)^{m/p}$

$= (a^j)^{m/p} = (a)^{\frac{jm}{p}}$

$\neq e$, a contradiction

$\therefore\ p \mid j$. Let $j = kp$. Then $x^p = a^j = a^{kp}$.

Let $\quad y = a^{-k}x$

Since $\quad x \notin A,\ y \notin A$

Also $\quad y^p = a^{-kp}\ x^p = a^{-j}\ a^j = e$

$\therefore\ o(y) = p$, contradiction (as there is no element of order p not in A by our assumption).

$\therefore\ G = A$ and so result is true in this case.

Hence by induction, result follows.

We are now ready to prove the fundamental theorem on finite abelian groups.

Theorem 12 : (The Fundamental Theorem on Finite Abelian Groups).

A finite abelian group is the direct product of cyclic groups.

Proof : Let G be a finite abelian group. We prove the result by induction on $o(G)$. If $o(G) = 1$, then result is trivially true. Assume that the result is true for all abelian groups of order $< o(G)$.

Let $o(G) = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r}$, $p_i s$ are distinct primes.

By theorem 10, $G = S_1 \times \ldots\ldots \times S_r$, where S_i is the Sylow p_i-subgroup of order $p_i^{\alpha_i}$ $(i = 1, 2, \ldots\ldots, r)$.

By theorem 11, $S_i = A_i \times Q_i$, where each A_i is a cyclic group.

$$\therefore \quad G = (A_1 \times Q_1) \times \ldots\ldots \times (A_r \times Q_r)$$
$$= (A_1 \times \ldots\ldots \times A_r) \times (Q_1 \times \ldots\ldots \times Q_r)$$

Now $o(Q_1 \times \ldots\ldots \times Q_r) < (o(G)$ and $Q_1 \times Q_2 \ldots\ldots \times Q_r$ is an abelian group. By induction hypothesis $Q_1 \times \ldots\ldots \times Q_r = T_1 \times \ldots\ldots \times T_s$, where each T_i is a cyclic subgroup of G.

$$\therefore \quad G = A_1 \times \ldots\ldots \times A_r \times T_1 \times \ldots\ldots \times T_s$$
$$= \text{direct product of cyclic subgroups.}$$

$\therefore$ result is true in this case as well.

By induction result is true for all finite abelian groups G.

Note : Suppose finite abelian group G is written as $G = A_1 \times \ldots\ldots \times A_k$, A_i = cyclic group.

Then
$$G = A_1 \times (A_2 \times \ldots\ldots \times A_k)$$
$$\Rightarrow o(G) = o(A_1)\ o(A_2 \times \ldots\ldots \times A_k)$$
$$= o(A_1)\ o(A_2)\ o(A_3 \times \ldots\ldots \times A_k)$$

In this way, we get $o(G) = o(A_1)\ o(A_2) \ldots\ldots o(A_k)$

Theorem 13 : *Let G be a finite abelian group of order p^n, p a prime. Suppose $G = A_1 \times \ldots\ldots \times A_k$ where each A_i is a cyclic group of order p^{n_i} with $n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$. Then the integers $n_1, \ldots\ldots, n_k$ are uniquely determined, called invariants of G.*

Proof : Suppose $G = A_1 \times \ldots\ldots \times A_k$

and $G = B_1 \times \ldots\ldots \times B_l$

where A_i and B_js are cyclic groups s.t. $o(A_i) = p^{n_i}$, $o(B_j) = p^{h_j}$, $n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$, $h_1 \geq h_2 \geq \ldots\ldots \geq h_l > 0$.

Our aim is to show that $k = l$ and $n_i = h_i$ for all i. Let $g \in G$. Then $g = a_1 a_2 \ldots\ldots a_k$, $a_i \in A_i$

Since $n_1 \geq n_i$ for all $i = 1, \ldots\ldots, k$

$$p^{n_i} \mid p^{n_1} \text{ for all } i = 1, \ldots\ldots, k$$

$$\therefore \quad p^{n_1} = p^{n_i} p^{u_i} \text{ for all } i = 1, \ldots\ldots, k$$

So,
$$g^{p^{n_1}} = a_1^{p^{n_1}} a_2^{p^{n_1}} \ldots\ldots a_k^{p^{n_k}}$$

$$= a_1^{p^{n_1}} a_2^{p^{n_2}} \ldots\ldots a_k^{p^{n_k}}$$

$$= e \text{ as } (a_i)^{p^{n_i}} = a_i^{o(A_i)} = e \text{ for all } i$$

$$\therefore \quad o(g) \mid p^{n_1} \text{ for all } g \in G$$

$$\Rightarrow o(g) \leq p^{n_1} \text{ for all } g \in G$$

Also A_1 is a cyclic group of order p^{n_1} $\Rightarrow \exists$ an element of order p^{n_1}.

So p^{n_1} is the maximal order of elements in G. Similarly, by taking $G = B_1 \times \ldots\ldots \times B_l$, we get p^{h_1} to be the maximal order of elements in G.

$$\therefore \quad p^{n_1} = p^{h_1} \Rightarrow n_1 = h_1$$

Suppose we have proved that $n_1 = h_1$, $n_2 = h_2, \ldots\ldots, n_{t-1} = h_{t-1}$. Suppose $n_t \neq h_t$. Let $n_t > h_t = m$. Define $C = \{ x^{p^m} \mid x \in G\}$. Since G is abelian, C is a subgroup of G.

Let $A_1 = \langle a_1 \rangle, \ldots\ldots, A_k = \langle a_k \rangle$, $o(a_i) = o(A_i) = p^{n_i}$

$B_1 = \langle b_1 \rangle, \ldots\ldots, B_k = \langle b_k \rangle$, $o(b_j) = o(B_j) = p^{h_j}$

We claim that

$$C = \langle b_1^{p^m} \rangle \times \ldots\ldots \times \langle b_{t-1}^{p^m} \rangle$$

Let $x^{p^m} \in C$, $x \in G$

Now $x \in G \Rightarrow x = x_1 \ldots\ldots x_{t-1} x_t \ldots\ldots x_l$, $x_j \in B_j$

$$x_j \in B_j \Rightarrow x_j = b_j^{r_j}$$

$\therefore \qquad x^{p^m} = x_1^{p^m} \ldots\ldots x_l^{p^m}$

$$= b_1^{r_1 p^m} \ldots\ldots b_{t-1}^{r_{t-1} p^m} \, b_t^{r_t p^m} \ldots\ldots b_l^{r_l p^m}.$$

Now $\qquad$ for all $j \geq t$, $o(B_j) = p^{h_j} \mid p^{h_t} = p^m$

$$\Rightarrow \; p^m = p^{h_j} p^{v_j} \quad \text{for all } j \geq t$$

$$\Rightarrow \; b_j^{p^m} = b_j^{p^{h_j} p^{v_j}} = e \quad \text{for all } j \geq t$$

$\therefore \qquad x^{p^m} = b_1^{r_1 p^m} \ldots\ldots b_{t-1}^{r_{t-1} p^m}$

$\therefore \qquad x^{p^m} = b_1^{r_1 p^m} \ldots\ldots b_{t-1}^{r_{t-1} p^m}$

$$\in \langle b_1^{p^m} \rangle \ldots\ldots \langle b_{t-1}^{p^m} \rangle$$

$\therefore \qquad C \subseteq \langle b_1^{p^m} \rangle \ldots\ldots \langle b_{t-1}^{p^m} \rangle$

But $\qquad b_j^{p^m} \in C \Rightarrow \langle b_j^{p^m} \rangle \subseteq C$

$\therefore \qquad C = \langle b_1^{p^m} \rangle \ldots\ldots\ldots \langle b_{t-1}^{p^m} \rangle$

Also $\qquad x \in \langle b_1^{p^m} \rangle \cap \langle b_2^{p^m} \rangle \ldots\ldots\ldots \langle b_{t-1}^{p^m} \rangle$

$$\Rightarrow \; x \in B_1, \; x \in B_2 \ldots\ldots B_{t-1}$$
$$\Rightarrow \; x \in B_1, \; x \in B_2 \ldots\ldots B_{t-1} \, B_t \ldots\ldots B_l$$
$$\Rightarrow \; x = e.$$

Similarly for other intersections.

$\therefore \qquad C = \langle b_1^{p^m} \rangle \times \ldots\ldots \times \langle b_{t-1}^{p^m} \rangle$

Thus $\qquad o(C) = o(b_1^{p^m}) \ldots\ldots o(b_{t-1}^{p^m})$

$$= \frac{o(b_1)}{(p^m, o(b_1))} \ldots\ldots \frac{o(b_{t-1})}{(p^m, o(b_{t-1}))}$$

$$= \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m}$$

Now $\qquad G = A_1 \times \ldots\ldots \times A_k = \langle a_1 \rangle \times \ldots\ldots \times \langle a_k \rangle$ and $C \leq G$

$$\Rightarrow \quad C = \langle a_1^{p^m} \rangle \times \ldots\ldots \times \langle a_k^{p^m} \rangle$$

$$\Rightarrow \quad o(C) = \frac{o(a_1)}{(p^m, o(a_1))} \ldots\ldots \frac{o(a_k)}{(p^m, o(a_k))}$$

$$= \frac{p^{n_1}}{(p^m, p^{n_1})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

Since $\quad n_1 = h_1, \ldots\ldots, n_{t-1} = h_{t-1}$

$$o(C) = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

So,
$$\frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} = \frac{p^{h_1}}{p^m} \ldots\ldots \frac{p^{h_{t-1}}}{p^m} \cdot \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\Rightarrow \quad 1 = \frac{p^{n_t}}{(p^m, p^{n_t})} \ldots\ldots \frac{p^{n_k}}{(p^m, p^{n_k})}$$

$$\geq \frac{p^{n_t}}{(p^m, p^{n_t})}, \quad \text{as } \frac{p^{n_j}}{(p^m, p^{n_j})} \geq 1$$

$$> 1 \text{ as } n_t > m \Rightarrow (p^m, p^{n_t}) = p^m$$

$$\Rightarrow \quad \frac{p^{n_t}}{(p^m, p^{n_t})} = \frac{p^{n_t}}{p^m} = p^{n_t - m} > 1$$

a contradiction.

$\therefore \; n_i = h_i$ for all i

So, $\quad o(G) = o(A_1) \ldots\ldots o(A_k) = o(B_1) \ldots\ldots o(B_l)$

$$\Rightarrow \quad p^{n_1} \ldots\ldots p^{n_k} = p^{h_1} \ldots\ldots p^{h_t}$$

If $k > l$, $\quad p^{n_1} \ldots\ldots p^{n_t} p^{n_{t+1}} \ldots\ldots p^{n_k} = p^{h_1} \ldots\ldots p^{h_t}$.

$$\Rightarrow \quad p^{n_{l+1}} + p^{n_k} = 1 \text{ as } n_i = h_i \text{ for all } i$$

which is not true.

$\therefore$ k is not greater then l. similarly l is not greater than k.

$\therefore \qquad k = l.$

Remark : In theorem 13, $n_1, \ldots\ldots, n_k$ are uniquely determined but not the corresponding cyclic groups. For example, G = Klein's 4 group can be written in 2 ways as direct product of cyclic groups.

$$G = A \times B = A \times C, \text{ where } A = \{I, (12)(34)\}$$
$$B = \{I, (13)(24)\}, \quad C = \{I, (14)(23)\}$$

A beautiful application of theorem 13 is

Theorem 14 : *Two abelian groups of order p^n are isomorphic if and only if they have the same invariants.*

Proof : Suppose G, G' are finite abelian groups of order p^n. Let G and G' be isomorphic and θ be an isomorphism from G onto G'.

Let $\quad G = A_1 \times \ldots\ldots \times A_k, \; A_i = \langle a_i \rangle, \; o(A_i) = p^{n_i}$

Since θ is an isomorphism, $\theta(A_i)$ is normal subgroup of G' for all $i = 1, \ldots\ldots, k$.

$\therefore \; \theta(A_1) \ldots\ldots \theta(A_k)$ is a subgroup of G

Also
$$g' \in G' \Rightarrow \exists \; g \in G \text{ s.t. } \theta(g) = g$$
$$g \in G \Rightarrow g = x_1 \ldots\ldots x_k, \; x_i \in A_i$$
$$\Rightarrow g' = \theta(g) = \theta(x_1) \ldots\ldots \theta(x_k)$$
$$\in \theta(A_1) \ldots\ldots \theta(A_k)$$
$$\Rightarrow G' \subseteq \theta(A_1) \ldots\ldots \theta(A_k)$$
$$\Rightarrow G' = \theta(A_1) \ldots\ldots \theta(A_k)$$

Also, $\theta(A_1) \cap \theta(A_2) \ldots\ldots \theta(A_k) = \{e'\}$, e' = identity of G'

as $\quad x \in \theta(A_1), \; x \in \theta(A_2) \ldots\ldots \theta(A_k)$

$$\Rightarrow x = \theta(x_1) = \theta(x_2) \ldots\ldots \theta(x_k), \; x_i \in A_i$$
$$\Rightarrow \theta(x_1) = \theta(x_2 \ldots\ldots x_k)$$
$$\Rightarrow x_1 = x_2 \ldots\ldots x_k$$
$$\Rightarrow x_1^{-1} x_2 \ldots\ldots x_k = e$$
$$\Rightarrow x_i = e \text{ for all } i$$
$$\Rightarrow x = e.$$

Similarly for other intersections.

$\therefore \; G' = \theta(A_1) \times \ldots\ldots \times \theta(A_k)$. Since $A_i = \langle a_i \rangle$, $\theta(A_i) = \langle \theta(a_i) \rangle$.

So
$$o(\theta(A_i)) = o(\theta(a_i)) = o(a_i) \text{ for all } i$$
$$= p^{n_i} \text{ for all } i$$

Thus, G and G' have same invariants.

Conversely, suppose G and G' have same invariants.

Let $\quad G = A_1 \times \ldots\ldots \times A_k, \; a_i = \langle a_i \rangle$

Then $\quad G' = B_1 \times \ldots\ldots \times B_k, \; B_i = \langle b_i \rangle \; o(A_i) = o(B_i)$

as G and G' have same invariants.

But any two cyclic groups of same order are isomorphic. A_i and B_i are isomorphic for all i. So $A_1 \times \ldots\ldots \times Ak = G$ and $B_1 \times \ldots\ldots \times B_k = G'$ are isomorphic.

We are now in a position to specify the number of non isomorphic finite abelian groups of order p^n through

Theorem 15 : *The number of non isomorphic abelian groups of order p^n, p a prime, equals the number of partitions of n.*

Proof : Let G be an abelian group of order p^n.

By theorem 3, $G = A_1 \times \ldots\ldots \times A_k$, $A_i = \langle a_i \rangle$, $o(A_i) = p^{n_i}$

$$\therefore \quad o(G) = o(A_1) \ldots\ldots o(A_k)$$

$$\Rightarrow p^n = p^{n_1} \ldots\ldots p^{n_k} = p^{n_1 + \ldots\ldots + n_k}$$

$$\Rightarrow n = n_1 + \ldots\ldots + n_k, \quad n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$$

is a partition of n.

Conversely, consider any partition of n.

Let $\quad n = n_1 + \ldots\ldots + n_k, \quad n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$

be a partition of n.

Let A_i be a cyclic group of order p^{n_i} for all i.

Let $G = A_1 \times \ldots\ldots \times A_k$. Then G is an abelian group of order $p^{n_1 + \ldots\ldots + n_k} = p^n$.

Let $\mathbf{X}$ = set of all non isomorphic abelian groups of order p^n.

$\mathbf{Y}$ = set of all partitions of n.

Define $\theta : \mathbf{X} \to \mathbf{Y}$ as follows :

Let $G \in \mathbf{X}$. Let $G = A_1 \times \ldots\ldots \times Ak$, $A_i = \langle a_i \rangle$. $o(A_i) = p^{n_i}$.

Let $\theta(G) = n_1 + \ldots\ldots + n_k = n$

Clearly, θ is well defined.

Also $\quad \theta(G) = \theta(G')$

$$\Rightarrow n_1 + \ldots\ldots + n_k = m_1 + \ldots\ldots + m_l = n$$

$$\Rightarrow k = l, \; n_i = m_i \text{ for all } i$$

$\Rightarrow$ G and G' have same invariants

$\Rightarrow$ G and G' are isomorphic

$$\Rightarrow G = G'$$

$\Rightarrow$ θ is 1-1

Let $n = n_1 + \ldots\ldots + n_k$, $n_1 \geq n_2 \geq \ldots\ldots \geq n_k > 0$ be a partition of n. Then as seen above $G = A_1 \times \ldots\ldots \times A_k$, $A_i = \langle a_i \rangle$, $o(A_i) = p^{n_i}$ is an abelian group of order p^n and

$$\theta(G) = n_1 + \ldots\ldots + n_k$$

$\therefore \quad \theta$ is onto.

$\therefore \quad o(\mathbf{X}) = o(\mathbf{Y})$, which proves the result.

It is not difficult to prove that two finite abelian groups are isomorphic if and only if their Sylow subgroups are isomorphic. Now from theorem 15, we get

Theorem 16 : *Let $n = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r}$ where p_is are distinct primes. Then the number of non isomorphic abelian groups of order n is $p(\alpha_1)\ p(\alpha_2) \ldots\ldots p(\alpha_r)$ where $p(\alpha_i)$ denotes the number of partitions of α_i.*

Problem 35 : *Find all the non isomorphic abelian groups of order*

(*i*) 8 (*ii*) 6 (*iii*) 20.

Solution :

(*i*) Since $8 = 2^3$, the number of non isomorphic abelian groups of order 8 is given by $p(3)$, where $p(3)$ denotes the number of partitions of 3.

Since $p(3) = 3$ as $3 = 1+1+1$, $3 = 1+2$, $3 = 3$ are the only partitions of 3, we find the number of non isomorphic abelian groups of order 8 is 3. The groups will be

$$Z_8, \quad Z_2 \times Z_4, \quad Z_2 \times Z_2 \times Z_2$$

(*ii*) As $6 = 2^1 \times 3^1$, the number of non isomorphic abelian groups is $p(1)\,p(1) = 1 \,.\, 1 = 1$. The group being the cyclic group $Z_2 \times Z_3 \cong Z_6$.

(*iii*) As $20 = 2^2 \times 5^1$, the number of non isomorphic abelian groups of order 20 is given by

$$p(2)\ p(1) = 2\ .1 = 2$$

The groups being $Z_4 \times Z_5$, $Z_2 \times Z_2 \times Z_5$.

Exercises

1. Find all non isomorphic abelian groups of order

(*i*) 360 [6]

(*ii*) 15 [1]

(*iii*) 35 [1]

(*iv*) p^3, p a prime. [3]

Chapter 6

Rings

A group we noticed is a system with a non empty set and a binary composition One can of course talk about non empty sets with two binary compositions also, the set of the integers under usual addition and multiplication being an example. Though this set forms a group under addition and not under multiplication, it does have certain specific properties satisfied with respect to multiplication as well. We single out some of these and generalise the concept in the form of a ring. We start with the formal definition.

Definition : A non empty set R, together with two binary compositions $+$ and $\cdot$ is said to form a *Ring* if the following axioms are satisfied :

(*i*) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$

(*ii*) $a + b = b + a$ for all $a, b \in R$

(*iii*) $\exists$ some element 0 (called zero) in R, s.t., $a + 0 = 0 + a = a$ for all $a \in R$

(*iv*) for each $a \in R$, $\exists$ an element $(-a) \in R$, s.t., $a + (-a) = (-a) + a = 0$

(*v*) $a . (b . c) = (a . b) . c$ for all $a, b, c \in R$

(*vi*) $a . (b + c) = a . b + a . c$

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

Remarks : (*a*) Since we say that $+$ and $\cdot$ are binary compositions on R, it is understood that the closure properties w.r.t. these hold in R. In other words, for all $a, b \in R$, $a + b$ and $a . b$ are unique in R.

(*b*) One can use any other symbol instead of $+$ and $\cdot$, but for obvious reasons, we use these two symbols (the properties look so natural with these). In fact, in future, the statement that R is a ring would mean that R has two binary compositions $+$ and $\cdot$ defined on it and satisfies the above axioms.

(*c*) Axiom (*v*) is named associativity w.r.t. $\cdot$ and axiom (*vi*) is referred to as distributivity (left and right) w.r.t. $\cdot$ and $+$.

(*d*) Axioms (*i*) to (*iv*) could be restated by simply saying that $< R, + >$ forms an abelian group.

(*e*) Since 0 in axiom (*iii*) is identity w.r.t. +, it is clear that this element is unique (see groups).

Definitions : A ring R is called a *commutative* ring if $ab = ba$ for all $a, b \in R$.

Again if $\exists$ an element $e \in R$ s.t.,

$$ae = ea = a \quad \text{for all} \quad a \in R$$

we say, R is a ring with *unity*. Unity is generally denoted by 1. (It is also called unit element or multiplicative identity).

It would be easy to see that if unity exists in a ring then it must be unique.

Remark : We recall that in a group by a^2 we meant $a \,.\, a$ where '.' was the binary composition of the group. We continue with the same notation in rings as well. In fact, we also introduce similar notation for addition, and shall write na to mean $a + a + \ldots\ldots + a$ (n times), n being an integer.

Example 1. Sets of real numbers, rational numbers, integers form rings w.r.t. usual addition and multiplication. These are all commutative rings with unity.

Example 2. Set **E** of all even integers forms a commutative ring, without unity (under usual addition and multiplication).

Example 3 (*a*). Let M be the set of all 2×2 matrices over integers under matrix addition and matrix multiplication. It is easy to see that M forms a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, but is not commutative.

(*b*). Let M be set of all matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ over integers under matrix addition and multiplication. Then M forms a non commutative ring without unity.

Example 4. The set $Z_7 = \{0, 1, 2, 3, 4, 5, 6,\}$ forms a ring under addition and multiplication modulo 7. (In fact, we could take n in place of 7).

Example 5. Let F be the set of all continuous functions $f : \mathbf{R} \to \mathbf{R}$, where $\mathbf{R}$ = set of real numbers. Then F forms a ring under addition and multiplication defined by :

for any $f, g \in F$

$$(f+g)\ x = f(x) \qquad \text{for all } x \in R$$

$$(fg)\ x = f(x)\ g(x) \qquad \text{for all } x \in R$$

zero of this ring is the mapping $O : \mathbf{R} \to \mathbf{R}$, s.t.,

$$O(x) = 0 \qquad \text{for all } x \in R$$

Also additive inverse of any $f \in F$ is the function $(-f) : \mathbf{R} \to \mathbf{R}$ s.t., $(-f)\ x = -f\ (x)$

In fact, F would have unity also, namely the function $i : \mathbf{R} \to \mathbf{R}$ defined by $i(x) = 1$ for all $x \in R$.

Remark : Although the same notation fg has been used for product here it should not be mixed up with fog defined earlier.

Example 6. Let $\mathbf{Z}$ be the set of integers, then $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$ forms a ring under usual addition and multiplication of complex numbers. $a + ib$ where $a, b \in \mathbf{Z}$ is called a Gaussian integer and $\mathbf{Z}[i]$ is called the ring of Guassian integers.

Example 7. Let X be a non empty set. Then $p(X)$ the power set of X (i.e., set of all subsets of X) forms a ring under + and . defined by

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

$$A \,.\, B = A \cap B$$

In fact, this is a commutative ring with unity and also satisfies the property $A^2 = A$ for all $A \in p(X)$.

Example 8. Let M = set of all 2×2 matrices over members from the ring of integers modulo 2. *It would be a finite non commutative ring.* M would have $2^4 = 16$ members as each element a, b, c, d in matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ can be chosen in 2 ways. Compositions in M are given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \oplus x & b \oplus y \\ c \oplus z & d \oplus u \end{bmatrix}$$

where $\oplus$ denotes addition modulo 2 and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} a \otimes x \oplus b \otimes z & a \otimes y \oplus b \otimes u \\ c \otimes x \oplus d \otimes z & c \otimes y \oplus d \otimes u \end{bmatrix}$$

$\otimes$ being multiplication modulo 2.

That M is non commutative follows as $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ But

$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Example 9 : Let $R = \{0, a, b, c\}$. Define + and $\cdot$ on R by

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	a	b	c
b	0	a	b	c
c	0	0	0	0

Then one can check that R forms a non commutative ring without unity. In fact (see later on page 234) it is an example of the smallest non commutative ring.

Theorem 1 : *In a ring R, the following results hold*

(*i*) $a \,.\, 0 = 0 \,.\, a = 0$ for all $a \in R$

(ii) $a(-b) = (-a)b = -ab$ for all $a, b \in R$

(iii) $(-a)(-b) = ab$

(iv) $a(b-c) = ab - ac.$

Proof : (i) $a.0 = a.(0+0)$

$\Rightarrow a.0 = a.0 + a.0$

$\Rightarrow a.0 + 0 = a.0 + a.0$

$\Rightarrow 0 = a.0$

using cancellation w.r.t. + in the group $<R, +>$.

(ii) $a.0 = 0$

$\Rightarrow a(-b+b) = 0$

$\Rightarrow a(-b) + ab = 0$

$\Rightarrow a(-b) = -(ab)$

similarly $(-a)b = -ab.$

(iii) $(-a)(-b) = -[a(-b)] = -[-ab] = ab$

(iv) $a(b-c) = a(b+(-c))$

$= ab + a(-c)$

$= ab - ac.$

Remarks : (i) If R is a ring with unity and $1 = 0$, then since for any $a \in R$, $a = a.1 = a.0 = 0$, we find $R = \{0\}$ which is called the *trivial* ring. We generally exclude this case and thus whenever, we say R is a ring with unity, it will be understood that $1 \neq 0$ in R.

(ii) If n, m are integers and a, b elements of a ring, then it is easy to see that

$n(a+b) = na + nb$

$(n+m)a = na + ma$

$(nm)a = n(ma)$

$a^m a^n = a^{m+n}$

$(a^m)^n = a^{mn}$ (see under groups).

We are so much used to the property that whenever $ab = 0$ then either $a = 0$ or $b = 0$ that it may need more than a bit of convincing that the result may not always be true. Indeed in the ring of integers (or reals or rationals) this property holds. But if we consider the ring of 2×2 matrices over integers, we notice, we can have two non zero elements A, B s.t., $AB = 0$, but $A \neq 0$, $B \neq 0$. In fact, take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$ then $A \neq 0$, $B \neq 0$. But $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. We formalise this notion through

Definition : Let R be a ring. An element $0 \neq a \in R$ is called a *zero-divisor*, if $\exists$ an element $0 \neq b \in R$ s.t., $ab = 0$ or $ba = 0$.

Definition : A commutative ring R is called an *Integral domain* if $ab = 0$ in $R \Rightarrow$ either $a = 0$ or $b = 0$. In other words, a commutative ring R is called an integral domain if R has no zero divisors.

An obvious example of an integral domain is $< \mathbf{Z}, +, \cdot >$ the ring of integers whereas the ring of matrices, talked about above is an example of a ring which is not an integral domain.

Remark : Some authors do not insist upon the condition of commutativity as part of the definition of an integral domain. One can have (see examples 10, 11 ahead), non commutative rings without zero divisors.

The following theorem gives us a necessary and sufficient condition for a commutative ring to be an integral domain.

Theorem 2 : *A commutative ring R is an integral domain iff for all $a, b, c \in R$ $(a \neq 0)$*

$$ab = ac \Rightarrow b = c.$$

Proof : Let R be an integral domain

Let $\quad ab = ac \quad (a \neq 0)$

Then $\quad ab - ac = 0$

$\Rightarrow a(b - c) = 0$

$\Rightarrow a = 0$ or $b - c = 0$

Since $\quad a \neq 0$, we get $b = c$.

Conversely, let the given condition hold.

Let $a, b \in R$ be any elements with $a \neq 0$.

Suppose $\quad ab = 0$

then $\quad ab = a \,.\, 0$

$\Rightarrow b = 0$ using given condition

Hence $ab = 0 \Rightarrow b = 0$ whenever $a \neq 0$ or that R is an integral domain.

Remark : A ring R is said to satisfy *left cancellation law* if for all $a, b, c \in R$, $a \neq 0$

$$ab = ac \Rightarrow b = c.$$

Similarly we can talk of *right cancellation law.* It might, of course, be noted that cancellation is of only non zero elements.

Definition : An element a in a ring R with unity, is called invertible (or a *unit*) w.r.t. multiplication if $\exists$ some $b \in R$ such that $ab = 1 = ba$.

Notice, unit and unit element (unity) are different concepts and should not be confused with each other.

Definition : A ring R with unity is called a *Division ring* or a *skew field* if non zero elements of R form a group w.r.t. multiplication.

In other words, a ring R with unity is a Division ring if non zero elements of R have multiplicative inverse.

Definition : A commutative division ring is called a *field.*

Real numbers form a field, whereas integers do not, under usual addition and multiplication. Since a division ring (field) forms groups w.r.t. two binary compositions, it must contain two identity elements 0 and 1 (w.r.t. addition and multiplication) and thus a division ring (field) has at least two elements (see remark on page 223).

Example 10 : *A division ring which is not a field.* Let M be the set of all 2×2 matrices of the type $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ where a, b are complex numbers and $\bar{a}, \bar{b}$ are their conjugates, i.e., if $a = x + iy$ then $\bar{a} = x - iy$. Then M is a ring with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ under matrix addition and matrix multiplication.

Any non zero element of M will be $\begin{bmatrix} x+iy & u+iv \\ -(u-iv) & x-iy \end{bmatrix}$

where x, y, u, v are not all zero.

One can check that the matrix $\begin{bmatrix} \dfrac{x-iy}{k} & -\dfrac{u+iv}{k} \\ \dfrac{u-iv}{k} & \dfrac{x+iy}{k} \end{bmatrix}$

where $k = x^2 + y^2 + u^2 + v^2$, will be multiplicative inverse of the above non zero matrix, showing that M is a division ring. But M will not be a field as it is not commutative as

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

But $$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

Example 11 : Consider

$D = \{a + bi + cj + dk \mid a, b, c, d \in \mathbf{R}\}$ with $i^2 = j^2 = k^2 = -1$, then D forms a ring under multiplication.

Since $i = 0 + 1i + 0j + 0k$, $j = 0 + 0i + 1j + 0k$ gives $ij = k$, $ji = -k$, we find D is not commutative and hence is not a field. D has unity $1 = 1 + 0i + 0j + 0k$.

If $a + bi + cj + dk$ be any non zero element of D (i.e., at least one of a, b, c, d is non zero) then $(a + bi + cj + dk)\dfrac{(a - bi - cj - dk)}{a^2 + b^2 + c^2 + d^2} = 1.$

Hence D is a division ring but not a field.

Theorem 3 : *A field is an integral domain.*

Proof : Let $< R, +, \cdot >$ be a field, then R is a commutative ring.

Let $ab = 0$ in R. We want to show either $a = 0$ or $b = 0$. Suppose $a \neq 0$, then a^{-1} exists (definition of field)

thus $\quad ab = 0$

$$\Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow b = 0$$

which shows that R is an integral domain.

A 'partial converse' of the above result also holds.

Theorem 4 : *A non zero finite integral domain is a field.*

Proof : Let R be a non zero finite integral domain.

Let R' be the subset of R containing non zero elements of R.

Since associativity holds in R, it will hold in R'. Thus R' is a finite semi group.

Again cancellation laws hold in R (for non zero elements) and therefore, these hold in R'.

Hence R' is a finite semi group w.r.t. multiplication in which cancellation laws hold.

$\therefore$ $< R', \cdot >$ forms a group.

In other words $< R, +, \cdot >$ is a field (it being commutative as it is an integral domain).

Aliter : Let $R = \{a_1, a_2, \ldots\ldots, a_n\}$ be a finite non zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, \ldots\ldots, aa_n$ are all in R and if $aa_i = aa_j$ for some $i \neq j$, then by cancellation we get $a_i = a_j$ which is not true. Hence $aa_1, aa_2, \ldots, aa_n$ are distinct members of R.

Since $a \in R$, $a = aa_i$ for some i

Let $x \in R$ be *any* element, then $x = aa_j$ for some j

Thus $\quad ax = (aa_i)x = a(a_i x)$

i.e., $\quad x = a_i x$

Hence using commutativity we find

$$x = a_i x = x a_i$$

or that a_i is unity of R. Let $a_i = 1$

Thus for $1 \in R$, since $1 = aa_k$ for some k

We find a_k is multiplicative inverse of a. Hence any non zero element of R has multiplicative inverse or that R is a field.

Example 12 : An infinite integral domain which is not a field is the ring of integers.

Definition : A ring R is called a *Boolean ring* if $x^2 = x$ for all $x \in R$.

Example 13 : The ring $\{0, 1\}$ under addition and multiplication mod 2 forms a Boolean ring.

Problem 1 : *Show that a Boolean ring is commutative.*

Solution : Let $a, b \in R$ be any elements

Then $\quad a + b \in R \quad$ (closure)

By given condition

$$(a+b)^2 = a+b$$
$$\Rightarrow a^2+b^2+ab+ba = a+b$$
$$\Rightarrow a+b+ab+ba = a+b$$
$$\Rightarrow ab+ba = 0$$
$$\Rightarrow ab = -ba \qquad \text{..... (1)}$$
$$\Rightarrow a(ab) = a(-ba)$$
$$\Rightarrow a^2b = -aba$$
$$\Rightarrow ab = -aba \qquad \text{..... (2)}$$

Again (1) gives

$$(ab)a = -(ba)a$$
$$\Rightarrow aba = -ba^2 = -ba \qquad \text{..... (3)}$$

(2) and (3) give

$$ab = ba \qquad (= -aba)$$

or that R is commutative.

Problem 2 : *Show that an element a in Z_n is a unit iff a and n are relatively prime.*

Solution : $Z_n = \{0, 1, 2, \ldots\ldots, n-1\}$ mod n

Let $a \in Z_n$ be a unit, then $\exists\ b \in Z_n$ s.t.,

$$a \otimes b = 1$$

i.e., when ab is divided by n, remainder is 1, in other words,

$$ab = nq+1$$

or

$$ab - nq = 1$$

$\Rightarrow a$ and n are relatively prime.

Conversely, let $(a, n) = 1$, then $\exists$ integers u, v s.t.,

$$au + nv = 1$$
$$\Rightarrow au = n(-v) + 1$$

Suppose, $\quad u = nq + r, \quad 0 \le r < n, \quad r \in Z_n$

Then $\quad au = anq + ar = n(-v) + 1$

$$\Rightarrow ar = n(-v - aq) + 1, \qquad r \in Z_n$$

i.e., $\quad a \otimes r = 1, \qquad r \in Z_n$

i.e., $\quad a$ is a unit.

Problem 3 : *Show that $Z_p = \{0, 1, 2, \ldots\ldots, p-1\}$ modulo p is a field iff p is a prime.*

Solution : Let Z_p be a field. Suppose p is not a prime then $\exists\ a, b,$ such that $p = ab,\ 1 < a, b < p$

$\Rightarrow a \otimes b = 0$ where a, b are non zero $\Rightarrow Z_p$ has zero divisors.

i.e., Z_p is not an integral domain, a contradiction as Z_p being a field is an integral domain.

Hence p is prime.

Conversely, let p be a prime. We need show that Z_p is an integral domain (it being finite will then be a field).

Let $\quad a \otimes b = 0 \qquad a, b \in Z_p$

Then $\quad ab$ is a multiple of p

$$\Rightarrow p \mid ab$$

$$\Rightarrow p \mid a \text{ or } p \mid b \text{ (} p \text{ being prime)}$$

$$\Rightarrow a = 0 \text{ or } b = 0 \text{ (Notice } a, b \in Z_p \Rightarrow a, b < p)$$

$$\Rightarrow Z_p \text{ is an integral domain and hence a field.}$$

Problem 4 : *If in a ring R, with unity, $(xy)^2 = x^2y^2$ for all $x, y \in R$ then show that R is commutative.*

Solution : Let $x, y \in R$ be any elements

then $\quad y + 1 \in R$ as $1 \in R$

By given condition

$$(x(y+1))^2 = x^2(y+1)^2$$

$$\Rightarrow (xy + x)^2 = x^2(y+1)^2$$

$$\Rightarrow (xy)^2 + x^2 + 2yx + xxy = x^2 \ (y^2 + 1 + 2y)$$

$$\Rightarrow x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$$

$$\Rightarrow xyx = x^2y \qquad \text{.... (1)}$$

Since (1) holds for all x, y in R, it holds for $x + 1, y$ also. Thus replacing x by $x + 1$, we get

$$(x+1)\ y\,(x+1) = (x+1)^2y$$

$$\Rightarrow (xy + y)\ (x+1) = (x^2 + 1 + 2x)y$$

$$\Rightarrow x^2y + xy + yx + y = x^2y + y + 2xy$$

$$\Rightarrow yx = xy \quad \text{using (1)}$$

Hence R is commutative.

Problem 5 : *Show that the ring R of real valued continuous functions on* [0, 1] *has zero divisors.*

Solution : Consider the functions f and g defined on [0, 1] by

$$f(x) = \tfrac{1}{2} - x, \qquad 0 \le x \le \tfrac{1}{2}$$

$$= 0, \qquad \tfrac{1}{2} \le x \le 1$$

and

$$g(x) = 0, \qquad 0 \le x \le \tfrac{1}{2}$$

$$= x - \tfrac{1}{2}, \qquad \tfrac{1}{2} \le x \le 1$$

then f and g are continuous functions and $f \neq 0$, $g \neq 0$

whereas $$gf(x) = g(x)\ f(x) = 0.\left(\tfrac{1}{2} - x\right) \text{ if } 0 \leq x \leq \tfrac{1}{2}$$

$$= \left(x - \tfrac{1}{2}\right).0 = 0 \text{ if } \tfrac{1}{2} \leq x \leq 1$$

i.e., $$gf(x) = 0 \text{ for all } x$$

i.e., $$gf = 0 \text{ but } f \neq 0,\ g \neq 0.$$

Exercises

1. Show that a ring R is commutative iff
$$(a+b)^2 = a^2 + b^2 + 2ab \text{ for all } a,\ b \in R.$$
2. If in a ring R, $x^2 = x$ for all x then show that $2x = 0$ and $x + y = 0 \Rightarrow x = y$.
3. If R is a ring with unity and $(ab)^2 = (ba)^2$ for all $a,\ b \in R$ and $2x = 0 \Rightarrow x = 0$ then show that R is commutative.
4. Let **R** be the set of real numbers. Show that $\mathbf{R} \times \mathbf{R}$ forms a field under addition and multiplication defined by
$$(a, b) + (c, d) = (a + c,\ b + d)$$
$$(a, b).(c, d) = (ac - bd,\ ad + bc).$$
5. Let R be a commutative ring with unity. Show that
   (*i*) a is a unit iff a^{-1} is a unit.
   (*ii*) $a,\ b$ are units iff ab is a unit.
6. Show that set of all units in a commutative ring with unity forms an abelian group.
7. Give an example of a non commutative ring R in which $(xy)^2 = x^2y^2$ for all $x,\ y \in R$.
8. If $< R, +, \cdot >$ be a system satisfying all conditions in the definition of a ring with unity except $a + b = b + a$, then show that this condition is also satisfied.
9. Show that if $1 - ab$ is invertible in a ring with 1 then so is $1 - ba$.
10. Show that a finite commutative ring R without zero divisors has unity. (See theorem 4 page 55).

Sub Rings

Definition : A non empty subset S of a ring R is said to be a *subring* of R if S forms a ring under the binary compositions of R.

The ring $< \mathbf{Z}, +, \cdot >$ of integers is a subring of the ring $< \mathbf{R}, +, . >$ of real numbers,

If R is a ring then $\{0\}$ and R are always subrings of R, called *trivial* subrings of R.

It is obvious that a subring of an integral domain will be an integral domain.

In practice it would be difficult and lengthy to check all axioms in the definition of a ring to find out whether a subset is a subring or not. The following theorem would make the job rather easy.

Theorem 5 : *A non empty subset S of a ring R is a subring of R iff $a, b \in S \Rightarrow ab,\ a-b \in S$.*

Proof : Let S be a subring of R

then $$a,\ b \in S \Rightarrow ab \in S \text{ (closure)}$$
$$a,\ b \in S \Rightarrow a-b \in S$$

as $<S, +>$ is a subgroup of $<R, +>$.

Conversely, since $a,\ b \in S \Rightarrow a-b \in S$, we find $<S, +>$ forms a subgroup of $<R, +>$. Again for any $a,\ b \in S$, since $S \subseteq R$

$$a,\ b \in R$$
$$\Rightarrow a+b = b+a$$

and so we find S is abelian.

By a similar argument, we find that multiplicative associativity and distributivity hold in S.

In other words, S satisfies all the axioms in the definition of a ring.

Hence S is a subring of R.

Definition : A non empty subset of S of a field F is called a *subfield*, if S forms a field under the operations in F. Similarly, we can define a *subdivision ring* of a division ring.

One can prove that S will be a subfield of F iff $a, b \in S,\ b \neq 0 \Rightarrow a-b,\ ab^{-1} \in S$.

We may also notice here that a subfield always contains at least two elements, namely 0 and 1 of the field. (Recall a subgroup contains identity of the group and a subfield is a subgroup of the field under both the compositions).

Sum of Two Sub Rings

Definition : Let S and T be two subrings of a ring R. We define

$$S+T = \{s+t \mid s \in S,\ t \in T\}$$

then clearly $S+T$ is a non void subset of R. Indeed $0 = 0+0 \in S+T$.

But our enthusiasm of defining the sum ends here when we find that *sum of two subrings may not be a subring.*

Take for instance the ring M of 2×2 matrices over integers.

Let S = set of all matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ $a,\ b$ integers, and

T = set of all matrices of the type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$, x an integer.

Then S and T are subrings of M, (an easy exercise for the reader).

$S+T$ would have members of the type

$$\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} + \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$$

i.e., matrices of the type $\begin{bmatrix} a & c \\ b & 0 \end{bmatrix}$.

That $S+T$ does not form a subring follows from the fact that closure w.r.t. multiplication does not hold, as

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 2 \end{bmatrix} \notin S + T.$$

Definition : Let S be a subset of a ring R, then the smallest subring of R containing S is called the *subring generated* by S.

Since intersection of subrings is a subring (see exercises) it is clear that the subring generated by a subset S of R will be the intersection of all subrings of R, containing S. We denote it by $<S>$. Clearly then $<S> = \{0\}$ if $S = \varphi$.

Definition : Let R be a ring, the set

$Z(R) = \{x \in R \mid xr = rx \text{ for all } r \in R\}$

is called *centre* of the ring.

It is an easy exercise to show that $Z(R)$ is subring of R.

Problem 6 : *If R is a division ring then show that the centre $Z(R)$ of R is a field.*

Solution : $Z(R)$ is a ring (as it is a subring).

$Z(R)$ is commutative by its definition.

$Z(R)$ has unity as $1 . x = x . 1 = x$ for all $x \in R$.

Thus we need show that every non zero element of $Z(R)$ has multiplicative inverse (in $Z(R)$).

Let $x \in Z(R)$ be any non zero element.

Then $x \in R$ and since R is a division ring, $x^{-1} \in R$.

Let $y \in R$ be any non zero element, then $y^{-1} \in R$. Now

$$x^{-1} y = (y^{-1} x)^{-1}$$
$$= (xy^{-1})^{-1} = yx^{-1}$$

$\Rightarrow x^{-1}$ commutes with all non zero elements of R.

Again as $x^{-1} . 0 = 0 . x^{-1} = 0$

We find $\quad x^{-1} r = r . x^{-1}$ for all $r \in R$

$\Rightarrow x^{-1} \in Z(R)$

Showing that $Z(R)$ is a field.

Problem 7 : *If in a ring R, the equation $ax = b$ for all a, b $(a \neq 0)$ has a solution, show that R is a division ring.*

Solution : We first show that R has no zero divisors.

Suppose $\quad ab = 0, \ a \neq 0, \ b \neq 0$

as $a \neq 0$, $ax = a$ has a solution, say $x = e_1$,

then $\quad ae_1 = a.$

Again $bx = e_1$ has a solution, let $x = e_2$ be a solution of this, then $be_2 = e_1$,

Now
$$\begin{aligned} ab = 0 &\Rightarrow (ab)e_2 = 0 . e_2 = 0 \\ &\Rightarrow a(be_2) = 0 \\ &\Rightarrow ae_1 = 0 \\ &\Rightarrow a = 0, \text{ but } a \neq 0 \end{aligned}$$

Hence R is without zero divisors.

Now for any $a \neq 0$

$ax = a$ has a solution,

Let $\quad x = e$ be a solution then $ae = a$

$\Rightarrow aex = ax$ for all x

$\Rightarrow a(ex - x) = 0$ for all x

But $\quad a \neq 0 \Rightarrow ex - x = 0$ for all x

or that e is left identity.

Again,
$$\begin{aligned} (xe - x)\, e &= xee - xe = x(ee) - xe \\ &= xe - xe \text{ (as } e \text{ is left identity)} \\ &= 0 \end{aligned}$$

But $e \neq 0$, thus $xe - x = 0$ or $xe = x$ for all x

i.e., e is right identity.

Now equation $ax = e$ has a solution for all $a \neq 0 \Rightarrow \exists\, b$ s.t., $ab = e$.

Hence a has right inverse. Since right identity also exists, $< R, \cdot >$ forms a group or that R is a division ring.

Problem 8 : *Let R be the ring of 3×3 matrices over reals. Show that*

$$S = \left\{ \begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix} \middle| \, x \text{ real} \right\}$$ *is a subring of R and has unity different from unity of R.*

Solution : It is easy to check that S is a subring of R. Indeed

$$\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}\begin{bmatrix} y & y & y \\ y & y & y \\ y & y & y \end{bmatrix}=\begin{bmatrix} 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \\ 3xy & 3xy & 3xy \end{bmatrix}$$

which belongs to S.

Again since $\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}=\begin{bmatrix} x & x & x \\ x & x & x \\ x & x & x \end{bmatrix}$ we find

S has unity $\begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{bmatrix}$ which is different from unity $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ of R.

Remark : In continuation to the above problem we make the following observations.

(*a*) $<\mathbf{Z}, +, \cdot>$ has unity 1, but its subring $<\mathbf{E}, +, \cdot>$ of even integers has no unity.

(*b*) $<\mathbf{Z}, +, \cdot>$ has same unity 1 as that of its *parent* ring $<\mathbf{Q}, +, \cdot>$.

(*c*) Finally, we notice we can have a ring without unity which has a subring with unity. Take, for instance, the ring $R = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| \, a, b \in \mathbf{Z}\right\}$.

Now if $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ is unity of this ring, then

$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & a \\ 0 & 0 \end{bmatrix}$ should be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

i.e., $a = 1$

Also $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ should be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ i.e., $a = 1 = b$

Therefore, if R has unity then it must be $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

But $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\neq\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Hence R has no unity.

It is easy to check that $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| \, a, \in \mathbf{Z} \right\}$ is a subring of R and has unity $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Problem 9 : *Show that (i) Any ring of prime order is commutative.*

(ii) A ring of order p^2, (p a prime) may not be commutative.

(iii) Smallest non commutative ring is of order 4

(iv) A ring with unit of order p^2, (p a prime) is commutative.

Solution : (*i*) Let R be a ring of prime order p. Then $< R, + >$ is a cyclic group. Let $< R, + > = < a >$, then $o(a) = o(R) = p$. Let $x, y \in R$ be any elements, then $x = na$, $y = ma$ for some integers n, m.

Now $xy = (na)(ma) = nma^2 = mna^2 = (ma)(na) = yx$. Hence R is commutative.

(*ii*) Let R be the set of 2×2 matrices $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ over Z_2 with second row having zero entries. Then R is a ring under matrix addition and matrix multiplication. Since $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, we find R is non commutative and also it has $4 = 2^2$ elements.

(*iii*) Ring of order 1 being the zero ring is commutative. Rings of order 2 and 3 will be commutative by part (*i*). Thus, in view of part (*ii*), we find the smallest non commutative ring has order 4.

(*iv*) Let R be a ring with unity and be of order p^2. If $< R, + >$ is a cyclic group then R is commutative (part (*i*)). If $< R, + >$ is not cyclic then every non - zero element of $< R, + >$ is of prime order p. [order of an element divides order of the group and if order of an element equals order of the group then the group is cyclic].

Let e denote unity of R, then $o(e) = p$ (under addition)

Let $S = < e >$ be the subring of R, of order p.

Then $\quad S = \{e, 2e, \ldots\ldots, (p-1)e, pe = 0\}$, $o(S) = p$

Since $\quad o(R) = p^2$, $\exists \; a \in R$, s.t., $a \notin S$ and $o(a) = p$ under addition.

Let $T = \{a, 2a, \ldots\ldots, (p-1)a, pa = 0\}$ be the subring of R of order p. Every non zero element in T is of order p under addition.

If na belonging to T, $(n \neq 0)$ also belongs to S then the subring $< na > = T$ under addition is contained in S.

But $\quad o(T) = o(S)$ and thus $< na > = T = S$.

i.e., $\quad a \in S$, a contradiction.

Hence $\quad S \cap T = \{0\}$.

Also $\quad o(S+T) = \dfrac{o(S).o(T)}{o(S \cap T)} = p^2 = o(R),$

Thus $\quad R = S + T$

Let $\quad x, y \in R,$ then

$x = ne + ma, \; y = re + sa,$ where n, m, r, s are integers

Now $\quad xy = (nr)\; e + (ns)\; a + (mr)a + msa^2$

$= yx$

Showing that R is commutative,

Characteristic of a Ring

Definition : Let R be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then R is said to have *finite characteristic* and also the smallest such positive integer is called the characteristic of R.

If no such positive integer exists then R is said to have *characteristic zero* (or infinity).

Characteristic of R is denoted by char R or ch R.

If ch of a ring is n then ch of any subring or extension ring is also n.

Example 14 : (*a*) Rings of integers, even integers, rationals, are all of ch zero.

(*b*) Consider $R = \{0, 1\}$ mod 2

then ch $R = 2$ as

$$2 . 1 = 1 \oplus 1 = 0$$

$$2 . 0 = 0 \oplus 0 = 0$$

thus 2 is the least +ve integer s.t., $2a = 0$ for all $a \in R$.

Note $1 \otimes 1 = 1 \neq 0$

Similarly one can check that $R = \{0, 1, 2\}$ mod 3 has ch 3.

Theorem 6 : *Let R be a ring with unity. If 1 is of additive order n then ch $R = n$. If 1 is of additive order infinity then ch R is 0.*

Proof : Let additive order of 1 be n. Then $n . 1 = 0$ and n is such least +ve integer.

Now for any $x \in R$

$$nx = x + x + \ldots\ldots + x = 1.x + 1.x + \ldots\ldots + 1.x$$

$$= (1 + 1 + \ldots\ldots + 1)x = 0.x = 0$$

Showing that ch $R = n$.

If 1 has infinite order under addition then $\exists$ no n s.t., $n . 1 = 0$ and thus ch $R = 0$.

Remarks (*i*) : The above result can be stated as

If R is a ring with unity then R has ch $n > 0$ iff n is the smallest positive integer s.t., $n . 1 = 0$.

(*ii*) Ch of Z_n, ring of integers modulo n is n.

Theorem 7 : *If D is an integral domain, then characteristic of D is either zero or a prime number.*

Proof : If ch D is zero, we have nothing to prove. Suppose D has finite characteristic then $\exists$ a +ve integer m, s.t., $ma = 0$ for all $a \in D$.

Let k be such least +ve integer then ch $D = k$, we show k is a prime.

Suppose k is not a prime, then we can write

$$k = rs, \quad 1 < r, \ s < k$$

Now $\quad ka = 0 \quad$ for all $a \in D$

$$\Rightarrow (rs)\, a^2 = 0 \qquad \forall\, a \in D$$

$$\Rightarrow a^2 + a^2 + \ldots\ldots + a^2 = 0 \ (rs \text{ times})$$

$$\Rightarrow (\underbrace{a + a + \ldots\ldots + a}_{r \text{ times}})\,(\underbrace{a + a + \ldots\ldots + a}_{s \text{ times}}) = 0$$

$$\Rightarrow (ra)\,(sa) = 0 \qquad \forall\ a \in D$$

$$\Rightarrow ra = 0 \text{ or } sa = 0 \qquad \forall\ a \in D \ (D \text{ is an integral domain})$$

In either case it will be a contradiction as $r, s < k$, but k is the least +ve integer s.t., $ka = 0$.

Hence k is a prime.

Problem 10 : *If D is an integral domain and if $na = 0$ for some $0 \neq a \in D$ and some integer $n \neq 0$ then show that the characteristic of D is finite.*

Solution : Since $na = 0$

$$(na)x = 0 \text{ for all } x \in D$$

$$\Rightarrow (a + a + \ldots\ldots + a)\ x = 0$$

$$\Rightarrow ax + ax + \ldots\ldots + ax = 0 \ (n \text{ times})$$

$$\Rightarrow a(x + x + \ldots\ldots + x) = 0 \text{ for all } x \in D$$

$$\Rightarrow x + x + \ldots\ldots + x = 0 \text{ for all } x \in D \text{ as } a \neq 0$$

$$\Rightarrow nx = 0 \text{ for all } x \in D,\ n \neq 0$$

$$\Rightarrow \text{ch } D \text{ is finite.}$$

Problem 11 : *Let R be a finite (non zero) integral domain, then $o(R) = p^n$, where p is a prime.*

Solution : We first show that R has finite characteristic. Let $0 \neq a \in R$ be any element. Then $a, 2a, 3a, \ldots\ldots$ belong to R. Since R is finite, $ia = ja$ for some $i, j, i \neq j$.

Let $i > j$, then $(i - j)a = 0$

$\Rightarrow \exists$ some $k = i - j$ s.t., $ka = 0\ \forall\ a$ in R. Hence ch R is finite and it will be a prime. (Theorem 7).

Let ch $R = p$, a prime.

Let q be a prime dividing $o(R)$. Since $< R, + >$ is a group, by Cauchy's theorem, $\exists\, a \in R$, s.t., $o(a) = q$

Also $\quad \text{ch}\, R = p \Rightarrow pa = 0$

$$\Rightarrow o(a) \mid p$$

$$\Rightarrow q \mid p$$

$$\Rightarrow q = p \text{ as } p, q \text{ are primes.}$$

Thus p is the only prime dividing $o(R)$

$$\Rightarrow o(R) = p^n.$$

Cor. : (*i*) Order of a finite field is p^n for some prime p.

(*ii*) There cannot be an integral domain with order that is divisible by two distinct primes (i.e., we cannot have an integral domain with order n where n can be expressed as product of more than one prime). So we cannot have integral domains with 6 or 10 or 12 etc. elements.

Remark : A finite integral domain has finite ch. Whereas an infinite integral domain may have finite or zero ch. See example 8, page 314 under polynomial rings.

Definitions : An element e in a ring R is called *idempotent* if $e^2 = e$.

An element $a \in R$ is called *nilpotent* if $a^n = 0$ for some positive integer n.

If R is a ring with unity, then 0 and 1 are idempotent elements. Also 0 is nilpotent element of R.

Problem 12 : *A non zero idempotent cannot be nilpotent.*

Solution : Let x be non zero idempotent, then $x^2 = x$.

If x is also nilpotent then $\exists$ integer $n \geq 1$ s.t.,

$$x^n = 0$$

But $\quad x^2 = x \Rightarrow x^3 = x^2 = x$

$$\Rightarrow x^4 = x^2 = x$$

$$\Rightarrow x^n = x \Rightarrow x = 0 \text{ a contradiction.}$$

Problem 13 : *In an integral domain R (with unity) the only idempotents are the zero and unity.*

Solution : Let $x \in R$ be any idempotent

Then $\quad x^2 = x \Rightarrow x^2 - x = 0$

$$\Rightarrow x(x-1) = 0$$

$$\Rightarrow x = 0 \text{ or } x = 1 \text{ as } R \text{ is an integral domain.}$$

Problem 14 : *If R is a ring with no non zero nilpotent elements then show that for any idempotent e, $ex = xe$ for all $x \in R$ and thus $e \in Z(R)$.*

Solution : e idempotent $\Rightarrow e^2 = e$

Let $x \in R$ be any element, then

$$(exe - ex)^2 = exeexe - exeex - exexe + exex$$

$$= 0 \text{ (using } e^2 = e)$$

$$\Rightarrow exe - ex \text{ is nilpotent.}$$

By given condition, $exe - ex = 0 \Rightarrow exe = ex$

Similarly, we get $exe = xe$

Hence $ex = xe$.

Problem 15 : *Find all the idempotent and nilpotent elements of the ring Z_4.*

Solution : $Z_4 = \{0, 1, 2, 3\}$ mod 4.

Since $0 \otimes 0 = 0$, $1 \otimes 1 = 1$, $2 \otimes 2 = 0$, $3 \otimes 3 = 1$ we find 0 and 1 are the idempotents.

Again since $2^2 = 2 \otimes 2 = 0$, 2 is nilpotent.

0, of course, is nilpotent, 3 is not nilpotent as $3^3 = 3 \otimes 3 \otimes 3 = 3$, $3^4 = 3 \otimes 3 \otimes 3 \otimes 3 = 1$, $3^5 = 3$, it is clear no power of 3 will give zero.

Product of Rings

Let R_1 and R_2 be two rings.

Let $R = \{(a, b) \mid a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) . (a_2, b_2) = (a_1 a_2, b_1 b_2)$$

i.e., under the usual compositions of component wise addition and multiplication. This ring is called the *direct product* of R_1 and R_2. One can similarly extend the definition to product of more than two rings. R_1 and R_2 are called the *component rings* of the direct product.

Problem 16 : *If R and S are two rings, then*

$$ch\ (R \times S) = 0 \text{ if } ch\, R = 0 \text{ or } ch\, S = 0$$

$$= k \text{ where } k = l.c.m.\ (ch\, R,\ ch\, S)$$

Solution : Let $\text{ch}\, R = 0$ and suppose $\text{ch}\,(R \times S) = t \neq 0$

Then $t\ (a, b) = (0, 0) \quad \forall\, a \in R,\ b \in S$

$\Rightarrow (ta, tb) = (0, 0)$

$\Rightarrow ta = 0 \quad \forall\, a \in R$, a contradiction as $\text{ch}\, R = 0$

Thus $\text{ch}\ (R \times S) = 0$

Similarly, if $\text{ch}\, S = 0$, then $\text{ch}\,(R \times S) = 0$

Let now $\text{ch}\, R = m$, $\text{ch}\, S = n$ and let $k = l.c.m.\ (m, n)$

Then $k(a, b) = (ka, kb) = (0, 0)\ \forall\, a \in R,\ b \in S$

as m, n divide k

Suppose $p(a, b) = (0, 0)$, then $(pa, pb) = (0, 0)$

$$\Rightarrow pa = 0 = pb \Rightarrow m \mid p,\ n \mid p$$

$$\Rightarrow k \mid p \Rightarrow k \leq p \Rightarrow \text{ch}\,(R \times S) = k.$$

Exercises

1. Show that intersection of two subrings (subfields) is a subring (subfield).
2. Give an example to show that union of two subrings may not be a subring. Prove that union of two subrings is a subring iff one of them is contained in the other.
3. Prove that centre of a ring is a subring.
4. Let R be a ring, $a \in R$. Define $N(a) = \{r \in R \mid ar = ra\}$

   Show that $N(a)$, (called the normaliser of a in R) is a subring of R.
5. If S be a subring of a division ring R, show that $ab = 0$ in $S \Rightarrow$ either $a = 0$ or $b = 0$.
6. Let S be a subring of a ring R with unity 1. If $1 \neq e \in S$ be such that $ea = ae = a$ for all $a \in S$ then show that e is a zero divisor in R.
7. Show that any subring of $< \mathbf{Z}, +, \cdot >$ the ring of integers is of the type $n\mathbf{Z}$, $n \in \mathbf{Z}$.
8. Let S be a subring of a commutative ring R. For $a, b \in R$, we say a is congruent to b modulo $S[a \equiv b \pmod{S}]$ iff $a - b \in S$, $(a - b)r \in S$ for all $r \in R$. Show that this is an equivalence relation in R.
9. Let R be a commutative ring. If $a, b \in R$ are nilpotent then show that so are $a \pm b$ and ar for any $r \in R$. Give an example of a non commutative ring in which a, b are nilpotent but $a + b$ is not.
10. Let e be idempotent in a ring R. Show that the set $eRe = \{eae \mid a \in R\}$ is a subring of R with unity e.
11. Show that a field of characteristic zero is infinite.
12. Show that ch of a Boolean ring is 2. (See exercise 2 on page 229).
13. Show that if an element of a ring with unity has more than one right inverse then it has infinitely many.
14. Show that $S = \{0, 2, 4, 6, 8\}$ is a subring of Z_{10} with unity different from unity of Z_{10}.
15. Show that an integral domain R of order p^n, p a prime, has characteristic p.
16. Let R be a ring with ch n. If M is the ring of 2×2 matrices over R then show that ch $M = n$.
17. Let R be a commutative ring with unity. Show that

    (*i*) If $a \in R$ is a unit then a is not nilpotent.

    (*ii*) If $x \in R$ is nilpotent then $1 + x$ is a unit.

    (*iii*) The sum of a nilpotent element and a unit is a unit.
18. In a ring without unity, show that every idempotent is a zero divisor but not nilpotent.
19. If a finite field of ch p has q elements then show that $q = p^n$ for some n.

Ideals

The notion of an ideal in a ring is parallel to the concept of a normal subgroup in groups. The normal subgroups led us to the formation of quotient groups, ideals do the job when we define quotient rings. Many analogous results follow. We start with

Definition : A non empty subset I of a ring R is called a *right ideal* of R if

(*i*) $a, b \in I \Rightarrow a - b \in I$

(*ii*) $a \in I,\ r \in R \Rightarrow ar \in I.$

I is called a *left ideal* of R if

(*i*) $a, b \in I \Rightarrow a - b \in I$

(*ii*) $a \in I,\ r \in R \Rightarrow ra \in I.$

I is called a two sided or both sided ideal of R, if it is both left and a right ideal. In fact, if we say I is an ideal of R, it would mean, I is two sided ideal of R.

Example 15 : In a ring R, $\{0\}$ and R are always both sided ideals.

Any ideal except these two is called a proper ideal (In fact, the name non trivial ideal will be more appropriate).

Example 16 : Let $< \mathbf{Z}, +, \cdot >$ be the ring of integers. Then

$\mathbf{E}$ = set of even integers is an ideal of $\mathbf{Z}$

$a, b \in \mathbf{E} \Rightarrow a = 2n, b = 2m$

Thus $\qquad a - b = 2\ (n - m) \in \mathbf{E}$

Again, if $2n \in \mathbf{E},\ r \in \mathbf{Z}$ then as

$(2n)r$ or $r(2n)$ are both in $\mathbf{E}$, $\mathbf{E}$ is an ideal.

Example 17 : Let R = ring of 2×2 matrices over integers.

Let $A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle| \ a, b \text{ integers} \right\}$

then A is a right ideal of R as

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in A$$

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & y \\ z & u \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bu \\ 0 & 0 \end{bmatrix} \in A$$

But A is not a left ideal of R as

$$\begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \in I, \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R$$

But $$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix} \notin A.$$

Example 18 : In the same ring as above, one can check that $B = \left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| \, a, b \text{ integers}\right\}$ forms a left (but not a right) ideal of R.

We shall encounter many more examples of ideals in the due course. Looking at the conditions in the definition of an ideal and a subring, one feels, the two are rather closely related. In fact it is easy to see that *an ideal is always a subring.*

Let I be an ideal of a ring R. To show that I is a subring we need show that for $a, b \in I$, $ab \in I$.

Now $\quad a, b \in I \Rightarrow a \in I, \; b \in I \subseteq R$

$$\Rightarrow ab \in I \text{ (def. of ideal)}$$

Hence I is a subring.

Example 19 : A subring may not be an ideal.

We know that $< \mathbf{Z}, +, \cdot >$ is a subring of $< \mathbf{Q}, +, \cdot >$ where $\mathbf{Z}$ = integers, $\mathbf{Q}$ = rationals.

$3 \in \mathbf{Z}, \frac{1}{5} \in \mathbf{Q}$. But $3 \cdot \frac{1}{5} \notin \mathbf{Z}$.

Thus $\mathbf{Z}$ is not an ideal.

We have been talking about intersection and union of subgroups, subrings etc. Similar results hold in case of ideals. Reader is referred to the exercises. It would, of course, be interesting to ask a question at this point :

What can we say about intersection of a left and a right ideal? Will it be an ideal? The answer is in the negative.

If we consider the ideals in example 17, 18, we find $A \cap B$ would have members of the type $\left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| \, a, \text{ an integer}\right\}$.

Since $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin A \cap B$

we notice $A \cap B$ is not a right ideal.

Problem 17 : *Let S be a non empty subset of a ring R. Show that $r(s) = \{x \in R \mid Sx = 0\}$ and $l(s) = \{x \in R \mid xS = 0\}$ are respectively right and left ideals of R.*

Solution : $r(s) \neq \varphi$ as $0 \in r(s)$

Again, $\quad x, y \in r(s) \Rightarrow sx = 0, sy = 0$

Now $\quad S(x - y) = Sx - Sy = 0 - 0 = 0$

$$\Rightarrow x - y \in r(s)$$

Again, if $r \in R$ be any element then

$$S(xr) = (Sx)r = 0 \cdot r = 0$$

$$\Rightarrow xr \in r(s)$$

Hence $r(s)$ is a right ideal. Similarly, $l(s)$ will form a left ideal.

$r(s)$ and $l(s)$ are called right and left *annihilators* of S, respectively.

$r(s)$ and $l(s)$ would both be ideals of R if S is an ideal. (Verify!)

Problem 18 : *Let R be a ring such that every subring of R is an ideal of R. Further, $ab = 0$ in $R \Rightarrow a = 0$ or $b = 0$. Show that R is commutative.*

Solution : Let $0 \neq a \in R$ be any element.

Then $N(a) = \{x \in R \mid xa = ax\}$ is a subring of R and, therefore, an ideal of R.

Let $r \in R$ be any element. Since $a \in N(a)$, $r \in R$ we find $ra \in N(a)$ (Def. of ideal)

Also then, $\quad a(ra) = (ra)a$

and so $\quad (ar - ra)a = 0$

$\Rightarrow \quad ar - ra = 0 \quad$ as $a \neq 0$

Thus $\quad ar = ra \quad \forall\, r \in R,\ \forall\ 0 \neq a \in R$

and as $0.r = r.0 = 0$ we find

$$ar = ra \qquad \forall\, a,\ r \in R$$

Hence R is commutative.

Sum of Two Ideals

Let A and B be two ideals of a ring R. We define $A + B$ to be the set $\{a + b \mid a \in A,\ b \in B\}$ called sum of the ideals A and B.

Theorem 8 : *If A and B are two ideals of R then $A + B$ is an ideal of R, containing both A and B.*

Proof : $A + B \neq \varphi$ as $0 = 0 + 0 \in A + B$

Again, $\quad x,\ y \in A + B$

$$\Rightarrow x = a_1 + b_1$$
$$y = a_2 + b_2 \quad \text{for some } a_1, a_2 \in A;\ b_1, b_2 \in B$$

Since
$$x - y = (a_1 + b_1) - (a_2 + b_2)$$
$$= (a_1 - a_2) + (b_1 - b_2)$$

we find $\quad x - y \in A + B$

Let $x = a + b \in A + B$, $r \in R$ be any elements then

$$xr = (a + b)r = ar + br \in A + B \quad \text{as } A,\ B \text{ are ideals}$$
$$rx = r(a + b) = ra + rb \in A + B$$

Thus $A + B$ is an ideal of R.

Again for any $a \in A$, since $a = a + 0 \in A + B$ and for any $b \in B$, since $b = 0 + b \in A + B$

we find $\quad A \subseteq A + B$

$$B \subseteq A + B.$$

Remarks : (*i*) We can show that A is an ideal of $A + B$.

$a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$ as A is an ideal of R. Again, if $a \in A$ and $s \in A + B$ be any elements then $s = a_1 + b_1$ for some $a_1 \in A$, $b_1 \in B$

also $\quad as = a(a_1 + b_1)$

$$= aa_1 + ab_1 \in A$$

as $\quad a, a_1 \in A \Rightarrow aa_1 \in A$

$$a \in A, \ b_1 \in B \subseteq R \Rightarrow ab_1 \in A$$

$$\Rightarrow aa_1 + ab_1 \in A$$

Similarly, $sa \in A$. Showing that A is an ideal of $A + B$.

(*ii*) If A is a left ideal and B, a right ideal of R then $A + B$ may not be an ideal of R.

Considering the same ideals as in examples 17, 18, we find

$A + B$ will have members of the type $\begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$

and as $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 \\ 2 & 2 \end{bmatrix} \notin A + B$

$A + B$ is not an ideal of R.

Definition : Let S be any subset of a ring R. An ideal A of R is said to be generated by S if

(*i*) $S \subseteq A$

(*ii*) for any ideal I of R, $S \subseteq I \Rightarrow A \subseteq I$.

We denote it by writing $A = \langle S \rangle$ or $A = (S)$.

In fact $\langle S \rangle$ will be intersection of all ideals of R that contain S, and is the smallest ideal containing S. If S in finite, we say $A = \langle S \rangle$ is finitely generated.

If $S = \varphi$ then as $\{0\}$ is an ideal of R containing $S = \varphi$, $\langle S \rangle \subseteq \{0\}$ and so $\langle S \rangle = \{0\}$.

If $S = \{a\}$ then we denote $\langle S \rangle$ by $\langle a \rangle$ or (a) and this case is of special interest to us as it is used rather extensively. By definition, $a \in \langle a \rangle$ and as it is an ideal, elements of the type ra, as, $r_1 a s_1$, na are in $\langle a \rangle$, where $r, r_1, s, s_1 \in R$ and n is an integer. Such an ideal is called a *principal ideal* generated by a. (See later also). One can verify that

(*i*) If R is a commutative ring, then

$$\langle S \rangle = \{\sum n_i x_i + \sum r_j y_j \mid n_i \in \mathbf{Z}, \ r_j \in R, \ x_i, y_j \in S\}$$

(*ii*) If R is commutative with unity then

$$\langle S \rangle = \{\sum r_j y_j \mid r_j \in R, y_j \in S\}$$

(*iii*) If $S = \{a\}$, then

$$\langle a \rangle = \langle S \rangle = \{na + ra + as + xay \mid n \in \mathbf{Z}, \ r, s, x, y \in R\}$$

(*iv*) Further if R has unity

$< a > = \{\sum xay \mid x, y \in R\}$

Summations being finite everywhere.

Theorem 9 : *If A and B be two ideals of a ring R, then*

$$A + B = < A \cup B >.$$

Proof : We have already proved that $A + B$ is an ideal of R, containing A and B, thus $A + B$ is an ideal containing $A \cup B$.

Let I be any ideal of R, s.t., $A \cup B \subseteq I$

Let $x \in A + B$ be any element

Then $x = a + b$ for some $a \in A$, $b \in B$

Since $a \in A \subseteq A \cup B \subseteq I$

$b \in B \subseteq A \cup B \subseteq I$

we find $a + b \in I$ as I is an ideal

$\Rightarrow x \in I$ or that $A + B \subseteq I$

which proves the theorem.

Thus $A + B$ is the smallest ideal of R, containing A & B. One can, of course, talk about sum of more than two ideals in the same manner.

Problem 19 : *If $a \in R$ be an element and $I = \{ar \mid r \in R\}$ where R is a commutative ring, then I is an ideal of R.*

Solution : $I \neq \varphi$ as $0 = a.0 \in I$

$x, y \in I \Rightarrow x = ar_1, y = ar_2$ for some $r_1, r_2 \in R$

$\Rightarrow x - y = a(r_1 - r_2) \in I$

again if $x = ar_1 \in I$ and $r \in R$ be any elements

then $xr = (ar_1)r = a(r_1 r) \in I$ shows that I is a right ideal. R being commutative, it will be both sided ideal.

Remark : If the ring is not commutative, one can show that aR is a right ideal and $Ra = \{ra \mid r \in R\}$ is a left ideal of R. (See exercises)

aR is always contained in $< a >$. If R is a commutative ring with unity then $aR = Ra = (a)$.

Let us understand the difference between aR and $< a >$ through the following example.

Example 20 : Let $(\mathbf{E}, +, \cdot)$ be the ring of even integers. It is commutative ring without unity. Let $a = 4 \in \mathbf{E}$.

Then
$$< 4 > = \{4n + (2m)\, 4 \mid n, m \in \mathbf{Z}\}$$
$$= \{4n + 8m \mid n, m \in \mathbf{Z}\}$$

whereas

$$4\mathbf{E} = \{4\,(2k) \mid k \in \mathbf{Z}\} = \{8k \mid k \in \mathbf{Z}\}$$

We notice then, $< 4 > \neq 4\mathbf{E}$ as $4 \in < 4 >$ but $4 \notin 4\mathbf{E}$.

Problem 20 : *If A is an ideal of a ring R with unity such that $1 \in A$ then show that $A = R$.*

Solution : Since $A \subseteq R$ always, all we need show is that $R \subseteq A$.

Let $r \in R$ be any element.

Since $1 \in A$ and A is an ideal

$$r = 1 . r \in A$$

$$\Rightarrow R \subseteq A \text{ or that } A = R.$$

Problem 21 : *Let L be a left ideal of a ring R and let*

$$\lambda(L) = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$$

then show that $\lambda(L)$ is an ideal of R.

Solution : $\lambda(L) \neq \varphi$ as $0.a = 0$ for all $a \in L$

$$\Rightarrow 0 \in \lambda(L)$$

$$x, y \in \lambda(L) \Rightarrow xa = 0, \ ya = 0 \text{ for all } a \in L$$

$$\Rightarrow (x - y)a = xa - ya = 0 - 0 = 0 \text{ for all } a \in L$$

$$\Rightarrow x - y \in \lambda(L)$$

Again, if $x \in \lambda(L)$, $r \in R$ be any elements, then

$$xa = 0 \text{ for all } a \in L$$

Now $\quad (rx)a = r(xa) = r.0 = 0$ for all $a \in L$

$$\Rightarrow rx \in \lambda(L)$$

$$\Rightarrow \lambda(L) \text{ is a left ideal of } R.$$

Also $\quad (xr)\,a = x(ra) \qquad r \in R, \ a \in L$

$$= 0 \text{ for all } a \in L \Rightarrow ra \in L$$

$$\Rightarrow xr \in \lambda(L)$$

$$\Rightarrow \lambda(L) \text{ is a right ideal of } R.$$

Problem 22 : *Show by means of an example that we can find $A \subseteq B \subseteq R$ where A is an ideal of B, B is an ideal of R, but A is not an ideal of R.*

Solution : Let R be the set containing matrices of the type $\begin{bmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{bmatrix}$ over integers,

then R forms a ring under matrix addition and multiplication.

Take $\quad A = \left\{ \begin{bmatrix} 0 & 0 & x \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \middle| \ x \text{ an integer} \right\}$

$$B = \left\{ \begin{bmatrix} 0 & 0 & u \\ 0 & 0 & v \\ 0 & 0 & 0 \end{bmatrix} \middle| \ u, v \text{ integers} \right\}$$

It would be easy to verify that A is an ideal of B, B is an ideal of R.

To see that A is not an ideal of R, we notice,

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \notin A.$$

Product of two Ideals

Let A, B be two ideals of a ring R. We define the product AB of A and B by

$$AB = \{\sum a_i b_i \mid a_i \in A,\ b_i \in B\}$$

where summation is finite.

Theorem 10 : *The product AB of any two ideals A & B of a ring R is an ideal of R.*

Proof : $AB \neq \varphi$ as $0 = 0 \,.\, 0 \in AB$

Let $x, y \in AB$ be any two members

then $$x = a_1 b_1 + a_2 b_2 + \ldots\ldots + a_n b_n$$
$$y = a'_1 b'_1 + \ldots\ldots + a'_m b'_m$$

for some $a_i, a'_j \in A$, $b_i, b'_j \in B$

$$x - y = (a_1 b_1 + \ldots\ldots + a_n b_n) - (a'_1 b'_1 + \ldots\ldots + a'_m b'_m)$$

which clearly belongs to AB, as the R.H.S. can be written as

$$x_1 y_1 + x_2 y_2 + \ldots\ldots + x_k y_k \qquad (k = n + m)$$

where $x_i \in A$, $y_i \in B$.

Again, for any $x = a_1 b_1 + \ldots\ldots + a_n b_n \in AB$ and $r \in R$,

$$rx = r\,(a_1 b_1 + \ldots\ldots + a_n b_n)$$
$$= (ra_1)\, b_1 + (ra_2)\, b_2 + \ldots\ldots + (ra_n)\, b_n \in AB$$

because $ra_i \in A$ as $a_i \in A$, $r \in R$, and A is an ideal.

Similarly $xr \in AB$

showing thereby that AB is an ideal of R.

Remarks (*i*) : Let $S = \{ab \mid a \in A,\ b \in B\}$

then $< S > = AB$.

Clearly $S \subseteq AB$ and as AB is an ideal, $< S > \subseteq AB$.

Again, $x \in AB \Rightarrow x = \Sigma a_i b_i,\ a_i \in A,\ b_i \in B$

$$a_i \in A,\ b_i \in B \Rightarrow a_i b_i \in S,\ \forall\, i = 1, 2, \ldots,$$
$$\Rightarrow a_i b_i \in < S > \ \forall\, i$$
$$\Rightarrow x \in < S >$$
$$\Rightarrow AB \subseteq < S >$$

and hence $< S > = AB$.

(*ii*) If R is a commutative ring with unity and A, B are finitely generated ideals of R then so are $A + B$ and AB. In fact if $A = < a_1, a_2, \ldots\ldots, a_n >$ and $B = < b_1, b_2, \ldots\ldots, b_s >$ then

$$A + B = < a_1, a_2, \ldots\ldots, a_r, b_1, b_2, \ldots\ldots, b_s >$$

$$AB = < a_1 b_1, \ldots\ldots, a_1 b_s, \ldots\ldots, a_r b_1, \ldots\ldots, a_r b_s >$$

This, however, may not be true for $A \cap B$. See exercises ahead.

The following problem gives us little more information about product of ideals.

Problem 23 : *If A is a left and B is a right ideal of a ring R then show that AB is a two sided ideal of R whereas BA need not be even a one-sided ideal of R.*

Solution : That AB will be a two sided ideal of R follows by the theorem above. We show by an example that BA need not be even a one-sided ideal.

Take $$A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle| \, a, b, \in \mathbf{Z} \right\}$$

$$B = \left\{ \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \middle| \, c, d, \in \mathbf{Z} \right\}$$

in the ring R of 2×2 matrices over integers then as seen earlier A is left and B is a right ideal of R.

BA would have members of the type $\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$

i.e., of the type $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, $x \in \mathbf{Z}$

Now if we take $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ in BA and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ in R

then $$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin BA$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin BA$$

Hence BA is neither a left nor a right ideal of R.

Problem 24 : If A, B, C are ideals of a ring R, s.t., $B \subseteq A$ then show that $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

Solution : Let $x \in A \cap (B + C)$ be any element

Then $x \in A$ and $x \in B + C$

$\Rightarrow x = b + c$ for some $b \in B,\ c \in C$

Now $b \in B \subseteq A$, also $b + c = x \in A$

$\Rightarrow (b + c) - b \in A$

$\Rightarrow c + b - b \in A$

$\Rightarrow c \in A$

$\Rightarrow x \in A \cap C$

i.e., $x = b + c,\ b \in B,\ c \in A \cap C$

thus $x \in B + (A \cap C)$

Hence $A \cap (B + C) \subseteq B + (A \cap C)$.

Again let $x \in B + (A \cap C)$

Then $x = b + k$ for some $b \in B,\ k \in A \cap C$

Since $b \in B,\ k \in C$

$x = b + k \in B + C$

and $b \in B \subseteq A,\ k \in A \Rightarrow b + k \in A$

$\Rightarrow x \in A$

$\Rightarrow x \in A \cap (B + C)$

or that $B + (A \cap C) \subseteq A \cap (B + C)$

which finally gives $A \cap (B + C) = B + (A \cap C)$

Also as $B \subseteq A,\ A \cap B = B$

thus $A \cap (B + C) = (A \cap B) + (A \cap C) = B + (A \cap C)$.

Remark : The above is sometimes called modular equality. See exercises also.

Definition : A ring $R \neq \{0\}$ is called a *simple ring* if R has no ideals except R and $\{0\}$.

Theorem 11 : *A division ring is a simple ring.*

Proof : Let R be a division ring. Let A be any ideal of R s.t., $A \neq \{0\}$ then $\exists$ at least one $a \in A$ s.t., $a \neq 0$. R being a division ring, $a^{-1} \in R$ and $aa^{-1} = 1$.

Since $a \in A,\ a^{-1} \in R,\ aa^{-1} \in A$ (def. of ideal)

$\Rightarrow 1 \in A$

$\Rightarrow A = R$ (see problem 20)

i.e., only ideals that R can have are R and $\{0\}$ or that R is a simple ring.

Problem 25 : *Let R be a ring with unity, such that R has no right ideals except $\{0\}$ and R. Show that R is a division ring.*

Solution : All that we need prove is that non zero elements of R form a group under multiplication.

Let $0 \neq a \in R$ be any non zero element.

Let $aR = \{ar \mid r \in R\}$

Then aR is a right ideal. See problem 19.

By given condition, then

$$aR = R$$

or $$aR = \{0\}$$

But $aR \neq \{0\}$ as $a \neq 0$ and $a = a \,.\, 1 \in aR$

Hence $aR = R$.

Now $1 \in R \Rightarrow 1 \in aR \Rightarrow \exists\, b \in R$, s.t., $1 = ab \Rightarrow b$ is right inverse of a (w.r.t. multiplication). Thus $< R - \{0\}, . >$ is a system in which associativity holds, right identity (unity) and right inverse exist (for every element).

i.e., $< R - \{0\}, . >$ forms a group or that R is a division ring.

Problem 26 : *Let R be a ring having more than one element such that $aR = R$, for all $0 \neq a \in R$. Show that R is a division ring.*

Solution : We first show that $xy = 0 \Rightarrow x = 0$ or $y = 0$ in R.

So let $xy = 0$ and suppose $x \neq 0$, $y \neq 0$

Then $$xR = yR = R$$

Also $$(xy)R = x(yR) = xR = R$$

$$\Rightarrow R = \{0\} \text{ as } xy = 0$$

contradicting that R has more than one element.

Hence our assertion is proved.

Again, as $R \neq \{0\}$, $\exists\, 0 \neq a \in R$ and by given condition then $aR = R$

$$\Rightarrow \exists\, e \in R \text{ s.t., } ae = a \qquad (e \neq 0 \text{ as } a \neq 0)$$

$$\Rightarrow ae^2 = ae$$

$$\Rightarrow a(e^2 - e) = 0$$

$$\Rightarrow e^2 = e \text{ as } a \neq 0.$$

We claim e is right unity of R.

If e is not right unity of R, then $\exists\, y \in R$ s.t., $ye \neq y$

But $(ye - y)\, e = ye^2 - ye = ye - ye = 0$

$\Rightarrow$ either $ye = y$ or $e = 0$, a contradiction

$\Rightarrow$ e is right unity of R.

Let $0 \neq a \in R$ be any element then $aR = R$

Now $e \in R$, $aR = R$

$\Rightarrow e \in aR \Rightarrow \exists\, b \in R$, s.t., $e = ab$

or that b is right inverse of a.

$\Rightarrow$ every non zero element of R has right inverse.

Hence R is a division ring.

Problem 27 : *Let R be a ring such that R and $\{0\}$ are the only right ideals of R. Show that either R is a division ring or has prime number of elements such that $ab = 0$ for all $a, b \in R$.*

Solution : Let $I = \{a \in R \mid aR = \{0\}\}$

then I is a right ideal of R (Verify).

By given condition then either $I = \{0\}$ or $I = R$.

If $I = \{0\}$ then $aR = \{0\}$ only when $a = 0$.

In other words, $aR = R$, for all $0 \neq a \in R$. (Notice aR is a right ideal).

Thus by previous problem, R is a division ring. (Note in this case R has more than one element, as if $R = \{0\}$ then $R = I$, which is the next case).

Now suppose $I \neq R$, then $aR = \{0\}$ for all $a \in R$

$$\Rightarrow ar = 0 \text{ for all } a, r \in R$$

If S be any subgroup of $< R, + >$ then S will be a right ideal of R ($a \in S \subseteq R$, $r \in R \Rightarrow ar = 0 \in S$). By given condition R has only two right ideals R and $\{0\}$. Thus $< R, + >$ can have only two subgroups namely R and $\{0\}$.

$\Rightarrow < R, + >$ is a cyclic group of prime order (see Groups)

Thus R has prime number of elements (and as seen above $ab = 0$ for all $a, b \in R$).

Exercises

1. Show that intersection of two ideals is an ideal.
2. Give an example to show that union of two ideals may not be an ideal.
3. Prove that union of two ideals is an ideal iff one of them is contained in the other.
4. If an ideal is contained in union of two ideals then show that it is wholly contained in one of them.
5. Show that a ring cannot be expressed as a union of two proper ideals, but it is possible to express it as a union of three proper ideals.
6. Let R be the ring of 2×2 matrices over integers. If $a = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in R$, then show that aR is not a left ideal of R.
7. If A is an ideal of a ring R, let
$$[R : A] = \{x \in R \mid rx \in A \text{ for all } r \in R\}$$
Show that $[R : A]$ is an ideal of R, containing A.
8. Let R be a non commutative ring with unity. Show that $Z(R)$, the centre of R is not an ideal of R. [Hint : $Z(R)$ is properly contained in R].
9. If A, B, C are three ideals of a ring R then show that
$$A(BC) = (AB)C.$$
10. If A, B be two ideals of a ring R then show that $AB \subseteq A \cap B$. Give an example to show that $\exists$ ideals A, B s.t., $AB \neq A \cap B$.
11. If A, B, C are ideals of a ring R, then show that

(*i*) $A(B + C) = AB + AC$.

(*ii*) $(A + C)(B + C) \subseteq AB + C$.

(*iii*) $(A \cap B)(A + B) \subseteq AB$.

12. If A, B are two ideals of a ring R s.t., $A \cap B = \{0\}$ then the sum $A + B$ is called direct sum of A & B and is denoted by $A \oplus B$. Show that each element of $A \oplus B$ is uniquely expressible as $a + b$ for $a \in A$, $b \in B$.

13. If F is a field, prove that its only ideals are $\{0\}$ and F.

14. If R be a commutative ring with unity whose only ideals are $\{0\}$ and R, then show that R is a field. (See problem 25).

15. Show that if an ideal A of a ring R with unity contains a unit of R then $A = R$.

16. Let A, B be two subrings of a ring R such that for all $a \in A$, $b \in B$, $ba \in A$ then show that

(*i*) $A + B$ is a subring of R.

(*ii*) A is an ideal of $A + B$.

(*iii*) $A \cap B$ is an ideal of B.

17. Show that $M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \text{ rationals} \right\}$ forms a simple ring under matrix operations.

18. Let R be a ring with unity and A be any proper ideal of R. Show that no element of A can have a multiplicative inverse.

19. Show by an example that it is possible to find ideals A, B, C, such that $A \cap (B + C) \neq (A \cap B) + (A \cap C)$.

20. Let R be a commutative ring and let A, B be ideals of R. Show that $\sqrt{A} = \{x \in R \mid x^n \in A \text{ for some +ve integer } n\}$ is an ideal of R such that

(*i*) $A \subseteq \sqrt{A}$ (*ii*) $\sqrt{\sqrt{A}} = \sqrt{A}$

(*iii*) If R has unity and $\sqrt{A} = R$ then $A = R$.

(*iv*) $\sqrt{AB} = \sqrt{A \cap B} = \sqrt{A} \cap \sqrt{B}$

(*v*) $\sqrt{A + B} = \sqrt{\sqrt{A} + \sqrt{B}}$

21. Let $I = (2)$, $J = (12)$ be ideals of the ring $\mathbf{Z}$ of integers. Determine

(*i*) $I + J$ (*ii*) $I \cap J$

(*iii*) $I : J$ where $I : J = \{m \in \mathbf{Z} \mid mJ \subseteq I\}$ (*iv*) IJ

[Hint : If $I = (m)$, $J = (n)$ then $I + J = (d)$, $I \cap J = (l)$, $IJ = (mn)$

$(I : J) = (m/d)$ where $d = gcd\ (a, b)$, $l = l.c.m.\ (a, b)$.

(See under PIDs in chapter 8 also)

22. Let A, B be ideals of a ring R. Define

$(A : B) = \{x \in R \mid xB \subseteq A\}$. Show that $(A : B)$ is an ideal of R. (It is called *quotient ideal*). Show further that

(*i*) $(A : B)\, B \subseteq A \subseteq (A : B)$

(*ii*) $(A : B)\, C = (A : BC)$

(*iii*) $((\bigcap_i A_i) : B) = \bigcap (A_i : B)$

(*iv*) $(A : \sum_i B_i) = \bigcap_i (A : B_i)$

A_i, B_i being ideals of R and $\Sigma B_i = \{x_1 + x_2 + \ldots\ldots + x_n \mid x_i \in B_i, n = \text{finite}\}$.

23. Let R be an integral domain with unity. Let A, B be finitely generated ideals of R such that $A + B$ is a principal ideal. Then show that $A \cap B$ is finitely generated.

Chapter 7

Homomorphisms and Imbedding of Rings

Normal subgroups provided us with quotient groups, ideals do the job in rings.

Quotient Rings

Let R be a ring and let I be an ideal of R. Since $a, b \in I \Rightarrow a - b \in I$, we find I is a subgroup of $< R, + >$. Again as $< R, + >$ is abelian, I will be a normal subgroup of R and thus we can talk of $\frac{R}{I}$, the quotient group

$\frac{R}{I} = \{r + I \mid r \in R\}$ = set of all cosets of I in R (clearly left or right cosets are equal).

We know R/I forms a group under 'addition' defined by

$$(r + I) + (s + I) = (r + s) + I$$

We now define a binary composition (product) on R/I by

$$(r + I)\ (s + I) = rs + I$$

It is a routine exercise to check that this product is well defind on R/I.

Since

$$\begin{aligned}(a + I)\,[(b + I)\,(c + I)] &= (a + I)\,(bc + I)\\ &= a(bc) + I\\ &= (ab)c + I\\ &= (ab + I)\,(c + I)\\ &= [(a + I)\,(b + I)]\,(c + I)\end{aligned}$$

Associativity holds w.r.t. this product.

Again, as $$\begin{aligned}(a + I)\,[(b + I) + (c + I)] &= (a + I)\,(b + c + I)\\ &= a(b + c) + I\end{aligned}$$

$$= (ab + ac) + I$$
$$= (ab + I) + (ac + I)$$
$$= (a + I)(b + I) + (a + I)(c + I)$$

We find left distributivity holds. Similarly one can check that right distributivity also holds in R/I and hence R/I forms a ring, called the *quotient ring* or *residue class ring* of R by I.

We look at it from another angle. Let R be a ring and I an ideal of R. Define, for $a, b \in R$, $a \equiv b \pmod{I}$ if $a - b \in I$. It is easy to check that this relation is an equivalence relation on R. Thus it partitions R into equivalence classes. Let for any $a \in R$, $cl(a)$ be the corresponding equivalence class of a.

Then
$$\begin{aligned} cl(a) &= \{r + R \mid r \equiv a \pmod{I}\} \\ &= \{r \in R \mid r - a \in I\} \\ &= \{r \in R \mid r - a = x \text{ for some } x \in I\} \\ &= \{r \in R \mid r = a + x \text{ for some } x \in I\} \\ &= \{a + x \mid x \in I\} \\ &= a + I \end{aligned}$$

Thus, the quotient ring $\dfrac{R}{I}$ is nothing but the ring of all equivalence classes as defined above.

In fact, the binary compositions defined earlier would translate to

$$cl(a) + cl(b) = cl(a + b) \qquad a, b \in R$$
$$cl(a) \,.\, cl(b) = cl(ab)$$

It would be an interesting exercise for the reader to verify that R/I thus defined forms a ring. In fact, if R has unity 1 then $cl(1)$ will be unity of R/I.

R/I is therefore also called *quotient ring* of R modulo I.

Remark : If $I = R$ then R/I is isomorphic to the zero ring $\{0\}$ and if $I = \{0\}$ then $\dfrac{R}{I} \cong$ R. See definition of *isomorphism* in next section.

Example 1 : Let $H_4 = \{4n \mid n \in \mathbf{Z}\}$, where $<\mathbf{Z}, +, \cdot>$ is the ring of integers. Then H_4 is an ideal of $\mathbf{Z}$ and thus $\dfrac{\mathbf{Z}}{H_4}$ is a quotient ring and is given by

$$\frac{\mathbf{Z}}{H_4} = \{H_4,\ H_4 + 1,\ H_4 + 2,\ H_4 + 3\}$$

This example also shows us that quotient ring of an integral domain may not be an integral domain.

Notice $(H_4 + 2)(H_4 + 2) = H_4 + 4 = H_4 =$ zero of $\dfrac{\mathbf{Z}}{H_4}$ but $H_4 + 2 \neq H_4$.

On the other hand if we consider

$R = \{0, 2, 4, 6, 8, 10\}$ mod 12

$S = \{0, 6\}$ mod 12

then R is not an integral domain whereas R/S is an integral domain.

We have, $R/S = \{S, S+2, S+4\}$

Since $(S+2)(S+2) = S+2$, $(S+2)(S+4) = S+8 = S+2$

and $(S+4)(S+4) = (S+16) = S+4$, we find

$\dfrac{R}{S}$ has no zero divisors.

Homomorphisms

Let $<R, +, \cdot> <R', *, o>$ be two rings. A mapping $\theta : R \to R'$ is called a *homomorphism* if

$$\theta(a+b) = \theta(a) * \theta(b)$$
$$\theta(ab) = \theta(a) \; o \; \theta(b) \qquad a, b \in R$$

Since we prefer to use the symbols + and . for the binary compositions in a ring, we will use these symbols, even while dealing with more than one ring. In that case, the above definition *simplifies* to saying that a mapping $\theta : R \to R'$ is called a homomorphism if

$$\theta(a+b) = \theta(a) + \theta(b)$$
$$\theta(ab) = \theta(a) . \theta(b)$$

One can similalry talk about *isomorphism* in rings as a one-one onto homomorphism.

Example 2 : Consider the map $f : \mathbf{C} \to \mathbf{C}$, s.t.,

$$f(a+ib) = a - ib$$

then f is a homomorphism, where $\mathbf{C}$ = complex numbers,

as
$$\begin{aligned} f[(a+ib)+(c+id)] &= f((a+c)+i(b+d)) \\ &= (a+c) - i(b+d) \\ &= (a-ib)+(c-id) \\ &= f(a+ib)+f(c+id) \end{aligned}$$

and
$$\begin{aligned} f[(a+ib)(c+id)] &= f((ac-bd)+i(ad+bc)) \\ &= (ac-bd)-i(ad+bc) \\ &= (a-ib)\;c-id(a-ib) \\ &= (a-ib)(c-id) \\ &= f(a+ib)\;f(c+id). \end{aligned}$$

Example 3 : Let R be a commutative ring and suppose $px = 0$ for all $x \in R$,

where p is a prime number. Then the mapping $f: R \to R$ defined by $f(x) = x^p$, $x \in R$ is a homomorphism.

In fact the result follows rather easily, if we can show that $p \mid p_{C_r}$, $1 \le r \le p-1$.

Now
$$n = p_{C_r} = \frac{p!}{(p-r)!\,r!}$$
$$= \frac{p(p-1)\ldots\ldots(p-r+1)(p-r)!}{(p-r)!\,1.2\ldots\ldots r}$$
$$\Rightarrow nr! = p(p-1)\ldots\ldots(p-r+1)$$

Since p divides R.H.S., it will divide $nr!$

$\Rightarrow p \mid n$ or $p \mid r!$ (whenever a prime divides product ab, it must divide at least one of a or b). But $p \nmid r!$ as $1, 2, \ldots\ldots, r-1$ are all less than p and none of them divides p, so p cannot divide any one of them. Thus $p \nmid r!$

i.e., $p \mid n$

Now for any $x, y \in R$

$$f(x+y) = (x+y)^p = x^p + p_{C_1} x^{p-1}y + p_{C_2} x^{p-2}y^2 + \ldots\ldots + y^p$$

(R being commutative)

Now $p_{C_1} x^{p-1}y = px^{p-1}y = 0$ as $x^{p-1}y \in R$

$$p_{C_2} x^{p-2}y^2 = (kp)\, x^{p-2}y^2 = 0 \text{ as } p \mid p_{C_2} \Rightarrow p_{C_2} = kp \text{ for some } k$$

Similalry each p_{C_r} would be some multiple of p giving that other terms are also zero.

Hence $f(x+y) = x^p + y^p = f(x) + f(y)$

Also $f(xy) = (xy)^p = x^p y^p$ (R commutative)

$= f(x)\, f(y)$

Thus f is a homomorphism.

Theorem 1 : *If $\theta : R \to R'$ be a homomorphism, then*

(*i*) $\theta(0) = 0'$

(*ii*) $\theta(-a) = -\theta(a)$

where 0, 0' *are zeros of the rings R and R' respectively.*

Proof : (*i*) Since $0 + 0 = 0$

we have $\theta(0+0) = \theta(0)$

$\Rightarrow \theta(0) + \theta(0) = \theta(0) + 0'$

$\Rightarrow \theta(0) = 0'$

(*ii*) Again, as $a + (-a) = 0$

$$\theta(a + (-a)) = \theta(0)$$
$$\Rightarrow \theta(a) + \theta(-a) = \theta(0) = 0$$
$$\Rightarrow -\theta(a) = \theta(-a)$$

Cor. : It is clear that

$$\theta(a-b) = \theta(a + (-b))$$
$$= \theta(a) - \theta(b)$$

Remark : The terminology of epimorphism, monomorphism etc. is extended to rings also in the same way as in groups.

Definition : Let $f: R \to R'$ be a homomorphism, we define *Kernel* of f by

$$\text{Ker } f = \{x \in R \mid f(x) = 0$$

where $0'$ is zero of R'.

The following two thoerems are easy to prove so we'll state the results without proof.

If : $R \to R'$ is a homomorphism then

Theorem 2 : *Ker f is an ideal of R.*

Theorem 3 : *Ker f = (0) iff f is one - one.*

Problem 1 : *If R is a ring with unity and $f: R \to R'$ is a homomorphism where R' is an integral domain such that Ker $f \neq R$ then show that $f(1)$ is unity of R'.*

Solution : Let $a' \in R'$ be any element. We show

$$f(1)\, a' = a' f(1) = a'$$

Now $\quad f(1)\, a' - f(1)\, a' = 0'$

$$\Rightarrow f(1 \,.\, 1)\, a' - f(1)\, a' = 0'$$
$$\Rightarrow f(1)\, f(1)\, a' - f(1)\, a' = 0'$$
$$\Rightarrow f(1)\, [f(1)\, a' - a'] = 0'$$

$\Rightarrow$ either $f(1) = 0'$ or $f(1)\, a' - a' = 0'$ as R' is an integral domain.

$f(1) = 0' \Rightarrow 1 \in \text{Ker } f \Rightarrow \text{Ker } f = R$ which is not true

Hence $\quad f(1)\, a' - a' = 0'$

$$\Rightarrow f(1)\, a' = a'$$

Similarly, we can show $a' = a' f(1)$.

Problem 2 : *Let $f: R \to R'$ be an onto homomorphism, where R is a ring with unity. Show that $f(1)$ is unity of R'.*

Solution . Let $\in R'$ be any element.

Since f is onto, $\exists\, a \in R$, s.t., $f(a) = a'$

Now $a' . f(1) = f(a) . f(1) = f(a \,.\, 1) = f(a) = a'$

Similarly $f(1) . a' = a'$

Showing thereby that $f(1)$ is unity of R'.

Problem 3 : *Show by an example that we can have a homomorphism $f: R \to R'$, such that $f(1)$ is not unity of R', when 1 is unity of R.*

Solution : Consider the map $f: \mathbf{Z} \to \mathbf{Z}$, s.t.,

$$f(x) = 0 \text{ for all } x \in \mathbf{Z}$$

where $\mathbf{Z}$ = ring of integers

then f is a homomorphism (verify)

Again $f(1) = 0$, but 0 is not unity of $\mathbf{Z}$.

Thus although $\mathbf{Z}$ (on R.H.S.) has unity it does not equal $f(1)$.

Remarks (*i*) : If we take the map $f: \mathbf{Z} \to \mathbf{E}$, where $\mathbf{E}$ = ring of even integers, defined by $f(x) = 0$ for all x, we find, $\mathbf{E}$ does not have unity, whereas 1 is unity of $\mathbf{Z}$.

(*ii*) We recall (see page 101) that the map $f: \mathbf{Z} \to \mathbf{E}$, s.t., $f(x) = 2x$ is a group isomorphism. Thus $\mathbf{Z}$ and $\mathbf{E}$ are isomorphic as groups whereas $\mathbf{Z}$ and $\mathbf{E}$ are not isomorphic as rings. Indeed, $\mathbf{Z}$ has unity but $\mathbf{E}$ does not possess unity.

Problem 4 : *Let $\mathbf{Z}$ be the ring of integers. Show that the only homomorphisms from $\mathbf{Z} \to \mathbf{Z}$ are the identity and zero mappings.*

Solution : Let $f: \mathbf{Z} \to \mathbf{Z}$ be a non zero homomorphism (i.e., $f(x) \neq 0$ for any $0 \neq x$).

Now $(f(1))^2 = f(1) f(1) = f(1 \,.\, 1) = f(1) \neq 0$

$\Rightarrow f(1)$ is idempotent in $f(\mathbf{Z})$

Since the only non zero idempotent in $\mathbf{Z}$ is 1 we find $f(1) = 1$

Now for any $x \in \mathbf{Z}$,

if $x > 0$ $\quad f(x) = f(\underbrace{1 + 1 + \ldots\ldots + 1}_{x \text{ times}}) = f(1) + f(1) + \ldots\ldots + f(1)$

$$= xf(1) = x \,.\, 1 = x$$

if $x < 0$ then let $x = -y$

$$f(x) = f(-y) = -f(y) = -f\ (1 + 1 + \ldots\ldots + 1) = [f(1) + f(1) + \ldots\ldots + f(1)]$$

$$= -y\ f(1) = x$$

Hence $f(x) = x$ for all $x \in \mathbf{Z}$

as the result $f(0) = 0$ holds for any homomorphism.

Theorem 4 : (Fundamental Theorem of ring Homomorphism)

If $f: R \to R'$ be an onto homomorphism, then R' is isomorphic to a quotient ring of R. In fact, $R' \cong \dfrac{R}{\operatorname{Ker} f}$.

Proof : Let $f: R \to R'$ be onto homomorphism

Define $\qquad \varphi : \dfrac{R}{\operatorname{Ker} f} \to R'$, s.t.,

$$\varphi(x + I) = f(x) \text{ for all } x \in R \text{ where } I = \operatorname{Ker} f$$

then φ is well defined as

$$x + I = y + I$$

$$\Rightarrow x - y \in I = \operatorname{Ker} f$$

$$\Rightarrow f(x-y) = 0$$
$$\Rightarrow f(x) - f(y) = 0$$
$$\Rightarrow f(x) = f(y)$$
$$\Rightarrow \varphi(x+I) = \varphi(y+I)$$

retracting the steps backwards we prove φ is 1-1.

Again, as

$$\varphi[(x+I)+(y+I)] = \varphi((x+y)+I) = f(x+y) = f(x)+f(y)$$
$$= \varphi(x+I)+\varphi(y+I)$$
$$\varphi[(x+I)(y+I)] = \varphi(xy+I) = f(xy) = f(x)f(y)$$
$$= \varphi(x+I)\varphi(y+I)$$

φ is a homomorphism.

Now if $r' \in R'$ be any element then as $f: R \to R'$ is onto, $\exists\ r \in R$, s.t., $f(r) = r'$ for this r, as $\varphi(r+I) = f(r) = r'$

we find $r+I$ is required pre-image of r' under φ showing thereby that φ is onto and hence an isomorphism.

Thus $\dfrac{R}{\text{Ker } f} \cong R'$. By summetry $R' \cong \dfrac{R}{\text{Ker } f}$.

Theorem 5 : (First Theorem of Isomorphism)

Let $B \subseteq A$ be two ideals of a ring R. Then

$$\frac{R}{A} \cong \frac{R/B}{A/B}.$$

Proof : Define a mapping $f: \dfrac{R}{B} \to \dfrac{R}{A}$ s.t.,

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

then f is an onto homomorphism (Prove !)

By fundamental theorem, $\dfrac{R}{A} \cong \dfrac{R/B}{\text{Ker } f}$

Again, since $r+B \in \text{Ker} f \Leftrightarrow f(r+B) = A$

$$\Leftrightarrow r+A = A$$
$$\Leftrightarrow r \in A$$
$$\Leftrightarrow r+B \in \frac{A}{B}$$

we find $\quad \text{Ker } f = A/B$

Hence $\quad \dfrac{R}{A} \cong \dfrac{R/B}{A/B}.$

Theorem 6 : (Second Theorem of Isomorphism)

Let A, B be two ideals of a ring R, then

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

Proof : Define a mapping $f: B \to \dfrac{A+B}{A}$ s.t.,

$$f(b) = b + A \text{ for all } b \in B$$

Then φ is a well defined homomorphism.

Again if $x + A \in \dfrac{A+B}{A}$. be any element then

$$x \in A + B \Rightarrow x = a + b, \ a \in A, \ b \in B$$

So, $x + A = (a+b) + A = (b+a) + A = b + (a + A) = b + A$

thus $\quad x + A = b + A = f(b)$

i.e., b is the pre-image of $x + A$ under f or that f is onto.

By Fundamental theorem then $\dfrac{A+B}{A} \cong \dfrac{B}{\text{Ker} f}$

Now $\quad x \in \text{Ker } f \Leftrightarrow f(x) = A$

$$\Leftrightarrow x + A = A \Leftrightarrow x \in A$$

$$\Leftrightarrow x \in A \cap B \qquad (x \in \text{Ker } f \subseteq B)$$

Hence $\quad \text{Ker } f = A \cap B$

and thus $\quad \dfrac{A+B}{A} \cong \dfrac{B}{A \cap B}.$

Remark : Clearly then $\dfrac{A+B}{B} \cong \dfrac{B}{A \cap B}.$

Theorem 7 : *If N be an ideal of a ring R then there exists a one-one onto mapping between the set of all ideals of R, containing N and the set of ideals of R/N.*

Proof : Let $f: R \to R/N$ be the natural homomorphism defined by $f(r) = r + N$.

Now, if A be any ideal of R then as $f: R \to R/N$ is onto homomorphism, $f(A)$ is an ideal of R/N.

Again,
$$\begin{aligned} f(A) &= \{f(a) \mid a \in A\} \\ &= \{a + N \mid a \in A\} \\ &= \frac{A}{N} \end{aligned}$$

Let now $\mathcal{K}$ be the set of all ideals of R, which contain N and $\mathcal{K}'$ be the set of all ideals of $\dfrac{R}{N}$.

Define $\varphi : \mathcal{K} \to \mathcal{K}'$ s.t.,

$$\varphi(A) = f(A) = \frac{A}{N}$$

φ is clearly well - defind.

Again, $\varphi(A) = \varphi(B)$

$$\Rightarrow f(A) = f(B)$$

$$\Rightarrow \frac{A}{N} = \frac{B}{N}$$

If $a \in A$ be any element then $a + N \in \frac{A}{N} \Rightarrow a + N \in \frac{B}{N}$

$$\Rightarrow a \in B$$

i.e., $A \subseteq B$.

Similarly, $B \subseteq A$ and thus $A = B$

showing that φ is one-one.

To show that φ is onto, let $X \in \mathcal{K}'$ be any member then X is an ideal of $\frac{R}{N}$.

Define $A = \{x \in R \mid f(x) \in X\}$.

We show A is the required pre-image of X under φ.

It is easy to check that A is an ideal of R.

Again, $n \in N = \text{Ker } f$

$$\Rightarrow f(n) = N = \text{zero of } \frac{R}{N}$$

$0 + N \in X$ [as ideal contains zero]

$\therefore$ $f(n) \in X \Rightarrow n \in A$

or that $N \subseteq A$.

Thus A is a member of $\mathcal{K}$.

Definition of A then confirms that it is the required pre-image. Hence φ is onto.

Cor. : If N is an ideal of a ring R then any ideal of R/N is of the type A/N where A is an ideal of R, containing N.

Problem 5 : *Show that* $Z_n \cong \frac{\mathbf{Z}}{(n)}$.

Solution : We have $Z_n = \{0, 1, 2, \ldots\ldots, n-1\}$

$$\frac{\mathbf{Z}}{(n)} = \{(n),\ 1 + (n),\ 2 + (n), \ldots\ldots, (\overline{n-1}) + (n)\}$$

Define $\theta : \frac{\mathbf{Z}}{(n)} \to Z_n$, s.t.,

$$\theta(r+(n)) = r, \quad 0 \le r \le n-1$$

Let $r+(n) = s+(n)$ and suppose $r \neq s$.

Then $r-s \in (n) \Rightarrow n \mid (r-s) \Rightarrow n \le r-s$

where $r, s \le n$. We thus get a contradiction.

Hence $r = s$ and so θ is well defined.

It is clearly seen to be 1-1.

Again, as

$$\theta((r+(n))+(s+(n)) = \theta(\overline{r+s}+(n)) = \theta((nq+t)+(n)) \text{ for some } q,\ t,\ 0 \le t < n$$

$$= \theta(t+(n)) = t = r \oplus s = \theta(r+(n)) \oplus \theta(s+(n))$$

$$\theta((r+(n))(s+(n)) = \theta(rs+(n)) = \theta((nq'+k+(n)) \text{ for some } q',\ k,\ 0 \le k < n$$

$$= \theta(k+(n)) = k = r \otimes s = \theta(r+(n)) \otimes \theta(s+(n))$$

we find θ is a homomorphism and hence an isomorphism.

Remark : The above result can also be proved by using Fundamental theorem. See remark on page 114 also.

Problem 6 : *Show that* $\dfrac{\mathbf{Z}}{(n)}$ *has no non zero nilpotent element iff n is square free.*

Solution : Suppose $\dfrac{\mathbf{Z}}{(n)}$ has no non zero nilpotent element.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$, where p_i are distinct primes.

Suppose n is not square free. Then some $\alpha_i \ge 2$. Let $\alpha_1 \ge 2$.

Let $m = p_1 . p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$, then $m < n$

Also $m+(n) \neq (n)$

Now $(m+(n))^{\alpha_1} = m^{\alpha_1} + (n) = (n)$

implies $m+(n)$ is a non zero nilpotent element in $\dfrac{\mathbf{Z}}{(n)}$, a contradiction.

Hence n is square free.

Conversely, let n be square free.

Suppose $m+(n)$ is a nilpotent element in $\dfrac{\mathbf{Z}}{(n)}$.

Then $(m+(n))^{\alpha} = (n)$ for some α

So $m^{\alpha} \in (n) \Rightarrow m^{\alpha} = nk$ for some k

Let $n = p_1 p_2 \ldots\ldots p_r$ where p_i are distinct primes

(Note n is square free)

Since $p_i \mid n \quad \forall\, i$,

$n = p_1 p_2 \ldots\ldots p_r$ divides $m \Rightarrow m + (n) = (n) =$ zero of $\dfrac{\mathbf{Z}}{(n)}$.

i.e., $\dfrac{\mathbf{Z}}{(n)}$ has no non zero nilpotent element.

Problem 7 : *Find all the nilpotent elements in* Z_{30}.

Solution : We know $Z_{30} \cong \dfrac{\mathbf{Z}}{(30)}$ and as $30 = 2 \times 3 \times 5$ is square free, $\dfrac{\mathbf{Z}}{(30)}$ or Z_{30} has no non zero nilpotent elements.

Remark : See problem 15 on page 238 also.

Exercises

1. Show that the relation of isomorphism in rings is an equivalence relation.
2. Let $f: R \to R'$ be a homomorphism and let A be an ideal of R. Show that $f(A) = \{x \in R' \mid \exists\, a \in A,\ x = f(a)\}$ is an ideal of $f(R)$.
3. Prove that any homomorphism of a field is either a monomorphism or takes each element to zero.
4. Show that homomorphic image of a commutative ring is commutative. Prove also that the converse may not hold.
5. Show that homomorphic image of a ring with unity is a ring with unity but the converse is not true.
6. Let I be an ideal of a ring R. Show that

   (*a*) if R is commutative then so is R/I

   (*b*) if R has unity 1 then $1 + I$ is unity of R/I

   (*c*) converse of (*a*) and (*b*) does not hold.

   Hint : Take R = ring of matrices of the type $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ and I of type $\begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix}$ over integers.
7. Show that there exists an onto homomorphism from a ring R to R/I, a quotient ring of R (called the natural homomorphism) (Define $f(r) = r + I$).
8. If I is an ideal of R, show that R/I has no zero divisors iff the following is true :

(*i*) whenever a product of two elements of R belongs to I, at least one of these belongs to I.

(*ii*) $r+I \in R/I$ is unity of R/I iff $rx-x \in I$ and $xr-x \in I$ for all $x \in R$.

9. Show that the set N of all nilpotent elements in a commutative ring R forms an ideal of R and that R/N has no non zero nilpotent elements.

10. Let $G=\{2n \mid n \in \mathbf{Z}\}$, $H=\{8n \mid n \in \mathbf{Z}\}$. Show that G/H and $\mathbf{Z}_4$ (ring of integers modulo 4) are isomorphic as groups but not as rings.

11. Show that $[0, 2, 4, 6, 8\}$ addition, multiplication mod 10 is isomorphic to $\mathbf{Z}_5$.

Imbedding of Rings

A non empty subset S of a ring R is defined to be a subring of R if S forms a ring under the binary compositions of R (restricted to S). Thus a subring inherits its compositions from the partent ring. We now come to the 'reverse' process. Given a ring S, can we find a super ring R so that S is a subring of R? The answer may not be a complete yes in the sense that a subring is defined only when we *have* a ring and the operations in the subring are got through these operations. But it is, of course, possible to have a ring R, so that our starting ring S is isomorphic to a subring of R. Then we can *identify* our ring S as a subring of this ring R. This is what is called imbedding of rings.

The usefulness of imbedding would be illustrated later through examples. To start with, we give

Definition : Let R and R' be two rings. A one - one homomorphism θ from R to R' is called an imbedding (embedding) mapping and in that case R' is called *extension ring or overring* of R.

Imbedding of a ring into a ring with unity.

Let R be any ring and let $\mathbf{Z}$ be the ring of integers.

Consider $\quad R \times \mathbf{Z} = \{(r, n) \mid r \in R,\ n \in \mathbf{Z}\}$

We show $R \times \mathbf{Z}$ forms a ring with unity, under addition and multiplication defined by

$$(r, n)+(s, m) = (r+s,\ n+m) \qquad r, s \in R,\ n, m \in \mathbf{Z}$$

$$(r, n) . (s, m) = (rs+ns+mr, nm)$$

Addition is well - defined as

Let $\quad (r, n) = (r', n')$ and $(s, m) = (s', m')$

Then $\quad r = r',\ n = n'$ and $s = s',\ m = m'$

$$\Rightarrow r+s = r'+s',\ n+m = n'+m'$$

$$\Rightarrow (r+s,\ n+m) = (r'+s',\ n'+m')$$

Similarly one can show that multiplication is well defined.

Associativity : $(r, n) + [(s, m) + (t, k)] = (r, n) + (s + t, m + k)$

$$= (r + (s + t), n + (m + k))$$
$$= ((r + s) + t, (n + m) + k)$$
$$= (r + s, n + m) + (t, k)$$
$$= [(r, n) + (s + m)] + (t, k)$$

Commutativity follows as above.

Again it is clear that (0, 0) will be the zero element and $(-r, -n)$ will be additive inverse of (r, n), where, of course, $-r$ is inverse of r in R and $-n$ is –ve of n in $\mathbf{Z}$.

It would be a routine exercise for the reader to check that associativity w.r.t. multiplication and distributive properties also hold.

Again, as $(r, n)(0, 1) = (r.0 + n.0 + 1r, n.1)$

$$= (r, n)$$

(0, 1) will be unity and hence $R \times \mathbf{Z}$ forms a ring with unity.

We show R can be imbedded into $R \times \mathbf{Z}$

Define a mapping $\theta : R \to R \times \mathbf{Z}$, s.t.,

$$\theta(r) = (r, 0)$$

then θ is clearly well defind mapping

Also $\theta(r) = \theta(s)$

$$\Rightarrow (r, 0) = (s, 0) \Rightarrow r = s$$

shows θ is one - one.

Again $\theta(r + s) = (r + s, 0) = (r, 0) + (s, 0) = \theta(r) + \theta(s)$

$$\theta(rs) = (rs, 0) = (r, 0)(s, 0) = \theta(r)\theta(s)$$

Thus θ is a homomorphism and therefore, an imbedding mapping.

Hence we get

Theorem 8 : *Any ring can be imbedded into a ring with unity.*

Imbedding of a ring into a ring of endomorphisms

We recall that a homomorphism from A to A is called an endomorphism.

Let $< V, + >$ be any additive abelian group. We denote by Hom (V, V) the set of all homomorphisms from V to V (i.e. it is set of all endomorphisms of V).

We show now Hom (V, V) forms a ring with unity under the operations defined by

$$(f + g) x = f(x) + g(x) \qquad x \in V$$
$$(fg) x = f(g(x)) \qquad x \in V$$

where $f, g \in$ Hom (V, V).

Closure : Let $f, g \in$ Hom (V, V)

Then $(f + g)(x + y) = f(x + y) + g(x + y)$

$$= (f(x) + f(y)) + (g(x) + g(y))$$

$$= (f(x) + g(x)) + (f(y) + g(y))$$
$$= (f + g)x + (f + g)y$$

$\Rightarrow f + g$ is an endomorphism of V

i.e., $f + g \in \text{Hom}\ (V, V)$

Again $(fg)\ (x + y) = f(g(x + y))$

$$= f(g(x) + g(y))$$
$$= f(g(x)) + f(g(y))$$
$$= (fg)x + (fg)y$$

$\Rightarrow fg \in \text{Hom}\ (V, V)$

Associativity : $[f + (g + h)]\, x = f(x) + [(g + h)\, x]$

$$= f(x) + (g(x) + h(x))$$
$$= (f(x) + g(x)) + h(x)$$
$$= (f + g)\ x + h(x)$$
$$= [(f + g) + h]\, x \text{ for all } x$$

$\Rightarrow f + (g + h) = (f + g) + h$

Commutativity follows as above.

Let $O : V \to V$ be defined by

$O(x) = 0$ for all $x \in V$

then O is easily seen to be a homomorphism.

Also since $(f + O)x = f\ (x) + O(x) = f(x) + 0 = f(x)$

$$= 0 + f(x) = O(x) + f(x) = (O + f)x \qquad \text{for all } x$$

we have

$$f + O = f = O + f$$

or that O is zero of Hom (V, V).

Again for any $f \in \text{Hom}\ (V, V)$, define a map

$(-f) : V \to V$, s.t.,

$(-f)x = -f(x)$

then $(-f)$ is a homomorphism and $f + (-f) = O = (-f) + f$

Showing thereby that $(-f)$ is inverse of f. Associativity and distributivity can be proved easily, establishing that Hom (V, V) is a ring. The map $i : V \to V$ s.t., $i(x) = x$ for all $x \in V$ will act as unity of this ring.

Hence Hom (V, V) forms a ring with unity for any additive abelian group V.

Theorem 9 : *Any ring R with unity can be imbedded into a ring of endomorphisms of some additive abelian group.*

Proof : Let $< R, +, \cdot >$ be the given ring with unity then $< R, + >$ is an additive abelian group. We denote it by R^+. By what is done in the preceeding pages, it follows that Hom (R^+, R^+) is a ring with unity (it being the ring of endomorphisms of the additive abelian group R^+).

Define a mapping $f: R \to \text{Hom}\ (R^+, R^+)$ s.t.,

$$f(r) = g_r \quad r \in R \text{ where } g_r(x) = rx \quad x \in R^+$$

To show that f is well defined, we first show that $g_r : R^+ \to R^+$ s.t., $g_r(x) = rx$ is a homomorphism.

Since $g_r(x+y) = r(x+y) = rx + ry = g_r(x) + g_r(y)$,

we find g_r is a homomorphism.

Thus $g_r \in \text{Hom}\ (R^+, R^+)$.

Again $\quad r_1 = r_2$

$$\Rightarrow r_1 x = r_2 x \quad \text{for all } x \in R^+$$

$$\Rightarrow g_{r_1}(x) = g_{r_2}(x) \quad \text{for all } x$$

$$\Rightarrow g_{r_1} = g_{r_2}$$

$$\Rightarrow f(r_1) = f(r_2)$$

or that f is a well defined mapping.

Again, $\quad f(r_1) = f(r_2)$

$$\Rightarrow g_{r_1} = g_{r_2}$$

$$\Rightarrow g_{r_1}(x) = g_{r_2}(x) \quad \text{for all } x \in R^+$$

$$\Rightarrow r_1 x = r_2 x \quad \text{for all } x \in R^+$$

$\Rightarrow$ In particular, $r_1.1 = r_2.1 \quad$ as $1 \in R^+$

$$\Rightarrow r_1 = r_2$$

or that f is one - one.

Again $\quad f(r_1 + r_2) = g_{r_1+r_2}$

and $\quad f(r_1) + f(r_2) = g_{r_1} + g_{r_2}$

where $\quad g_{r_1+r_2}(x) = (r_1 + r_2)x = r_1 x + r_2 x = g_{r_1}(x) + g_{r_2}(x)$

$$= (g_{r_1} + g_{r_2})x \text{ for all } x$$

means $\quad g_{r_1+r_2} = g_{r_1} + g_{r_2}$

or that $\quad f(r_1 + r_2) = f(r_1) + f(r_2)$.

Now $\quad f(r_1 r_2) = g_{r_1 r_2}$ and $f(r_1)\ f(r_2) = g_{r_1} g_{r_2}$

where $\quad g_{r_1 r_2}(x) = (r_1 r_2)x = r_1(r_2 x) = g_{r_1}(r_2 x) = g_{r_1}(g_{r_2}(x))$

$$= (g_{r_1} g_{r_2})x \text{ for all } x$$

$$\Rightarrow g_{r_1 r_2} = g_{r_1} g_{r_2}$$

or that $$f(r_1 r_2) = f(r_1) f(r_2).$$

Showing thereby that f is a homomorphism and hence an imbedding mapping.

Which proves the result.

Summing up all that we have done in the last few pages on imbedding and using the idea of composition of mappings, we have established

Theorem 10 : *Any ring R can be imbedded into a ring of endomorphisms of some additive abelian group.*

Problem 8 : *If* $< \mathbf{Z}, +, \cdot >$ *be the ring of integers then show that Hom* $(\mathbf{Z}^+, \mathbf{Z}^+)$ *is isomorphic to* $\mathbf{Z}$, *where by* $\mathbf{Z}^+$ *we mean the additive abelian group* $< \mathbf{Z}, + >$.

Solution : Define a mapping $f: \mathbf{Z} \to \text{Hom } (\mathbf{Z}^+, \mathbf{Z}^+)$, s.t.,

$$f(r) = g_r \text{ for all } r \in \mathbf{Z}$$

where $$g_r(x) = rx \text{ for all } x \in \mathbf{Z}^+$$

then f will be a one - one homomorphism (as seen in the theorem earlier). We need show ontoness. So let $\theta \in \text{Hom } (\mathbf{Z}^+, \mathbf{Z}^+)$ be any element, then θ is a homomorphism from $\mathbf{Z}^+ \to \mathbf{Z}^+$. Since $1 \in \mathbf{Z}^+$, $\theta(1) \in \mathbf{Z}^+$, let $\theta(1) = t$.

We claim $\theta = g_t = f(t)$, i.e., t is the required pre-image of θ under f. For this, we show

$$\theta(x) = g_t(x) \text{ for all } x \in \mathbf{Z}$$

Case (i) : x is a +ve integer.

$$\theta(x) = \theta(\underbrace{1 + 1 + \ldots\ldots + 1}_{(x \text{ times})}) = \theta(1) + \theta(1) + \ldots\ldots + \theta(1) \quad (x \text{ times})$$

$$= t + t + \ldots\ldots + t \quad (x \text{ times})$$

$$= xt = tx = g_t(x)$$

Case (ii) : x is a –ve integer

Let $x = -y$, then

$$\theta(x) = \theta(-y) = -\theta(y) = -ty = t(-y) = tx = g_t(x)$$

Case (iii) : x is zero

then $$\theta(x) = \theta(0) = 0 \quad (\theta \text{ is a homomorphism})$$

$$= t \,.\, 0 = g_t(0) = g_t(x)$$

Hence, in any case $\theta(x) = g_t(x) \; \forall \, x$

$$\Rightarrow \theta = g_t$$

and thus the result follows.

Problem 9 : *Show by an example that extension ring of an integral domain need not essentially be an integral domain.*

Solution : Let $\mathbf{E}$ = ring of even integers,

then $\mathbf{E}$ can be imbedded into $\mathbf{E} \times \mathbf{Z}$, by defining

$$f: \mathbf{E} \to \mathbf{E} \times \mathbf{Z}, \text{ s.t.,}$$

$$f(r) = (r, 0)$$

Here **E** is an integral domain, whereas $\mathbf{E} \times \mathbf{Z}$ is not an integral doimain as $(2, -2) . (-2, 0) = (0, 0)$.

Theorem 11 : *An integral domain can be imbedded into a field.*

Proof : Let D be an integral domain.

Let $$S = \{(a, b) \mid a, b \in D, b \neq 0\}$$

Define a relation $\sim$ on S by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

It is easy to see that $\sim$ is an equivalence relation. Thus it partitions S into equivalence classes. Let equivalence class of (a, b) be denoted by $[a, b]$. Let F be the set of all these equivalence classes. We show F forms a field under addition and multiplication defined by

$$[a, b] + [c, d] = [ad + bc, bd]$$

$$[a, b] . [c, d] = [ac, bd]$$

Addition is well-defined

Let $[a, b] = [a', b']$ and $[c, d] = [c', d']$

Then $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$

$$\Rightarrow ab' = ba' \text{ and } cd' = dc'$$

$$\Rightarrow (ab')dd' = (ba')dd' \text{ and } (cd')bb' = (dc')bb' \quad \text{.... (1)}$$

We want to show that

$$[ad + bc, bd] = [a'd' + b'c', b'd']$$

which will hold if

$$(ad + bc, bd) \sim (a'd' + b'c', b'd')$$

or if $$(ad + bc)\ b'd' = bd\ (a'd' + b'c')$$

or if $$ab'dd' + bb'cd' = ba'dd' + bb'dc'$$

which is true if we add equations (1) above.

Hence addition is well defined.

To verify that multiplication is well defined

Let $[a, b] = [a', b'], [c, d] = [c', d']$

then as before $ab' = ba'$ and $cd' = dc'$

$$\Rightarrow ab'cd = ba'dc' \quad \text{... (2)}$$

Now $[a, b] . [c, d] = [a', b'] [c', d']$

if $[ac, bd] = [a'c', b'd']$

or if $(ac, bd) \sim (a'c', b'd')$

or if $acb'd' = bda'c'$

which is true by (2).

That addition is commutative and associative will be a routine affair to prove.

Existence of zero element

Let $[a, b] \in F$ be any element. Then

$$[a, b] + [0, b] = [ab + b0, b^2] = [ab, b^2] = [a, b]$$

as $$[ab, b^2] = [a, b]$$

$$\Leftrightarrow (ab, b^2) \sim (a, b) \Leftrightarrow abb = b^2a$$

$$\Leftrightarrow ab^2 = ab^2$$

thus $[0, b]$ will be zero of F. One might notice here that $[0, x] = [0, y]$ for any non zero, $x, y \in D$, as $(0, x) \sim (0, y) \Leftrightarrow 0 . y = 0 . x$.

Existence of additive inverse

For any $[a, b]$ in F, $[-a, b]$ will be its additive inverse, as $[a, b] + [-a, b] = [ab - ba, b^2] = [0, b^2] = [0, b]$. Thus $< F, + >$ forms an abelian group.

We leave it to the reader to verify that multiplication is commutative, associative and is distributive over addition.

Again, since for any $0 \neq x$ in D and for any $[a, b]$ in F.

$$[a, b] . [x, x] = [ax, bx] = [a, b]$$

we notice $[x, x]$ will act as unity in F. Let now $[a, b]$ be any non zero element of F then $a \neq 0$ (b, of course is non zero). So we can talk of $[b, a]$ in F and as

$$[a, b]\ [b, a] = [ab, ba] = [ab, ab] = [x, x]$$

we find every non zero element of F has multiplicative inverse.

Hence F is a field.

We show D can be imbedded into F. Define a mapping

$$\varphi : D \to F, \text{ s.t.,}$$

$$\varphi(a) = [ax, x] \text{ where } 0 \neq x \in D$$

φ *is well - defined*

Let $$a = b$$

Then $$ax = bx$$

$$\Rightarrow axx = xbx$$

$$\Rightarrow (ax, x) \sim (bx, x)$$

$$\Rightarrow [ax, x] = [bx, x]$$

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

φ *is* 1-1

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

Then $$[ax, x] = [bx, x]$$

$$\Rightarrow (ax, x) \sim (bx\ x)$$

$$\Rightarrow axx = xbx$$

$$\Rightarrow x^2 (a - b) = 0$$

$$\Rightarrow a - b = 0 \text{ as } x^2 \neq 0$$

$$\Rightarrow a = b.$$

φ *is a homomorphism*

$$\varphi(a+b) = [(a+b)\ x,\ x] = [ax+bx,\ x]$$

$$\varphi(a)+\varphi(b) = [ax,\ x]+[bx,\ x] = [axx+xbx,\ x^2]$$

$$= [ax^2+bx^2,\ x^2] = [ax+bx,\ x]$$

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

Also $\varphi(ab) = [abx,\ x]$

$$\varphi(a)\ \varphi(b) = [ax,\ x]\ [bx,\ x] = [abx^2,\ x^2] = [abx,\ x]$$

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

Hence φ is 1-1 homomorphism, and is the required imbedding mapping.

Remark : The above field F is called the *field of quotients* or the quotient field of D. The reader is, however, cautioned not to confuse it with R/I.

We also sometimes use the notation $\frac{a}{b}$ to denote $[a,\ b]$. The logic behind this notation is clear if we consider imbedding of $\mathbf{Z}$ into $\mathbf{Q}$.

In fact, at times this notation looks more natural and convenient. For instance, $[a,\ b]+[c,\ d] = [ad+bc,\ bd]$.

would read as $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$

or $[a,\ b] = [c,\ d]$ would mean $\frac{a}{b}=\frac{c}{d}$ or $ad = bc$

Summing up, we can, therefore, say that any integral domain D can be *enlarged* to a field F so that each element of F can be expressed as a quotient of two elements of D.

Problem 10 : *Prove that if K is any field which contains D then K contains a subfield isomorphic to F, where F is the field of quotients of the integral domain D. (In this sense F is the smallest field containing D).*

Solution : Define a map $\theta : F \to K$, s.t.,

$$\theta([a,\ b]) = ab^{-1}$$

Since $a,\ b \in D \subseteq K,\ b \neq 0,\ \therefore\ b^{-1}$ exists in K. θ is well defined, 1-1 map as

$$[a_1,\ b_1] = [a_2,\ b_2]$$

$$\Leftrightarrow (a_1,\ b_1) \sim (a_2,\ b_2)$$

$$\Leftrightarrow a_1b_2 = b_1a_2 \Leftrightarrow a_1b_1^{-1} = a_2b_2^{-1}$$

$$\Leftrightarrow \theta([a_1,\ b_1]) = \theta([a_2,\ b_2])$$

Again, as
$$\begin{aligned}\theta([a_1, b_1]) + [a_2, b_2]) &= \theta([a_1b_2+b_1a_2,\ b_1b_2]) \\ &= (a_1b_2+b_1a_2)\ (b_1b_2)^{-1} \\ &= a_1b_2b_2^{-1}b_1^{-1}+b_1a_2b_2^{-1}b_1^{-1} \\ &= a_1b_1^{-1}+a_2b_2^{-1} \\ &= \theta[(a_1,\ b_1)]+\theta([a_2,\ b_2)]\end{aligned}$$

and
$$\begin{aligned}\theta([a_1,b_1]\,[a_2,b_2]) &= \theta([a_1a_2,\ b_1b_2])\\ &= (a_1a_2)\ (b_1b_2)^{-1} = a_1a_2b_2^{-1}b_1^{-1}\\ &= (a_1b_1^{-1})\ (a_2b_2^{-1}) = \theta([a_1,b_1])\,\theta([a_2,b_2])\end{aligned}$$

we find θ is a homomorphism. Thus F will be isomorphic to $\theta(F)$ which will be a subfield of K. Thus quotient field is the smallest field containing D.

Problem 11 : *If D_1 and D_2 be two isomorphic integral domains then show that their respective fields of quotients F_1 and F_2 are also isomorphic.*

Solution : Let $f: D_1 \to D_2$ be the given isomorphism. The fields of quotients F_1 and F_2 are given by

$$F_1 = \{[a,\ b] \mid a,\ b \in D_1,\ b \neq 0\}$$
$$F_2 = \{[x,\ y] \mid x,\ y \in D_2,\ y \neq 0\}$$

Define a map $\varphi : F_1 \to F_2$ s.t.,

$$\varphi([a,\ b]) = [f(a),\ f(b)]$$
$$[a,\ b] \in F_1 \Rightarrow a,\ b \in D_1,\ b \neq 0$$
$$\Rightarrow f(a),\ f(b) \in D_2 \text{ and } f(b) \neq 0$$
$$\Rightarrow [f(a),\ f(b)] \in F_2$$

φ is then well-defined and one-one as

$$\varphi([a,\ b]) = \varphi([a',\ b'])$$
$$\Leftrightarrow [f(a),\ f(b)] = [f(a'),\ f(b')]$$
$$\Leftrightarrow (f(a),\ f(b)) \sim (f(a'),\ f(b'))$$
$$\Leftrightarrow f(a)\ f(b') = f(b)\ f(a')$$
$$\Leftrightarrow f(ab') = f(ba')$$
$$\Leftrightarrow ab' = ba'$$
$$\Leftrightarrow (a,\ b) \sim (a',\ b') \Leftrightarrow [a,\ b] = [a',\ b'].$$

φ is onto, as for any $[x,\ y] \in F_2$, $x,\ y \in D_2 \Rightarrow \exists\, a,\ b \in D_1$ s.t., $f(a) = x$, $f(b) = y$

Also then $\varphi([a,\ b]) = [f(a),\ f(b)] = [x,\ y]$

φ *is a homomorphism*

$$\begin{aligned}\varphi([a,\ b] + [a',\ b']) &= \varphi([ab' + ba',\ bb'])\\ &= [f(ab' + ba'),\ f(bb')]\\ \varphi([a,\ b]) + \varphi([a',\ b']) &= [f(a),\ f(b)] + [f(a'),\ f(b')]\\ &= [f\ (a)\ f(b') + f(b)\ f(a'),\ f(b)\ f(b')]\\ &= [f(ab' + ba'),\ f(bb')]\end{aligned}$$

Again
$$\begin{aligned}\varphi([a,\ b]\,[a',b']) &= \varphi([aa',\ bb']) = [f(aa'), f(bb')]\\ &= [f(a)\ f(a'),\ f(b)\ f(b')]\\ &= [f(a),\ f(b)]\ [f(a'),\ f(b')]\\ &= \varphi([a,\ b])\ \varphi([a',\ b'])\end{aligned}$$

which shows that φ is an isomorphism.

Remark : The converse is not true, for example the field of quotients of even integers and that of integers are same (the rationals) whereas even integers & integers are not isomorphic as integral domains.

Any two fields of quotients of an integral domain are isomorphic (showing thereby the 'uniqueness' of the field of quotients).

Problem 12 : *Let D be an integral domain, $a, b \in D$ be such that $a^n = b^n$, $a^m = b^m$ for two relatively prime positive integers m, n. Prove that $a = b$.*

Solution : If $a = 0$ then $a^n = 0 \Rightarrow b^n = 0 \Rightarrow b = 0$.

Similarly $b = 0 \Rightarrow a = 0$.

Let now a, b be non zero. Let F be the field of quotients of D and let $\theta : D \to F$ be the imbedding map. Suppose $\theta(a) = a_1$ and $\theta(b) = b_1$.

Since m, n are relatively prime, $\exists$ integers x, y s.t.,

$$mx + ny = 1$$

Then $\theta(a) = a_1 = a_1^{mx+ny} = (a_1^m)^x (a_1^n)^y$

Now $a_1^m = (\theta(a))^m = \theta(a) . \theta(a) ..... \theta(a)$

$$= \theta(a . a ..... a) = \theta(a^m)$$

$$= \theta(b^m) = (\theta(b))^m = b_1^m$$

Similarly, $a_1^n = b_1^n$

Thus, $\theta(a) = (a_1^m)^x (a_1^n)^y = (b_1^m)^x (b_1^n)^y$

$$= b_1^{mx+ny} = b_1 = \theta(b)$$

which gives $a = b$ as θ is 1-1.

Remark : The above solution exhibits the 'utility' of the field of quotients. What we did with a_1 and b_1 could not be done with a, b, as a, b are memebers of an integral domain and existence of multiplicative inverse could not be assured in D, whereas a_1, b_1 being members of a field, we could talk of the inverse elements. Note x, y being integers could also be negative. This is why the solution of the problem could not be taken as

$$a = a^{mx+ny} = (a^m)^x . (a^n)^y = (b^m)^x (b^n)^y = b^{mx+ny} = b.$$

Problem 13 : *Show that the result of the previous problem may fail to hold in case D is not an integral domain.*

Solution : Consider the ring $D = \{0, 1, 2, ..., 7\}$ mod 8

Take $a = 2$, $b = 4$, $m = 3$, $n = 4$, $(m, n) = 1$

then $a^n = 2^4 = 2 \otimes 2 \otimes 2 \otimes 2 = 0 = 4^4 = b^n$

$$a^m = 2^3 = 0 = 4^3 = b^m$$

But $a \neq b$

We notice D is not an integral domain as $4 \otimes 2 = 0$ whereas 4, 2 are non zero.

Problem 14 : *Find the field of quotients of the integral domain* $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$

Solution : Let F be the field of quotients of $\mathbf{Z}[i]$

then
$$F = \left\{\frac{d_1}{d_2} \mid d_1, d_2 \in \mathbf{Z}[i], d_2 \neq 0\right\}$$
$$= \left\{\frac{a+ib}{c+id} \mid a, b, c, d \in \mathbf{Z}, c+id \neq 0\right\}$$
$$= \left\{\frac{(a+ib)(c-id)}{c^2+d^2} \mid a, b, c, d \in \mathbf{Z}\right\}$$
$$= \left\{\frac{ac+bd}{c^2+d^2} + i\frac{(bc-ad)}{c^2+d^2} \mid a, b, c, d \in \mathbf{Z}\right\}$$
$$\subseteq F_1 = \{x + iy \mid x,\ y \in \mathbf{Q}\}$$

Now if $x + iy \in F_1$ be any element then as $x,\ y \in \mathbf{Q}$,

$$x + iy = \frac{p_1}{q_1} + i\frac{p_2}{q_2} \quad \text{where } p_1,\ p_2,\ q_1,\ q_2 \in \mathbf{Z} \text{ and } q_1 \neq 0,\ q_2 \neq 0$$

$$= \frac{p_1q_2 + ip_2q_1}{q_1q_2 + i.o} + \frac{e_1}{e_2}, \text{ where } e_1,\ e_2 \in \mathbf{Z}[i] \text{ and } e_2 \neq 0$$

$\Rightarrow x + iy \in F$

or that $F = F_1$

Showing that $F_1 = \{x + iy \mid x,\ y \in \mathbf{Q}\}$ is the field of quotients of $\mathbf{Z}[i]$.

In fact, the mapping $\theta : \mathbf{Z}[i] \to F_1$, s.t.,

$$\theta(a + ib) = a + ib$$

will be the required imbedding mapping.

Exercises

1. Give an example of an imbedding mapping in which unity is not mapped to unity.
2. Show that field of reals can be imbedded into the field of complex numbers.
3. Find the field of quotients of the integral domain $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$.
4. Show that field of quotients of a finite integral domain is the integral domain itself.

More On Ideals

Definition : Two ideals A and B are called *comaximal* if $A + B = R$.

Theorem 12 : *If R is a commutative ring with unity and A, B are comaximal ideals of R, then $AB = A \cap B$.*

Proof : One can prove that, in general,

$$AB \subseteq A \cap B \text{ (See exercises on page 250)}$$

Let now $x \in A \cap B$ be any element.

Then $\quad x \in A$ and $x \in B$

Since $\quad 1 \in R = A + B$

$$\exists\, a \in A,\ b \in B \text{ s.t., } 1 = a + b$$

$$\Rightarrow x \,.\, 1 = x \,.\, (a + b)$$

$$\Rightarrow x = xa + xb$$

$$\Rightarrow x = ax + xb$$

Now $\quad a \in A,\ x \in B;\ x \in A,\ b \in B \Rightarrow ax + xb \in AB$

i.e., $\quad x \in AB$

or that $\quad A \cap B \subseteq AB$

and thus $\quad AB = A \cap B.$

Theorem 13 : *Let R be a commutative ring with unity and let I_1 and I_2 be two ideals of R. Then*

(*i*) $\varphi : R \to \dfrac{R}{I_1} \times \dfrac{R}{I_2}$, *s.t.,* $\varphi(x) = (x + I_1, x + I_2)$ *is a homomorpism s.t., Ker* $\varphi = I_1 \cap I_2$.

(*ii*) I_1 *and* I_2 *are comaximal ideals of R iff* φ *is onto.*

Proof : (*i*) We leave it for the reader to verify that φ is a homomorphism.

Since $x \in \text{Ker}\,\varphi \Leftrightarrow \varphi(x) = (I_1, I_2)$

$$\Leftrightarrow (x + I_1, x + I_2) = (I_1, I_2)$$

$$\Leftrightarrow x + I_1 = I_1,\ x + I_2 = I_2$$

$$\Leftrightarrow x \in I_1,\ x \in I_2$$

$$\Leftrightarrow x \in I_1 \cap I_2$$

we find Ker $\varphi = I_1 \cap I_2$.

(*ii*) Suppose φ is onto. Then given $(1 + I_1,\ 0 + I_2) \in \dfrac{R}{I_1} \times \dfrac{R}{I_2}$, $\exists\ x \in R$, s.t.,

$$\varphi(x) = (1 + I_1, I_2)$$

$$\Rightarrow (x + I_1, x + I_2) = (1 + I_1, I_2)$$

$$\Rightarrow x + I_1 = 1 + I_1,\ x + I_2 = I_2$$

$$\Rightarrow 1 - x \in I_1,\ x \in I_2$$

$$\Rightarrow (1 - x) + x \in I_1 + I_2 \Rightarrow 1 \in I_1 + I_2 \Rightarrow I_1 + I_2 = R$$

or that I_1 and I_2 are comaximal.

Conversely, let $I_1 + I_2 = R$ (i.e., I_1, I_2 be comaximal)

Since $1 \in R$, $1 \in I_1 + I_2$ giving $1 = x + y, \quad x \in I_1, y \in I_2$

Now $$(1 + I_1, I_2) = (x + y + I_1, I_2)$$
$$= (y + I_1, I_2)$$
$$= (y + I_1, y + I_2) = \varphi(y)$$

Similarly, $$(I_1, x + I_2) = \varphi(x)$$

Now for any $(a_1 + I_1, a_2 + I_2) \in \dfrac{R}{I_1} \times \dfrac{R}{I_2}$, since

$$(a_1 + I_1, a_2 + I_2) = (1 + I_1, I_2)(a_1 + I_1, a_1 + I_1) + (I_1, 1 + I_2)(a_2 + I_1, a_2 + I_2)$$
$$= \varphi(y)\ \varphi(a_1) + \varphi(x)\ \varphi(a_2)$$
$$= \varphi(ya_1 + xa_2)$$

we find φ is onto.

Remarks (*i*) : If φ is onto, by Fundamental theorem,

$$\frac{R}{\operatorname{Ker}\varphi} \cong \frac{R}{I_1} \times \frac{R}{I_2}$$

i.e., $$\frac{R}{I_1 \cap I_2} \cong \frac{R}{I_1} \times \frac{R}{I_2}.$$

(*ii*) Let $R = \mathbf{Z}$ the integers and suppose m, n are co-prime integers. Then $\exists$ integers x, y s.t.,

$$1 = mx + ny \in (m) + (n)$$
$$\Rightarrow (m) + (n) = R$$
$$\Rightarrow (m), (n) \text{ are comaximal ideals}$$
$$\Rightarrow \varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto}$$
$$\Rightarrow \frac{\mathbf{Z}}{(m) \cap (n)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$$
$$\Rightarrow \frac{\mathbf{Z}}{(mn)} \cong \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)}$$
$$\Rightarrow Z_{mn} \cong Z_m \times Z_n \text{ if } m, n \text{ are co-prime.}$$

(*iii*) Let m, n be co-prime integers, then

$$\varphi : \mathbf{Z} \to \frac{\mathbf{Z}}{(m)} \times \frac{\mathbf{Z}}{(n)} \text{ is onto}$$

Consider $(a + (m), b + (n)) \in \dfrac{\mathbf{Z}}{(m)} \times \dfrac{\mathbf{Z}}{(n)}$, then $\exists$ an integer x s.t., $\varphi(x) = (a + (m), b + (n))$

Thus

$$(x+(m),\ x+(n)) = (a+(m),\ b+(n))$$
$$\Rightarrow x+(m) = a+(m),\ x+(n) = b+(n)$$
$$\Rightarrow x-a \in (m),\ x-b \in (n)$$
$$\Rightarrow x-a = \text{multiple of } m,\ x-b = \text{multiple of } n$$
$$\Rightarrow x \equiv a \pmod{m},\ x \equiv b \pmod{n}$$

Proving what is popularly known as *Chinese Remainder theorem.*

Maximal Ideals

Definition : Let R be a ring. An ideal $M \neq R$ of R is called a *maximal ideal* of R if whenever A is an ideal of R s.t., $M \subseteq A \subseteq R$ then either $A = M$ or $A = R$.

Example 4 : A field F has only two ideals F and $\{0\}$. It is easy to see then that $\{0\}$ is the only maximal ideal of F.

Example 5 : Let $<\mathbf{E}, +, \cdot>$ be the ring of even integers.

Let $H_4 = \{4n \mid n \text{ an integer}\}$

then H_4 is an ideal of $\mathbf{E}$ and as $2 \notin H_4$, $H_4 \neq \mathbf{E}$.

Let A be any ideal of $\mathbf{E}$, s.t., $H_4 \subseteq A \subseteq \mathbf{E}$

Suppose $H_4 \neq A$. We show $A = \mathbf{E}$.

Since $H_4 \subset A$, $\exists$ some $x \in A$ s.t., $x \notin H_4$

By division algorithm, we can write

$x = 4q + r$ where $0 < r < 4$

Note $r = 0$ would mean $x = 4q \in H_4$. But $x \notin H_4$ so $r \neq 0$. Again, $r = 1, 3$ would imply x is odd which is not true. Hence the only value that r can have is 2.

Thus $\qquad x = 4q + 2 \Rightarrow 2 = x - 4q \in A$

as $x \in A$, $4q \in H_4 \subseteq A \Rightarrow x - 4q \in A$

$2 \in A \Rightarrow$ members of the type $2+2,\ 2+2+2, \ldots\ldots, 0-2$ are all in A

$\Rightarrow \mathbf{E} \subseteq A$. But $A \subseteq \mathbf{E}$

Hence $\qquad A = \mathbf{E}$.

Example 6 : Let R^c = ring of all real valued continuous functions on [0, 1], under the operations

$$(f+g)\,x = f(x) + g(x)$$
$$(fg)\,x = f(x)\ g(x)$$

Let $\qquad M = \{f \in R^c \mid f(½) = 0\}$

then M is a maximal ideal of R.

Let g be a function from [0, 1] to the real nos., defined by

$$g(x) = 0 \text{ for all } x \in [0,\ 1]$$

then g is a real valued function and $g(½) = 0$, hence $g \in M$. Thus $M \neq \varphi$.

Again, if $f, g \in M$ be any two members, then

$$f(\tfrac{1}{2}) = g(\tfrac{1}{2}) = 0$$

$$(f-g)(\tfrac{1}{2}) = f(\tfrac{1}{2}) - g(\tfrac{1}{2}) = 0 - 0 = 0 \Rightarrow f-g \in M$$

Also for $\quad f \in M, \; h \in R^c$

$$(hf)\tfrac{1}{2} = h(\tfrac{1}{2})\, f(\tfrac{1}{2}) = h(\tfrac{1}{2}) \,.\, 0 = 0 = (fh)\tfrac{1}{2}$$

$$\Rightarrow hf, \; fh \in M$$

or that M is an ideal.

Define now, θ a function from $[0, 1]$ to the reals by

$$\theta(x) = 1 \text{ for all } x \in [0, 1]$$

then θ is a continuous function. Thus $\theta \in R^c$.

But $\theta \notin M$ as $\theta(\tfrac{1}{2}) = 1 \neq 0$

So $\quad M \neq R^c$

Let I be any ideal of R^c s.t., $M \subset I \subseteq R^c$

then $\exists\, \lambda \in I$ s.t., $\lambda \notin M$

i.e., $\quad \lambda(\tfrac{1}{2}) \neq 0$

Let $\quad \lambda(\tfrac{1}{2}) = c \neq 0$

Define β from $[0, 1]$ to reals such that

$$\beta(x) = c \text{ for all } x \in [0, 1]$$

then $\quad \beta \in R^c$

Let $\quad \psi = \lambda - \beta$

then $\quad \psi(\tfrac{1}{2}) = \lambda(\tfrac{1}{2}) - \beta(\tfrac{1}{2}) = c - c = 0$

$$\Rightarrow \psi \in M$$

$$\Rightarrow \psi \in I \text{ as } M \subseteq I$$

i.e., $\quad \beta = \lambda - \psi \in I \qquad [\lambda, \psi \text{ belong to } I]$

If γ be the function from $[0, 1]$ to reals s.t.,

$$\gamma(x) = \frac{1}{c} \quad (c \neq 0)$$

then $\quad \gamma \in R^c$

Now $\quad (\gamma\beta)(x) = \gamma(x)\,\beta(x) = \dfrac{1}{c} \,.\, c = 1 = \theta(x)$ for all x

$$\Rightarrow \gamma\beta = \theta$$

Since $\quad \beta \in I, \; \gamma\beta \in I$

we find $\theta \in I$

But θ is unity of the ring R^c,

thus I is an ideal containing unity

$$\Rightarrow I = R^c$$

Hence M is maximal.

Aliter : that M is maximal ideal can also be proved by using the Fundamental theorem of homomorphism.

Define a function $\theta : R^c \to \mathbf{R}$, s.t.,

$$\theta(f) = f(½) \text{ for all } f \in R^c$$

where $\mathbf{R}$ = set of real numbers

then θ is a homomorphism as

$$\theta(f+g) = (f+g)(½) = f(½) + g(½) = \theta(f) + \theta(g)$$

$$\theta(fg) = (fg)(½) = f(½)\, g(½) = \theta(f)\, \theta(g)$$

To check ontoness, we notice, if $r \in \mathbf{R}$ be any element we can define another map $\varphi : [0, 1] \to \mathbf{R}$, s.t.,

$$\varphi(x) = r \text{ for all } x \in [0, 1]$$

then φ being constant function will be continuous.

Thus $\varphi \in R^c$

Also $\theta(\varphi) = \varphi(½) = r$, showing that φ is pre image of r under θ

i.e., θ is onto

Thus by Fundamental theorem of homomorphism

$$\frac{R^c}{\text{Ker}\,\theta} \cong \mathbf{R}$$

Now

$$\begin{aligned} f \in \text{Ker}\,\theta &\Leftrightarrow \theta(f) = 0 \\ &\Leftrightarrow f(½) = 0 \\ &\Leftrightarrow f \in M \\ \Rightarrow \text{Ker}\,\theta &= M \end{aligned}$$

Hence $\dfrac{R^c}{M} \cong \mathbf{R}$, but $\mathbf{R}$ being a field, $\dfrac{R^c}{M}$ will be a field.

i.e., M is maximal ideal of R^c (see theorem 14 below).

Example 7 : $\{0\}$ in the ring $\mathbf{Z}$ of integers is not a maxiaml ideal as $\{0\} \subset H_4 \subset \mathbf{Z}$ where $H_4 = \{4n \mid n \in \mathbf{Z}\}$

Theorem 14 : *Let R be a commutative ring with unity. An ideal M of R is maximal ideal of R iff $\dfrac{R}{M}$ is a field.*

Proof : Let M be maximal ideal of R. Since R is commutative ring with unity, $\dfrac{R}{M}$ is also a commutative ring with unity. Thus all that we need prove is that non zero elements of $\dfrac{R}{M}$ have multiplicative inverse.

Let $x + M \in \dfrac{R}{M}$ be any non zero element

then $\quad x + M \neq M \Rightarrow x \notin M$

Let $\quad xR = \{xr \mid r \in R\}$

It is easy to verify that xR is an ideal of R. Since sum of two ideals is an ideal, $M + xR$ will be an ideal of R.

Again as $x = 0 + x \,.\, 1 \in M + xR$ and $x \notin M$ we find

$$M \subset M + xR \subseteq R$$

M, maximal $\Rightarrow M + xR = R$

Thus $\quad 1 \in R \Rightarrow 1 \in M + xR$

$$\Rightarrow 1 = m + xr \text{ for some } m \in M,\ r \in R$$

$$\Rightarrow 1 + M = (m + xr) + M$$

$$= (m + M) + (xr + M) = xr + M$$

$$= (x + M)\ (r + M)$$

$\Rightarrow (r + M)$ is multiplicative inverse of $x + M$

Hence $\dfrac{R}{M}$ is a field.

Conversely, let $\dfrac{R}{M}$ be a field.

Let I be any ideal of R s.t., $M \subset I \subseteq R$

then $\exists$ some $a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is a non zero element of $\dfrac{R}{M}$, which being a field, means $a + M$ has multiplicative inverse. Let $b + M$ be its inverse. Then

$$(a + M)\ (b + M) = 1 + M$$

$$\Rightarrow ab + M = 1 + M$$

$$\Rightarrow ab - 1 \in M$$

$$\Rightarrow ab - 1 = m \text{ for some } m \in M$$

$$\Rightarrow 1 = ab - m \in I \text{ (using def. of ideal)}$$

$\Rightarrow I = R$ (ideal containing unity, equals the ring)

Hence M is maximal ideal of R.

Remarks (*i*) : $\dfrac{R}{M}$ being a field contains at least two elements and thus unity and zero elements of $\dfrac{R}{M}$ are different i.e., $0 + M \neq 1 + M$ i.e., $1 \notin M$ or that $M \neq R$.

(*ii*) In the converse part of the above theorem we do not require R to have

unity or it to be commutative, i.e., if R is a ring and M is an ideal of R s.t., $\frac{R}{M}$ is a field then M is maximal.

Suppose I is an ideal of R s.t., $M \subset I \subseteq R$. Then $\exists\, a \in I$, s.t., $a \notin M$

Now $a \notin M \Rightarrow a + M \neq M \Rightarrow a + M$ is non zero element of $\frac{R}{M}$ and therefore has multiplicative inverse, say, $b + M$. If $c + M$ be unity of $\frac{R}{M}$ (Note $\frac{R}{M}$ can have unity even if R doesn't have unity. See exercises ahead)

Now $\quad (a + M)(b + M) = c + M$

$\Rightarrow \quad ab + M = c + M$

$\Rightarrow \quad c - ab \in M \subset I$

But $a \in I \Rightarrow ab \in I$ and so $(c - ab) + ab \in I$

$\Rightarrow \quad c \in I$

Let $r \in R$ be any element

Then $\quad (r + M)(c + M) = r + M$

$\Rightarrow \quad rc + M = r + M$

$\Rightarrow \quad r - rc \in M \subset I$

Since $c \in I$, $rc \in I$ and thus $(r - rc) + rc \in I \Rightarrow r \in I \Rightarrow R \subseteq I$

Hence $I = R$ and thus M is maximal ideal of R.

Cor. : A commutative ring R with unity is a field iff it has no proper (non trivial) ideals.

If R is a field then it has no proper ideals (see exercise 13 page 250).

Conversely, if R has no proper ideals then $\{0\}$ must be a maximal ideal. Thus $\frac{R}{\{0\}}$ is a field and as $\frac{R}{\{0\}} \cong R$, R is a field.

Definition :

Prime Ideal : An ideal $P \neq R$ of a ring R is called a *prime ideal* if $ab \in P \Rightarrow a \in P$ or $b \in P$.

Example 8 : $\{0\}$ in the ring $\mathbf{Z}$ of integers is a prime ideal as $ab \in \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

$$\Rightarrow a \in \{0\} \text{ or } b \in \{0\}$$

It is an example of a prime ideal which is not maximal.

Example 9 : $H_4 = \{4n \mid n \in \mathbf{Z}\}$ we've seen is a maximal ideal in the ring $\mathbf{E}$ of even integers.

H_4, however, is not a prime ideal as $2 \,.\, 2 = 4 \in H_4$ but $2 \notin H_4$

In fact, H_4 is neither a maximal nor a prime ideal in $\mathbf{Z}$. (See exercise 1 also)

Example 10 : $H_p = \{pn \mid n \in \mathbf{Z}\}$ will be a prime ideal in $\mathbf{Z}$ for any prime p.

The converse, howe .., is not true in view of example 8. (See exercise 1 also)

Theorem 15 : *Let R be a commutative ring. An ideal P of R is prime iff* $\frac{R}{P}$ *is an integral domain.*

Proof : Let P be a prime ideal of R

Let $(a+P)(b+P) = 0+P$

Then $ab + P = P$

$\Rightarrow ab \in P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow a + P = P$ or $b + P = P$

thus $\frac{R}{P}$ is an integral domain.

Conversely, let $\frac{R}{P}$ be an integral domain.

Let $ab \in P$ then $ab + P = P$

$\Rightarrow (a+P)\ (b+P) = P$

$\Rightarrow a + P = P$ or $b + P = P$ (R/P is an integral domain)

$\Rightarrow a \in P$ or $b \in P$

Hence the result.

Theorem 16 : *Let R be a commutative ring. An ideal P of R is a prime ideal if and only if for two ideals A, B of R, $AB \subseteq P$ implies either $A \subseteq P$ or $B \subseteq P$.*

Proof : Let P be a prime ideal of R and let $AB \subseteq P$ for two ideal A, B of R.

Suppose $A \nsubseteq P$ then $\exists$ some element $a \in A$ s.t., $a \notin P$.

Since $AB \subseteq P$, we get in particular

$aB \subseteq P$

$\Rightarrow ab \in P$ for all $b \in B$

Since P is prime, we get either $a \in P$ or $b \in P$ but $a \notin P$, hence $b \in P$ for all $b \in B$.

$\Rightarrow B \subseteq P$

Conversely, we show P is prime. Let $ab \in P$.

Let A and B be the ideals generated by a and b then $A = (a)$, $B = (b)$. If $x \in AB$ is any element then it is of the type

$$x = a_1b_1 + a_2b_2 + \ldots\ldots + a_nb_n \qquad a_i \in A,\ b_i \in B$$
$$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \ldots\ldots + (\alpha_n a)(\beta_n b)$$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a)$, $b_i \in B = (b)$

Thus $$x = (\alpha_1\beta_1)(ab) + (\alpha_2\beta_2)(ab) + \ldots\ldots + (\alpha_n\beta_n)(ab)$$

(R is commutative)

$$x = (\alpha_1\beta_1 + \alpha_2\beta_2 + \ldots\ldots + \alpha_n\beta_n)\, ab$$

Since $ab \in P$, P is an ideal, all multiples of ab are in P. Thus $x \in P$

i.e., $AB \subseteq P$

$\Rightarrow A \subseteq R$ or $B \subseteq P$

$\Rightarrow (a) \subseteq P$ or $(b) \subseteq P$

$\Rightarrow a \in P$ or $b \in P \Rightarrow P$ is prime.

Problem 15 : *Let R be a commutative ring with unity. If every ideal of R is prime show that R is a field.*

Solution : To show that R is a field, we need show that every non zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ s.t., $ab = 0$

Then $ab \in \{0\}$ which is an ideal of R and is, therefore, prime ideal

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

i.e., $a = 0$ or $b = 0$

thus R is an integral domain.

Let now $a \in R$ be any non zero element and let

$$a^2R = \{a^2r \mid r \in R\}$$

then a^2R is an ideal of R (Verify!) and is therefore prime ideal.

Now $a \,.\, a = a^2 = a^2 \,.\, 1 \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

$\Rightarrow a(1 - ab) = 0$

$\Rightarrow 1 - ab = 0$ as $a \neq 0$

$\Rightarrow b$ is multiplicative inverse of a.

Hence R is a field.

Problem 16 : *Let R be a commutative ring with unity. Show that every maximal ideal of R is prime.*

Solution : We know that an ideal M of R is maximal iff $\dfrac{R}{M}$ is a field.

Thus if M is maximal, then $\dfrac{R}{M}$ is a field and hence an integral domain.

$\Rightarrow M$ is a prime ideal (theorem 15).

Problem 17 : *Let R be a commutative ring with unity and let M be a maximal ideal of R such that $M^2 = \{0\}$. Show that if N is any maximal of R then $N = M$.*

Solution : Let $m \in M$ be any element

then $m \,.\, m \in M^2 = (0)$

$\Rightarrow m^2 = 0 \in N$ (N is an ideal)

By previous problem, N will be prime

$$\Rightarrow m \in N$$

$$\Rightarrow M \subseteq N$$

Thus $M \subseteq N \subseteq R$

Since M is maximal, $N = M$ or $N = R$

But N is maximal in R, thus $N \neq R$

Hence $N = M$.

Problem 18 : *Show that in a Boolean ring R, every prime ideal $P \neq R$ is maximal.*

Solution : Let P be prime and I be any ideal s.t.,

$$P \subset I \subseteq R$$

then $\exists$ some $x \in I$, s.t., $x \notin P$ and as $x \in R$, $x^2 = x$

Let now, $y \in R$ be any element, then

$$x^2 y = xy$$

$$\Rightarrow x(xy - y) = 0 \in P \quad (P \text{ is an ideal})$$

$$\Rightarrow xy - y \in P \text{ as } x \notin P \text{ and } P \text{ is prime}$$

$$\Rightarrow xy - y = p \text{ for some } p \in P$$

Then $y = xy - p \in I$

as $x \in I$, $y \in R$, $xy \in I$ and also $p \in P \subseteq I$,

Thus $y \in I$

$$\Rightarrow R \subseteq I \Rightarrow I = R \Rightarrow P \text{ is maximal.}$$

Problem 19 : *Show by an example that we can have a finite commutative ring in which every maximal ideal need not be prime.*

Solution : Consider the ring $R = \{0, 2, 4, 6\}$ under addition and multiplication modulo 8.

Let $M = \{0, 4\}$ then M is easily seen to be an ideal of R.

Again as $2 \otimes 6 = 4 \in M$ but $2, 6 \notin M$, we find M is not a prime ideal. We show M is maximal.

Let $M \subseteq N \subseteq R$, where N is an ideal of R.

Since $< M, + >$ will be a subgroup of $< N, + >$, bv Lagrange's theorem $o(M) \mid o(N)$. Similarly, $o(N) \mid o(R) = 4$

i.e., $2 \mid o(N)$, $o(N) \mid 4$

i.e., $o(N) = 2$ or 4

if $o(N) = 2$, then $M = N$ as $M \subseteq N$

if $o(N) = 4$, then $N = R$ as $N \subseteq R$

Hence M is maximal ideal of R.

Remark : In case the finite commutative ring contains unity, then every prime ideal is maximal. See exercises.

Problem 20 : *Let $A \neq R$ be an ideal of R, then for any $x \in R$, $x \notin A$, if $A + (x) = R$, show that A is maximal ideal of R and conversely.*

Solution : Let I be an ideal of R, such that

$$A \subset I \subseteq R$$

then $\exists$ some $x \in I$, s.t., $x \notin A$

Let (x) be the ideal generated by x.

then $A + (x)$ is an ideal of R.

Also by given condition $A + (x) = R$

Again $\quad A \subseteq I,\ x \in I \Rightarrow (x) \subseteq I$

thus $\quad A + (x) \subseteq I$

$$\Rightarrow R \subseteq I \Rightarrow I = R$$

i.e., A is maximal.

Conversely, let A be maximal, $A \neq R$. Let $x \in R$, $x \notin A$.

Then $I = A + (x)$ being sum of two ideals is an ideal of R and $A \subseteq A + (x) \subseteq R$.

Since A is maximal, $A \neq A + (x)$ as $x \notin A$. $\therefore$ $A + (x) = R$.

Definition : An ideal I of a commutative ring R is called *semi prime ideal* if $a^2 \in I \Rightarrow a \in I$, for all $a \in R$

Clearly then every prime ideal is semi prime.

Example 11 : Consider the ideal $I = \{6n \mid n \in \mathbf{Z}\}$ in the ring of integers. Suppose $a^2 \in I$

Then $\quad a^2$ is a multiple of 6

i.e., $\quad 6 \mid a^2$

Since $2 \mid 6$, we find $2 \mid a^2 \Rightarrow 2 \mid a$ (as 2 is prime)

Similarly $3 \mid a$

$$\Rightarrow 6 \mid a \text{ as } g.c.d.(2, 3) = 1$$

$$\Rightarrow a \in I$$

Hence I is semi prime, but I is not prime as $2 \cdot 3 = 6 \in I$ but $2, 3 \notin I$.

Exercises

1. In the ring of integers, show that every ideal is generated by some integer. Show further that an ideal is maximal iff it is generated by a prime.
2. Show that intersection of two prime ideals may not be a prime ideal.
3. Show that intersection of two prime ideals is a semi prime ideal and so is the intersection of two semi prime ideals.
4. Let R be a commutative ring. Let I be an ideal of R and let P be a prime ideal of I. Show that P is an ideal of R.

5. Show that a commutative ring R is an integral domain iff $\{0\}$ is a prime ideal.
6. Let R be a finite commutative ring with unity. Show that every prime ideal of R is a maximal ideal.
7. Show that $M = \{0, 3, 6, 9\}$ is a maximal ideal of Z_{12}.
8. Show that I is semi prime ideal of R iff $\frac{R}{I}$ has non zero nilpotent elements.
9. Let $\{Pi\}\ i \in X$ be a chain of prime ideals. Show that $\bigcap_i P_i$ and $\bigcup_i P_i$ are prime ideals. (By a chain, we mean either $P_i \subseteq P_j$ or $P_j \subseteq P_i$ for all $i, j \in X$).
10. Let $P \neq R$ be an ideal of R. Show P is prime ideal of R iff $R - P$ is closed under multiplication.
11. Show that an ideal A is maximal iff the pair A, B for all ideals $B \not\subseteq A$ is maximal. (See problem 20 also).
12. Show that an ideal P in a commutative ring R with unity is prime iff for ideals A, B in R, $P \subsetneqq A$, $P \subsetneqq B \Rightarrow AB \not\subseteq P$.
13. Show that $M = \{0, 6\}$ is a maximal ideal of the ring $R = \{0, 2, 4, 6, 8, 10\}$ mod 12 and hence R/M is a field. (Notice R has no unity, whereas $4 + M$ is unity of R/M.

Chapter 8

Euclidean and Factorization Domains

We discussed divisibility under results in Number theory. We now talk about this concept in rings in a generalized form.

Definition : Let R be a commutative ring. $a, b \in R$, $a \neq 0$, then we say $a \mid b$ (a divides b) if $\exists\ c \in R$ s.t., $b = ac$. a is then called a *factor* of b.

If $a, b \in R$ then an element $d \in R$ is called *greatest common divisor* (or highest common factor) of a and b if

(*i*) $d \mid a,\ d \mid b$

(*ii*) whenever $c \mid a,\ c \mid b$ then $c \mid d$

and in that case we write $d = g.c.d.(a, b)$. In fact sometimes only (a, b) is used to denote *g.c.d.* of a and b.

Remark : One can prove that

(*i*) If $a \mid b,\ b \mid c$ then $a \mid c$

(*ii*) If $a \mid b,\ a \mid c$ then $a \mid b \pm c$

(*iii*) If $a \mid b$ then $a \mid bx$ for all $x \in R$

(*iv*) If R has unity then $1 \mid x$ for all $x \in R$ and if a is a unit then $a \mid x$ for all $x \in R$.

Example 1 : Consider the ring $R = \{0, 1, 2, \ldots\ldots, 7\}$ modulo 8

then since $\quad 2 \otimes 3 = 6, \quad 2 \mid 6$

$\quad 2 \otimes 2 = 4, \quad 2 \mid 4$

Again, if $c \mid 4,\ c \mid 6$ then $c \mid 6 - 4 \Rightarrow c \mid 2$

Thus $\quad g.c.d.\ (4, 6) = 2$

Also as $\quad 6 = 6 \otimes 1,\ 4 = 6 \otimes 6$

we find $\quad 6 \mid 6$ and $6 \mid 4$

Now if $c \mid 6,\ c \mid 4$

then as $c \mid 6$, we get *g.c.d.* $(4, 6) = 6$. Thus it is possible to have more than one g.c.d. for the same pair of elements.

Example 2 : In the ring **E** of even integers we notice 4 and 6 do not have a g.c.d.

2 (the only possibility) is not a g.c.d. of 4, 6 as $2 \nmid 6$ in **E**. Indeed $6 = 2 . 3$ but then $3 \notin$ **E**.

Definition : Let R be a commutative ring. A non zero element $l \in R$ is called *least common multiple* (l.c.m.) of two (non zero) elements $a, b \in R$ if

(*i*) $a \mid l, b \mid l$

(*ii*) if $a \mid x, b \mid x$ then $l \mid x$

We denote l by l.c.m. $(a, b) = [a, b]$

Just as proved above one can show that a pair of elements in a ring may not have an l.c.m. and a pair could have more than one l.c.m. See exercises.

Definition : Let R be a commutative ring with unity. Then $a, b \in R$ are called *associates* if $b = ua$ for some unit u in R.

We recall here that by a unit we mean an element which has multiplicative inverse. The above definition will not be 'complete' unless we show that the relation 'is an associate of' is an equivalence relation. If we denote the relation by $\sim$

then $\quad a \sim a$ as $a = 1 . a$ and 1 is a unit

$$a \sim b \Rightarrow b = ua \text{ where } u \text{ is a unit}$$
$$\Rightarrow u^{-1} b = a$$
$$\Rightarrow b \sim a$$

Indeed u^{-1} will be a unit if u is a unit.

Finally $\quad a \sim b, b \sim c \Rightarrow b = ua$

$$c = vb \text{ for units } u, v$$

Since $\quad c = vb = v(ua) = (vu)a$

Showing $\quad c \sim a$

as $uu^{-1} = 1, vv^{-1} = 1 \Rightarrow (vu)(vu)^{-1} = (vu)(u^{-1} v^{-1}) = 1$

we notice vu is a unit.

Example 3 : $3i - 4$ is an associate of $4i + 3$ in complex nos.

Problem 1 : *Let R be an integral domain with unity and $a, b \in R$ be non zero elements such that $a \mid b$ and $b \mid a$, then a and b are associates and conversely.*

Solution : $\quad a \mid b \Rightarrow b = xa$

$$b \mid a \Rightarrow a = yb \text{ for some } x, y \in R$$

$\therefore \quad b = xa = x(yb)$

$$\Rightarrow b(1 - xy) = 0$$
$$\Rightarrow 1 - xy = 0 \text{ as } b \neq 0$$
$$\Rightarrow y \text{ is a unit in } R \text{ and } a = yb.$$

Conversely, if a, b are associates then $\exists$ a unit u, s.t., $a = bu$ (and so $au^{-1} = b$).

$$\Rightarrow b \mid a \text{ and } a \mid b.$$

Theorem 1 : *Let R be an integral domain with unity. If d_1 = g.c.d.(a, b) in R then d_2 is also a g.c.d.(a, b) iff d_1 and d_2 are associates.*

Proof : One may remark here that we prove this result only after assuming the existence of *g.c.d.*

Let d_1 and d_2 be both *g.c.d.*(a, b).

Then $\quad d_1 \mid a,\ d_1 \mid b$

and $\quad d_2 \mid a,\ d_2 \mid b$

by definition, we get $d_1 \mid d_2$ and $d_2 \mid d_1$

$\Rightarrow d_1$ and d_2 are associates. (using problem 1)

Conversely, let d_1 = g.c.d.(a, b) and d_2 be an associate of d_1.

then $\quad ud_2 = d_1$ for some unit u

$\Rightarrow d_2 \mid d_1$ and as $d_1 \mid a,\ d_1 \mid b$

we find $\quad d_2 \mid a$ and $d_2 \mid b$

Let $x \mid a,\ x \mid b$ then $x \mid d_1$ as d_1 is *g.c.d.*(a, b)

Also as $\quad d_2 = d_1 u^{-1}$

$d_1 \mid d_2$

and thus $\quad x \mid d_2$

$\Rightarrow d_2$ = g.c.d.(a, b).

Theorem 2 : *Let R be an integral domain with unity. If l_1 = l.c.m.(a, b) in R then l_2 is also an l.c.m.(a, b) iff l_1 and l_2 are associates.*

Proof : Follows similarly as the above theorem.

Problem 2 : *Let R be an integral domain with unity. If* g.c.d.$(a, b) = d$ *for $a, b \in R$ then*

cd and g.c.d.(ca, cb) are associates.

Solution : Let g.c.d.$(ca, cb) = d'$

Since $d \mid a$, $\quad a = dk$

$\Rightarrow ac = dkc = cdk$

$\Rightarrow cd \mid ca$

Similarly $\quad cd \mid cb \Rightarrow cd \mid d' \Rightarrow d' = cdt$

Again $\quad d' \mid ca \Rightarrow ca = d's$

$\Rightarrow ca = d's = cdts$

$\Rightarrow a = (dt)\, s \Rightarrow dt \mid a$

Similarly $\quad dt \mid b$

$\Rightarrow dt \mid d \Rightarrow d = dtp \Rightarrow d\,(1 - tp) = 0$

$\Rightarrow 1 = tp \Rightarrow t$ is a unit

$\Rightarrow$ g.c.d$(ca, cb) = d' = cdt$

i.e., cd and d' are associates.

Euclidean Domains

Definition : An integral domain R is called a *Euclidean domain* (or a Euclidean ring) if for all $a \in R$, $a \neq 0$ there is defined a non -ve integer $d(a)$ s.t.,

(*i*) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $d(a) \leq d(ab)$

(*ii*) for all $a, b \in R$, $a \neq 0$, $b \neq 0$, $\exists$ t and r in R s.t.,

$$a = tb + r$$

where either $r = 0$ or $d(r) < d(b)$.

Example 4 : Consider the integral domain $< \mathbf{Z}, +, \cdot >$ of integers. For any $0 \neq a \in \mathbf{Z}$, define $d(a) = |a|$, then $d(a)$ is non -ve integer.

Again, let $a, b \in \mathbf{Z}$ be any elements s.t., $a \neq 0$, $b \neq 0$

then $\quad d(a) = |a|$

$\quad d(ab) = |ab| = |a|\,|b|$

thus $\quad d(a) \leq d(ab)$ as $|a| \leq |a|\,|b|$

Again let $a, b \in \mathbf{Z}$ $(a, b \neq 0)$

Suppose $b > 0$, then it is possible to write

$$a = tb + r \text{ where } 0 \leq r < b$$

$$t, r \in \mathbf{Z}$$

If $r \neq 0$ then $r < b \Rightarrow |r| < |b|$

$$\Rightarrow d(r) < d(b)$$

If $b < 0$ then $(-b) > 0$, $\therefore$ $\exists$ $t, r \in \mathbf{Z}$ s.t.,

$$a = (-b)\ t + r \qquad \text{where } 0 \leq r < -b$$

$$a = (-t)\ b + r$$

and if $r \neq 0$, $r < -b \Rightarrow |r| < |b|$

$$\Rightarrow d(r) < d(b)$$

Hence $< \mathbf{Z}, +, \cdot >$ is a Euclidean domain.

Remarks (*i*) : When we say, in the definition, that $\exists$ a non -ve integer $d(a)$ for any $0 \neq a$, we mean, $\exists$ a function d from $R - \{0\}$ to $\mathbf{Z}^+ \cup \{0\}$ where $\mathbf{Z}^+$ is set of +ve integers. This function d is called Euclidean valuation on R. Also the last condition in the definition is called *Euclidean algorithm*.

(*ii*) We can show that the t and r mentioned in the last (Euclidean algorithm) condition in the definition of Euclidean domain are uniquely determined iff

$$d(a + b) \leq \text{Max. } \{d(a), d(b)\}.$$

Let $\quad d(a + b) \leq \text{Max. } \{d(a), d(b)\}$ and

Suppose $\quad a = tb + r = t_1 b + r_1$

Let $\quad r_1 - r \neq 0$, then $b(t - t_1) = r_1 - r \neq 0$, and so $t - t_1, \neq 0$

Now $\quad d(b) \leq d(b(t - t_1))$

$$= d(r_1 - r)$$

$$\leq \text{Max. } \{d(r_1), d(-r)\} \quad \text{(given condition)}$$
$$= \text{Max. } \{d(r_1), d(-r)\}$$
$$< d(b) \text{ -which is not possible.}$$

Thus $r_1 - r = 0 \Rightarrow b(t - t_1) = 0$

or $t - t_1 = 0$ as $b \neq 0$

$\Rightarrow t = t_1$ and $r = r_1$

Conversely, let t, r be uniquely determined and suppose $d(a+b) > \text{Max.}\{d(a), d(b)\}$ for some a, b (non zero) in R.

Now $b = 0(a+b) + b = 1 . (a+b) - a$

Also $d(-a) = d(a) < d(a+b)$

and $d(b) < d(a+b)$

Thus for $b, 1 \in R$, $\exists\, t = 0$, $r = b$ or $t_1 = 1$, $r_1 = -a$ s.t., $b = t . 1 + r$, $b = t_1 1 + r_1$ where $r \neq r_1$ (as $a + b \neq 0$) $t \neq t_1$, a contradiction to the uniqueness.

Hence $d(a+b) \leq \text{Max}\,(d(a), d(b))$. Note that a Euclidean domain contains unity (see cor. ahead).

Theorem 3 : *Let R be a Euclidean domain and let A be an ideal of R, then $\exists\, a_o \in A$ s.t. $A = \{a_o x \mid x \in R\}$.*

Proof : If $A = \{0\}$, we can take $a_o = 0$.

Suppose $A \neq \{0\}$, then $\exists$ at least one $0 \neq a \in A$.

Let $a_o \in A$ be such that $d(a_o)$ is minimal, [Existence is ensured by the well ordering principle which states that every non empty subset of non -ve integers has least element].

We claim A is generated by this a_o.

Let $a \in A$, $a \neq 0$ then by definition, $\exists\, t, r \in R$, s.t.,

$$a = a_o t + r \text{ where either } r = 0 \text{ or } d(r) < d(a_o)$$

Suppose $\quad r \neq 0$

Then $\quad a_o \in A,\ t \in R \Rightarrow ta_o \in A$

$\therefore \quad a \in A,\ ta_o \in A \Rightarrow a - ta_o \in A$

$$\Rightarrow r \in A$$

But $d(a_o)$ is the smallest d-value in A and $d(r) < d(a_o)$, which leads to a contradiction

hence $\quad r = 0$

$$\Rightarrow a = ta_o$$

Thus any $a \in A$ can be put in the form ta_o

$$\Rightarrow A \subseteq \{a_o x \mid x \in R\}$$

But $\{a_o x \mid x \in R\} \subseteq A$ as $a_o \in A \Rightarrow xa_o \in A$ for all $x \in R$

Hence $\quad A = \{a_o x \mid x \in R\}$

which proves the theorem.

Definition : Such an ideal A which contains multiples of an element a_o, including

a_o of R is called a *Principal Ideal* of R, generated by a_o. We denote this by $A = (a_o)$. (See page 243 also)

In other words, the smallest ideal of R which contains a_o is called Principal Ideal generated by a_o.

In view of this definition the previous theorem will read as

Theorem 4 : *Every ideal in a Euclidean domain is a principal ideal.*

Cor. : A Euclidean domain possesses unity.

Proof : Let R be a Euclidean domain then R is its own ideal and, therefore, R is generated by some element r_o of R.

Thus each element of R is a multiple of r_o.

In particular r_o is a multiple of r_o

i.e., $r_o = r_o k$ for some $k \in R$

Now if $a \in R$ is any element then as $R = (r_o)$

$$a = xr_o \text{ for some } x$$

hence $ak = (xr_o)\ k = x(r_o k) = xr_o = a$

i.e., k is unity of R.

Definition : An integral domain R with unity is called a *Principal Ideal Domain* (PID) if every ideal of R is a principal ideal.

In fact, if R happens to be a commutative ring with unity with above condition, we call it a principal ideal ring.

In view of the previous theorem and cor., we get

Theorem 5 : *A Euclidean domain is a PID.*

In particular thus, the ring $< \mathbf{Z}, +, \cdot >$ of integers is a PID. This result follows independently if we recall (see exercise 1, page 285) that every ideal in $< \mathbf{Z}, +, \cdot >$ is a principal ideal.

Remarks (*i*) : A field F is always a PID as it has only two ideals F and $\{0\}$. F is generated by 1 and $\{0\}$ by 0.

(*ii*) One can show that there exist PIDs which are not Euclidean domains. In particular, $\mathbf{Z}[\sqrt{-19}] = \{a + \sqrt{-19}\, b \mid a, b \in \mathbf{Z}\}$ where a, b are both odd or both even, is a PID but not a Euclidean domian.

(*iii*) See page 319 for an example of an ideal which is not principal.

Problem 3 : *Show that in a PID every non zero prime ideal is maximal.*

Solution : Let $P = (p)$, $p \neq 0$, be a non zero prime ideal in a PID R.

Suppose $P \subseteq Q = (q) \subseteq R$

Then $P \in P \subseteq Q = (q)$

$$\Rightarrow p = qr$$

$$\Rightarrow qr \in P$$

$$\Rightarrow q \in P \text{ or } r \in P$$

If $q \in P$ then all multiples of q are in $P \Rightarrow Q \subseteq P$

thus $\quad Q = P$

If $r \in P$ then $\quad r = pt \Rightarrow r = qrt$

$$\Rightarrow r(1 - qt) = 0$$

$$\Rightarrow 1 = qt \qquad (r \neq 0)$$

But $q \in Q,\ t \in R \Rightarrow qt \in Q \Rightarrow 1 \in Q \Rightarrow Q = R$

Note $r = 0$ would mean $p = q \,.\, 0 \Rightarrow p = 0 \Rightarrow P = (0)$.

Remark : In view of problem 16 page 283 we find a non zero ideal in a PID is prime iff it is maximal.

Problem 4 : *Find all the prime ideals of* $\dfrac{Z_n}{(n)}$, $(n > 1)$ *and hence of* Z_n.

Solution : We know any ideal of R/N is of the type $\dfrac{A}{N}$, where A is an ideal of R, containing N. (See Cor. Page 261)

Let $(n) = N$ and $n = p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots\ldots p_r^{\alpha r}$, where p_i are distinct primes.

Let $\dfrac{A}{N}$ be any prime ideal of $\dfrac{\mathbf{Z}}{N}$, then A is an ideal of $\mathbf{Z}$. We show it is a prime ideal of $\mathbf{Z}$. Since A is an ideal of $\mathbf{Z}$, it is of the type $A=(a)$. Suppose A is not a prime ideal of $\mathbf{Z}$. Then $\exists x, y \in \mathbf{Z}$, s.t., $xy \in A$ but x and y are not in A.

Now $xy \in A \Rightarrow Nxy \in A/N \Rightarrow NxNy \in A/N$

$\Rightarrow Nx$ or $Ny \in A/N$ as A/N is prime ideal

$\Rightarrow x$ or y is in A, a contradiction.

Hence $A = (a)$ is a prime ideal and thus a is a prime (see remark on page 308 and exercise 1 page 285) Also $(n) \subseteq (a)$. Since $n \in (n) \subseteq (a)$ we find $a|n$.

But primes dividing n are $p_1, p_2, \ldots\ldots, p_r$

Thus $a = p_i$ for same i, $1 \leq i \leq r$

Hence if $A/(n)$ is any prime ideal of $\dfrac{\mathbf{Z}}{(n)}$ then it is of the type $\dfrac{(p_i)}{(n)}$ for sam i, $1 \leq i \leq r$.

Conversely, any ideal of the type $\dfrac{(p_i)}{(n)}$, $1 \leq i \leq r$ will be a prime ideal of $\dfrac{\mathbf{Z}}{(n)}$ as $\dfrac{\mathbf{Z}/(n)}{(p_i)/(n)} \cong \dfrac{\mathbf{Z}}{(p_i)}$.

Since (p_i) is a prime ideal of $\mathbf{Z}$, $\dfrac{\mathbf{Z}}{(p_i)}$ is an integral domain

Thus $\dfrac{\mathbf{Z}/(n)}{(p_i)/(n)}$ is an integral domain and hence $\dfrac{(p_i)}{(n)}$ are prime ideals of $\dfrac{\mathbf{Z}}{(n)}$ $1 \le i \le r$.

where p_i are all the primes dividing n.

We thus conclude that if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ then $\dfrac{(p_1)}{(n)}, \dfrac{(p_2)}{(n)}, \ldots\ldots, \dfrac{(p_r)}{(n)}$ are precisely the prime ideals of $\dfrac{\mathbf{Z}}{(n)}$

We've seen earlier (see page 261) that

$\theta : \dfrac{\mathbf{Z}}{(n)} \to Z_n$, s.t.,

$\theta(m + (n)) = m \quad 0 \le m < n$

is an isomorphism.

Now if P is a prime ideal of $\dfrac{\mathbf{Z}}{(n)}$, then $\theta(P)$ is a prime ideal of Z_n.

Since $\dfrac{(p_i)}{(n)}$ are all the prime ideals of $\dfrac{\mathbf{Z}}{(n)}$, their images under θ are the prime ideals of Z_n i.e., (p_1), (p_2) ,....., (p_r) are all the prime ideals of Z_n.

Remarks (*i*) : In particular, prime ideal of Z_p where p is a prime is $(p) = (0)$ as $p = 0$ in Z_p. Recall, a field has no non - trivial ideals and Z_p is an ideal when p is prime.

(*ii*) : Since a non zero ideal in $\mathbf{Z}$ is maximal iff it is prime, the above result can similarly be proved for maximal ideals.

Problem 5 : *Show that* $\mathbf{Z}[i] = \{a + ib \mid a, b \in \mathbf{Z}\}$, *the ring of Gaussian integers is a Euclidean domain.*

Solution : We know that $\mathbf{Z}[i]$ is an integral domain.

For any $0 \ne x \in \mathbf{Z}[i]$, where $x = a + ib$, define

$$d(x) = d(a + ib) = a^2 + b^2$$

Then as $x \ne 0$, either $a \ne 0$ or $b \ne 0$

thus $\quad d(a + ib) = a^2 + b^2 > 0$

Let now $x, y \in \mathbf{Z}[i]$, s.t., $x \ne 0$, $y \ne 0$ and let $x = a + ib$, $y = c + id$.

Then
$$\begin{aligned} d(xy) &= d((a + ib)(c + id)) = d((ac - bd) + i(ad + bd)) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (a^2 + b^2)(c^2 + d^2) \\ &= d(x)\, d(y) \end{aligned}$$

Since $y \neq 0$, $d(y) \geq 1$ [$y \neq 0$ means c or d is non zero]

Thus $d(xy) \geq d(x)$

We now prove the last condition in the definition of a Euclidean domain.

Let $x, y \in \mathbf{Z}[i]$ be two members where x is an ordinary +ve integer $n(x = n + io)$ and $y = a + ib$

By Euclid's division algorithm,

$$a = un + r_1 \qquad 0 \leq r_1 < n$$
$$b = vn + r_2 \qquad 0 \leq r_2 < n$$

Now either $r_1 \leq \frac{n}{2}$ or $r_1 > \frac{n}{2}$

if $r_1 > \frac{n}{2}$ then $-r_1 < -\frac{n}{2}$

$$\Rightarrow n - r_1 < n - \frac{n}{2} = \frac{n}{2}$$

Thus
$$\begin{aligned} a &= un + r_1 = un + n - n + r_1 \\ &= n(u+1) - (n - r_1) \\ &= nq + k_1 \text{ where } k_1 = -(n - r_1) \end{aligned}$$
$$|k_1| = n - r_1 < \frac{n}{2}$$

Thus whether $r_1 \leq \frac{n}{2}$ or $\frac{n}{2} < r_1$

we can express

$$a = nq + k_1 \text{ where } |k_1| \leq \frac{n}{2}$$

Similarly, $b = nq + k_2$ where $|k_2| \leq \frac{n}{2}$

i.e., $a + ib = n(q + iq') + (k_1 + ik_2)$

or $y = tn + r$ $[t = q + iq',\ r = k_1 + ik_2]$

where either $r = 0$ (k_1 & k_2 could be zero)

or $d(r) = d(k_1 + ik_2) = k_1^2 + k_2^2 \leq \frac{n^2}{4} + \frac{n^2}{4} < n^2 = d(n)$

Thus, under this particular case, the result is proved.

Let now $x, y \in \mathbf{Z}[i]$ be any two non zero members then $x\bar{x}$ is a + ve integer, say, n.

We apply the above result proved, to $y\bar{x}$ and n and find that

For $y\bar{x}$ and n, $\exists$ $t, r \in \mathbf{Z}[i]$, s.t.,

$$y\bar{x} = tn + r$$

where either $r = 0$ or $d(r) < d(n)$

If $r = 0$ then $y\bar{x} = tn = tx\bar{x} \Rightarrow y = tx + 0$

If $d(r) < d(n)$ then $d(y\bar{x} - tn) < d(x\bar{x})$

$$\Rightarrow d(y\bar{x} - tx\bar{x}) < d(x)\, d(\bar{x})$$

$$\Rightarrow d(\bar{x})\ d(y - tx) < d(x)\, d(\bar{x})$$

$$\Rightarrow d(y - tx) < d(x) \qquad [d(\bar{x}) > 0]$$

Put $\quad y - tx = r_0$ then $d(r_0) < d(x)$

So $\quad y = tx + r_0$ where $d(r_0) < d(x)$

combining, we get

$y = tx + r_0$, where either $r_0 = 0$ or $d(r_0) < d(x)$.

Hence the result is proved.

Problem 6 : *Show that* $\mathbf{Z}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbf{Z}\}$ *is a Euclidean domain*

Solution : It is easy to see that $\mathbf{Z}[\sqrt{2}]$ is an integral domain. Define a mapping $d : \mathbf{Z}[\sqrt{2}] - \{0\} \to \mathbf{Z}$, by

$$d(a + \sqrt{2}\, b) = |a^2 - 2b^2|$$

then $|a^2 - 2b^2| \geq 1$ as $a^2 - 2b^2 = 0 \Rightarrow \sqrt{2} = \dfrac{a}{b}$ which is not possible.

Again,
$$\begin{aligned} d[(a + \sqrt{2}\, b)(c + \sqrt{2}\, d)] &= d[(ad + 2bd) + \sqrt{2}\,(ad + bc)] \\ &= |(ac + 2bd)^2 - 2\,(ad + bc)^2| \\ &= |(a^2 - 2b^2)\,(c^2 - 2d^2)| \\ &= |a^2 - 2b^2|\,|c^2 - 2d^2| \qquad \text{.....(1)} \\ &\geq |a^2 - 2b^2| = d(a + \sqrt{2}\, b) \end{aligned}$$

i.e.,
$$d(a + \sqrt{2}\, b) \leq d[(a + \sqrt{2}\, b)(c + \sqrt{2}\, d)]$$

Let now $a + \sqrt{2}\, b$ and $c + \sqrt{2}\, d$ be two members of $\mathbf{Z}[\sqrt{2}]$ and suppose $c + \sqrt{2}\, d \neq 0$, then

$$\frac{a + \sqrt{2}b}{c + \sqrt{2}d} = \frac{(a + \sqrt{2}b)\ (c - \sqrt{2}d)}{c^2 - 2d^2} = \frac{ac - bd}{c^2 - 2d^2} + \frac{\sqrt{2}\,(bc - ad)}{c^2 - 2d^2}$$

$$= m + \sqrt{2}\, n \qquad \text{(say)}$$

then m and n are rationals.

Now $m = [m] + \theta$ where $[m]$ is the greatest integer not greater than m and θ is fractional part of m.

If $0 \le \theta \le \frac{1}{2}$, take $p = [m]$

and if $\frac{1}{2} < \theta < 1$, take $p = [m] + 1$

Thus $\exists$ an integer p, s.t., $|m - p| \le \frac{1}{2}$

Similarly we can find an integer q, s.t., $|n - q| \le \frac{1}{2}$

Put $m - p = \alpha$, $n - p = \beta$, then $|\alpha| \le \frac{1}{2}$, $|\beta| \le \frac{1}{2}$

Also then $\dfrac{a + \sqrt{2}b}{c + \sqrt{2}d} = (p + \alpha) + \sqrt{2}\,(q + \beta)$

$$\Rightarrow \frac{a + \sqrt{2}b}{c + \sqrt{2}d} = (p + \sqrt{2}\,q) + (\alpha + \sqrt{2}\,\beta)$$

$$\Rightarrow a + \sqrt{2}\,b = (c + \sqrt{2}\,d)\,(p + \sqrt{2}\,q) + (c + \sqrt{2}\,d)\,[(m - p)] + \sqrt{2}\,(n - q)]$$

where, of course, $(p + \sqrt{2}\,q) \in \mathbf{Z}[\sqrt{2}\,]$ as p, q are integers

we can thus write

$$a + \sqrt{2}\,b = (c + \sqrt{2}\,d)\,(p + \sqrt{2}\,q) + r$$

where $\quad r = (c + \sqrt{2}\,d)\,[(m - p) + \sqrt{2}\,(n - q)]$

and as $\quad r = (a + \sqrt{2}\,b) - (c + \sqrt{2}\,d)\,(p + \sqrt{2}\,q)$

we notice $\quad r \in \mathbf{Z}[\sqrt{2}\,]$

Now if $r \ne 0$, $d(r) = d\,[(c + \sqrt{2}\,d)\,\{(m - p) + (n - q)\sqrt{2}\,\}]$

$$= [d\,(c + \sqrt{2}\,d)]\,[d((m - p) + \sqrt{2}\,(n - q))]$$

[using (1) one may notice here that in proving (1) we do not essentially require that a, b, c, d are integers]

$$\Rightarrow d(r) = |c^2 - 2d^2|\,|(m - p)^2 - 2\,(n - q)^2|$$

$$\le |c^2 - 2d^2|\,|(m - p)^2 + 2\,(n - q)^2|$$

$$\le |c^2 - 2d^2|\,\left|\frac{1}{4} + \frac{2}{4}\right|$$

$$\le |c^2 - 2d^2| = d\,(c + \sqrt{2}\,d)$$

Hence, for $a+\sqrt{2}\,b,\ c+\sqrt{2}\,d \in \mathbf{Z}[\sqrt{2}]\ \exists\ p+\sqrt{2}\,q,\ r \in \mathbf{Z}[\sqrt{2}]$ s.t.,

$$(a+\sqrt{2}\,b) = (c+\sqrt{2}\,d)\ (p+\sqrt{2}\,d) + r$$

where either $r = 0$ or $d(r) < d(c+\sqrt{2}\,d)$

showing that $\mathbf{Z}[\sqrt{2}]$ is a Euclidean domain.

Theorem 6 : *Let a, b be two non zero elements of a Euclidean domain R. If b is not a unit in R then* $d(a) < d(ab)$.

Proof : Let $A = (a)$ be the ideal generated by a.

By definition of a Euclidean domain

$$d(a) \le d(xa) \text{ for all } 0 \ne x \in R$$

Since $\quad xa \in A$ for all $x \in R$

$d(a) \le d(xa)$ for all members xa of A

or all members of A

Thus d-value of a is minimum among the d-values of all elements of A.

Since $\quad ab \in A,\ d(a) \le d(ab)$

If $d(a) = d(ab)$ then we claim $A = (ab)$.

Let $ab = a_0$,

Since d-value of a is min. and $d(a) = d(ab) = d(a_0)$, d-value of a_0 is min. among d-values of all elements of A.

Let $0 \ne x \in A$ be any element. By def. of Euclidean domain, $\exists\ t,\ r \in R$, s.t., $x = ta_0 + r$ where either $r = 0$ or $d(r) < d(a_0)$

If $r \ne 0$ then as $a_0 \in A,\ t \in R,\ ta_0 \in A$

$$\Rightarrow x - ta_0 \in A$$

$$\Rightarrow r \in A$$

thus $r \in A$ and $d(r) < d(a_0)$, a contradiction to the minimality of $d(a_0)$.

Hence $r = 0$ and thus any $x \in A$ is such that $x = ta_0$

$$\Rightarrow A = (a_0)$$

$$\Rightarrow A = (ab).$$

Now, as $a \in A$, $a = aby$ for some y

$$\Rightarrow a(1-by) = 0$$

$$\Rightarrow 1 - by = 0 \text{ as } a \ne 0$$

$$\Rightarrow b \text{ is a unit, a contradiction}$$

Hence $\quad d(a) \ne d(ab)$

i.e., $\quad d(a) < d(ab)$.

Remark : $d(a) \le d(ab)$ follows by definition of a Euclidean domain. We do early part of the proof only to establish that $d(a)$ is minimum d-value amongst all d-values of members of A.

Problem 7 : *Show that an element x in a Euclidean domain is a unit if and only if $d(x) = d(1)$.*

Solution : Let $d(x) = d(1)$.

Suppose x is not a unit, then by above theorem

$$d(1) < d(1 \,.\, x) \qquad \text{Taking } a = 1,\ b = x$$

i.e., $d(1) < d(x)$

a contradiction

$\therefore$ x is a unit.

Conversely, let x be a unit in R, then $\exists\, y \in R$ s.t.,

$$xy = 1$$

Now $d(x) \le d(xy)$ (by definition)

$$\Rightarrow d(x) \le d(1)$$

Also $d(1) \le d(1 \,.\, x)$

$$\Rightarrow d(1) \le d(x)$$

Hence $d(x) = d(1)$.

Problem 8 : *Show by an example that it is possible to find two elements a, b in a Euclidean domain such that $d(a) = d(b)$ but a, b are not associates.*

Solution : Consider $D = \{a + ib \mid a,\ b \in \mathbf{Z}\}$

and let $d(a + ib) = a^2 + b^2$

then D is a Euclidean domain.

Here $d(2 + i3) = 13 = d(2 - 3i)$

but $2 + 3i$ and $2 - 3i$, are not associates.

Notice that units of D are ± 1, $\pm i$ and thus an associate of $2 + 3i$ can be

$$(2 + 3i)\ 1,\ (2 + 3i)\ (-1),\ (2 + 3i)\ i,\ (2 + 3i)\ (-i)$$

i.e., $2 + 3i$, $-2 - 3i$, $2i - 3$, $3 - 2i$

which are all different from $2 + 3i$.

Theorem 7 : *Any two non zero elements a, b in a Euclidean domain R have a g.c.d. d and it is possible to write*

$$d = \lambda a + \mu b \text{ for some } \lambda,\ \mu \in R.$$

Proof : Let $A = \{ra + sb \mid r,\ s \in R\}$

then A is an ideal of R as

$$0 = 0 \,.\, a + 0 \,.\, b \in A \Rightarrow A \ne \varphi$$

$$x,\ y \in A$$

$$\Rightarrow x = r_1 a + s_1 b,\ y = r_2 a + s_2 b \qquad r_1,\ r_2,\ s_1,\ s_2 \in R$$

Thus $x - y = (r_1 - r_2)\, a + (s_1 - s_2)\, b \in A$

Again $x \in A,\ r \in R,\ x = r_1 a + s_1 b$

$$\Rightarrow rx = r(r_1 a + s_1 b) = (rr_1)\, a + (rs_1)\, b \in A$$

Showing that A is an ideal of R.

Since a Euclidean domain is a PID, A will be generated by some element, say, d.

We claim $\quad d = g.c.d.(a, b)$

Now $d \in A \Rightarrow d = \lambda a + \mu b$ for some $\lambda, \mu \in R$

Again since $\quad a = 1 . a + 0 . b \in A$

$$b = 0 . a + 1 . b \in A$$

(Note R being a Euclidean domain has unity)

So $a \in A,\ A = (d) \Rightarrow a = \alpha d$ for some $\alpha \in R$

$b \in A,\ A = (d) \Rightarrow b = \beta d$ for some $\beta \in R$

$$\Rightarrow d \mid a \text{ and } d \mid b$$

Again, if $c \mid a$ and $c \mid b$

then $c \mid \lambda a,\ c \mid \mu b$

$$\Rightarrow c \mid \lambda a + \mu b$$

i.e. $\quad c \mid d \Rightarrow d = g.c.d.(a, b)$.

Remark : The theorem clearly then holds in a PID, and the next result that we prove in a PID holds in a Euclidean domain.

Theorem 8 : *Any two non zero elements a, b in a PID R have a least common multiple.*

Proof : Let $A = (a)$, $B = (b)$ be the ideals generated by a and b.

Then $A \cap B$ is an ideal of PID R. Suppose it is generated by l.

We show $\quad l = l.c.m.(a, b)$

$$A \cap B \subseteq A, A \cap B \subseteq B$$

$$l \in (l) \Rightarrow l \in (a) \Rightarrow l = au \text{ for some } u$$

$$l \in (l) \Rightarrow l \in (b) \Rightarrow l = bv \text{ for some } v$$

$$\Rightarrow a \mid l \text{ and } b \mid l$$

Again, suppose $a \mid x$ and $b \mid x$

$$\Rightarrow x = a\alpha,\ x = b\beta \quad \alpha, \beta \in R$$

$$\Rightarrow x \in (a), x \in (b)$$

$$\Rightarrow x \in A \cap B = (l)$$

$$\Rightarrow x = kl \Rightarrow l \mid x$$

Hence $\quad l = l.c.m.(a, b)$

Definition : In an integral domain R, with unity, a, b (non zero) are said to be *co-prime* or *relatively prime*, if $g.c.d.(a, b)$ is a unit in R.

Problem 9 : *Two elements a, b in an integral domain with unity are co-prime iff* $g.c.d.(a, b) = 1$.

Solution : Let a, b be co-prime. By theorem 1 any associate of a $g.c.d.$ is a $g.c.d.$

Since 1 is associate of any unit

1 will be an associate of $d = g.c.d.(a, b) =$ a unit

$$\Rightarrow 1 = g.c.d.(a, b)$$

Converse is obvious as 1 is a unit.

Problem 10 : *Let R be a PID and a, b be two non zero elements of R. Show that $[a, b]\,(a, b) = abu$ where u is a unit and $(a, b) = g.c\,d\,(a, b)$, $[a, b] = l.c.m.\,(a, b)$.*

Solution : Let $g.c.d.(a, b) = d$

$l.c.m.(a, b) = l$

Since R is a PID exercise of d and l is ensured. We show $dl \mid ab$ and $ab \mid dl$

Since $l = l.c.m.(a, b)$, $a \mid l$ and $b \mid l$

we get $l = au$, $l = bv$ for some $u, v \in R$

Again $d = g.c.d.(a, b) \Rightarrow \exists\ x, y \in R$, s.t.,

$ax + by = d$ (theorem done)

$$\Rightarrow l(ax + by) = dl$$

$$\Rightarrow lax + lby = dl$$

$$\Rightarrow bvax + auby = dl$$

$$\Rightarrow ab(vx + uy) = dl \Rightarrow ab \mid dl \qquad \text{....(1)}$$

Again as $d \mid a$, $d \mid b$, $a = d\alpha$, $b = d\beta$, $\alpha, \beta \in R$

$$\Rightarrow ab = d\alpha\, d\beta = d(\alpha\beta d)$$

Now $a = d\alpha$ and $d\alpha \mid d\alpha\beta$

$b = d\beta$ and $d\beta \mid d\alpha\beta$

$\therefore$ $a \mid d\alpha\beta, b \mid d\alpha\beta$

$$\Rightarrow l \mid d\alpha\beta$$

$$\Rightarrow d\alpha\beta = lk \text{ for some } k$$

Thus $ab = d(\alpha\beta k) = (dl)k$

$$\Rightarrow dl \mid ab \qquad \text{... (2)}$$

(1) and (2) imply $dl = uab$

where u is a unit (result proved).

Note : See page 321 for method explaining how to find g.c.d. in general.

Prime and Irreducible Elements

Definitions : Let R be a commutative ring with unity. An element $p \in R$ is called a *prime element* if

(*i*) $p \neq 0$, p is not a unit.

(*ii*) For any $a, b \in R$, if $p \mid ab$ then $p \mid a$ of $p \mid b$.

Let R be a commutative ring with unity. An element $p \in R$ is called an *irreducible element* if

Department of Mathematics
P380
LIBRARY

(*i*) $p \neq 0$, p is not a unit.

(*ii*) whenever $p = ab$ then one of a or b must be a unit. (In other words, p has no proper factors).

Example 5 : In the ring $< \mathbf{Z}, +, \cdot >$ of integers, every prime number is a prime element as well as irreducible element.

Example 6 : Consider the ring

$$\mathbf{Z}(\sqrt{-5}) = \{a + \sqrt{-5}\, b \mid a,\ b \in \mathbf{Z}\}$$

under the operations defined by

$$(a + \sqrt{-5}\, b) + (c + \sqrt{-5}\, d) = (a + c) + \sqrt{-5}\ (b + d)$$

$$(a + \sqrt{-5}\, b)\ .\ (c + \sqrt{-5}\, d) = (ac - 5bd) + \sqrt{-5}\,(ad + bc)$$

(*i*) We show $\sqrt{-5}$ is a prime element.

$\sqrt{-5} \neq 0$, it is also not a unit as, if it were a unit then $\exists\ a + \sqrt{-5}\, b$, s.t.,

$$\sqrt{-5}\,(a + \sqrt{-5}\, b) = 1$$

$\Rightarrow \sqrt{-5} = 1 + 5b$, which is not possible as R.H.S. is an integer whereas L.H.S. is not an integer.

Suppose now $\sqrt{-5}$ divides $(a + \sqrt{-5}\, b)\ (c + \sqrt{-5}\, d)$,

then $\exists\ (x + \sqrt{-5}\, y)$ s.t.,

$$\sqrt{-5}\,(x + \sqrt{-5}\, y) = (a + \sqrt{-5}\, b)\ (c + \sqrt{-5}\, d)$$

which on comparison gives,

$$-5y = ac - 5bd$$

$$5(bd - y) = ac \Rightarrow 5 \mid ac$$

But 5 being a prime number

either $\quad 5 \mid a$ or $5 \mid c$.

If $5 \mid a$ then $\quad (\sqrt{-5})(\sqrt{-5}) \mid a$

$$\Rightarrow \sqrt{-5} \mid a$$

$$\Rightarrow \sqrt{-5} \mid a + b\sqrt{-5}$$

Similarly, if $5 \mid c$ then $\sqrt{-5} \mid c + \sqrt{-5}\, d$

Hence $\sqrt{-5}$ is a prime element.

(*ii*) We show further that 3 is an irreducible element which is not prime.

Suppose $\quad 3 = (a + \sqrt{-5}\, b)\ (c + \sqrt{-5}\, d), \qquad a,\ b,\ c,\ d \in \mathbf{Z}$

Taking conjugates, we get

$$\bar{3} = (a - \sqrt{-5}\, b)\ (c - \sqrt{-5}\, d)$$

Thus $\quad 3 . \bar{3} = (a^2 + 5b^2)\ (c^2 + 5d^2)$

i.e., $\quad 9 = (a^2 + 5b^2)\ (c^2 + 5d^2)$

$\Rightarrow \quad a^2 + 5b^2 = 1,\ 3$ or 9

Now $a^2 + 5b^2 = 3$ is not possible as $a,\ b \in \mathbf{Z}$

If $a^2 + 5b^2 = 1$ then $a = \pm 1$ and $b = 0$

If $a^2 + 5b^2 = 9$ then $a^2 + 5d^2 = 1$, giving $c = \pm 1$ and $d = 0$

Thus, if $a^2 + 5b^2 = 1$ then $a^2 + \sqrt{-5}\, b = \pm 1 =$ unit (see below).

and if $a^2 + 5b^2 = 9$ then $c + \sqrt{-5}\, d = \pm 1 =$ unit

Hence 3 is an irreducible element of $\mathbf{Z}[\sqrt{-5}]$.

Now $(2 + \sqrt{-5})\ (2 - \sqrt{-5}) = 9$ and thus

$$3 | (2 + \sqrt{-5})\,(2 - \sqrt{-5})$$

We show it does not divide any one of these. Suppose $3 | (2 + \sqrt{-5})$ in $\mathbf{Z}[\sqrt{-5}]$

Then $(2 + \sqrt{-5}) = 3\,(a + \sqrt{-5}\, b) \qquad a, b \in \mathbf{Z}$

$$\Rightarrow 2 - \sqrt{-5} = 3\,(a - \sqrt{-5}\, b)$$

$$\Rightarrow 9 = 9\,(a^2 + 5b^2)$$

$$\Rightarrow 1 = a^2 + 5b^2 \Rightarrow a = \pm 1,\ b = 0$$

$$\Rightarrow 2 + \sqrt{-5} = \pm 3 \text{ which is not possible}$$

Thus $3 \nmid (2 + \sqrt{-5})$. Similarly $3 \nmid (2 - \sqrt{-5})$

Hence 3 is not a prime element of $\mathbf{Z}[\sqrt{-5}]$.

Problem 12 : *Find all the units of* $\mathbf{Z}[\sqrt{-5}]$.

Solution : Suppose $a + \sqrt{-5}\, b$ is a unit in $\mathbf{Z}[\sqrt{-5}]$

Then $(a + \sqrt{-5}\, b)\ (c + \sqrt{-5}\, b) = 1 + \sqrt{-5}\ .\ 0$ for some $c,\ d \in \mathbf{Z}$

So, $(a - \sqrt{-5}\, b)\ (c - \sqrt{-5}\, b) = \bar{1} = 1$

giving $(a^2 + 5b^2)\ (c^2 + 5d^2) = 1$ in $\mathbf{Z}$

$\Rightarrow a^2 + 5b^2 = 1 \Rightarrow a = \pm 1,\ b = 0$

Thus $a + \sqrt{-5}\, b = \pm 1$ are the units in $\mathbf{Z}[\sqrt{-5}]$.

The following theorem exhibits the 'closeness' of prime and irreducible elements.

Theorem 9 : *In a PID an element is prime if and only if it is irreducible.*

Proof : Let D be a PID and let $p \in D$ be a prime element. We need prove only that if $p = ab$, then a or b is a unit.

So let $p = ab$ then $p \mid ab$

$$\Rightarrow p \mid a \text{ or } p \mid b \quad (p \text{ is prime})$$

If $p \mid a$ then $a = px$ for some x

So
$$p = ab = (px)b$$
$$\Rightarrow p(1 - xb) = 0$$
$$\Rightarrow 1 - xb = 0 \text{ as } p \neq 0$$
$$\Rightarrow xb = 1 \Rightarrow b \text{ is a unit.}$$

Similarly, if $p \mid b$ then a will be a unit.

Conversely, let p be irreducible element and suppose $p \mid ab$. We show either $p \mid a$ or $p \mid b$.

If $p \mid a$, we have nothing to prove.

Suppose $\quad p \nmid a$

Since p, a are elements of a PID they have a g.c.d., say, d.

We show d is a unit.

Now $d \mid p$ and $d \mid a$

$\Rightarrow \exists\, u, v$ s.t., $p = du$, $a = dv$

If d is not a unit then as p is irreducible and $p = du$, u will be a unit

$$\Rightarrow u^{-1} \text{ exists}$$
$$\Rightarrow pu^{-1} = d$$
$$\therefore \quad a = pu^{-1} v \Rightarrow p \mid a \text{ which is not so.}$$

Thus d is a unit.

Again, we know that d can be expressed as

$$d = \lambda a + \mu p$$

which gives
$$dd^{-1} = d^{-1}\lambda a + d^{-1}\mu p$$
$$\Rightarrow b \,.\, 1 = \lambda d^{-1} ab + \mu d^{-1} bp$$

But
$$p \mid ab, \; p \mid \mu d^{-1} bp$$
$$\therefore \quad p \mid (ab\lambda d^{-1} + \mu d^{-1} bp)$$
$$\Rightarrow p \mid b$$

Hence the result follows.

Cor. : In an integral domain with unity, every prime element is irreducible. The converse is not true. See exercises.

Remark : Combining the results of example 6 and the above theorem, we can say $\mathbf{Z}[\sqrt{-5}]$ is not a PID.

Example 7 : Consider the ring $Z_6 = \{0, 1, 2, 3, 4, 5,\}$ mod 6.

2 is a prime element in Z_6 but is not irreducible.

2 is, of course, non zero, non unit.

Suppose $2 \mid a \otimes b$

Since $ab = 6q + a \otimes b$ for some q

and as $2 \mid 6q$, $2 \mid a \otimes b$, we find $2 \mid ab$

$\Rightarrow 2 \mid a$ or $2 \mid b$

$\Rightarrow 2 \mid a$ or $2 \mid b$ in Z_6

Hence 2 is a prime element.

Again, as $2 \otimes 4 = 2$, where neither 2 nor 4 is a unit, we find 2 is not irreducible. (Note, Z_6 is not an integral domain).

Theorem 10 : *Let R be a PID which is not a field, then an ideal $A = (a_o)$ is a maximal ideal if and only if a_o is an irreducible element.*

Proof : Let $A = (a_o)$ be a maximal ideal.

(*i*) $a_o \neq 0$

Suppose $a_o = 0$, then since R is not a field, $\exists$ at least one $0 \neq b \in R$, s.t., b^{-1} does not exist. Let $B = (b)$ and as $a_o = 0$, $A = (0)$

and $(0) \subseteq B \subseteq R \Rightarrow A \subseteq B \subseteq R$

Now $B \neq A$ as $b \in B$, $b \neq 0$, and $A = (0)$

$B \neq R$ as $1 \in R$, but $1 \notin B$

Note if $1 \in B = (b)$ then $\exists$ some x s.t., $1 = bx$.

Showing that b is invertible which is not so.

Hence $a_o \neq 0$

(*ii*) a_o is not a unit

Suppose a_o is a unit, then $a_o a_o^{-1} = 1$

$a_o \in A$, $a_o^{-1} \in R \Rightarrow a_o a_o^{-1} \in A$

$\Rightarrow 1 \in A$

$\Rightarrow A = R$

which is not possible as A is maximal.

Thus a_o is not a unit.

(*iii*) Let now $a_o = bc$ for some $b, c \in R$. We show either b or c is a unit.

Let $B = (b)$

Since $a_o = bc$, $a_o \in B$

$\Rightarrow$ all multiples of a_o are in B

$\Rightarrow A \subseteq B$

But A is maximal thus either $B = R$ or $B = A$

If $B = R$, then $1 \in B = (b)$ as $1 \in R$

$\Rightarrow 1 = xb$ for some x

$\Rightarrow b$ is a unit.

If $B = A$, then $b \in A = (a_o)$

$$\Rightarrow b = ya_o \text{ for some } y$$
$$\Rightarrow a_o = bc = ya_oc$$
$$\Rightarrow a_o - ya_oc = 0$$
$$\Rightarrow a_o\ (1 - yc) = 0$$
$$\Rightarrow 1 - yc = 0 \text{ (as } a_o \neq 0)$$
$$\Rightarrow c \text{ is a unit.}$$

Hence the result is proved.

Conversely, let a_o be irreducible element.

We show $A = (a_o)$ is maximal.

Let I be any ideal s.t., $A \subseteq I \subseteq R$.

Since R is a PID, I is generated by some element, say, x

Now $x \notin A$ as if $x \in A$

then $(x) \subseteq A$

i.e., $I \subseteq A$ but $A \subseteq I$

means $A = I$ which is not so.

Thus $x \notin A$.

Again, $A = (a_o) \subseteq I$

$$\Rightarrow a_o = xy \text{ for some } y$$

a_o is irreducible $\Rightarrow x$ or y is a unit

If y is a unit, then $yy^{-1} = 1$

and $a_o = xy$

$$\Rightarrow a_oy^{-1} = x$$

But $a_o \in A,\ y^{-1} \in R \Rightarrow a_oy^{-1} \in A$

$$\Rightarrow x \in A, \text{ which is not true.}$$

Thus y is not a unit.

So x is a unit and $xx^{-1} = 1$.

Now $x \in I,\ x^{-1} \in R,\ I$ is an ideal

$\therefore$ $xx^{-1} \in I \Rightarrow 1 \in I \Rightarrow I = R$

$$\Rightarrow A \text{ is maximal ideal of } R.$$

Remark : Recall, a field F has only two ideals F and $\{0\}$. F is not maximal and 0 is not irreducible.

Exercises

1. In a Euclidean domain R with valuation d, show that

   (*i*) $d(a) = d(-a)$ for all $0 \neq a \in R$

(*ii*) if a, b are associates then $d(a) = d(b)$

(*iii*) if $a \mid b$ and $d(a) = d(b)$ then a, b are associates

(*iv*) if for $0 \neq a \in R$, $d(a) = 0$ then a is a unit

(*v*) for a, b (non zero) in R, $d(a) = d(ab)$ iff b is a unit

2. In a commutative ring R with unity, prove that associate of a prime (irreducible) element is prime (irreducible).

3. If p, q are prime elements in an integral domain with unity such that $p \mid q$ then show that p, q are associates.

4. Show that

(*i*) in Z_8, *l.c.m.* $(3, 6) = 6$ and 2

(*ii*) in $\dfrac{\mathbf{Z}}{(20)}$, *g.c.d.* $(9, 18) = 9$, *l.c.m.*$(9, 18) = 18$

(*iii*) in ring of even integers, *l.c.m.*$(4, 6)$ does not exist

(*iv*) in $\dfrac{\mathbf{Z}}{(12)}$, $6, 8$ have no *l.c.m.*

5. Let R be a PID. Show that

(*i*) if $a \mid bc$ and a, b are co-prime then $a \mid c$

(*ii*) two non zero elements a, b are coprime iff $\exists\, x, y \in R$ s.t., $ax + by = 1$

6. Show that every field is a Euclidean domain.

7. Prove that in $\dfrac{\mathbf{Z}}{(8)}$, 2 is a prime element but not irreducible.

8. If A, B, C are ideals in a PID R, prove that

(*i*) $A \cap (B + C) = A \cap B + A \cap C$

(*ii*) $A + (B \cap C) = (A + B) \cap (A + C)$

9. Show that quotient ring of a PID is a PID and the same is true of the homomorphic image.

10. Show that $\pm 1, \pm i$ are the units in $\mathbf{Z}[i]$ and prove that if $a + ib$ is not a unit in $\mathbf{Z}[i]$ then $a^2 + b^2 > 1$

11. Prove that $1 + i$ is an irreducible element in the ring $\mathbf{Z}[i]$ of Gaussian integers.

12. In the ring $\mathbf{Z}[\sqrt{-5}] = \{a + \sqrt{-5}\, b \mid a, b \in \mathbf{Z}\}$, show that $1 + 3\sqrt{-5}$ is irreducible element but is not prime.

13. Show that in $\mathbf{Z}[\sqrt{-3}]$, $1 + \sqrt{-3}$ is irreducible but not prime element.

14. Find *g.c.d.* of $3 + 4i$ and $4 - 3i$ in $\mathbf{Z}[i]$. Are these associates?

15. Show that in an integral domain R with unity, any pair of non zero elements has *g.c.d.* iff it has *l.c.m.*

16. Show that $\mathbf{Z}[\sqrt{3}] = \{a + \sqrt{3}\, b \mid a,\ b \in \mathbf{Z}\}$ is a Euclidean domain.
17. Let $A = (a)$, $B = (b)$ be two ideals in an integral domain with unity. Show that $A = B$ iff a and b are associates. Show further that if $(a) + (b) = (d)$, then $d = g.c.d.(a, b)$.
18. Let R be an integral domain with unity. Show that an element $0 \neq b \in R$ is a prime element iff (p) is a prime ideal.

Polynomial rings

Let R be a ring. By a polynomial over R, we mean an expression of the form

$$f(x) = a_o + a_1x + a_2x^2 + \ldots\ldots + a_mx^m,\ a_i \in R$$

What is x? The symbols $x, x^2, \ldots\ldots$ here are not unknown elements or variables from the ring R. These are there only for convenience, say as place indicators for the elements a_o, a_1, $a_2, \ldots$ of the ring. The idea behind the notation is only our familiarity to polynomials of this type that we are so used to (and there, of couse, x does represent a variable). A further justification of this notation follows when we come to definining addition and multiplication of polynomials in the *usual way*.

Alternatively, any infinite sequence $(a_o, a_1, a_2, \ldots)$ of elements of R is called a polynomial over R if all except finite number of its terms a_i are zero. (Thus after a finite number of terms, all members will be zero). The first term a_o is called the constant term of the polynomial. If m is the largest non negative integer such that $a_m \neq 0$, then a_m is called the last (or leading) coefficient of the polynomial.

If
$$f(x) = a_o + a_1x + \ldots\ldots + a_mx^m, \qquad a_i \in R$$
$$g(x) = b_o + b_1x + \ldots\ldots + b_nx^n, \qquad b_j \in R$$

be two polynomials over R, then we say $f(x) = g(x)$ if $m = n$ and $a_i = b_i$ for all i.

Again, addition of polynomials $f(x)$ and $g(x)$ is defined by

$$f(x) + g(x) = (a_o + b_o) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + \ldots$$

Product is also defined in the usual way.

$$\begin{aligned} f(x)\, g(x) &= (a_o + a_1x + \ldots\ldots + a_mx^m)\,(b_o + b_1x + \ldots\ldots + b_nx^n) \\ &= a_ob_o + (a_1b_o + a_ob_1)\, x + \ldots\ldots \\ &= c_o + c_1x + c_2x^2 + \ldots\ldots + c_{m+n}\, x^{m+n} \end{aligned}$$

where $\qquad c_k = a_ob_k + a_1b_{k-1} + \ldots\ldots + a_kb_o$

Let now $R[x]$ be the set of all polynomials over R. Then $R[x]$ is a non empty set and addition and multiplication as defined above on the members of $R[x]$, clearly are binary compositions. It is easy to see that $R[x]$ forms a ring under these operations. Zero of the ring will be the zero polynomial

$$O(x) = 0 + 0x + 0x^2 + \ldots\ldots$$

Additive inverse of $f(x) = a_o + a_1x + \ldots\ldots + a_mx^m$ will be the polynomial $-f(x) = -a_o - a_1x + \ldots\ldots + (-a_m)\, x^m$. In fact, if R has unity 1 then the polynomial

$$e(x) = 1 + 0x + 0x^2 + \ldots\ldots$$

will be unity of $R[x]$. $e(x)$ is also sometimes denoted by 1. Instead of a ring R if we start with a field F we get the corresponding ring $F[x]$ of polynomials.

Remark : Let $R = Z_3 = \{0, 1, 2\}$ modulo 2. Define

$$f: Z_3 \to Z_3, \text{ s.t., } f(x) = x^3 + 2x \text{ and}$$

$$g: Z_3 \to Z_3 \text{ s.t., } g(x) = x^5 + 2x$$

Then $$f(0) = 0 = g(0),\ f(1) = 1 + 2 = g(1)$$

$$f(2) = 5 + 1 = 2 + 4 = g(2)$$

Hence $$f(a) = g(a)\ \forall\, a \in Z_3$$

and thus $f(x) = g(x)$ by our definition of a function.

On the other hand we notice

$$f(x) = (0, 2, 0, 1, 0, 0, \ldots\ldots)$$

$$g(x) = (0, 2, 0, 0, 0, 1, 0, \ldots\ldots)$$

are not equal as polynomials over Z_3. Thus $f(x) \neq g(x)$ in $Z_3[x]$.

Definition : Let $f(x) = a_o + a_1x + a_2x^2 + \ldots\ldots + a_mx^m$ be any non zero polynomial in $R[x]$. We say $f(x)$ has *degree* m if $a_m \neq 0$ and $a_i = 0$ for all $i > m$, and write $\deg f(x) = m$.

We do not define degree of zero polynomial.

We say degree of $f(x)$ is zero if $a_o \neq 0$, $a_i = 0$ for all $i > 0$. In that case it is called a constant polynomial. Also clearly, $\deg(-f(x)) = \deg f(x)$.

Suppose R is any ring and $R[x]$ is the corresponding ring of polynomials over R. If we define a map

$$f: R \to R[x], \text{ s.t.,}$$

$$f(a) = a + 0 \,.\, x + 0x^2 + \ldots\ldots$$

then it is easy to see that f will be 1-1 homomorphism. Indeed,

$$\begin{aligned} f(a+b) &= (a+b) + 0x + 0x^2 + \ldots\ldots \\ &= (a + 0x + 0x^2 + \ldots\ldots\ldots) + (b + 0x + 0x^2 + \ldots\ldots) \\ &= f(a) + f(b) \end{aligned}$$

$$\begin{aligned} f(ab) &= ab + 0.x + 0.x^2 + \ldots\ldots \\ &= (a + 0x + 0x^2 + \ldots\ldots)(b + 0x + \ldots\ldots) \\ &= f(a)\ f(b) \end{aligned}$$

Hence R can be imbedded into the ring $R[x]$. In other words, R is isomorphic to a subring of $R[x]$.

Thus R can be *identified* with a subring of $R[x]$ in view of which we sometimes take the liberty of calling R to be a subring of $R[x]$. The following theorem is now easy to prove.

Theorem 11 : *Let $R[x]$ be the ring of polynomials over a ring R then*

(*i*) *R is commutative iff $R[x]$ is commutaive.*

(*ii*) *R has unuy iff $R[x]$ has unity.*

Proof : (*i*) If $R[x]$ is commutative then any subring of $R[x]$ is commutative and as R is isomorphic to a subring of $R[x]$, R will be commutative.

Conversely, if R is commutative

and
$$f(x) = a_o + a_1x + a_2x^2 + \ldots.. + a_mx^m$$
$$g(x) = b_o + b_1x + b_2x^2 + \ldots.. + b_nx^n$$

be two members of $R[x]$, then by definition of product

$$\begin{aligned} f(x)\,g(x) &= a_ob_o + (a_1b_o + a_ob_1)\ x + \ldots\ldots \\ &= b_oa_o + (b_1a_o + b_oa_1)\ x + \ldots.. \\ &= g(x)\ f(x). \end{aligned}$$

(*ii*) If R has unity 1 then the polynomial

$e(x) = 1 + 0x + 0x^2 + \ldots..$ is unity of $R[x]$ as $f(x)\ e(x)$ will be $f(x)$ for any polynomial $f(x)$.

Conversely, let $R[x]$ have unity.

Define a map $\theta : R[x] \to R$, s.t.,

$$\theta(f(x)) = \theta(a_o + a_1x + \ldots.. + a_mx^m) = a_o$$

then θ is an onto homomorphism. (See theorem 15).

Thus R is a homomorphic image of $R[x]$ and hence has unity, as homomorphic image of a ring with unity is a ring with unity. In fact, $\theta(e(x))$ will be unity of R where $e(x)$ is unity of $R[x]$.

Theorem 12 : *Let $R[x]$ be the ring of polynomial of a ring R and suppose*

$$f(x) = a_o + a_1x + \ldots\ldots. + a_mx^m$$
$$g(x) = b_o + b_1x + \ldots.. + b_nx^n$$

are two non zero polynomials of degree m and n respectively, then

(*i*) *If $f(x) + g(x) \neq 0$, deg $(f(x) + g(x)) \leq$ max (m, n)*

(*ii*) *If $f(x)\ g(x) \neq 0$, deg $(f(x)\ g(x)) \leq m + n$*

(*iii*) *If R is an integral domain, deg $(f(x)\ g(x)) = m + n$*

(*iv*) *R is an integral domain iff $R[x]$ is an integral domain.*

(*v*) *If F is a field, $F[x]$ may not be a field.*

Proof : (*i*) By definition,

$$f(x) + g(x) = (a_o+b_o) + (a_1+b_1)x + (a_2+b_2)x^2 + \ldots. + (a_t+b_t)x^t$$

where $t = \max\ (m, n)$.

Now $a_k + b_k = 0$ for all $k > t$ as $a_k = 0,\ b_k = 0$

thus degree of $f(x) + g(x)$ is less than or equal to $t = \max\ (m, n)$. Notice it is possible to have deg $(f(x) + g(x)) < \max\ (m, n)$. Consider the ring $\mathbf{Z}$ of integers.

Let
$$f(x) = 1 + 2x - 2x^2$$
$$g(x) = 2 + 3x + 2x^2$$

be two members of $\mathbf{Z}[x]$,

then
$$\begin{aligned} f(x)+g(x) &= (1 + 2) + (2x + 3x) + (-2x^2 + 2x^2) \\ &= 3 + 5x \end{aligned}$$

Thus $\deg(f(x)+g(x)) = 1$ whereas $\deg f(x) = 2 = \deg g(x)$.

(*ii*) Let $f(x)\,g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots$

where $\quad c_k = (a_kb_o + a_{k-1}b_1 + \ldots\ldots + a_ob_k)$.

Here
$$c_{m+n} = a_ob_{m+n} + a_1b_{m+n-1} + \ldots\ldots + a_mb_n + \ldots\ldots + a_{m+n}b_o$$
$$= a_mb_n$$

as all other terms would be zero. ($a_{m+i} = 0$, $b_{n+j} = 0$ for all $i, j > 0$).

Again, $c_{m+n+t} = 0$ for all $t > 0$ and

thus $\deg(f(x)\ g(x)) \le m+n$ (a_mb_n can be zero even if $a_m \ne 0$ $b_n \ne 0$).

We show that it is possible that $\deg(f(x)\,g(x)) < m+n$.

Consider the ring $R = \{0, 1, 2, 3, 4, 5\}$ modulo 6

Take
$$f(x) = 1 + 2x^3$$
$$g(x) = 2 + x + 3x^2$$

two polynomials in $R[x]$ of degree 3 and 2 respectively.

Here $\quad f(x)\,g(x) = 2 + x + 3x^2 + 4x^3 + 2x^4$

which of degree of $4 < 5$.

Notice, here R is not an integral domain.

(*iii*) If R is an integral domain then as $a_m \ne 0$, $b_n \ne 0$, therefore, $a_mb_n \ne 0$ and hence $c_{m+n} = a_mb_n \ne 0$ showing that $\deg(f(x)\,g(x)) = m+n$.

(*iv*) If $R[x]$ is an integral domain then since R is isomorphic to a subring of $R[x]$, R will also be an integral domain.

Conversely, suppose R is an integral domain,

let $f(x)$, $g(x)$ be any two non zero members of $R[x]$ s.t.,
$$f(x)\,g(x) = 0$$

where
$$f(x) = a_o + a_1x + \ldots\ldots + a_mx^m$$
$$g(x) = b_o + b_1x + \ldots\ldots + b_nx^n$$

Now both $f(x)$ and $g(x)$ cannot be constant polynomials as then $a_o \ne 0$, $b_o \ne 0$ (so $c_o = a_ob_o \ne 0$)

$\therefore \quad f(x)\,g(x) \ne 0$

Since at least one of $f(x)$, $g(x)$ is non constant polynomial, its degree is ≥ 1.

$\therefore \quad \deg(f(x)+g(x)) \ge 1$

R being an integral domain
$$\Rightarrow \deg(f(x)\ g(x)) = \deg f(x) + \deg g(x) \ge 1$$

which is a contradiction as it implies then $c_k \ne 0$ for some $k > 0$

whereas $\quad f(x)\,g(x) = 0.$

Hence $\quad f(x)\,g(x) = 0 \Rightarrow f(x) = 0$ or $g(x) = 0$

$\Rightarrow R[x]$ is an integral domain.

(*v*) Let F be a field, then since F is commutative, has unity, by previous results we find $F[x]$ will be a commutative ring with unity. In fact F being an integral

domain, $F[x]$ will also be an integral domain. We show, not all non zero elements of $F[x]$ have multiplicative inverse. Consider the non zero polynomial

$$f(x) = 0 + 1x + 0x^2 + 0x^3 + \ldots\ldots (= a_o + a_1x + a_2x^2 + \ldots\ldots)$$

Suppose $g(x) = b_o + b_1x + b_2x^2 + \ldots\ldots$ is its multiplicative inverse

then $f(x)\ g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots$

should be unity $e(x) = 1 + 0x + 0x^2 + \ldots\ldots$ of $F[x]$

$$\Rightarrow c_o = 1,\ c_i = 0 \text{ for all } i > 0$$

where $c_o = a_ob_o = 0 \,.\, b_o = 0 \neq 1$

Hence no $g(x)$ can be multiplicative inverse of $f(x) = x$.

Showing that $F[x]$ is not a field.

If R is a ring, we get $R[x]$ the corresponding ring of polynomials. Since $R[x]$ is a ring, we can similarly get $R[x, y]$ the corresponding ring of polynomial of $R[x]$ and the process can be extended. If F is a field then $F[x]$ is a ring with unity and similarly $F[x, y]$ will be a ring with unity. We shall use it a little later when we come to factorisation domains.

Theorem 13 : *If F is a field, then $F[x]$ is a Euclidean domain.*

Proof : We have seen that $F[x]$ is an integral domain with unity.

For any $f(x) \in F[x],\ f(x) \neq 0$, define

$$d(f(x)) = \deg f(x) \text{ which is non-ve integer}$$

Since, for any $f(x),\ g(x) \in F[x],\ f(x),\ g(x) \neq 0$

$$\deg (f(x)\ g(x)) = \deg f(x) + \deg g(x)$$

we get $\deg (f(x))) \leq \deg (f(x)\, g(x)),$ as $\deg (g(x)) \geq 0$

$\therefore$ $d(f(x)) \leq d(f(x)\, g(x))$

Lastly, we show for any non zero $f(x)$, $g(x)$ in $F[x]$, $\exists\ t(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = t(x)\ g(x) + r(x)$$

where either $r(x)$ is zero or $\deg r(x) < \deg g(x)$

If $\deg f(x) < \deg g(x)$

then $f(x) = 0 \,.\, g(x) + f(x)$ gives the result.

Assume now the result is true for all (non zero) polynomials in $F[x]$ of deg. less than $\deg f(x)$.

Let $f(x) = a_o + a_1x + \ldots\ldots + a_mx^m$

$g(x) = b_o + b_1x + \ldots\ldots + b_nx^n$

Suppose $\deg f(x) \geq \deg g(x)$

Define $f_1(x) = f(x) - a_mb_n^{-1}\ x^{m-n}\, g(x)$

then coefficient of x^m in $f_1(x)$ is

$$a_m - a_mb_n^{-1} \,.\, b_n = a_m - a_m = 0$$

$\therefore$ either $f_1(x) = 0$ (zero polynomial) or $\deg f_1(x) < m$

If $f_1(x) = 0$, then

$$0 = f(x) - a_m b_n^{-1} x^{m-n} g(x)$$

gives $$f(x) = a_m b_n^{-1} x^{m-n} g(x) + 0$$

So by taking $t(x) = a_m b_n^{-1} x^{m-n}$ and $r(x) = 0$ we get the required result.

Suppose $$f_1(x) \neq 0,$$

then $$\deg f_1(x) < m$$

i.e., $$\deg f_1(x) < \deg f(x).$$

By induction hypothesis

$$f_1(x) = t_1(x)\, g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore$ $$f(x) - a_m b_n^{-1} x^{m-n}\, g(x) = t_1(x)\, g(x) + r(x)$$

or $$f(x) = [a_m b_n^{-1} x^{m-n} + t_1(x)]\, g(x) + r(x)$$
$$= t(x)\, g(x) + r(x)$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$

and hence $F[x]$ is a Euclidean domain (and also, therefore, a PID)

Remarks (*i*) : Thus $\mathbf{Q}[x]$ is a Euclidean domain which is not a field.

(*ii*) One can show that the above defined $t(x)$ and $r(x)$ are unique.

See remark on page 290. To prove it independently

Suppose $f(x) = t(x)\, g(x) + r(x)$ where either $r(x) = 0$ or $\deg r < \deg g$

and $f(x) = t'(x)\, g(x) + r'(x)$ where either $r'(x) = 0$ or $\deg r' < \deg g$

then $$t(x)\, g(x) + r(x) = t'(x)\, g(x) + r'(x)$$

$$\Rightarrow g(t - t') = r' - r \qquad \ldots (1)$$

Suppose $$t(x) \neq t'(x)$$

then $t - t' \neq 0$ and thus has degree ≥ 0

(1) $$\Rightarrow \deg (g(t - t')) = \deg (r' - r)$$

$$\Rightarrow \deg g + \deg (t - t') = \deg (r' - r) \qquad \ldots (2)$$

Also since $g(t - t')$ has positive degree ($\geq n$), $r' - r$ cannot be zero, otherwise $g(t - t')$ would be a constant polynomial, so its degree cannot be $\geq n$

$r' - r$ cannot be zero $\Rightarrow$ both r and r' cannot be zero together.

Now L.H.S. of (2) is greater than or equal to $\deg g$

whereas R.H.S. of (2) is $\leq \max\ (\deg r', \deg r) < \deg g$

as if both r, r' are non zero then $\deg r < \deg g$

$$\deg r' < \deg g$$

$$\Rightarrow \max\ (\deg r, \deg r') < \deg g$$

If one of r, r' is zero, the other has deg less than $\deg g$. In any case R.H.S. $< \deg g$,

which is a contradiction.

Thus $\quad t - t' = 0 \Rightarrow t = t'$

$\therefore$ (1) $\quad \Rightarrow r = r'$.

Hence the uniqueness is established.

If F is a field then $F[x]$ being a Euclidean domain will be a PID. Hence we can state

Theorem 14 : *If F is a field, every ideal in $F[x]$ is principal.*

Example 8 : Let $R = \{0, 1\}$ mod 2, then $R[x]$ is an infinite integral domain. If $f(x) \in R[x]$ be any member and if,

$$f(x) = a_o + a_1x + \ldots\ldots + a_mx^m \text{ then we have}$$

$$\begin{aligned} 2f(x) &= f(x) + f(x) \\ &= (a_o \oplus a_o) + (a_1 \oplus a_1)\ x + \ldots\ldots + (a_m \oplus a_m)\ x^m \\ &= 0 + 0 \,.\, x + 0 \,.\, x^2 + \ldots\ldots \\ &= O(x), \text{ zero of } R[x] \end{aligned}$$

Thus $2f(x) = 0\ \forall f \in R[x]$, showing that $R[x]$ is of finite characteristic (although it is infinite).

Problem 13 : *Let R be a commutative ring with unity. Let A be an ideal of R. Show that* $\dfrac{R[x]}{A[x]} \cong \dfrac{R}{A}[x]$.

Hence or otherwise prove or disprove

A is prime ideal of $R \Rightarrow A[x]$ is prime ideal of $R[x]$.

Solution : Define a mapping

$$\theta : R[x] \to \frac{R}{A}[x] \text{ s.t.,}$$

$$\begin{aligned} \theta(f(x)) &= \theta(a_o + a_1x + \ldots. + a_nx^n) \\ &= (a_o + A) + (a_1 + A)\ x + \ldots\ldots + (a_n + A)\ x^n \end{aligned}$$

then θ is clearly well defined.

If
$$\begin{aligned} f(x) &= a_o + a_1x + a_2x^2 + \ldots\ldots \\ g(x) &= b_o + b_1x + b_2x^2 + \ldots\ldots \\ f(x)\ g(x) &= c_o + c_1x + c_2x^2 + \ldots\ldots \end{aligned}$$

then

$$\begin{aligned} \theta(f(x) + g(x)) &= \theta((a_o + b_o) + (a_1 + b_1)\,x + \ldots\ldots) \\ &= [(a_o + b_o) + A] + [(a_1 + b_1) + A]\,x + \ldots\ldots \\ &= (a_o + A) + (b_o + A) + (a_1 + A)\ x + (b_1 + A)\,x + \ldots\ldots \\ &= ((a_o + A) + (a_1 + A)\,x + \ldots\ldots) + ((b_o + A) + (b_1 + A)\,x + \ldots\ldots) \\ &= \theta(f(x)) + \theta(g(x)) \\ \theta(f(x)\,g(x)) &= \theta(c_o + c_1x + c_2x^2 + \ldots\ldots) \\ &= (c_o + A)\,(c_1 + A)\,x + \ldots\ldots \end{aligned}$$

$$= (a_o b_o + A) + (a_1 b_o + a_o b_1 + A)\, x + \ldots\ldots$$
$$= (a_o + A)(b_o + A) + [(a_1 b_o + A) + (a_o b_1 + A)\, x + \ldots$$
$$= (a_o + A)\ (b_o + A) +$$
$$[(a_1 + A) + (b_o + A)\ + (a_o + A) + (b_1 + A)]\, x + \ldots\ldots$$

Also $\theta(f(x))\,\theta\, g(x)) = [(a_o + A) + (a_1 + A)\ x + \ldots\ldots]\ [(b_o + A) + \ldots\ldots]$

$$= (a_o + A)(b_o + A) + \ [(a_1 + A)(b_o + A) + (a_o + A)(b_1 + A)]\, x + \ldots.$$

$\Rightarrow$ θ is a homomorphism.

That θ is onto is evident from the definition, hence by Fundamental theorem

$$\frac{R[x]}{\text{Ker}\,\theta} \cong \frac{R}{A}[x].$$

Now $\quad f(x) \in \text{Ker}\ \theta \Leftrightarrow \theta(f(x)) = (0 + A) + (0 + A)\, x + \ldots\ldots$

$$\Leftrightarrow (a_o + A) + (a_1 + A)\, x + \ldots\ldots = (0 + A) + (0 + A)\, x + \ldots\ldots$$
$$\Leftrightarrow a_i + A = A \text{ for all } i$$
$$\Leftrightarrow a_i \in A \text{ for all } i$$
$$\Leftrightarrow f(x) \in A[x]$$

Hence $\quad \dfrac{R[x]}{A[x]} \cong \dfrac{R}{A}[x]$

Finally, let A be a prime ideal of R.

Then $\dfrac{R}{A}$ is an integral domain

$\Rightarrow \dfrac{R}{A}[x]$ is an integral domain

$\Rightarrow \dfrac{R[x]}{A[x]}$ is an integral domain, because of the isomorphism

$\Rightarrow A[x]$ is a prime ideal of $R[x]$.

Remark : It is clear then if A is an ideal of a ring R then $A[x]$ is an ideal of $R[x]$. (Kernels are ideals).

Problem 14 : *Show that* $\dfrac{Z_3[x]}{I}$, *where* $I = \langle x^2 + x + 1 \rangle$ *is not an integral domain*

Solution : $\quad (x + 2) + I \in \dfrac{Z_3[x]}{I}$

and $\quad ((x + 2) + I)^2 = (x + 2)^2 + I = (x^2 + 1\,.\,x + 1) + I$

$$= I = \text{zero of } \frac{Z_3[x]}{I}$$

but $(x+2)+I$ is not zero of $\dfrac{Z_3[x]}{I}$

Hence $\dfrac{Z_3[x]}{I}$ is not an integral domain.

Notice 3 being prime, Z_3 is an integral domain and thus $Z_3[x]$ is also an integral domain. So quotient ring of an integral domain may not be an integral domain, a result we discussed earlier also. (See page 254).

Theorem 15 : *For any commutative ring R with unity,* $\dfrac{R[x]}{<x>} \cong R$.

Proof : Define a map $\theta : R[x] \to R$, s.t.,

$$\theta(a_o + a_1x + \ldots\ldots + a_nx^n) = a_o$$

then θ is clearly well defined. Also

$$\theta[(a_o + a_1x + \ldots\ldots + a_nx^n) + (b_o + b_1x + \ldots\ldots + b_mx^m)]$$
$$= \theta[(a_o + b_o) + (a_1 + b_1)x + \ldots\ldots]$$
$$= a_o + b_o = \theta(a_o + a_1x + \ldots\ldots + a_nx^n) + \theta(b_o + b_1x + \ldots\ldots + b_mx^m)$$

Similarly the result for product follows.

Thus θ is a homomorphism which is clearly onto. By Fundamental theorem, we get

$$\frac{R[x]}{\text{Ker } \theta} \cong R$$

Let
$$f(x) = a_o + a_1x + \ldots\ldots + a_nx^n \in \text{Ker } \theta$$
$$\Leftrightarrow \theta(a_o + a_1x + \ldots\ldots + a_nx^n) = 0$$
$$\Leftrightarrow a_o = 0$$
$$\Leftrightarrow f(x) = x\,[a_1 + a_2x + \ldots\ldots + a_nx^{n-1}] = xh(x)$$
$$\Leftrightarrow f(x) \in <x>$$

Hence Ker $\theta = <x>$ which proves our result.

Theorem 16 : *Let R be a commutative ring with unity such that $R[x]$ is a PID, then R is a field.*

Proof : By previous theorem

$$\frac{R[x]}{<x>} \cong R.$$

We claim $<x>$ is a maximal ideal of $R[x]$.

Suppose I is any ideal s.t. $<x> \subseteq I \subseteq R[x]$.

Since $R[x]$ is a PID, $I = <f(x)>$ for some $f(x) = a_o + a_1x + \ldots\ldots + a_nx^n$

Now
$$x \in <x> \subseteq I = <f(x)>$$
$$\Rightarrow x = f(x)\,g(x) \text{ for some } g(x) \in R[x]$$

which implies either $f(x) = x,\ g(x) = 1.$ (unity of $R[x]$)

or $f(x) = \alpha x,\ g(x) = \alpha^{-1} \quad \alpha \in R$

or $f(x) = 1,\ g(x) = x$

(Second case being conditional to the existence of α^{-1})

If $f(x) = x,\ I = <f(x)> \Rightarrow I = <x>$

if $f(x) = \alpha x,\ I = <f(x)> \Rightarrow I = <\alpha x> = <x>$

if $f(x) = 1,\ I = <f(x)> \Rightarrow I = <1> = R[x]$

Hence $<x>$ is a maximal ideal.

$$\therefore \quad \frac{R[x]}{<x>} \text{ is a field.}$$

Hence R is a field.

Theorem 17 : *An integral domain R with unity is a field iff $R[x]$ is a PID.*

Proof : If $R[x]$ is a PID, we've proved then R is a field (previous theorem).

Conversely, let R be a field.

Then $R[x]$ is a Euclidean domain (theorem 13)

$\Rightarrow R[x]$ is a PID. (Theorem 5)

The above theorem can be restated as

If R is an integral domain with unity, which is not a field then $R[x]$ is not a PID.

Cor. 1 : $\mathbf{Z}[x]$ is not a PID as $\mathbf{Z}$ is not a filed.

For another proof see Problem 18.

Cor. 2 : If F is a field then $F[x, y]$ is not a PID.

Proof : If $F[x, y]$ is a PID then $F[x]$ is a field which is not true as x is not invertible. See theorem 12 earlier.

Problem 15 : *Show that $<x^2 + 1>$ is not a prime ideal of $Z_2[x]$.*

Solution : We notice that

$$(x+1)^2 = x^2 + 2x + 1$$
$$= x^2 + 1 \quad \text{in } Z_2[x]$$

Thus $x^2 + 1 = (x+1)^2 = (x+1)\ (x+1) \in <x^2 + 1>$

but $(x+1) \notin <x^2 + 1>$.

Problem 16 : *Prove that the ideal $<x>$ of $\mathbf{Z}[x]$ is a prime ideal but not maximal.*

Solution : Let $f(x) = a_o + a_1x + \ldots\ldots + a_mx^m$

$$g(x) = b_o + b_1x + \ldots\ldots + b_nx^n$$

be two polynomials of $\mathbf{Z}[x]$ such that $f(x)\,g(x) \in <x>$

then

$(a_o + a_1x + \ldots\ldots + a_mx^m)\,(b_o + b_1x + b_2x^2 + \ldots\ldots + b_nx^n) \in <x>$

$\Rightarrow c_o + c_1x + c_2x^2 + \ldots\ldots \in <x>$, where $c_k = a_ob_k + a_1b_{k-1} + \ldots\ldots + a_kb_o$

$\Rightarrow\ c_o + c_1x + c_2x^2 + \ldots\ldots = x\,[d_o + d_1x + d_2x^2 + \ldots\ldots + d_tx^t]$

Comparing co - efficients, we get

$$c_o = a_ob_o = 0$$

$$\Rightarrow a_o = 0 \text{ or } b_o = 0$$

If $a_o = 0$ then $f(x) = a_1x + a_2x^2 + \ldots\ldots + a_mx^m$

$$= x\,(a_1 + a_2x + \ldots\ldots + a_mx^{m-1}) \in \langle x \rangle$$

If $b_o = 0$ then $g(x) \in \langle x \rangle$

thus $\langle x \rangle$ is prime ideal of $\mathbf{Z}[x]$.

We show $\langle x \rangle$ is not maximal.

Consider $A = \{xf(x) + 2g(x) \mid f(x),\ g(x) \in \mathbf{Z}[x]\}$

then A is an ideal of $\mathbf{Z}[x]$ as

$$[xf(x) + 2g(x)] - [x\ f'(x) + 2g'(x)]$$

$$= x\,[f(x) - f'(x)] + 2\ [g(x) - g'(x)] \in A$$

and for $h(x) \in \mathbf{Z}[x]$

$$[xf(x) + 2g(x)]\,h(x) = xf(x)\,h(x) + 2g(x)\,h(x) \in A$$

Now $2 \in A$, $2 \notin \langle x \rangle$

As $2 = x\,(0 + 0\,.\,x + \ldots\ldots) + 2\,(1 + 0\,.\,x + 0\,.\,x^2 + \ldots\ldots)$

Thus $\langle x \rangle \subset A$. Notice $\langle x \rangle \subseteq A$ by definition of A.

Again, $A \neq \mathbf{Z}[x]$, because if $A = \mathbf{Z}[x]$ then as $1 \in \mathbf{Z}[x]$

$1 \in A \Rightarrow 1 = xf(x) + 2g(x)$

$\Rightarrow 1 = x\,(a_o + a_1x + \ldots\ldots + a_mx^m) + 2\,(b_o + b_1x + \ldots\ldots + b_nx^n)$

$\Rightarrow 1 = 2b_o,\ b_o \in \mathbf{Z}$

a contradiction

Hence $A \neq \mathbf{Z}[x]$

or that $\langle x \rangle \subset A \subset \mathbf{Z}[x]$

showing thereby that $\langle x \rangle$ is not maximal.

Note : $\langle x \rangle$ will be maximal in $\mathbf{Q}[x]$.

Problem 17 : *Let R be a commutative ring with unity and $\langle x \rangle$ be a prime ideal of $R[x]$. Show that R must be an integral domain.*

Solution : Let $a,\ b \in R$ be such that $ab = 0$

Then the polynomials

$$(0 + 1x + 0x^2 + \ldots\ldots) + (a + 0x + 0x^2 + \ldots\ldots) \text{ and}$$

$$(0 + 1x + 0x^2 + \ldots\ldots) + (b + 0x + 0x^2 + \ldots\ldots) \text{ belong to } R[x]$$

$\Rightarrow x + a,\ x + b \in R[x]$

$\Rightarrow (x + a)\ (x + b) \in R[x]$

$\Rightarrow x^2 + x\ (a + b) + ab \in R[x]$

Since $ab = 0$, $x^2 + x(a + b) = x\ [x + a + b] \in \langle x \rangle$

thus $(x+a)(x+b) \in \langle x \rangle$

$\Rightarrow (x+a) \in \langle x \rangle$ or $(x+b) \in \langle x \rangle$ as $\langle x \rangle$ is prime ideal

Now $(x+a) \in \langle x \rangle \Rightarrow x + a = xf(x)$ for some $f(x) \in R[x]$

$= x\ (a_o + a_1 x + \ldots\ldots)$

$\Rightarrow a = 0$

Similarly if $(x+b) \in \langle x \rangle$ then $b = 0$

Hence R is an integral domain.

Problem 18 : *Show that the ideal*

$A = \{xf(x) + 2g(x) \mid f(x),\ g(x) \in \mathbf{Z}[x]\}$ *of* $\mathbf{Z}[x]$ *is not a principal ideal.*

Solution : Suppose A is a principal ideal generated by $k(x)$, $k(x) \in \mathbf{Z}[x]$

Since

$x = x(1 + 0x + 0x^2 + \ldots\ldots) + 2\ (0 + 0x + 0x^2 + \ldots\ldots) \in A = \langle k(x) \rangle$

$x = k(x)\, h(x)$

Also $2 \in \langle k(x) \rangle \Rightarrow 2 = k(x)\, t(x)$. (1)

Thus $xk(x)\, t(x) = 2k(x)\, h(x)$

$\Rightarrow 2h(x) = xt(x)$

$\Rightarrow$ each coefficient of $t(x)$ is an even integer.

i.e., $t(x) = 2r(x)$ for some $r(x) \in \mathbf{Z}[x]$

$\Rightarrow 2 = 2k(x)\, r(x)$

$\Rightarrow r(x)\, k(x) = 1$

$\Rightarrow 1 \in \langle k(x) \rangle$

$\Rightarrow \langle k(x) \rangle = \mathbf{Z}[x]$ [ideal with unity]

$\Rightarrow A = \mathbf{Z}[x]$

which is not true as A is proper ideal of $\mathbf{Z}[x]$ as seen in problem 16.

Remark : The above problem shows us that $\mathbf{Z}[x]$ is not a PID, a result we proved earlier also.

Problem 19 : *Show that the above ideal* A *is maximal ideal in* $\mathbf{Z}[x]$.

Solution : Let I be an ideal such that $A \subset I \subseteq \mathbf{Z}[x]$.

Since $A \neq I$, $\exists\ h(x) \in I$ s.t., $h(x) \notin A$.

Let $h(x) = b_o + b_1 x + b_2 x^2 + \ldots\ldots + b_m x^m$

then b_o is odd as if b_o is even then $h(x) \in A$

$h(x) = 2k + b_1 x + b_2 x^2 + \ldots\ldots + b_m x^m = g(x) + xf(x)$ type

Thus $h(x) = (2a+1) + b_1 x + b_2 x^2 + \ldots\ldots + b_m x^m$

$h(x) = g(x) + 1$

$\Rightarrow 1 = h(x) - g(x)$

$\Rightarrow 1 \in I$ as $h(x) \in I$, $g(x) \in A \subseteq I$

$\Rightarrow I = \mathbf{Z}[x]$

$\Rightarrow A$ is maximal

Note : We also use the notation $(2, x)$ for the ideal A.

Problem 20 : *Let R be a commutative ring. If $f(x) = a_o + a_1x + \ldots\ldots + a_mx^m \in R[x]$ is a zero divisor, show that there exists an element $b \neq 0$ in R such that $ba_o = ba_1 = \ldots\ldots = ba_m = 0$.*

Solution : Since $f(x)$ is a zero divisor, $\exists$ some $g(x) \neq 0$ s.t.,

$$f(x)\ g(x) = 0$$

Let $g(x)$ be such polynomial with least degree

and suppose $\quad g(x) = b_o + b_1x + \ldots\ldots + b_nx^n$

Let $\quad f(x)\ g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots \qquad \ldots (1)$

Since $\quad f(x)\ g(x) = 0$, we get $c_o = c_1 = c_2 = \ldots\ldots = 0$

Now $\quad 0 = c_{m+n} = a_{m+n}b_o + a_{m+n-1}\,b_1 + \ldots\ldots + a_mb^n + \ldots\ldots$

$\Rightarrow a_mb_n = 0$ as each $a_ib_j = 0$ when $i > m$ or when $j > n$

Consider $\quad a_mg(x) = a_mb_o + a_mb_1x + \ldots\ldots + a_mb_nx^n$

Since $\quad a_mb_n = 0$

$\deg\ (a_mg) < n = \deg g$

Now if $a_mg \neq 0$ then since

$$f.a_mg = a_mfg = 0 \quad \text{as } fg = 0$$

we find a_mg is a polynomial such that $f(a_mg) = 0$

with $\quad \deg\ (a_mg) < \deg g$

a contradiction to the choice of g.

Hence $\quad a_mg = 0$

We claim now $\quad a_{m-r}g = 0 \qquad$ for all r, $0 \leq r \leq m$.

Result is true (proved) for $r = 0$. Suppose it is true for $r-1$, we show it holds for r.

So we are given that $a_{m-(r-1)}\,g = 0$

we show $\quad a_{m-r}g = 0$

Consider, coefficient of x^{m+n-r} in (1), it is c_{m+n-r} which is, of course, zero. So

$$0 = c_{m+n-r} = a_{m+n-r}\,b_o + a_{m+n-r+1}b_1 + \ldots\ldots + \ldots\ldots$$

$$\Rightarrow 0 = a_mb_{n-r} + a_{m-1}\,b_{n-r+1} + \ldots\ldots + a_{m-r}b_n$$

(rest of the terms being zero)

Since result $\quad a_{m-i}g = 0$ holds when $i < r$

we find $\quad a_mb_{n-r} = a_{m-1}\,b_{n-r+1} = \ldots\ldots = 0$

Note $\quad a_{m-i}\,g = a_{m-i}\,b_o + a_{m-i}\,b_1x + \ldots\ldots + a_{m-i}\,b_nx^n = 0$

$\Rightarrow a_{m-i}\,b_o = 0,\ a_{m-i}\,b_i = 0, \ldots\ldots, a_{m-i}\,b_n = 0$

Hence $\quad a_{m-r}\,b_n = 0 \Rightarrow \deg\ (a_{m-r}g) < n = \deg g$

$$a_{m-r}g = a_{m-r}\,b_o + a_{m-r}\,b_1x + \ldots\ldots + a_{m-r}\,b_nx^n$$

Also $\quad f.\, a_{m-r}g = a_{m-r}fg = 0$

Since $\quad \deg a_{m-r}g < \deg g$

we find $\quad a_{m-r}g = 0$ for all $r = 0, 1, 2, \ldots\ldots$

Thus $\quad a_o g = 0,\ a_1 g = 0, \ldots\ldots,\ a_m g = 0$

$$\Rightarrow a_o b_n = 0,\ a_1 b_n = 0,\ a_2 b_n = 0, \ldots\ldots,\ a_m b_n = 0$$

$$b_n \neq 0 \text{ in } R.$$

Problem 21 : *We have seen earlier (exercises on page 250) that for ideals A, B, C of a ring R,*

$$(A + C)(B + C) \subseteq AB + C, \quad (A \cap B)(A + B) \subseteq AB \quad \textit{hold.}$$

Show by an example that equality does not hold in both cases.

Solution : Consider the ideals

$$A = \langle 3x \rangle,\ B = \langle 2 \rangle,\ C = \langle x^2 \rangle \text{ in } \mathbf{Z}[x]$$

Then $\quad AB = \langle bx \rangle,\ A + C = \langle 3x, x^2 \rangle,\ B + C = \langle 2, x^2 \rangle$

$$AB + C = \langle bx, x^2 \rangle,\ (A + C)(B + C) = \langle 6x, 3x^3, 2x^2, x^4 \rangle$$

Now $\quad x^2 \in AB + C$ and if $x^2 \in (A + C)(B + C)$, then

$$x^2 = f(x)\, 6x + g(x)\ 3x^2 + h(x)\ 2x^2 + r(x)x^4$$

for $f, g, h, r \in \mathbf{Z}[x]$

Suppose $\quad f(x) = \alpha_0 + \alpha_1 x + \ldots\ldots$

$$h(x) = \beta_0 + \beta_1 x + \ldots\ldots \qquad \alpha_i, \beta_i \in \mathbf{Z}$$

Then comparing coefficients of x^2 on both sides

we get

$1 = 6\alpha_1 + 2\beta_0$ which is not possible and hence equality cannot hold in first case.

Again, $\quad A \cap B = \langle 6x \rangle = AB, \quad A + B = \langle 3x, 2 \rangle$

$$(A \cap B)(A + B) = \langle 18x^2, 12x \rangle$$

Now $\quad 6x \in AB$ and if $6x \in (A \cap B)(A + B)$, then

$$6x = f(x)\, 2x + g(x)\, 18x^2, \qquad f, g \in \mathbf{Z}[x]$$

If $\quad f = \alpha_0 + \alpha_1 x + \ldots\ldots, \qquad \alpha_i \in \mathbf{Z}$

Then comparing coefficients of x we get

$6 = 12\alpha_0$ i.e., $1 = 2\alpha_0$, $\alpha_0 \in \mathbf{Z}$, which is not possible. Hence equality cannot hold in second case also.

Greatest Common Divisor

We now discuss a method that enables us to find g.c.d. of any two members of $F[x]$.

Let $f_1, f_2 \in F[x]$ be any two members.

Divide f_1 by f_2 to get $f_1 = f_2 q_1 + f_3$ $\deg f_3 < \deg f_2$

Divide f_2 by f_3 to get $f_2 = f_3 q_2 + f_4$ $\deg f_4 < \deg f_3$

Continuing like this, we'll finally reach

$$f_{n-1} = f_n q_{n-1} + 0$$

then we claim $f_n = g.c.d.(f_1, f_2)$

Consider the ideal (f_1, f_2) generated by f_1 & f_2.

$(f_1, f_2) = \{g f_1 + h f_2 \mid g, h \in F[x]\}$

Let $g f_1 + h f_2$ be any member of this ideal, then

$$g f_1 + h f_2 = g(f_2 q_1 + f_3) + h f_2$$
$$= f_2 (g q_1 + h) + g f_3 \in (f_2, f_3)$$

giving that $(f_1, f_2) \subseteq (f_2, f_3)$

Similarly we can show $(f_2, f_3) \subseteq (f_1, f_2)$ and hence $(f_1, f_2) = (f_2, f_3)$ which would finally lead us to the result

$(f_1, f_2) = (f_2, f_3) = \ldots\ldots = (f_n, 0) = (f_n)$

That f_n is $g.c.d.(f_1, f_2)$ now follows from exercise 17 page 308.

What we have done above for $F[x]$, can be used in other domains by applying the same proceedure (assuming the existence of *g.c.d.*).

We illustrate this through the following

Problem 22 : *Find g.c.d. of*

(*i*) 9, 15; 7, 10 *in* $\mathbf{Z}$

(*ii*) $11 + 7i$, $18 - i$ *in* $\mathbf{Z}[i]$

(*iii*) $x^4 + x^3 + 2x^2 + x + 1$, $x^3 - 1$; $x^2 + 1$, $x^6 + x^3 + x + 1$ *in* $\mathbf{Q}[x]$

Solution : (*i*) We have

$$15 = 9 \times 1 + 6 \qquad 10 = 7 \times 1 + 3$$
$$9 = 6 \times 1 + 3 \qquad 7 = 3 \times 2 + 1$$
$$6 = 3 \times 2 + 0 \qquad 3 = 1 \times 3 + 0$$

i.e., $g.c.d.(9, 15) = 3$ and $g.c.d.(7, 10) = 1$

(*ii*) Dividing $18 - i$ by $11 + 7i$, we get

$$\frac{18-i}{11+7i} = \frac{(18-i)(11-7i)}{(11+7i)(11-7i)} = \frac{191}{170} - \frac{137}{170} i$$

$$= \left(1 + \frac{21}{170}\right) - \left(1 - \frac{33}{170}\right) i = (1-i) + \left(\frac{21}{170} + \frac{33i}{170}\right)$$

Thus $\qquad 18 - i = (11 + 7i)(1 - i) + 3i \qquad \ldots (1)$

Dividing $11 + 7i$ by $3i$, we get

$$\frac{11+7i}{3i} = \frac{(11+7i)(-3i)}{3i(-3i)} = \frac{21}{9} - \frac{33}{9}i = \frac{7}{3} - \frac{11}{3}i = (2-3i) + \left(\frac{1}{3} - \frac{2i}{3}\right)$$

Giving $\quad 11 + 7i = 3i\ (2 - 3i) + (2 + i) \quad \ldots. (2)$

Again, $$\frac{3i}{2+i} = \frac{3i\,(2-i)}{(2+i)\,(2-i)} = i + \left(\frac{3}{5} + \frac{1}{5}i\right)$$

or $$3i = i\ (2+i) + \left(\frac{3}{5} + \frac{1}{5}i\right)\ (2+i)$$

$$3i = i\ (2+i) + (1+i) \quad \ldots (3)$$

Dividing $(2 + i)$ by $1 + i$, we get

$$\frac{2+i}{1+i} = \frac{2+i}{1+i} \cdot \frac{1-i}{1-i} = \frac{3}{2} - \frac{1}{2}i = \left(\frac{1}{2} - \frac{1}{2}i\right)$$

$\therefore \quad 2 + i = (1 + i) \,.\, 1 + 1 \quad \ldots (4)$

Dividing $1 + i$ by 1 we have $(1 + i) = 1.(1 + i) + 0$

Hence $g.c.d.(11 + 7i,\ 18 - i) = 1$.

If we retrace the steps backwards from (4) to (1) we get

$$1 = (11 + 7i)\ (6 - 6i) - (6 - i)\ (18 - i)$$

i.e., we can express the g.c.d. in the form $\lambda a + \mu b$.

(*iii*) By actual division

$$\begin{array}{r|l} & x+1 \\ \hline x^3-1 & x^4 + x^3 + 2x^2 + x + 1 \\ & x^4 - \\ & - \quad + \\ \hline & x^3 + 2x^2 + 2x + 1 \\ & x^3 - 1 \\ & - \quad + \\ \hline & 2x^2 + 2x + 2 \end{array}$$

we find

$$x^4 + x^3 + 2x^2 + x + 1 = (x^3 - 1)\,(x + 1) + (2x^2 + 2x + 2)$$

Similarly,

$$x^3 - 1 = (2x^2 + 2x + 2)\left(\frac{x}{2} - \frac{1}{2}\right) + 0$$

Hence required g.c.d. is $2x^2 + 2x + 2$.

One can similarly tackle the second part. We notice

$$x^6 + x^3 + x + 1 = (x^2 + 1)\,x^2 + (x + 1) \qquad \text{(Dividing } x^6 + x^3 + x + 1 \text{ by } x^2 + 1)$$

$$x^2 + 1 = (x + 1)(x - 1) + 2 \qquad \text{(Dividing } x^2 + 1 \text{ by } x + 1)$$

$$x + 1 = 2(\tfrac{1}{2}x) + 1 \qquad \text{(Dividing } x + 1 \text{ by } 2)$$

$$2 = 1 \times 2 + 0 \qquad \text{(Dividing } 2 \text{ by } 1)$$

Thus g.c.d. is 1

Unique Factorisation Domains

Definition : Let R be an integral domain with unity then R is called a *unique factorisation domain* (UFD) if

(*i*) every non zero, non unit element a of R can be expressed as a product of finite number of irreducible elements of R and

(*ii*) if $a = p_1 p_2 \ldots\ldots p_m$

$a = q_1 q_2 \ldots\ldots q_n$

where p_i and q_j are irreducible in R then $m = n$ and each p_i is an associate of some q_j.

(It would, of course, be possible to write q_js in such a manner that each p_i will be an associate of q_i)

Example 9 : The ring $<\mathbf{Z}, +, \cdot>$ of integers is a UFD. We know it is an integral domain with unity. If $n \in \mathbf{Z}$ be any non zero, non unit element (i.e., $n \neq 0, \pm 1$) of $\mathbf{Z}$ then if $n > 0$, we can write

$$n = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots\ldots p_m^{\alpha_m} \quad \text{where } p_i \text{ are primes}$$

$$\Rightarrow n = (p_1 p_1 \ldots\ldots p_1)\,(p_2 p_2 \ldots\ldots p_2) \ldots\ldots (p_r p_r \ldots\ldots p_r)$$

or that n is a product of prime (and thus irreducible) elements of $\mathbf{Z}$. Again this representation of n is unique (by Fundamental theorem of Arithmetic).

In case $n < 0$, let $n = (-m)$ where $m > 0$ then we can express m as product of primes (therefore, irreducibles) in $\mathbf{Z}$

say, $\quad m = q_1 q_2 \ldots\ldots q_k$

then $\quad (-m) = n = (-q_1)\,(q_2) \ldots\ldots (q_k)$

Example 10 : A field $<F, +, .>$ is always a UFD as it contains no non zero, non unit elements.

Example 11 : $\mathbf{Z}[\sqrt{-5}\,]$ is an integral domain which is not a UFD.

$46 \in \mathbf{Z}[\sqrt{-5}\,]$ is a non unit, non zero element and we can express it as product of irreducibles in two ways

$$46 = 2 \,.\, 23$$

$$46 = (1 + 3\sqrt{-5}\,)\,(1 - 3\sqrt{-5}\,)$$

But 2 is not an associate of $1+3\sqrt{-5}$ or $1-3\sqrt{-5}$. Hence $\mathbf{Z}[\sqrt{-5}]$ is not a UFD. To prove that 2 is irreducible, mimic the proof of example 6.

Remark : As in example 6 on page 302 we can show that 2 is irreducible but not prime in $\mathbf{Z}[\sqrt{-5}]$ and thus by using next theorem, $\mathbf{Z}[\sqrt{-5}]$ cannot be a UFD.

Theorem 18 : *In a UFD R an element is prime iff it is irreducible.*

Proof : Let $a \in R$ be a prime element, then since R is an integral domain with unity, a will be irreducible (See Cor after theorem 9).

Conversely, let $a \in R$ be irreducible. Then a is non zero. .on .unit. Let $a \mid bc$

then $\qquad bc = ak$ for some k

Case (i) : b is a unit

then $\qquad c = akb^{-1} = a\ (kb^{-1}) \Rightarrow a \mid c.$

Case (ii) : c is a unit then similarly, $a \mid b$.

Case (iii) : b, c are non units

If k is a unit, then $bc = ak$

$$\Rightarrow a = b(ck^{-1})$$

Since a is irreducible, either b or ck^{-1} is a unit. But b is not a unit. Thus ck^{-1} is a unit.

But that implies c is a unit, which is again not true. Hence k is not a unit.

We can thus express

$$b = p_1 p_2 \ldots\ldots p_m$$
$$c = q_1 q_2 \ldots\ldots q_n$$
$$k = r_1 r_2 \ldots\ldots r_t$$

as product of irreducibles (by def. of UFD).

So $\qquad bc = ak$ becomes

$$p_1 p_2 \ldots\ldots p_m q_1 q_2 \ldots\ldots q_n = a r_1 r_2 \ldots\ldots r_t = x \text{ (say)}$$

Then x is an element having two representations as product of irreducible elements. By Def. of UFD each element in one representation is an associate of some element in the other.

$\Rightarrow a$ is an associate of some p_i or some q_j

$\Rightarrow ua = p_i$ or $ua = q_j$ for some unit u

$$\Rightarrow a \mid p_i \text{ or } a \mid q_j$$
$$\Rightarrow a \mid b \text{ or } a \mid c \qquad (p_i \mid b,\ q_j \mid c)$$

$\Rightarrow a$ is prime element.

Theorem 19 : *If R is an integral domain with unity in which every non zero, non unit element is a finite product of irreducible elements and every irreducible element is prime, then R is a UFD.*

Proof : To show that R is a UFD we need prove that if $a \in R$ be a non zero non unit element and

$$a = p_1 p_2 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$$

where p_i and q_j are irreducible elements then $m = n$ and each p_i is an associate of some q_j.

We use induction on n.

Let $n = 1$, then $a = p_1 p_2 \ldots\ldots p_m = q_1$ and as q_1 is irreducible some p_i is a unit. But each p_i being irreducible cannot be a unit. Thus $m = 1$.

$\therefore$ $a = p_1 = q_1$ or that the result is true for $n = 1$. Let it be true for $n - 1$.

Let now $\quad a = p_1 p_2 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$

Then $\quad p_1 p_2 \ldots\ldots p_m = q_1 (q_2 \ldots\ldots q_n)$

$$\Rightarrow q_1 \mid p_1 p_2 \ldots\ldots p_m$$

Since q_1 is irreducible, it is prime (given)

$$\Rightarrow q_1 \mid p_i \text{ for some } i$$

Without loss of generality, we can take $i = 1$

then $\quad q_1 \mid p_1 \Rightarrow p_1 = q_1 u_1$

But p_1 irreducible $\Rightarrow$ q_1 or u_1 is a unit,

As q_1 is not a unit (being irreducible), u_1 will be a unit and thus p_1, q_1 are associates.

Now $\quad (q_1 u_1)\ p_2 p_3 \ldots\ldots p_m = q_1 q_2 \ldots\ldots q_n$

or $\quad (u_1 p_2)\ p_3 \ldots\ldots p_m = q_2 q_3 \ldots\ldots q_n$

$\Rightarrow p'_2 p_3 \ldots\ldots p_m = q_2 q_3 \ldots\ldots q_n$, $\quad p'_2 = u_1 p_2$ is irreducible.

R.H.S. contains $n - 1$ elements and result being true for $n - 1$, we find $m - 1 = n - 1 \Rightarrow m = n$.

Also, just as we showed that q_1 is an associate of p_1, we can show that q_2 is an associate of p_2, by considering $p_1 p_2 \ldots\ldots p_m = q_2\ (q_1 q_3 \ldots\ldots q_n)$

Thus q_i will be an associate of p_i.

Hence R is a UFD.

Since we've already prove that in a UFD every irreducible element is prime, we have proved

Theorem 20 : *An integral domain R with unity is a UFD if and only if every non zero, non unit element is a finite product of irreducible elements and every irreducible element is prime.*

Which could be taken as a second definition of a UFD.

Theorem 21 : *An integral domain R with unity is a UFD iff every non zero, non unit element is finite product of primes.*

Proof : If R is a UFD then every non zero, non unit element is a finite product of irreducibles (by def.) and also every irreducible element is prime, hence the result follows.

Conversely, let $a \in R$ be a non zero, non unit element. Then $a = p_1 p_2 \ldots\ldots p_n$, where p_i are prime elements $\forall\ i$. Since R is an integral domain, prime elements

are irreducible and so each p_i is irreducible. We now show that every irreducible element of R is a prime element. Let $x \in R$ be any irreducible element. Then $x \neq 0$, non unit. Thus $x = q_1 q_2 \ldots\ldots q_m$ where q_j are prime. Suppose $m > 1$. Since x is irreducible, either q_1 or $(q_2 q_3 \ldots\ldots q_m)$ is a unit. But q_1 is prime and thus cannot be a unit. So $(q_2 q_3 \ldots\ldots q_m)$ is a unit which implies q_2 is a unit but that is not true as q_2 is a prime. Hence $m = 1$ or that x is prime. By theorem 20 then, R is a UFD. Summing up the above results we have proved.

Theorem 22 : *If R is an integral domain with unity then the following are equivalent :*

(*i*) *R is a UFD*

(*ii*) *Every non zero, non unit element of R is a finite product of irreducible elements and every irreducible element is prime.*

(*iii*) *Every non zero, non unit element of R is finite product of prime elements.*

Theorem 23 : *In a UFD R any two non zero elements have a g.c.d.*

Proof : Let a, b be any two non zero elements of R.

Suppose one of them (say a) is a unit then $aa^{-1} = 1$

$$\therefore \qquad b = (aa^{-1})\, b = a\,(a^{-1}b)$$

$$\Rightarrow \quad a \mid b$$

Also $\qquad a = 1 \,.\, a \Rightarrow a \mid a$

Now if $c \mid a$ and $c \mid b$ then as it means $c \mid a$

we get $\qquad a = g.c.d.(a,\ b)$.

Similarly if b is a unit, $b = g.c.d.(a,\ b)$.

Let now a & b be non units. Since R is a UFD we can express

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_n^{\alpha_n}$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots\ldots p_n^{\beta_n}$$

as product of irreducibles (Note it is possible to express both a, b as product of *same* irreducibles by suitably choosing the powers).

Let $\qquad s_i = \min\,(\alpha_i,\ \beta_i)$

we show $\qquad d = p_1^{s_1} p_2^{s_2} \ldots\ldots p_n^{s_n}$ is $g.c.d.(a,\ b)$

Now $\qquad a = (p_1^{s_1} p_2^{s_2} \ldots\ldots p_n^{s_n})\,(p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots\ldots p_n^{\alpha_n - s_n})$

$$= d\ (p_1^{\alpha_1 - s_1} p_2^{\alpha_2 - s_2} \ldots\ldots p_n^{\alpha_n - s_n})$$

$$\Rightarrow \quad d \mid a$$

Similarly $\qquad d \mid b$

Let now $c \mid a$ and $c \mid b$

If c is a unit, $d = (cc^{-1})\, d \Rightarrow c \mid d$

If c is not a unit, we can write

$$c = p_1^{r_1} p_2^{r_2} \ldots\ldots p_n^{r_n}$$

Since $\quad c \mid a, \quad r_i \leq \alpha_i$ for all i

$c \mid b, \quad r_i \leq \beta_i$ for all i

$\Rightarrow r_i \leq \min(\alpha_i, \beta_i) = s_i$ for all i

Thus $\quad d = p_1^{s_1} p_2^{s_2} \ldots\ldots p_n^{s_n} = (p_1^{r_1} p_2^{r_2} \ldots\ldots p_n^{r_n})(p_1^{s_1 - r_1} \ldots\ldots p_n^{s_n - r_n})$

$\Rightarrow c \mid d$

Hence $\quad d = g.c.d.(a, b)$

which proves our result.

As seen earlier, if d_1 and d_2 are two g.c.d. of a, b then d_1 and d_2 are associates.

It should now be a simple exercise for the reader to prove

Theorem 24 : *Any two non zero elements in a UFD have an l.c.m.*

Problem 23 : *If in a UFD R, a, b are relatively prime then* $a \mid bc \Rightarrow a \mid c$.

Solution : Let $a \mid bc$ then $\exists\ r$ such that $bc = ar$

If a is a unit

$c = (aa^{-1})c = a(a^{-1}c) \Rightarrow a \mid c$

If b is a unit

$$ba = ar \Rightarrow c = b^{-1}ar$$
$$\Rightarrow c = a(b^{-1}r) \Rightarrow a \mid c$$

If c is a unit

$$bc = ar$$
$$\Rightarrow b = arc^{-1} \Rightarrow a \mid b$$
$$\Rightarrow g.c.d.(a, b) = a$$

But a, b being relatively prime

$g.c.d.(a, b)$ will be a unit

$\Rightarrow a$ is a unit

$\Rightarrow a \mid c$ as before

If r is a unit

then $\quad bc = ar$

$\Rightarrow bcr^{-1} = a \Rightarrow b \mid a$

$\Rightarrow g.c.d.(a, b) = b \Rightarrow b$ is a unit

$\Rightarrow a \mid c$ as before.

Suppose now none of a, b, c, r are units.

If $b = 0$, $g.c.d.(a, b) = a$, a unit which is not true

$\therefore \quad b \neq 0.$

If $c = 0$, then $c = a \cdot 0 \Rightarrow a \mid c$

So assuming that $b \neq 0$, $c \neq 0$, we'll get $a \neq 0$, $r \neq 0$ (as $bc = ar$)

Now a, b, c, r being non zero, non units in a UFD we can express

$$a = a_1 a_2 \ldots\ldots a_m$$
$$b = b_1 b_2 \ldots\ldots b_n$$
$$c = c_1 c_2 \ldots\ldots c_t$$
$$r = r_1 r_2 \ldots\ldots r_k$$

as product of irreducible elements.

Thus $(b_1 b_2 \ldots\ldots b_n)(c_1 c_2 \ldots\ldots c_t) = (a_1 a_2 \ldots\ldots a_m)(r_1 r_2 \ldots\ldots r_k) = x$ (say)

then x has two representations as product of irreducible elements. Therefore, by def. of a UFD these representations should have same number of elements and each element on one side will be associate of an element on the other. So $n + t = m + k$ and each a_i is an associate of some b_i or c_i

If a_i is an associate of some b_i then

$$b_i = a_i u \text{ for a unit } u$$
$$\Rightarrow a_i | b_i \text{ and as } b_i | b$$

we get $a_i | b$

$$\Rightarrow a_i | g.c.d.(a, b) = 1 \text{ as } a_i | a$$
$$\Rightarrow a_i \text{ is a unit, which is not true as } a_i \text{ is irreducible}$$

Hence each a_i has to be an associate of some c_i

$$\Rightarrow a_i = c_i u_i \text{ for unit } u_i$$

which gives

$$(b_1 b_2 \ldots\ldots b_n)(c_1 c_2 \ldots\ldots c_t) = (c_1 u_1 c_2 u_2 \ldots\ldots c_m u_m)(r_1 r_2 \ldots\ldots r_k)$$
$$\Rightarrow b(c_{m+1} c_{m+2} \ldots\ldots c_t) = (u_1 u_2 \ldots\ldots u_m) r$$
$$\Rightarrow b(c_{m+1} c_{m+2} \ldots\ldots c_t)(u_1 u_2 \ldots\ldots u_m)^{-1} = r$$
$$\Rightarrow b | r \Rightarrow r = bd \text{ for some } d$$
$$\Rightarrow bc = ar = abd$$
$$\Rightarrow b(c - ad) = 0 \Rightarrow c = ad. \Rightarrow a | c.$$

Lemma 1 : *In a ring R, the union of an ascending chain of ideals* $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots\ldots$ *is an ideal of R.*

Proof : Let $A = \cup A_i$

$$x, y \in A \Rightarrow x \in A_i, y \in A_j \text{ for some } i, j$$

Without loss of generality we take $i \leq j$ then $A_i \subseteq A_j$

$$\therefore \quad x, y \in A_j \Rightarrow x - y \in A_j \subseteq A.$$

Again $x \in A$, $r \in R$ would imply, similalry that xr, $rx \in A$. Hence the lemma.

Lemma 2 : (Ascending Chain Condition) : *In a PID R every ascending chain of ideals must terminate after finite number of steps.*

Proof : Let $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots\ldots$ be the given chain.

Let $$A = \cup A_i$$

Then A is an ideal of R, which being a PID means A is a principal ideal. Let $A = (a)$.

Then $$a \in (a) = A = \cup A_i$$

$$\Rightarrow a \in A_i \text{ for some } i$$

$$\Rightarrow \text{all multiples of } a \text{ are in } A_i \Rightarrow (a) \subseteq A_i$$

$$\Rightarrow A \subseteq A_i \subseteq A_{i+1} \subseteq \ldots\ldots$$

i.e., $$A \subseteq A_t \text{ for each } t \geq i$$

i.e., $$A \subseteq A_i \subseteq A_t \subseteq A$$

$$\Rightarrow A_i = A_t$$

which proves our assertion.

Lemma 3 : *Every non zero, non unit element in a PID R is divisible by an irreducible element.*

Proof : Let $a \in R$, be a non zero, non unit element.

Let $$I_1 = (a).$$

If I_1 is maximal ideal, then a is irreducible and as $a \mid a$, our lemma stands proved. Suppose I_1 is not maximal, then $\exists$ some ideal $I_2 \neq R$, s.t., $I_1 \subset I_2 \subset R$.

Let $$I_2 = (p_2).$$

If I_2 is maximal then p_2 will be irreducible and as $p_2 \mid a$, the lemma is proved. $(a \in I_1 \subset I_2 = (p_2) \Rightarrow a = p_2 t)$.

Suppose I_2 is not maximal, then $\exists$ an ideal I_3 such that $I_1 \subset I_2 \subset I_3 \subset R$ and proceeding like this we get an ascending chain of ideals in R which by lemma 2 must terminate after a finite number of steps, say at $I_n = (p_n)$ which will then be maximal and p_n will be irreducible with $p_n \mid a$.

We are now ready to prove

Theorem 25 : *A PID R is a UFD.*

Proof : Let $a \in R$ be any non zero, non unit element. If a is irreducible then as $a = a$, we can express a as finite product of irreducibles. If a is not irreducible then by lemma 3, a is divisible by some irreducible element p_1.

$$p_1 \mid a \Rightarrow a = a_1 p_1 \text{ for some } a_1$$

If a_1 is irreducible, we've been able to express a as a product of finite number of irreducible elements.

Suppose a_1 is not irreducible.

Then a_1 is a non zero, non unit element as $a_1 = 0 \Rightarrow a = 0$, which is not so. Again if a_1 is a unit then as $a = a_1 p_1$, we find a and p_1 are associates and so a is irreducible as p_1 is irreducible (see exercises). But a_1 is not irreducible.

Thus again by lemma 3, $\exists$ an irreducible element p_2 such that $p_2 \mid a_1$

$$\Rightarrow a_1 = p_2 a_2 \text{ for some } a_2$$

If a_2 is irreducible, then as

$$a = a_1 p_1 = p_2 p_1 a_2$$

We are done. If a_2 is not irreducible, we continue like this.

Consider the ideals (a), (a_1), (a_2), ...

Then $(a) \subseteq (a_1) \subseteq (a_2) \subseteq .....$

as $x \in (a) \Rightarrow x = ar = p_1 a_1 r \in (a_1)$ etc..

Thus we get an ascending chain of ideals which must terminate after a finite number of steps (by lemma 2). Hence we'll get some irreducible element a_n so that

$$a = p_1 p_2 ..... p_n a_n$$

i.e., a is expressed as a product of finite number of irreducible elements.

We need show now that if a has more than two such representations then the number of elements is same in both and each element in one representation is an associate of an element in the other.

Let $a = p_1 p_2 ..... p_m = q_1 q_2 ..... q_n$

and proceed exactly as in the theorem 18 and our result is proved.

Remark : For example of a UFD which is not a PID, see examples 15, 16 page 341.

Problem 24 : *Show that in any PID every non zero ideal is a unique product of prime ideals.*

Solution : Let $I \neq 0$ be any ideal in a PID R.

Suppose $I \neq R$.

Since R is a PID, $I = <a>$ for some a, where a will not be a unit otherwise $I = R$.

Thus a is non zero non unit element of R.

Now R being a PID is a UFD

$$a = p_1 p_2 ..... p_r \text{ where } p_i \text{ are irreducible.}$$

Let $P_i = <p_i>$ then each P_i is a maximal ideal

$\Rightarrow$ each P_i is a prime ideal. (See problem 16, page 283)

Now $a = p_1 p_2 ..... p_r \in P_1 P_2 ..... P_r$

$\Rightarrow$ multiples of a are in $P_1 P_2 ..... P_r$

$$\Rightarrow <a> \subseteq P_1 P_2 ..... P_r$$

$$\Rightarrow I \subseteq P_1 P_2 ..... P_r$$

Again let $b \in P_1 P_2 ..... F_r$ be any element then

$$b = x_1 x_2 ..... x_r) + (y_1 y_2 ..... y_r) + ... \text{ (finite sum)}$$

$$x_i, y_i, ... \in P_i$$

Now $x_1 \in P_1 = <p_1> \Rightarrow x_1 = p_1 k_1$

Similalry $x_2 = p_2 k_2$

.....

$x_r = p_r k_r$

$\Rightarrow x_1x_2 \ldots\ldots x_r = p_1p_2 \ldots\ldots p_r \; k_1k_2 \ldots\ldots k_r = a(k_1k_2 \ldots\ldots k_r) \in \langle a \rangle = I$

Similalry, $y_1y_2 \ldots\ldots y_r \in I$ and others are also in I

$$\Rightarrow b \in I$$

$$\Rightarrow P_1P_2 \ldots\ldots P_r \subseteq I$$

$$\Rightarrow I = P_1P_2 \ldots\ldots P_r$$

uniqueness follows from the fact that each p_i is uniquely determined.

Definition : Let R be an integral domain with unity and let $f(x) = a_o + a_1x + \ldots\ldots + a_nx^n \in R[x]$ be a non zero polynomial. Then $d = g.c.d.(a_o, a_1, \ldots\ldots, a_n)$ is called the *content* of $f(x)$ and is denoted by $c(f)$.

A polynomial $f(x)$ is called *primitive* if $c(f)$ is a unit.

Since g.c.d. is not essentially unique, one may have more than one content of a polynomial. Two contents would, however, be associates.

Example 10 : $f(x) = 8x^3 + 6x + 1 \in \mathbf{Z}[x]$ is primitive

whereas $g(x) = 8x^3 + 6x + 2 \in \mathbf{Z}[x]$ is not primitive

as $c(f) = g.c.d.(8, 6, 1) = 1$ whereas $c(g) = 2$

Since $\quad g(x) = 2(4x^3 - 3x - 1) = 2g_1(x)$ where $c(g_1) = 1$

we find it is possible to write

$$g(x) = 2g_1(x) \text{ where } g_1(x) \text{ is primitive}$$

In fact, we can prove

Theorem 26 : *If $f(x)$ be a non zero polynomial in $R[x]$ where R is an integral domain with unity, then $f(x) = df_1(x)$ where f_1 is primitive and $d = c(f)$.*

Proof : Let $f(x) = a_o + a_1x + \ldots\ldots + a_nx^n$

and let $\quad c(f) = d = g.c.d.(a_o, a_1, \ldots\ldots, a_n)$

Then $\quad d \mid a_i$ for all i

$$\Rightarrow a_i = du_i \text{ for some } u_i$$

$$\therefore \quad f(x) = du_o + du_1x + \ldots\ldots + du_nx^n$$

$$= d(u_o + u_1x + \ldots\ldots + u_nx^n) = df_1(x) \text{ where } f_1(x) \text{ will be}$$

primitive.

Note : If $t = g.c.d.(u_o, u_1, \ldots\ldots, u_n)$

then $\quad t \mid u_i \;\forall i \Rightarrow td \mid du_i \;\forall i$

$$\Rightarrow td \mid a_i \;\forall i \text{ and thus } td \mid d$$

$$\Rightarrow t \mid 1 \text{ or that } t \text{ is a unit.}$$

Theorem 27 : (Gauss' Lemma) : *Let R be a UFD, then in $R[x]$ the product of two primitive polynomials is a primitive polynomial.*

Proof : Let $\quad f(x) = a_o + a_1x + \ldots\ldots + a_mx^m$

$$g(x) = b_o + b_1x + \ldots\ldots + b_nx^n$$

be two primitive polynomials in $R[x]$, then $f(x)$ and $g(x)$ are non zero (by definition). Thus

$f(x)\ g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots$ is also non zero.

Let $\qquad d = g.c.d.(c_o,\ c_1,\ c_2, \ldots\ldots)$

We show d is a unit. Suppose it is not, then there exists an irreducible element p s.t., $p \mid d$.

[Recall that in a UFD, a non unit element a can be expressed as a product of irreducibles, $a = p_1p_2 \ldots\ldots p_n \Rightarrow p_1 \mid a$]

Thus $p \mid d \Rightarrow p \mid c_i$ for all i ....(1)

Now if $p \mid a_i$ for all i then $p \mid g.c.d.(a_o,\ a_1, \ldots\ldots,\ a_m)$, which is a unit, say, u.

Now $\qquad p \mid u \Rightarrow u = pk \Rightarrow 1 = p(ku^{-1})$

$\qquad\qquad \Rightarrow p$ is a unit,

which is not true as p is irreducible.

$\therefore \qquad p \nmid a_i$ for some i

Let i be such least +ve integer, then

$$p \mid a_o,\ p \mid a_1, \ldots\ldots, p \mid a_{i-1}, p \nmid a_i$$

Similarly $\exists$ some integer j, s.t.,

$$p \mid b_o,\ p \mid b_1, \ldots\ldots, p \mid b_{j-1}, p \nmid b_j$$

Now $\qquad c_{i+j} = (a_ob_{i+j} + a_1b_{i+j-1} + \ldots\ldots + a_{i-1}\,b_{j+1})$

$\qquad\qquad + a_ib_j + (a_{i+1}\,b_{j-1} + \ldots\ldots + a_{i+j}b_o)$

Since $p \mid c_{i+j}$ by (1)

$$p \mid (a_ob_{i+j} + a_1b_{i+j-1} + \ldots\ldots + a_{i-1}\,b_{j+1}),$$
$$p \mid (a_{i+1}\,b_{j-1} + \ldots\ldots + a_{i+j}b_o)$$

$\therefore\ p \mid a_ib_j$, but p being irreducible in a UFD is prime

$\Rightarrow p \mid a_i$ or $p \mid b_j$, a contradiction. Hence the result.

Cor. : If R is a UFD and $f(x),\ g(x) \in R[x]$, then

$$c(fg) = c(f)\ c(g) \text{ (upto units)}$$

Since we can write $f(x) = d f_1(x),\ d = c(f)$

$$g(x) = d'g_1(x),\ \ d' = c(g)$$
$$f(x)\ \ g(x) = dd'f_1(x)\ \ g_1(x)$$

where $f_1,\ g_1$ being primite give f_1g_1 to be primitive

$$c(f_1g_1) = 1 \text{ (or a unit)}$$

$\therefore \qquad c(fg) = dd' = c(f)\ c(g)$

Converse of Gauss' Lemma is also true as we can prove

Theorem 28 : *If $f(x)\ g(x)$ is primitive polynomial in $R[x]$, R being a UFD then so are $f(x)$ and $g(x)$.*

Proof : fg is primitive

$\qquad \Rightarrow c(fg)$ is a unit

$\qquad \Rightarrow \exists$ an element $r \in R$ s.t., $c(fg)\,r = 1$

$$\Rightarrow c(f)\ c(g)\ r = 1$$
$$\Rightarrow c(f)\ [c(g) \cdot r] = 1$$
$$\Rightarrow c(f) \text{ is a unit} \Rightarrow f \text{ is primitive.}$$

Similalry $c(g)$ is a unit $\Rightarrow g$ is primitive.

Theorem 29 : *If R is an integral domain with unity, then units of R and $R[x]$ are same.*

Proof : Let a_o be a unit of R.

Then $\exists\ b_o \in R$ s.t., $a_o b_o = 1$

Let $f(x) = a_o + 0 \cdot x + 0 \cdot x^2 + \ldots..$

$g(x) = b_o + 0 \cdot x + 0 \cdot x^2 + \ldots..$

then $f(x)\, g(x) = a_o b_o + 0 \cdot x + 0 \cdot x^2 + \ldots..$

$= 1 = 1 + 0 \cdot x + 0 \cdot x^2 + \ldots..$

$\Rightarrow f(x)$ is a unit in $R[x]$

i.e., a_o is a unit in $R[x]$.

Conversely, let $f(x)$ be any unit of $R[x]$

Then $\exists\ g(x) \in R[x]$ s.t.,

$f(x)\, g(x) = 1\ (= 1 + 0 \cdot x + 0 \cdot x^2 + \ldots\ldots)$

$\Rightarrow \deg(fg) = \deg 1$

$\Rightarrow \deg f + \deg g = 0$

$\Rightarrow \deg f = \deg g = 0$

$\Rightarrow f$ and g are constant polynomials

i.e., $f(x) = a_o + 0x + 0x^2 + \ldots..\qquad a_o \in R$

$g(x) = b_o + 0x + 0x^2 + \ldots\ldots\qquad b_o \in R$

Since $fg = a_o b_o = 1$

we find, $a_o = f(x)$ is a unit of R

Hence the result.

Problem : *Show that $2x + 1$ is a unit in $Z_4[x]$.*

Solution : Since $(2x+1)(2x+1) = 0x^2 + 0x + 1 = 1$

$[4 = 0 \text{ in } Z_4]$

we find $2x + 1$ is a unit in $Z_4[x]$.

Remark : Notice $2x + 1$ is a non constant polynomial and therefore, does not belong to Z_4 and thus cannot be a unit in Z_4. But then Z_4 is not an integral domain. In fact, 1 and 3 are units of Z_4. $[3 \otimes 3 = 1]$.

Theorem 30 : *If R is an integral domain with unity and a is an irreducible element of R then a is irreducible element of $R[x]$.*

Proof : Suppose a is not irreducible element of $R[x]$ then $\exists\ p(x), q(x) \in R[x]$ s.t., $a = p(x)\ q(x)$

where $p(x)$ and $q(x)$ are non units.

Now $\quad a = pq$

$$\Rightarrow \deg a = \deg p + \deg q$$

$$\Rightarrow 0 = \deg p + \deg q$$

$$\Rightarrow \deg p = \deg q = 0$$

$\Rightarrow p, q$ are constant polynomials $\Rightarrow p, q \in R$

Thus $a = pq$, $p, q \in R$ and p, q are non units [units of R and $R[x]$ are same], a contradiction to the fact that a is irreducible in R.

Hence the result follows. (See theorem 32 also).

Definition : Let R be an integral domain with unity. A polynomial $f(x) \in R[x]$ of positive degree (i.e., of deg ≥ 1) is said to be an *irreducible polynomial* over R if it cannot be expressed as product of two polynomials of positive degree.

In other words, if whenever $f(x) = g(x)\, h(x)$,

then $\quad \deg g = 0$ or $\deg h = 0$

A polynomial of positive degree which is not irreducible is called *reducible* over R.

Example 12 : $x^2 + 1 \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Z}$.

whereas it is reducible over $\mathbf{C}$

as $\quad x^2 + 1 = (x - i)(x + i)$

Again $x^2 - 2$ is irreducible over $\mathbf{Z}$, but reducible over $\mathbf{R}$, the reals as $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Remarks : (*a*) Any polynomial of degree 1 is irreducible over a field F.

(*b*) If $f(x) \in F[x]$ is any polynomial of degree > 1 and $f(a) = 0$ for some $a \in F$ then $f(x)$ is reducible over F.

By division algorithm, for $f(x)\, g(x) = (x - a)$, we can find t and r such that $f(x) = (x - a)\, t(x) + r$, where, either $r = 0$ or deg $r <$ deg $(x - a)$, i.e., either $r = 0$ or is a constant polynomial.

Since $f(a) = 0$, we get $0 = f(a) = r$

$$\Rightarrow f(x) = (x - a)\, t(x)$$

$$\Rightarrow \deg f = \deg (x - a) + \deg t(x)$$

$$\Rightarrow \deg t(x) \geq 1 \text{ as } \deg f > 1,\ \deg (x - a) = 1$$

thus f is reducible.

(*c*) Let $f(x) \in F[x]$ be a polynomial of degree 2 or 3 then $f(x)$ is reducible implies $\exists\ a \in F$, s.t., $f(a) = 0$

$f(x)$ is reducible $\Rightarrow f(x) = g(x)\, h(x)$ where $\deg g$, $\deg h \geq 1$

Now $\quad \deg f = \deg g + \deg h$

$$\Rightarrow 2, 3 = \deg g + \deg h$$

$$\Rightarrow \text{one of } \deg g \text{ or } \deg h \text{ is } 1$$

Let $\deg g = 1$ and suppose $g(x) = a_o + a_1 x$, $(a_1 \neq 0)$

then $$g(-a_o a_1^{-1}) = 0$$

$$\Rightarrow f(-a_o a_1^{-1}) = 0. \text{ Take } a = -a_o a_1^{-1}.$$

(*d*) $f(x) \in F[x]$ a polynomial of degree 2 or 3 is reducible iff $\exists\ a \in F$ such that $f(a) = 0$

Follows by (*b*) and (*c*)

(*e*) The fact that $f(a) = 0$ is also expressed by saying that a is a *root* or a *zero* of the polynomial $f(x)$.

We should be careful while talking about irreducible elements and irreducible polynomials as the following example shows us the differentce between the two.

Example 13 : Consider the polynomial $2x^2 + 2$

Since it cannot be expressed as product of two positive degree polynomials in $\mathbf{Z}[x]$, we notice it is irreducible polynomial over $\mathbf{Z}$.

Again $$2x^2 + 2 = 2(x^2 + 1)$$
$$= \text{product of two polynomials}$$
$$= gh \text{ (say)}$$

Since g and h are non units in $\mathbf{Z}[x]$ as $1, -1$ are the only units of $\mathbf{Z}$ and, therefore, of $\mathbf{Z}[x]$ we find $2x^2 + 2$ can be expressed as product of two non units and thus $2x^2 + 2$ is *not* an irreducible element in $\mathbf{Z}[x]$. Hence *an irreducible polynomial need not be an irreducible element.*

The converse, however, follows by

Theorem 31 : *Every irreducible element in $R[x]$ is an irreducible polynomial, R being an integral domain with unity.*

Proof : Let $f(x) \in R[x]$ be any irreducible element.

Suppose $f(x)$ is reducible polynomial,

then $f(x) = g(x)\, h(x)$, $g,\ h \in R[x]$, with $\deg g > 0$, $\deg h > 0$

Since degree of g and h is positive, g and h are not constant polynomials

$$\therefore \quad g,\ h \notin R$$
$$\Rightarrow g,\ h \text{ cannot be units in } R$$
$$\Rightarrow g,\ h \text{ cannot be units in } R[x]$$
$$\Rightarrow f \text{ is not irreducible element.}$$

a contradiction which proves our result. (See remark on page 338)

Example 14 : The polynomial $f(x) = x^2 - 2x - 15$

is both primitive as well as reducible over $\mathbf{Z}$ as

$$c(f) = g.c.d.(1, -2, -15) = 1$$

and $$x^2 - 2x - 15 = (x-5)(x+3)$$

However, the polynomial $x^2 - 2$ is primitive as well as irreducible over $\mathbf{Z}$.

Theorem 32 : *If R is a UFD then any $f(x) \in R[x]$ is an irreducible element of $R[x]$ iff either f is an irreducible element of R or f is an irreducible primitive polynomial of $R[x]$.*

Proof : Let $f(x) \in R[x]$ be an irreducible element of $R[x]$. If $f \in R$ then f will be irreducible element of R as well. [Units of R and $R[x]$ are same].

Suppose $f \notin R$, we show f is then irreducible primitive polynomial of $R[x]$.

Suppose $f = gh$ for some $g, h \in R[x]$.

Since f is irreducible element of $R[x]$, one of g or h must be a unit of $R[x]$.

$\Rightarrow$ one of g or h must be in R (as units of $R[x]$ and R are same).

$\Rightarrow$ deg $g = 0$ or deg $h = 0$

thus f is not reducible or that f is irreducible polynomial of $R[x]$.

(In fact, it follows by theorem 31).

Again since any polynomial $f(x)$ can be written as a product of $c(f)$ and a primitive polynomial we can write $f = df_1$ where $c(f) = d \in R$ and f_1 is primitive.

Since $d \in R$, $\deg f_1 = \deg f$

$\Rightarrow \deg f_1 \geq 1$

$\Rightarrow f_1 \notin R$

$\Rightarrow f_1$ cannot be a unit of $R[x]$.

Thus $f = df_1$, f_1 is not a unit, f is irreducible element.

$\Rightarrow d$ is a unit

$\Rightarrow c(f) =$ unit

$\Rightarrow f$ is primitive polynomial

Conversely, if f is an irreducible element of R then f is an irreducible element of $R[x]$, (see theorem 27).

Suppose now f is an irreducible primitive polynomial of $R[x]$. We show f is irreducible element of $R[x]$.

Since f is irreducible polynomial, $\deg f \geq 1$

and so $f \notin R$

$\Rightarrow f$ cannot be a unit [as units of R and $R[x]$ are same]. Also, of course, f is non zero.

Suppose now $f(x) = g(x)\,h(x)$ for some $g, h \in R[x]$.

Since f is irreducible polynomial

either $\deg g = 0$ or $\deg h = 0$

Without any loss of generality, we can take $\deg g = 0$.

$\Rightarrow g$ is a constant polynomial say, $b_o + 0x + 0x^2 + \ldots\ldots$

$\Rightarrow g \in R$

Now $c(f) = c(gh) = c(g)\,c(h)$

f being primitive, $c(f) =$ unit u

$$c(g) = c(h) = u \Rightarrow c(g) \mid u$$
$$\Rightarrow c(g) \text{ is a unit}$$

or that g is a unit of $R[x]$.

(Unit $= c(g) = g.c.d.(b_o) = b_o = g$)

Hence $f(x)$ is irreducible element of $R[x]$.

Remark : If F is a field then every irreducible polynomial of $F[x]$ is irreducible element of $F[x]$ and conversely.

Let $f(x)$ be irreducible polynomial in $F[x]$ and suppose $f = gh$.

Since f is irreducible polynomial,

either $\deg g = 0$ or $\deg h = 0$.

Suppose $\deg g = 0$, then g is a constant polynomial, say,

$$g(x) = b_o + 0 \,.\, x + 0x^2 + \ldots..$$

where $\quad b_o \in F,\ b_o \neq 0,\ \therefore\ b_o^{-1} \in F$

i.e., $b_o = g$ is a unit in F and, therefore, a unit in $F[x]$.

Thus f is irreducible element of $F[x]$.

Notice, since f is irreducible polynomial, $\deg f \geq 1$ and so f is non zero, non unit element of $F[x]$.

Converse follows by theorem 31.

Theorem 33 : *If F is a field then an ideal $<p(x)> \neq \{0\}$ in $F[x]$ is maximal iff $p(x)$ is irreducible in $F[x]$.*

Proof : If $p(x)$ is irreducible polynomial over F, then it is irreducible element of $F[x]$ and also since F is a field, $F[x]$ is a PID which is not a field. (See page 313). The result now follows by theorem 10 on page 305.

Problem 25 : *Show that $\dfrac{\mathbf{Q}[x]}{I}$ where $I = <x^2 - 5x + 6>$ is not a field.*

Solution : Since $x^2 - 5x + 6 = (x-2)(x-3)$ we find it is not irreducible polynomial over $\mathbf{Q}$.

Thus $I = <x^2 - 5x + 6>$ is not a maximal ideal of $\mathbf{Q}[x]$ and hence $\dfrac{\mathbf{Q}[x]}{I}$ is not a field.

Lemma : *If R is a UFD and $p(x)$ is primitive polynomials in $R[x]$ then it can be factored in a unique way as a product of irreducible elements of $R[x]$.*

Proof : Let K be the field of quotients of R, then $K[x]$ is a Euclidean domain and hence a PID and thus a UFD.

Now $p(x) \in R[x] \Rightarrow p(x) \in K[x]$ and as $K[x]$ is a UFD we can express $p(x) = p_1(x)\, p_2(x) \ldots\ldots p_k(x)$

as product of irreducible elements $p_i(x)$ of $K[x]$.

Again $\qquad p_i(x) \in K[x] \Rightarrow p_i(x) = \dfrac{1}{a_i} f_i(x)$

where $a_i \in R, \quad f_i \in R[x]$

Since $p_i(x) \in K[x] \Rightarrow p_i\ (x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots$

where $\alpha_i \in K$, which being field of quotients of R, means each α_i can be expressed as $\frac{b_i}{a_i}$ a_i, $b_i \in R$, $a_i \neq 0$

or that
$$p_i(x) = \frac{b_o}{a_o} + \frac{b_1}{a_1} x + \frac{b_2}{a_2} x^2 + \ldots\ldots$$
$$= \frac{1}{a}\ [c_o + c_1 x + c_2 x^2 + \ldots\ldots] = \frac{1}{a}\ f(x), \qquad f \in R[x]$$

Again $p_i(x)$ is irreducible element in $K[x]$.

$\Rightarrow f_i(x)$ will be irreducible element in $K[x]$ because if it is not so then we can write it as $f_i = g_i h_i$, where g_i, h_i are non units.

$\Rightarrow p_i = \frac{1}{a_i} g_i h_i$, where g_i, h_i are non units

$\Rightarrow p_i$ is not irreducible element

Again $f_1(x) \in R[x] \Rightarrow f_i = d_i\ f_i^*(x)$ where $f_i^*(x)$ is primitive and $d_i = c(f_i)$

$$\therefore\ p_i = \frac{d_i}{a_i} f_i^*,\ i = 1, 2, \ldots\ldots, k$$

$$\Rightarrow p_1 p_2 \ldots\ldots p_k = \frac{d_1 d_2 \ldots\ldots d_k}{a_1 a_2 \ldots\ldots a_k} f_1^* f_2^* \ldots\ldots f_k^*$$

$$\Rightarrow p = \frac{d_1 d_2 \ldots\ldots d_k}{a_1 a_2 \ldots\ldots a_k} f_1^* f_2^* \ldots\ldots f_k^*$$

$$\Rightarrow (a_1 a_2 \ldots\ldots a_k)\ p = (d_1 d_2 \ldots\ldots d_k)\ (f_1^* f_2^* \ldots\ldots f_k^*) \qquad \ldots\ldots (1)$$

Now as $p_i = \frac{d_i}{a_i} f_i^*$ and p_i is irreducible element we find f_i^* will also be irreducible element of $K[x]$ otherwise p_i will not remain irreducible element (as seen earlier).

Content of L.H.S. of (1) is $(a_1 a_2 \ldots\ldots a_k)\ u$ for some unit u as p is primitive and content of R.H.S. of (1) is $(d_1 d_2 \ldots\ldots d_k)\ v$, for some unit v as f_i^* are primitive.

Equating the contents of both sides we get

$a_1 a_2 \ldots\ldots a_k = (d_1 d_2 \ldots\ldots d_k) w$ where $w = v u^{-1}$ is a unit.

Thus $p(x) = (w^{-1} f_1^*)\ (f_2^* f_3^* \ldots\ldots f_k^*)$

which is a product of irreducible elements in $K[x]$. Again f_i^* being primitive

and irreducible elements in $K[x]$, we find f_i^* will be irreducible elements in $R[x]$. To show uniqueness

Let $p(x) = r_1(x)\, r_2(x) \ldots\ldots r_k(x)$, where $r_i(x)$ are irreducible in $R[x]$.

(Notice the number of elements in the product remain same as k as we are in a UFD)

Now $p(x)$ primitive $\Rightarrow$ each r_i is primitive

because $\quad p = r_1 r_2 \ldots\ldots r_k \Rightarrow c(p) = c(a_1)\, c(a_2) \ldots\ldots c(a_k)$

$\Rightarrow d = d_1 d_2 \ldots\ldots d_k$

$\Rightarrow$ each d_i is a unit

$\Rightarrow$ each a_i is primitive

Hence each a_i is primitive and irreducible element in $R[x]$

$\Rightarrow r_i(x)$ is irreducible in $K[x]$ for all i

But $K[x]$ being a UFD, each r_i is uniquely determined upto associates in $K[x]$.

$$\Rightarrow r_i \;\&\; f_i^* \text{ are associates for all } i$$

$$\Rightarrow r_i = u_i f_i^*$$

where u_i is a unit in $K[x]$ and thus in $K \Rightarrow u_i$ is of the form $\dfrac{a_i}{b_i}$

Hence $$r_i = \frac{a_i}{b_i} f_i^*$$

$$\Rightarrow b_i r_i = a_i f_i^*$$

Equating contents on both sides, we get

$b_i = u a_i$ for some unit u in R or $\dfrac{a_i}{b_i} = u^{-1}$ a unit in R or that r_i is associate of f_i^* in $R[x]$.

Theorem 34 : *R is a UFD $\Rightarrow R[x]$ is a UFD.*

Proof : Let $f \in R[x]$ be non zero non unit element.

Let $f = d f^*(x)$ when $d = c(f)$, f^* is primitive.

By lemma

$f^* = f_1^* f_2^* \ldots\ldots f_x^*$ where f_i^* are irreducible elements of $R[x]$ and this representation is unique upto associates.

Also $d \in R$ and R is a UFD, thus either d is a unit or it can be written as

$$d = d_1 d_2 \ldots\ldots d_r$$

where d_i are irreducible elements in R.

If d is a unit

$$f = d.f^* \text{ gives}$$

$$f = (d f_1^*)\ f_2^* \ldots\ldots f_k^*, df_1^*, f_2^*, \ldots\ldots f_x^* \text{ are irreducible,}$$

which gives us the result.

If d is not a unit, let $d = d_1 d_2 \ldots\ldots d_r$

Since each d_i is irreducible element of R each d_i will be irreducible element of $R[x]$, thus f = finite product of irreducible elements in $R[x]$ and representation is unique upto associates thereby proving our theorem.

Remark : $a, b \in R$ are associates in R iff a, b are associates in $R[x]$. The result follows as units of R and $R[x]$ are same.

Example 15 : Let F be a field then we've already seen that $F[x, y]$ is not a PID.

Now F being a field is a UFD and therefore by above theorem $F[x, y]$ will be a UFD. Thus $F[x, y]$ is as example of a UFD which is not a PID.

Example 16 : $\mathbf{Z}$ is a PID and $\therefore$ a UFD $\Rightarrow$ $\mathbf{Z}[x]$ is UFD.

But $\mathbf{Z}[x]$ is not a PID otherwise $\mathbf{Z}$ has to be a field, which it is not and hence $\mathbf{Z}[x]$ is a UFD but not PID. (See Cor. 1 page 317).

Theorem 35 : *Let R be a UFD and $f(x) \in R[x]$ be primitive polynomial. If $f(x)$ is irreducible element of $K[x]$ then $f(x)$ is an irreducible element of $R[x]$.*

Proof : Suppose $f(x)$ is not irreducible elementof $R[x]$

Then $\quad f = gh,\ g,\ h \in R[x]$ are non units

Also we can write

$$g = dg^*(x)$$

$$h = d'h^*(x), \text{ where } g^* \text{ and } h^* \text{ are primitive}$$

$$\Rightarrow f = dd'g^*h^*$$

Equating contents on both sides, we get

$$u = dd'vw \text{ as } f \text{ is primitive and so are } g^*,\ h^*$$

Where u, v, w are units

Thus $\quad 1 = dd'vwu^{-1}$

$$\Rightarrow d \text{ is a unit}$$

similarly $\quad d'$ is a unit

$$\Rightarrow g = dg^*$$

$$\Rightarrow c(g) = c(dg^*) = dc(g^*) = \text{unit} \times \text{unit} = \text{unit}$$

$$\Rightarrow g \text{ is primitive}$$

Similalry h is primitive

Again $\quad g, h \in R[x] \Rightarrow g, h \in K[x]$

Now $f = gh$, f is irreducible element of $K[x]$

$\Rightarrow$ g or h is a unit *of* $K[x]$

Without any loss of generality let g be a unit in $K[x]$

Then $\exists\, r \in K[x]$, s.t., $gr = 1$

$\Rightarrow$ $\deg g + \deg r = 0$

$\Rightarrow$ $\deg g = \deg r = 0$

$\Rightarrow$ $g,\ r \in K$

Let $g = \dfrac{\alpha}{\beta},\ \alpha,\ \beta \in R$

Then $f = \dfrac{\alpha}{\beta} h$ or that $\beta f = \alpha h$

$\Rightarrow$ $c(\beta f) = c(\alpha h)$

$\Rightarrow$ $\beta u = \alpha v,\ u,\ v$ being units, ($f,\ g$ primitive)

$$\Rightarrow \frac{\alpha}{\beta} = uv'$$

$$\Rightarrow g = \frac{\alpha}{\beta} = uv' = \text{unit in } R$$

$\Rightarrow$ g is a unit in $R[x]$

a contradiction giving us the result.

We now prove the converse in

Theorem 36 : *If $f(x) \in R[x]$ is both primitive and irreducible element of $R[x]$ then $f(x)$ is irreducible element of $K[x]$.*

Proof : Suppose $f(x)$ is not irreducible element of $K[x]$

then $f = gh$, where $f,\ g$ are non units in $K[x]$

thus $f,\ g$ are non units of K.

i.e., $f,\ g \notin K$

Note if $g \in K$, then as $g \neq 0$, it will have multiplicative inverse being an element of a field and hence will be a unit.

Thus $\deg g,\ \deg h > 0$

Now $g(x) = \dfrac{1}{d}\, g_o(x)$

$\Rightarrow$ $g_o(x) = dg(x) \in R[x]$

Similarly $h_o(x) = d'h(x) \in R[x]$

Again $g_o(x) = \alpha g^*(x)$

$h_o(x) = \beta h^*(x)$ where $g^*,\ h^*$ are primitive

and $\alpha,\ \beta$ are g.c.d. of coeffs. of g_o and h_o

$$\therefore \qquad c(g_o) = \alpha, \; c(h_o) = \beta$$

$$\therefore \qquad f(x) = \frac{1}{dd'} \alpha\beta \; g^* h^*$$

$$\Rightarrow \; dd'f = \alpha\beta g^* h^*$$

Since g^*, h^* are primitive, by Gauss Lemma $g^* h^*$ will be primitive

$$\Rightarrow \; c(dd'f) = c(\alpha\beta g^* h^*) = \alpha\beta$$

$$\Rightarrow \; dd' = u\alpha\beta \text{ as } f \text{ is primitive}$$

$$\Rightarrow \; f(x) = u^{-1} g^*(x) \; h^*(x), \qquad g^*, \; h^* \in R[x], \; u \in R$$

$$\deg u^{-1} = g^* = \deg g^* = \deg \alpha g^*$$

$$= \deg g_o = \deg \frac{1}{d} g_o = \deg g > 0$$

Also $\qquad \deg h^* = \deg h > 0$

$\therefore \qquad u^{-1} g^*, \; h^*$ are non units in $R[x]$

Note $\deg h^* > 0 \Rightarrow h^*$ is not a member of R

i.e., h^* cannot be a unit of R and therefore, a unit of $R[x]$

Hence $f = (u^{-1} g^*) \; h^*$

where $u^{-1} g^*$ & h^* are non units in $R[x]$

$\Rightarrow f$ is not irreducible in $R[x]$

a contradiction, proving our result.

Problem 26 : *Show that $f(x) = x^3 - 9$ is reducible in Z_{11}.*

Solution : Since $4 \otimes 4 \otimes 4 = 9$ in Z_{11}, we find $(x-4)$ is a factor of $x^3 - 9$. By actual division we find

$x^3 - 9 = (x-4) \; (x^2 + 4x + 5)$ in Z_{11}.

Hence $x^3 - 9$ is reducible.

Problem 27 : *Show that $Z_5[x]$ is a UFD. Is $x^2 + 2x + 3$ reducible over $Z_5[x]$?*

Solution : Since 5 is a prime Z_5 is a field

$$\Rightarrow \; Z_5 \text{ is a UFD}$$

$$\Rightarrow \; Z_5[x] \text{ is a UFD.}$$

Again $x^2 + 2x + 3$ will be reducible over Z_5 is if it has a root in Z_5, but none of the elements in Z_5 is a root $x^2 + 2x + 3$, hence it is an irreducible polynomial over Z_5.

Problem 28 : *Find g.c.d.(2, x) in $\mathbf{Z}[x]$ and show that it cannot be-put in the form $2r(x) + x\,s(x)$, for any $r(x)$, $s(x) \in \mathbf{Z}[x]$.*

Solution : We have

$$2 = 2 + 0 \,.\, x + 0 \,.\, x^2 + \ldots\ldots$$

$$x = 0 + 1 \,.\, x + 0 \,.\, x^2 + \ldots\ldots$$

Now $1 \mid 2$ and $1 \mid x$ is obvious by definition as 1 is unity.

Suppose $f \mid 2$ and $f \mid x$. We show that $f \mid 1$

Now $\quad f \mid 2 \Rightarrow 2 = fg$ for some g

$$\Rightarrow \deg 2 = \deg f + \deg g$$

$$\Rightarrow 0 = \deg f + \deg g$$

$$\Rightarrow \deg f = 0 \text{ or that } f \text{ is a constant polynomial}$$

Let $f = a_o + 0 \,.\, x + 0 \,.\, x^2 + \ldots\ldots$

Again, $f \mid x \Rightarrow a_o \mid x \Rightarrow x = a_o h(x)$

Thus $\deg x = 0 + \deg h$ which gives $\deg h = 1$

Let $h(x) = b_o + b_1 x + 0 \,.\, x^2 + 0 \,.\, x^3 + \ldots\ldots$

Then $x = a_o h = a_o(b_o + b_1 x) = a_o b_o + a_o b_1 x$

$$\Rightarrow 1 = a_o b_1 = f(x)\ b_1$$

or that $f \mid 1$

Hence $1 = g.c.d.(2,\ x)$

In view of theorem 1 page 289, any other *g.c.d.* $(2,\ x)$ will be an associate of 1. Thus $1, -1$ are the *g.c.d.* of 2 and x in $\mathbf{Z}[x]$. (Recall units of $\mathbf{Z}$ and $\mathbf{Z}[x]$ are same and also associate of a unit will be a unit).

Now suppose it is possible to express any g.c.d. f of $(2, x)$ as $f = 2r + xs$, then $1 = (2r + xs)\, b_1 = 2b_1\,(c_o + c_1 x + c_2 x^2 + \ldots..) + b_1 xs(x)$ where $r(x) = c_o + c_1 x + c_2 x^2 + \ldots\ldots$ i.e., $1 = 2b_1 c_o$, showing that 2 is a unit in $\mathbf{Z}$, which is not true. Hence the result follows.

Note : $\mathbf{Z}[x]$ is a UFD but not a PID. See example 16 page 341.

We now give a test for the irreducibility of a polynomial in $\mathbf{Z}[x]$ over $\mathbf{Q}$ the ring of rationals.

Theorem 37 : (Eisenstein's Criterion) :

Let $f(x) = a_o + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$ be a polynomial with integer coefficients (i.e., $f(x) \in \mathbf{Z}[x]$). Suppose that for some prime number p,

$$p \mid a_o,\ p \mid a_1,\ p \mid a_2 \ldots\ldots, p \mid a_{n-1},\ p \nmid a_n,\ p^2 \nmid a_o$$

then $f(x)$ is irreducible polynomial over $\mathbf{Q}$, the ring of rationals.

We first prove.

Lemma : *If $f(x) \in \mathbf{Z}[x]$ is primitive and $f(x)$ is irreducible over $\mathbf{Z}$ then f is irreducible over $\mathbf{Q}$.*

Proof : Suppose f is not irreducible over $\mathbf{Q}$,

then we can write $f = gh,\ g, h \in \mathbf{Q}[x]$

with $\deg g,\ \deg h > 0$

Then $\quad g(x) \in \mathbf{Q}[x] \Rightarrow g = \dfrac{1}{\alpha}\, g_1(x) \qquad$ where $g_1(x) \in \mathbf{Z}[x]$

$$h(x) \in \mathbf{Q}[x] \Rightarrow h = \frac{1}{\beta}\, h_1(x) \qquad \text{where } h_1(x) \in \mathbf{Z}[x]$$

(For instance, if $g(x) = \frac{2}{3}x^2 + \frac{1}{2}x + 1 \in \mathbf{Q}[x]$ then $g(x) = \frac{1}{6}(4x^2 + 3x + 6)$, where then $g_1(x) = 4x^2 + 3x + 6 \in \mathbf{Z}[x]$).

Again $g_1(x) \in \mathbf{Z}[x] \Rightarrow g_1 = dg_1^*$ where g_1^* is primitive

$h_1(x) \in \mathbf{Z}[x] \Rightarrow h_1 = d'h_1^*$ where h_1^* is primitive

Thus $f = gh = \dfrac{1}{\alpha\beta} dd' g_1^* h_1^*$

$\Rightarrow \alpha\beta f = dd' g_1^* h_1^*$

$\Rightarrow c(\alpha\beta f) = c(dd' g_1^* h_1^*)$

Since f is primitive polynomial in $\mathbf{Z}[x]$, its content is a unit in $\mathbf{Z}$ and as units in $\mathbf{Z}$ are 1 or -1 $c(f) = \pm 1$. Similarly, $c(g_1^*)$, $c(h_1^*)$ can be ± 1.

Equating the contents on both sides we get

$\pm\alpha\beta = \pm dd'$

i.e., $\alpha\beta = \pm dd'$

and hence the equation $\alpha\beta f = dd' g_1^* h_1^*$ reduces to $f = \pm g_1^* h_1^*$

Now $\deg(\pm g_1^*) = \deg g_1^* = \deg d g_1^* = \deg g_1$

$= \deg \dfrac{1}{\alpha} g_1 = \deg g > 0$

Similarly, $\deg(h_1^*) > 0$.

Thus we can write $f = \pm g_1^* h_1^*$ where $\pm g_1^*, h_1^*$ are polynomials in $\mathbf{Z}[x]$ and have positive degree

$\Rightarrow f$ is reducible over $\mathbf{Z}$, a contradiction

hence the lemma is proved.

We now come to the *proof of the main theorem.*

We show f is irreducible over $\mathbf{Z}$.

Suppose it is not irreducible over $\mathbf{Z}$

then $\exists\, g, h \in \mathbf{Z}[x]$ s.t., $f = gh$

with $\deg g, \deg h > 0$

Let $g(x) = b_o + b_1 x + \ldots\ldots + b_s x^s$

$h(x) = c_o + c_1 x + \ldots\ldots\ldots + c_t x^t$

then $g(x)\, h(x) = b_o c_o + (b_1 c_o + b_o c_1)\, x + \ldots\ldots$

So $f = gh$

$$\Rightarrow a_o + a_1x + \ldots\ldots = b_oc_o + (b_1c_o + b_oc_1)\ x + \ldots\ldots$$

$$\Rightarrow a_o = b_oc_o$$

Now $\quad p \mid a_o \Rightarrow p \mid b_oc_o \Rightarrow p \mid b_o$ or $p \mid c_o$ as p is prime

Suppose $\quad p \mid b_o$ then $p \nmid c_o$ as $p^2 \nmid a_o$

$$[p \mid b_o,\ p \mid c_o \Rightarrow p^2 \mid b_oc_o \Rightarrow p^2 \mid a_o]$$

Again, p cannot divide all of $b_o, b_1, b_2, \ldots, b_s$ as if it does then p divides each term of the type

$$b_oc_o,\ b_1c_o + b_oc_1, \ldots\ldots$$

i.e., p divides all of $a_o, a_1, \ldots, a_n$

But $p \nmid a_n$

Let k be the smallest integer such that $p \nmid b_k$, $k \leq s < n$

So $\quad p \mid b_o,\ p \mid b_1, \ldots, p \mid b_{k-1},\ p \nmid b_k$

Now $\quad a_k = b_kc_o + b_{k-1}c_1 + \ldots\ldots + b_oc_k$

$p \mid a_k$ by given condition as $k < n$

Also $\quad p \mid (b_{k-1}c_1 + b_{k-2}c_2 + \ldots\ldots + b_oc_k)$

$$\Rightarrow p \mid b_kc_o \Rightarrow p \mid b_k \text{ or } p \mid c_o$$

both leading to a contradiction, Hence $f(x)$ is irreducible over $\mathbf{Z}$.

If $f(x)$ is primitive, it will be irreducible over $\mathbf{Q}$ by lemma. If $f(x)$ is not primitive we can write $f = df_1$ where f_1 is primitive and $d = c(f)$

Then f irreducible over $\mathbf{Z} \Rightarrow df_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow f_1$ is irreducible over $\mathbf{Z}$

$\Rightarrow f_1$ is irreducible over $\mathbf{Q}$ (as f_1 is primitive)

$\Rightarrow df_1$ is irreducible over $\mathbf{Q}$

$\Rightarrow f$ is irreducible over $\mathbf{Q}$

Hence the theorem is proved.

Remark : Since $f(x) = g(x)\,h(x) \Leftrightarrow f(x+1) = g(x+1)\,h(x+1)$

we find $f(x)$ will be recucible (irreducible) iff $f(x+1)$ is reducible (irreducible). In fact one can take any integer in place of 1 above.

Example 17 : The polynomial $x^2 - 4x + 2$ is irreducible over $\mathbf{Q}$, as if we take $p = 2$, then $p \mid 4$, $p \mid 2$ $p \nmid 1$, $p^2 \nmid 2$.

Again, consider the polynomial $x^2 + 1 = f(x)$.

Since there is no prime p which divides 1, we cannot apply the Eisenstein's criterion to $f(x)$.

Consider $\quad f(x+1) = (x+1)^2 + 1$

$$= x^2 + 2x + 2 \qquad (a_o = 2,\ a_1 = 2,\ a_2 = 1)$$

Take $p = 2$, then $p \mid 2$, $p \nmid 1$, $p^2 \nmid 2$

Hence $f(x+1)$ is irreducible.

$\Rightarrow f(x)$ is irreducible (by using above remark)

Again, let $\quad f(x) = x^3 + x^2 - 2x - 1$

Since there is no prime that divides 1, we cannot apply the criterion here

Consider
$$f(x+1) = (x+1)^3 + (x+1)^2 - 2\ (x+1) - 1$$
$$= x^3 + 4x^2 + 3x - 1$$

we have the same situation. Let us consider
$$f(x-1) = (x-1)^3 + (x-1)^2 - 2\ (x-1) - 1$$
$$= x^3 - 2x^2 - x + 1$$

Again it is not possible to apply the criterion.

Consider $\quad f(x+2) = x^3 + 7x^2 + 14x + 7$

then $p = 7$ will do as here $a_0 = 7$, $a_1 = 14$, $a_2 = 7$, $a_3 = 1$ and $7 \mid 7$, $7 \mid 14$, $7 \mid 7$, $7 \nmid 1$, $7^2 \nmid 7$.

thus by criterion $f(x+2)$ and therefore, $f(x)$ is irreducible.

Remark : One may note that Eisenstein's criterion is not necessary for irreducibility of a polynomial as we've seen there does not exist any prime p such that $p \mid 1$ (although the polynomial could be irreducible). $x^3 - x + 1$ is irreducible over $\mathbf{Q}$, but Eisenstein's criterion is not applicable.

The polynomial $f(x) = x^3 - x + 1$ is irreducible over $\mathbf{Q}$, as suppose it is reducible then it has a root in $\mathbf{Q}$.

Let $\dfrac{m}{n}$, [m, n integers, $n \neq 0$, $(m, n) = 1$] be a root

Then
$$\frac{m^3}{n^3} - \frac{m}{n} + 1 = 0$$
$$\Rightarrow m^3 - mn^2 + n^3 = 0$$
$$\Rightarrow m^3 = n^2\ (m - n)$$
$$\Rightarrow n^2 \mid m^3 \Rightarrow n \mid m^3 . 1 \Rightarrow n \mid 1 \text{ as } (m, n) = 1$$
$$\Rightarrow n = \pm 1$$
$$\Rightarrow \frac{m}{n} \pm m$$

or that
$$m^3 - m + 1 = 0$$
$$\Rightarrow m\ (m^2 - 1) = -1$$
$$\Rightarrow m \mid 1 \text{ or that } m = \pm 1$$
$$\Rightarrow \frac{m}{n} = \pm 1 \text{ which gives}$$
$$\pm 1 \mp 1 + 1 = 0, \text{ which is not possible.}$$

Hence $x^3 - x + 1$ is not reducible over $\mathbf{Q}$.

Problem 29 : *For any prime p, show that the polynomial* $x^{p-1}+x^{p-2}+.....+x^2+x+1$ *is irreducible over* **Q**.

Solution : Let $f(x) = x^{p-1}+x^{p-2}+.....+x^2+x+1$

$$= \frac{x^p-1}{x-1} \text{ (sum of a G.P.)}$$

Now

$$f(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = \frac{x^p+p_{c_1}x^{p-1}+.....+p_{c_r}x^{p-2}+.....+p_{c_p}-1}{x}$$

$$= \frac{x^p+p_{c_1}x^{p-1}+.....+p_{c_{p-1}}x}{x}$$

$$= x^{p-1}+p_{c_1}x^{p-2}+.....+p_{c_{p-1}}$$

Since p is a prime number $p \mid p_{c_r}$ for all $1 \le r \le p-1$. (See example 3, page 255)

Also $\qquad p_{c_{p-1}} = p$ or $p^2 \nmid p_{c_{p-1}}$

Hence by Eisenstein's criterion $f(x+1)$ and, therefore, $f(x)$ is irreducible.

Exercises

1. If R is a UFD and $f(x) \in R[x]$ then it is possible to write $f(x) = ag(x)$, $a \in R$, $g(x) \in R[x]$ being primitive. Show that if $f(x) = ag(x) = bh(x)$, $a, b \in R$, g, h being primitive then a, b are associates and so are $g(x)$ and $h(x)$
2. Give example of a polynomial, which is
   (*i*) primitive and irreducible.
   (*ii*) primitive and reducible.
   (*iii*) not primitive but irreducible.
   (*iv*) not primitive but reducible.
3. Show that the following polynomials are irreducible over **Q**, (the rationals)
   (*i*) $8x^3-6x-1$
   (*ii*) $x^4+x^3+x^2+x+1$
   (*iii*) $2x^{10}-25x^3+10x^2-30$. ($p = 5$).
4. Find g.c.d. of (*i*) $3+4i$ and $4-3i$ in $\mathbf{Z}[i]$. Are these associates?
   (*ii*) $2x^2+x^3-6x^2+7x-2$, $2x^3-7x^2+8x-4$ in $\mathbf{Q}[x]$.
   (*iii*) $11+7i$ and $3+7i$ in $\mathbf{Z}[i]$
   (*iv*) $10+11i$ and $8+i$ in $\mathbf{Z}[i]$

5. (*i*) Show that the ideal $< x^2 + 1 >$ is maximal ideal in $\mathbf{R}[x]$.

   (*ii*) Show that $\dfrac{\mathbf{Q}[x]}{I}$, where $I = < x^2 - 6x + 6 >$ is a field.

6. Show that in a PID, every ideal is contained in a maximal ideal.
7. Show that $x^2 + 1$ and $x^2 + x + 4$ are irreducible over F the field of integers modulo 11. Prove also that $\dfrac{F[x]}{< x^2 + 1 >}$ and $\dfrac{F[x]}{< x^2 + x + 4 >}$ are isomorphic fields each having 121 elements.
8. If P is a prime ideal of $R[x]$ then show that $P \cap R$ is a prime ideal of R.
9. Let K be the field of quotients of a UFD R then show that primitive polynomials $f, g \in R[x]$ are associates in $R[x]$ iff f, g are associates in $K[x]$.
10. Let M be a proper ideal of a Boolean ring R with unity. Show that $\dfrac{R}{M}$ is a Boolean ring and $\dfrac{R}{M} \cong \dfrac{\mathbf{Z}}{(2)}$ iff M is a maximal ideal of R.
11. If $A = (2)$, show that $A[x]$ is not a maximal ideal of $\mathbf{Z}[x]$.
12. Show that the set of all polynomials with even coeffecients is a prime ideal in $\mathbf{Z}[x]$.
13. Show that $\mathbf{Z}[\sqrt{-3}\,]$ is not a UFD. (See exercise 13 page 307).
14. If F is a field, show that every non zero prime ideal of $F[x]$ is a maximal ideal.
15. Show that in a UFD R, every non zero prime ideal ($\neq$ R) contains a prime element.
16. Factorize $x^2 + x + 5$ in $F[x]$, where F is the field of integers mod 11.
17. Let R be an integral domain with unity. Show that a prime element in R is a prime element in $R[x]$.

Chapter 9

Vector Spaces

The motivating factor in rings was set of integers and in groups the set of all permutations of a set. A vector space originates from the notion of a vector that we are familiar with in mechanics or geometry. Our aim in this volume is not to go into details of that. Reader would recall that a vector is defined as a directed line segment, which in algebraic terms is defined as an ordered pair (a, b) , being coordinates of the terminal point relative to a fixed coordinate system. Addition of vectors is given by the rule

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

One can easily verify that set of vectors under this forms an abelian group. Also scalar multiplication is defined by the rule $\alpha\ (a, b) = (\alpha a, \alpha\beta)$ which satisfies certain properties. This concept is extended similarly to three dimensions. We generalise the whole idea through definition of a vector space and vary the scalars not only in the set of reals but in any field F. A vector space thus differs from groups and rings in as much as it also *involves* elements from outside itself.

Definition : Let $< V, + >$ be an abelian group and $< F, +, . >$ be a field. Define a function. (called scalar multiplication) from $F \times V \to V$, s.t., for all $\alpha \in F$, $v \in V$, $\alpha . v \in V$. Then V is said to form a *vector space* over F if for all $x, y \in V$, $\alpha, \beta \in F$, the following hold

(*i*) $(\alpha + \beta) x = \alpha x + \beta x$

(*ii*) $\alpha (x + y) = \alpha x + \alpha y$

(*iii*) $(\alpha\beta) x = \alpha (\beta x)$

(*iv*) $1 . x = x$, 1 being unity of F.

Also then, members of F are called *scalars* and those of V are called *vectors*.

Remark : We have used the same symbol + for the two different binary compositions of V and F, for convenience. Similarly same symbol . is used for scalar multiplication and product of the field F.

Since $< V, + >$ is a group, its identity element is denoted by 0. Similarly the field F would also have zero element which will also be represented by 0. In case of doubt one can use different symbols like 0_v and 0_F etc..

Since we generally work with a fixed field we shall only be writing V is a vector space (or sometimes $V(F)$ or V_F) .It would always be understood that it is a vector space over F (unless stated otherwise)

We defined the scalar multiplication from $F \times V \to V$. One can also define it from $V \times F \to V$ and have a similar definition. The first one is called a left vector space and the second a right vector space. It is easy to show that if V is a left vector space over F then it is a right vector space over F and conversely. In view of this result it becomes redundant to talk about left or right vector spaces. We shall thus talk of only vector spaces over F.

One can also talk about the above system when the scalars are allowed to take values in a ring instead of a field, which leads us to the definition of modules.

Theorem 1 : *In any vector space $V(F)$ the following results hold*

(*i*) $0 . x = 0$

(*ii*) $\alpha . 0 = 0$

(*iii*) $(-\alpha)x = -(\alpha x) = \alpha(-x)$

(*iv*) $(\alpha - \beta)x = \alpha x - \beta x$

Proof : (*i*) $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$

$\Rightarrow 0 + 0 \cdot x = 0 \cdot x + 0 \cdot x$

$\Rightarrow 0 = 0 . x$ (cancellation in V)

(*ii*) $\alpha \cdot 0 = \alpha \cdot (0+0) = \alpha \cdot 0 + \alpha \cdot 0 \Rightarrow \alpha \cdot 0 = 0$

(*iii*) $(-\alpha)\, x + \alpha x = [(-\alpha) + \alpha]\, x = 0 \cdot x = 0$

$\Rightarrow (-\alpha x) = -\alpha x$

(*iv*) follows from above.

Example 1 : If $< F, +, \cdot >$ be a field, then F is a vector space over F as $< F, + > = < V, + >$ is an additive abelian group. Scalar multiplication can be taken as the product of F. All properties are seen to hold. Thus $F(F)$ is a vector space.

Example 2 : Let $< F, +, \cdot >$ be a field

Let $V = \{(\alpha_1, \alpha_2) \mid \alpha_1, \alpha_2 \in F\}$

Define + and $\cdot$ (scalar multiplication) by

$$(\alpha_1, \alpha_2) + (\beta_1, \beta_2) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$

$$\alpha\,(\alpha_1, \alpha_2) = (\alpha\alpha_1, \alpha\alpha_2)$$

One can check that all conditions in the definition are satisfied. Here $V = F \times F = F^2$

One can extend this to F^3 and so on. In general we can take n–tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_i \in F$ and define F^n or $F^{(n)} = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_i \in F\}$ as a Vector space over F.

Example 3 : If $F \subseteq K$ be two fields then $K(F)$ will form a vector space, where addition of $K(F)$ is + of K and for any $\alpha \in F$, $x \in K$, $\alpha . x$ is taken as product of α and x in K.

Thus **C(R)**, **C(C)**, **R(Q)** would be some examples of vector spaces, where **C** = complex nos., **R** = reals and **Q** = rationals.

Example 4 : Let V = set of all real valued continuous functions defined on $[0, 1]$. Then V forms a vector space over the field **R** of reals under addition and scalar multiplication defined by

$$(f+g)x = f(x) + g(x) \qquad f, g \in V$$
$$(\alpha f)x = \alpha f(x) \qquad \alpha \in R$$
$$\text{for all } x \in [0, 1]$$

It may be recalled here that sum of two continuous functions is continuous and scalar multiple of a continuous function is continuous.

Example 5 : Let P = set of all polynomials over a field F, then P forms a vector space under addition and scalar multiplication defined by

$$f(x) + g(x) = (f+g)x$$
$$\alpha(f(x)) = (\alpha f)(x) \qquad \alpha \in F$$

Example 6 : $M_{m \times n}(F)$, the set of all $m \times n$ matrices with entries from a field F forms a vector space under addition and scalar multiplication of matrices.

Subspaces

Definition : A non empty subset W of a vector space $V(F)$ is said to form a *subspace* of V if W forms a vector space under the operations of V.

Theorem 2 : *A necessary and sufficient condition for a non empty subset W of a vector space $V(F)$ to be a subspace is that W is closed under addition and scalar multiplication.*

Proof : If W is a subspace, the result follows by definition.

Conversely, let W be closed under addition and scalar multiplication.

Let $\quad x, y \in W$, since $1 \in F$, $-1 \in F$

$\therefore \quad -1 \,.\, y \in W \Rightarrow -y \in W$

$x, -y \in W \Rightarrow x - y \in W$

$\Rightarrow \; < W, + >$ forms a subgroup of $< V, + >$.

Rest of the conditions in the definition follow trivially.

Theorem 3 : *A non empty subset W of a vector space $V(F)$ is a subspace of V iff $\alpha x + \beta y \in W$ for $\alpha, \beta \in F$, $x, y \in W$.*

Proof : If W is a subspace, result follows by definition.

Conversely, let given condition hold in W.

Let $x, y \in W$ be any elements. Since $1 \in F$

$$1 \,.\, x + 1 \,.\, y = x + y \in W$$

$\Rightarrow W$ is closed under addition.

Again, $x \in W$, $\alpha \in F$ then

$$\alpha x = \alpha x + 0 \,.\, y \text{ for any } y \in W,\ 0 \in F$$

which is in W. (Note here 0 may not be in W)

Hence W is closed under scalar multiplication.

The result thus follows by previous theorem.

Example 7 : Consider the vector space $\mathbf{R}^2(\mathbf{R})$

then $$W_1 = \{(a, 0) \mid a \in \mathbf{R}\}$$
$$W_2 = \{(0, b) \mid b \in \mathbf{R}\}$$

are subspaces of $\mathbf{R}^2$

As for any $\alpha, \beta \in \mathbf{R}$, $(a_1, 0), (a_2, 0) \in W_1$, we find

$$\alpha(a_1, 0) + \beta(a_2, 0) = (\alpha a_1, 0) = (\beta a_2, 0)$$
$$= (\alpha a_1 + \beta a_2, 0) \in W_1$$

Hence W_1 is a subspace. Similarly we can show W_2 is a subspace of $\mathbf{R}^2$.

Problem 1 : *Show that union of two subspaces may not be a subspace.*

Solution : Consider the previous example.

$W_1 \cup W_2$ will be the set containing all pairs of the type $(a, 0)$, $(0, b)$

In particular $(1, 0), (0, 1) \in W_1 \cup W_2$

But $(1, 0) + (0, 1) = (1, 1) \notin W_1 \cup W_2$.

Hence $W_1 \cup W_2$ is not a subspace.

Reader is referred to exercises for more results pertaining to intersection and union of subspaces.

Sum of Subspaces

If W_1 and W_2 be two subspaces of a vector space $V(F)$ then we define

$$W_1 + W_2 = \{w_1 + w_2 \mid w_1 \in W_1, w_2 \in W_2\}$$
$$W_1 + W_2 \neq \varphi \text{ as } 0 = 0 + 0 \in W_1 + W_2$$

Again, $x, y \in W_1 + W_2$, $\alpha, \beta \in F$ implies

$$x = w_1 + w_2$$
$$y = w'_1 + w'_2 \qquad w_1, w'_1 \in W_1, \; w_2, w'_2 \in W_2$$
$$\alpha x + \beta y = \alpha(w_1 + w_2) + \beta(w'_1 + w'_2)$$
$$= (\alpha w_1 + \beta w'_1) + (\alpha w_2 + \beta w'_2) \in W_1 + W_2$$

Showing thereby that sum of two subspaces is a subspace.

Definition : We say a vector space V is the *direct sum* of two subspaces W_1 and W_2 if

(*i*) $V = W_1 + W_2$

(*ii*) every $v \in V$ can be expressed uniquely as the sum $w_1 + w_2$, $w_1 \in W_1$ and $w_2 \in W_2$

and in that case we write $V = W_1 \oplus W_2$.

Theorem 4 : $V = W_1 \oplus W_1 \Leftrightarrow V = W_1 + W_2$, $W_1 \cap W_2 = (0)$.

Proof : Let $V = W_1 \oplus W_2$

We need prove $W_1 \cap W_2 = (0)$

Let $x \in W_1 \cap W_2 \Rightarrow x \in W_1$ and $x \in W_2$

$$\Rightarrow x = 0 + x \in W_1 + W_2 = V$$

$$\Rightarrow x = x + 0 \in W_1 + W_2 = V$$

Since x has been expressed as $x = x + 0$ and $0 + x$ and the representation has to be unique, we get $x = 0$

$$\Rightarrow W_1 \cap W_2 = (0).$$

Conversely, let $v \in V$ be any element and suppose

$$v = w_1 + w_2$$

$$v = w'_1 + w'_2$$

are two representations of v

then $\quad w_1 + w_2 = w'_1 + w'_2 \ (= v)$

$$\Rightarrow w_1 - w'_1 = w'_2 - w_2$$

Now L.H.S. is in W_1 and R.H.S belongs to W_2

i.e., each belongs to $W_1 \cap W_2 = (0)$

$$\Rightarrow w_1 - w'_1 = w'_2 - w_2 = 0$$

$$\Rightarrow w_1 = w'_1, \ w_2 = w'_2.$$

Hence the result.

Example 8 : Consider the space $V(F) = F^2(F)$ where F is a field

Let $\quad W_1 = \{(a, 0) \mid a \in F\}$

$\quad W_2 = \{(0, b) \mid b \in F\}$

then V is direct sum of W_1 and W_2

$$v \in V \Rightarrow v = (a, b) = (a, 0) + (0, b) \in W_1 + W_2$$

thus $\quad V \subseteq W_1 + W_2$

or that $\quad V = W_1 + W_2$

Again if $(x, y) \in W_1 \cap W_2$ be any element then

$$(x, y) \in W_1 \text{ and } (x, y) \in W_2$$

$$\Rightarrow y = 0 \text{ and } x = 0$$

$$\Rightarrow (x,y) = (0, 0)$$

$$\Rightarrow W_1 \cap W_2 = (0)$$

Hence $\quad V = W_1 \oplus W_2.$

Problem 2 : *Let V be the vector space of all functions from* $\mathbf{R} \to \mathbf{R}$. *Let* $V_e = \{f \in V \mid f \text{ is even}\}$, $V_o = [\, f \in V \mid f \text{ is odd}\}$. *Then V_e and V_o are subspaces of V and* $V = V_e \oplus V_o$.

Solution : Addition and scalar multiplication in V are given by the rule $(f + g)\, x = f(x) + g(x)$; $(\alpha f)x = \alpha f(x)$

Now $V_e \neq \varphi$ as $0(x) = 0(-x) = 0 \Rightarrow 0(x) = 0(-x)$

$$\Rightarrow 0 \in V_e$$

Again for $\alpha, \beta \in \mathbf{R}$, $f, g \in V_e$, we have

$$(\alpha f + \beta g)(-x) = (\alpha f)(-x) + (\beta g)(-x) = \alpha(f(-x)) + \beta(g(-x))$$
$$= \alpha f(x) + \beta g(x)$$
$$= (\alpha f + \beta g)x$$

$$\Rightarrow \alpha f + \beta g \in V_e$$
$$\Rightarrow V_e \text{ is a subspace of } V$$

Similarly, V_0 is a subspace of V.

Thus $V_e + V_0$ is a subspace of V. We show $V \subseteq V_e + V_0$

Let $f \in V$ be any member

Let $g : \mathbf{R} \to \mathbf{R}$ be such that $g(x) = f(-x)$, then $g \in V$

Also then $f = (\frac{1}{2}f + \frac{1}{2}g) + (\frac{1}{2}f - \frac{1}{2}g)$

Since $(\frac{1}{2}f + \frac{1}{2}g)(-x) = \frac{1}{2}f(-x) + \frac{1}{2}g(-x) = \frac{1}{2}g(x) + \frac{1}{2}f(x)$

$$= (\tfrac{1}{2}f + \tfrac{1}{2}g)x$$

we find $\quad \frac{1}{2}f + \frac{1}{2}g \in V_e$

Similarly, $\quad \frac{1}{2}f - \frac{1}{2}g \in V_0$

$$\Rightarrow f \in V_e + V_0 \Rightarrow V \subseteq V_e + V_0$$

or that $\quad V = V_e + V_0$

Finally, $\quad f \in V_e \cap V_0 \Rightarrow f \in V_e, f \in V_0$

$$\Rightarrow f(-x) = f(x) \text{ and } f(-x) = -f(x)$$
$$\Rightarrow f(x) = -f(x) \Rightarrow f(x) + f(x) = 0 = 0(x)$$
$$\Rightarrow 2f(x) = 0\ (x) \text{ for all } x$$
$$\Rightarrow 2f = 0 \Rightarrow f = 0 \Rightarrow V_e \cap V_0 = (0).$$

Hence the result.

Problem 3 : *If L, M, N are three subspaces of a vector space V, such that $M \subseteq L$ then show that $L \cap (M + N) = (L \cap M) + (L \cap N) = M + (L \cap N)$.*

Also give an example, where the result fails to hold when $M \not\subseteq L$.

Solution : We leave the first part for the reader to try. Recall a similar result was proved for ideals in rings. The equality is called modular equality.

Consider now the vector space $V = \mathbf{R}^2$

Let
$$L = \{(a, a) \mid a \in \mathbf{R}\}$$
$$M = \{(a, 0) \mid a \in \mathbf{R}\}$$
$$N = \{(0, b) \mid b \in \mathbf{R}\}$$

It is a routine matter to cheek that L, M, N are subspaces of V. Indeed

$$\alpha(a, a) + \beta(a', a') = (\alpha a, \alpha a) + (\beta a', \beta a')$$
$$= (\alpha a + \beta a', \alpha a + \beta a') \in L \text{ etc.}$$

Now $\quad (x, y) \in L \cap M \Rightarrow (x, y) \in L$ and $(x, y) \in M$

$$\Rightarrow y = x \text{ and } y = 0$$
$$\Rightarrow x = 0 = y \Rightarrow (x, y) = (0, 0)$$

Similarly, $\quad L \cap N = \{(0, 0)\}$

$$\Rightarrow L \cap M + L \cap N = \{(0, 0)\}$$

Again, $M + N = \{(a, b) \mid a, b \in \mathbf{R}\}$ and as $(1, 1) \in M + N$

$$(1, 1) \in L$$

we find $(1, 1) \in L \cap (M + N)$, but $(1, 1) \notin L \cap M + L \cap N$

Hence $\quad L \cap (M + N) \neq (L \cap M) + (L \cap N)$, when $M \not\subseteq L$.

Quotient Spaces

If W be a subspace of a vector space $V(F)$ then since $< W, + >$ forms an abelian group of $< V, + >$, we can talk of cosets of W in V. Let $\frac{V}{W}$ be the set of all cosets $W + v$, $v \in V$, then we show that $\frac{V}{W}$ also forms a vector space over F, under the operations defined by

$$(W + x) + (W + y) = W + (x + y) \qquad x, y \in V$$
$$\alpha(W + x) = W + \alpha x \qquad \alpha \in F$$

Addition is well defined, since,

$$W + x = W + x'$$
$$W + y = W + y'$$
$$\Rightarrow x - x' \in W, y - y' \in W$$
$$\Rightarrow (x - x') + (y - y') \in W$$
$$\Rightarrow (x + y) - (x' + y') \in W$$
$$\Rightarrow W + (x + y) = W + (x' + y')$$

Again, $\quad W + x = W + x'$

$$\Rightarrow x - x' \in W,$$
$$\Rightarrow \alpha(x - x') \in W \qquad \alpha \in F$$
$$\Rightarrow \alpha x - \alpha x' \in W$$
$$\Rightarrow W + \alpha x = W + \alpha x'$$
$$\Rightarrow \alpha(W + x) = \alpha(W + x')$$

Thus, scalar multiplication is also well defined. It should now be a routine exercise to check that all conditions in the definition of a vector space are satisfied.

$W + 0$ will be zero of $\dfrac{V}{W}$

$W - x$ will be inverse of $W + x$

Also,

$$\alpha((W + x) + (W + y)) = \alpha(W + (x + y)) = W + \alpha(x + y) = W + (\alpha x + \alpha y)$$
$$= (W + \alpha x) + (W + \alpha y) = \alpha(W + x) + \alpha(W + y) \text{ etc.}$$

Hence, V/W forms a vector space over F, called the quotient space of V by W.

Exercises

1. Show that in a vector space $V(F)$
   (*i*) $\alpha v = \beta v \Rightarrow \alpha = \beta$
   (*ii*) $\alpha v_1 = \alpha v_2 \Rightarrow v_1 = v_2$
   (*iii*) $\alpha v = 0,\ v \neq 0 \Rightarrow \alpha = 0$
   (*iv*) $\alpha v = 0,\ \alpha \neq 0 \Rightarrow v = 0$ where $\alpha, \beta \in F;\ v, v_1, v_2 \in V$
2. Let $V = \{(z_1, z_2, z_3) \mid z_1, z_2, z_3 \in \mathbf{C}\} = \mathbf{C}^3$ be the vector space over $\mathbf{C}$. Check whether
   (*i*) $W_1 = \{(z_1, z_2, z_3) \mid z_1 \text{ is a real number}\}$
   (*ii*) $W_2 = \{(z_1, z_2, z_3) \mid z_1 + z_2 = 0\}$
   (*iii*) $W_3 = \{(z_1, z_2, z_3) \mid z_1 + z_2 = 1\}$
   is a subspace of V or not.
3. Show that intersection of two subspaces is a subspace.
4. Prove that union of two subspaces is a subspace iff one of them is contained in the other.
5. If V is a vector space over an infinite field F then show that it is not possible to write V as union of a finite number of proper subspaces.
6. Let $V = \mathbf{R}^4$. Show that
   $$W_1 = \{(a, b, c, d) \mid a = b + c + d\}$$
   $$W_2 = \{(a, b, c, d) \mid a = 3c,\ b = 4d\}$$
   are subspaces of V.
7. Let V be the vector space of all $n \times n$ matrices over $\mathbf{R}$. Let W_1 be the set of all symmetric matrices in V and W_2 be the set of all skew symmetric matrices in V. Show that W_1 and W_2 are subspaces of V and $V = W_1 \oplus W_2$.

Homomorphisms Or Linear Transformations

We are already familiar with the concept of a homomorphism in case of groups and rings. We introduce the same in vector spaces.

Definition : Let V and U be two vector spaces over the same field F, then a mapping $T: V \to U$ is called a homomorphism or a linear transformation if

$$T(x+y) = T(x) + T(y) \quad \text{for all } x, y \in V$$
$$T(\alpha x) = \alpha T(x) \quad \alpha \in F$$

One can combine the two conditions to get a single condition

$$T(\alpha x + \beta y) = \alpha T(x) + \beta T(y) \quad x, y \in V; \ \alpha, \beta \in F$$

It is easy to see that both are equivalent. If a homomorphism happens to be one - one onto also we call it an *isomorphism*, and say the two spaces are isomorphic. (Notation $V \cong U$) .

Example 9 : Identity map $I: V \to V$, s.t.,

$$I(v) = v$$

and the zero map $O: V \to V$, s.t.,

$$O(v) = 0$$

are clearly linear transformations.

Example 10 : For a field F, consider the vector spaces F^2 and F^3. Define a map $T: F^3 \to F^2$, by

$$T(\alpha, \beta, \gamma) = (\alpha, \beta)$$

then T is a linear transformation as

for any $x, y \in F^3$, if $x = (\alpha_1, \beta_1, \gamma_1)$

$y = (\alpha_2, \beta_2, \gamma_2)$

then $T(x+y) = T(\alpha_1+\alpha_2, \beta_1+\beta_2, \gamma_1+\gamma_2) = (\alpha_1+\alpha_2, \beta_1+\beta_2)$

$= (\alpha_1, \beta_1) + (\alpha_2, \beta_2) = T(x) + T(y)$

and $T(\alpha x) = T(\alpha(\alpha_1, \beta_1, \gamma_1)) = T(\alpha\alpha_1, \alpha\beta_1, \alpha\gamma_1)$

$= (\alpha\alpha_1, \alpha\beta_1) = \alpha(\alpha_1, \beta_1) = \alpha T(x)$

Example 11 : Let V be the vector space of all polynomials in x over a field F. Define

$T: V \to V$, s.t.

$$T(f(x)) = \frac{d}{dx} f(x)$$

then $$T(f+g) = \frac{d}{dx}(f+g) = \frac{d}{dx}f + \frac{d}{dx}g = T(f) + T(g)$$

$$T(\alpha f) = \frac{d}{dx}(\alpha f) = \alpha \frac{d}{dx} f = \alpha T(f)$$

shows that T is a linear transformation.

In fact, if $U: V \to V$ be defined such that

$$U(f) = \int_0^x f(t)\, dt$$

then U will also be a linear transformation.

Example 12 : Consider the mapping

$$T : \mathbf{R}^3 \to \mathbf{R} \text{ s.t.,}$$

$$T(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$$

then T is not a linear transformation.

Consider, for instance,

$$T((1, 0, 0) + (1, 0, 0)) = T(2, 0, 0) = 4$$

$$T(1, 0, 0) + T(1, 0, 0) = 1 + 1 = 2.$$

Exercises

Check which of the following are linear transformations

1. $T : \mathbf{R}^2 \to \mathbf{R}^2$ s.t., $T(x_1, x_2) = (1 + x_1, x_2)$
2. $T : \mathbf{R}^2 \to \mathbf{R}^2$ s.t., $T(x_1, x_2) = (x_2, x_1)$
3. $T : \mathbf{C} \to \mathbf{C}$, s.t., $T(z) = \bar{z}$, Where $\mathbf{C}$ is vector space of complex numbers over reals.
4. $T : \mathbf{C} \to \mathbf{C}$, s.t., $T(x + iy) = x$
5. $T : \mathbf{R}^3 \to \mathbf{R}^4$ s.t., $T(x_1, x_2, x_3) = (x_1, x_1 + x_2, x_1 + x_2 + x_3, x_3)$
6. $T : \mathbf{R}^2 \to \mathbf{R}^3$ s.t., $T(x_1, x_2) = (x_1, x_1 + x_2, x_2)$
7. $T : \mathbf{R} \to \mathbf{R}^3$ s.t., $T(x) = (x, x^2, x^3)$

In the theorems that follow, we take V and U to be vector spaces over the same field F.

Theorem 5 : *Under a homomorphism* $T : V \to U$,

(*i*) $T(0) = 0$

(*ii*) $T(-x) = -T(x)$.

Proof : $T(0) = T(0 + 0) = T(0) + T(0)$

$$\Rightarrow T(0) = 0$$

Again $T(-x) + T(x) = T(-x + x) = T(0) = 0$

$$\Rightarrow -T(x) = T(-x).$$

Definition : Let $T : V \to U$ be a homomorphism, then *kernel of* T is defined by

$$\text{Ker } T = \{x \in V \mid T(x) = 0\}$$

It is also called the *null space of* T.

Theorem 6 : *Let* $T : V \to U$ *be a homomorphism, then Ker* T *is a subspace of* V.

Proof : $\text{Ker } T \neq \varphi$ as $0 \in \text{Ker } T$

Let $\alpha, \beta \in F$, $x, y \in \text{Ker } T$ be any elements

then $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$

$$= \alpha . 0 + \beta . 0 = 0 + 0 = 0$$

$$\Rightarrow \alpha x + \beta y \in \text{Ker } T.$$

Theorem 7 : *Let $T: V \to U$ be a homomorphism, then*

$$\text{Ker } T = \{0\} \text{ iff } T \text{ is one-one.}$$

Proof : Let Ker $T = \{0\}$. If $T(x) = T(y)$

then $T(x) - T(y) = 0$

$\Rightarrow T(x-y) = 0$

$\Rightarrow (x-y) \in \text{Ker } T = \{0\}$

$\Rightarrow x - y = 0$

$\Rightarrow x = y$

Conversely, let T be one-one

if $x \in \text{Ker } T$ be any element, then $T(x) = 0$

$\Rightarrow T(x) = T(0)$

$\Rightarrow x = 0$

$\Rightarrow \text{Ker } T = \{0\}$.

Definition : Let $T: V \to U$ be a linear transformation then range of T is defined to be

$$T(V) = \{T(x) \mid x \in V\} = \text{Range } T = R_T$$
$$= \{u \in U \mid u = T(v),\ v \in V\}$$

Theorem 8 : *Let $T: V \to U$ be a L.T. (linear transformation) then range of T is a subspace of U.*

Proof : Since $T(0) = 0,\ 0 \in V$

$\therefore$ $T(0) \in \text{Range } T$

i.e., Range $T \neq \varphi$

Let $\alpha, \beta \in F$, $T(x), T(y) \in T(V)$ be any elements

then $x, y \in V$

Now $\alpha T(x) + \beta T(y) = T(\alpha x + \beta y) \in T(V)$

as $\alpha x + \beta y \in V$

Hence the result.

Note : $T(V) = U$ iff T is onto.

Theorem 9 : *Let $T: V \to U$ be a L.T. then*

$$\frac{V}{\text{Ker } T} \cong \textit{Range } T = T(V).$$

Proof : Let $T: V \to U$ and put Ker $T = K$, then K being a subspace of V, we can talk of V/K.

Define a mapping $\theta: V/K \to T(V)$,s.t.,

$$\theta(K + x) = T(x)\ ,\ x \in V$$

Then θ is well defined, one-one map as

$$\begin{aligned} & K + x = K + y \\ \Leftrightarrow\ & x - y \in K = \operatorname{Ker} T \\ \Leftrightarrow\ & T(x - y) = 0 \\ \Leftrightarrow\ & T(x) = T(y) \\ \Leftrightarrow\ & \theta(K + x) = \theta(K + y) \end{aligned}$$

If $T(x) \in T(V)$ be any element, then $x \in V$ and $\theta(K + x) = T(x)$, showing that θ is onto.

Finally,
$$\begin{aligned} \theta((K + x) + (K + y)) &= \theta(K + (x + y)) \\ &= T(x + y) \\ &= T(x) + T(y) \\ &= \theta(K + x) + \theta(K + y) \end{aligned}$$

and
$$\theta(\alpha((K + x)) = \theta(K + \alpha x) = T(\alpha x) = \alpha T(x) = \alpha\theta(K + x)$$

shows θ is a *L.T.* and hence an isomorphism.

Note : The above is called the *Fundamental Theorem of homomorphism* for vector spaces.

If the map T is also onto, then we have proved $\dfrac{V}{\operatorname{Ker} T} \cong U$.

Theorem 10 : *If A and B be two subspaces of a vector space $V(F)$, then*

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}.$$

Proof : A being a subspace of $A + B$ and $A \cap B$ being a subspace of B, we can talk of $\dfrac{A+B}{A}$ and $\dfrac{B}{A \cap B}$.

Define a map $\theta : B \to \dfrac{A+B}{A}$ s.t.,

$$\theta(b) = A + b,\ b \in B$$

Since $b_1 = b_2 \Rightarrow A + b_1 = A + b_2$, we find θ is well defined.

Again, as
$$\begin{aligned} \theta(\alpha b_1 + \beta b_2) &= A + (\alpha b_1 + \beta b_2) \\ &= (A + \alpha b_1) + (A + \beta b_2) \\ &= \alpha(A + b_1) + \beta(A + b_2) \\ &= \alpha\theta(b_1) + \beta\theta(b_2) \end{aligned}$$

θ is a *L.T.*

For any $A + x \in \dfrac{A+B}{A}$, we find $x \in A + B$

$$\Rightarrow x = a + b,\ a \in A,\ b \in B$$

$$\therefore \qquad A + x = A + (a + b)$$
$$= (A + a) + (A + b) = A + (A + b) = A + b = \theta(b).$$

Showing that b is the required pre image of $A + x$ under θ and thus θ is onto. Hence by Fundamental theorem

$$\frac{A+B}{A} \cong \frac{B}{\text{Ker}\,\theta}.$$

We claim $\quad \text{Ker}\ \theta = A \cap B$

Indeed $\quad x \in \text{Ker}\,\theta \Leftrightarrow \theta(x) = A$

$$\Leftrightarrow A + x = A$$
$$\Leftrightarrow x \in A, \text{ also } x \in \text{Ker}\,\theta \subseteq B$$
$$\Leftrightarrow x \in A \cap B$$

Hence $\quad \dfrac{A+B}{A} \cong \dfrac{B}{A \cap B}$

Note : By interchanging A and B, we get $\dfrac{B+A}{B} \cong \dfrac{A}{B \cap A}$

i.e., $\quad \dfrac{A+B}{A} \cong \dfrac{B}{A \cap B}.$

Cor. : If $A + B$ is the direct sum then as $A \cap B = \{0\}$

we get $\quad \dfrac{A}{(0)} \cong \dfrac{A \oplus B}{B}$

But $\dfrac{A}{(0)} \cong A$ (see remark below) gives us $A \cong \dfrac{A \oplus B}{B}$.

Theorem 11 : *Let W be a subspace of V, then $\exists$ an onto L.T. $\theta : V \to \dfrac{V}{W}$ such that Ker $\theta = W$.*

Proof : Define $\theta : V \to \dfrac{V}{W}$ s.t.,

$$\theta(x) = W + x$$

then θ is clearly well defined.

Also $\quad \theta(\alpha x + \beta y) = W + (\alpha x + \beta y)$

$$= (W + \alpha x) + (W + \beta y)$$
$$= \alpha(W + x) + \beta(W + y) = \alpha\theta(x) + \beta\theta(y)$$

Shows θ is a *L.T.*

θ is clearly onto.

Again, $x \in \operatorname{Ker}\theta \Leftrightarrow \theta(x) = W$

$$\Leftrightarrow W + x = W$$

$$\Leftrightarrow x \in W$$

Hence $\operatorname{Ker}\theta = W.$

T is called the *natural homomorphism* or the *quotient map.*

Remark : In case $W = (0)$ in the above we find θ will be 1–1 also as

$$\theta(a) = \theta(b)$$

$$\Rightarrow W + a = W + b$$

$$\Rightarrow a - b \in W = (0)$$

$$\Rightarrow a - b = 0$$

$$\Rightarrow a = b.$$

Hence in that case $V \cong \dfrac{V}{W}$ or $V \cong \dfrac{V}{(0)}$.

Note $W = (0) \Rightarrow \operatorname{Ker}\theta = (0) \Rightarrow \theta$ is one - one.

Problem 4 : *Let W and U be subspaces of $V(F)$ such that $W \subset U \subset V$. Let $V \to V/W$ be the quotient map. Show that $f(U)$ is a proper subspace of V/W.*

Solution : Since f is a *L.T.*, $f(U)$ is a subspace of V/W.

If $f(U) = 0$ then $f(x) = 0$ for all $x \in U$

$$\Rightarrow W + x = W \text{ for all } x \in U$$

$$\Rightarrow x \in W \text{ for all } x \in U$$

$$\Rightarrow U \subseteq W, \text{ a contradiction}$$

Again since $U \neq V$, $\exists\, v_0 \in V$ s.t., $v_0 \notin U$.

If $f(v_0) \in f(U)$ then $f(v_0) = f(x)$ for some $x \in U$

$$\Rightarrow f(v_0 - x) = 0$$

$$\Rightarrow W + (v_0 - x) = W$$

$$\Rightarrow v_0 - x \in W$$

$$\Rightarrow v_0 = x + w \text{ for some } w \in W$$

$$\Rightarrow v_0 \in U, \text{ a contradiction}$$

Hence $f(v_0) \notin f(U) \Rightarrow f(U) \neq \dfrac{V}{W}$

or that $f(U)$ is a proper subspace of $\dfrac{V}{W}$.

Theorem 12 : *Let $V \to U$ be an onto homomorphism with $\operatorname{Ker} T = W$. Then there exists a one–one onto mapping between the subspaces of U and the subspaces of V which contain W.*

Proof : Let $\mathscr{A}$ = set of all subspaces of V, which contain W

$\mathscr{B}$ = set of all subspaces of U

Define a mapping $\theta : \mathscr{A} \to \mathscr{B}$, s.t.,

$$\theta(W_1) = T(W_1)$$

Since $T : V \to U$, $T(W_1)$ will be a subspace of U as

for any $T(x)$, $T(y) \in T(W_1)$ and α, $\beta \in F$.

$$\alpha T(x) + \beta T(y) = T(\alpha x + \beta y) \in T(W_1) \text{ , as } x, y \in W_1$$

Again $\quad W_1 = W_1'$

$\Rightarrow T(W_1) = T(W_1')$

$\Rightarrow \theta$ is well defined.

Now if $\quad \theta(W_1) = \theta(W_1')$

Then $\quad T(W_1) = T(W_1') \Rightarrow W_1 = W_1'$

as $\quad x \in W_1 \Rightarrow T(x) \in T(W_1) = T(W_1')$

$\Rightarrow T(x) \in T(W_1')$

$\Rightarrow T(x) = T(y), \quad y \in W_1'$

$\Rightarrow T(x - y) = 0$

$\Rightarrow x - y \in \operatorname{Ker} T = W \subseteq W_1'$

$\Rightarrow x \in W_1'$ as $y \in W_1'$

$\Rightarrow W_1 \subseteq W_1'$. Similarly $W_1' \subseteq W_1$

Hence θ is 1–1.

Let $U_1 \in \mathscr{B}$ be any member.

Define $\quad T^{-1}(U_1) = \{x \in V \mid T(x) \in U_1\}$

Then $0 \in T^{-1}(U_1)$ as $T(0) = 0 \in U_1$

$\Rightarrow T^{-1}(U_1) \neq \varphi$

For α, $\beta \in F$, x, $y \in T^{-1}(U_1)$, we have

$T(x) \in U_1$, $T(y) \in U_1$

$\Rightarrow \alpha T(x) + \beta T(y) \in U_1$

$\Rightarrow T(\alpha x + \beta y) \in U_1$

$\Rightarrow \alpha x + \beta y \in T^{-1}(U_1)$

or that $T^{-1}(U_1)$ is a subspace of V.

Let $x \in W$ then $x \in \operatorname{Ker} T$

$\Rightarrow T(x) = 0 \in U_1$

$\Rightarrow x \in T^{-1}(U_1)$

$\Rightarrow W \subseteq T^{-1}(U_1)$

$\Rightarrow T^{-1}(U_1) \in \mathrm{A}$

Also $\quad T(T^{-1}(U_1)) = \{T(x) \in V \mid T(x) \in U_1\} \subseteq U_1$.

Let $\quad y \in U_1 \Rightarrow y \in U \Rightarrow \exists\ x \in V$ s.t. $T(x) = y$

as T is onto, $\quad x \in T^{-1}(U_1)$

$$\Rightarrow \; y = T(x) \in T(T^{-1})\,(U_1))$$
$$\Rightarrow \; T(T^{-1}(U_1)) = U_1$$
$$\Rightarrow \; \theta(T^{-1}(U_1)) = U_1$$
$$\Rightarrow \; \theta \text{ is onto.}$$

Hence the theorem is proved.

Linear Span

Definition : Let $V(F)$ be a vector space, $v_i \in V$, $\alpha_i \in F$ be elements of V and F respectively. Then elements of the type $\sum_{i=1}^{n} \alpha_i v_i$ are called *linear combinations* of $v_1, v_2, \ldots, v_n$ over F.

Let S be a non empty subset of V, then the set

$$L(S) = \left\{ \sum_{i=1}^{n} \alpha_i v_i \mid \alpha_i \in F, v_i \in S, n \text{ finite} \right\}$$

i.e., the set of all linear combinations of finite sets of elements of S is called *linear span* of S. It is also denoted by $< S >$.

Theorem 13 : *$L(S)$ is the smallest subspace of V, containing S.*

Proof : $L(S) \neq \varphi$ as $v \in S \Rightarrow v = 1.v,\ 1 \in F$

$$\Rightarrow \; v \in L(S)$$

thus, in fact, $S \subseteq L(S)$.

Let $x, y \in L(S)$, $\alpha, \beta \in F$ be any elements

then $x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$

$y = \beta_1 v'_1 + \beta_2 v'_2 + \ldots \beta_m v'_m \qquad v_i, v'_j \in S,\ \alpha_i, \beta_j \in F$

Thus $\alpha x + \beta y = \alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + \ldots \alpha\alpha_n v_n + \beta\beta_1 v'_1 + \ldots + \beta\beta_m v'_m$.

R.H.S. being a linear combination belongs to $L(S)$

Hence $L(S)$ is a subspace of V, containing S.

Let now W be any subspace of V, containing S

We show $L(S) \subseteq W$

$$x \in L(S) \Rightarrow x = \Sigma\alpha_i v_i \qquad v_i \in S,\ \alpha_i \in F$$

$v_i \in S \subseteq W$ for all i and W is a subspace

$\Rightarrow \Sigma\alpha_i v_i \in W \Rightarrow x \in W$

$\Rightarrow L(S) \subseteq W$

Hence the result follows.

Theorem 14 : *If S_1 and S_2 are subsets of V, then*

(*i*) $S_1 \subseteq S_2 \Rightarrow L(S_1) \subseteq L(S_2)$

(*ii*) $L(S_1 \cup S_2) = L(S_1) + L(S_2)$

(*iii*) $L(L(S_1)) = L(S_1)$.

Proof : (*i*) $x \in L(S_1) \Rightarrow x = \Sigma\alpha_i v_i \quad v_i \in S_1,\ \alpha_i \in F$

thus $v_i \in S_1 \subseteq S_2$ for all i

$\Rightarrow \quad \Sigma\alpha_i v_i \in S_2 \Rightarrow x \in L(S_2)$

$\Rightarrow \quad L(S_1) \subseteq L(S_2)$.

(*ii*) $\quad S_1 \subseteq S_1 \cup S_2 \Rightarrow L(S_1) \subseteq L(S_1 \cup S_2)$

$S_2 \subseteq S_1 \cup S_2 \Rightarrow L(S_2) \subseteq L(S_1 \cup S_2)$

$\Rightarrow \quad L(S_1) + L(S_2) \subseteq L(S_1 \cup S_2)$

Again $\quad S_1 \subseteq L(S_1) \subseteq L(S_1) + L(S_2)$

$S_2 \subseteq L(S_2) \subseteq L(S_1) + L(S_2)$

$\Rightarrow \quad S_1 \cup S_2 \subseteq L(S_1) + L(S_2)$.

Hence $\quad L(S_1 \cup S_2) \subseteq L(S_1) + L(S_2)$

as $L(S_1 \cup S_2)$ is the smallest subspace containing $S_1 \cup S_2$ and $L(S_1) + L(S_2)$ is a subspace, being sum of two subspaces (and contains $S_1 \cup S_2$).

Thus $\quad L(S_1 \cup S_2) = L(S_1) + L(S_2)$.

(*iii*) Let $L(S_1) = K$ then we show $L(K) = L(S_1)$

Now $K \subseteq L(K) \quad \therefore \quad L(S_1) \subseteq L(L(S_1))$

Again $x \in L(L(S_1)) \Rightarrow x$ is linear combination of members of $L(S_1)$ which are linear combinations of members of S_1.

So x is a linear combination of members of S_1

$\Rightarrow \quad x \in L(S_1)$

Thus $\quad L(L(S_1)) \subseteq L(S_1)$

Hence $\quad L(L(S_1)) = L(S_1)$.

Theorem 15 : *If W is a subspace of V, then $L(W) = W$ and conversely.*

Proof : $W \subseteq L(W)$ by definition and since $L(W)$ is the smallest subspace of containing W and W is itself a subspace

$L(W) \subseteq W$

Hence $\quad L(W) = W$.

Conversely, let, $L(W) = W$

Let $\quad x,\ y \in W,\ \alpha,\ \beta \in F$

Then $\quad x,\ y \in L(W)$

$\Rightarrow x,\ y$ are linear combinations of members of W

$\Rightarrow \alpha x + \beta y$ is a linear combination of members of W

$$\Rightarrow \alpha x + \beta y \in L(W)$$
$$\Rightarrow \alpha x + \beta y \in W$$
$$\Rightarrow W \text{ is a subspace.}$$

Definition : If $V = L(S)$, we say S spans (or generates) V. The vector space V is said to be *finite - dimensional* (over F) if there exists a finite subset S of V such that $V = L(S)$. We use notation *F.D.V.S.* for a finite dimensional vector space.

It now follows, from the results we've proved that

If S_1 and S_2 are two subspaces of V, then $S_1 + S_2$ is the subspace spanned by $S_1 \cup S_2$

Indeed, $L(S_1 \cup S_2) = L(S_1) + L(S_2) = S_1 + S_2$.

Problem 5 : *Let $S = \{(1, 4), (0, 3)\}$ be a subset of $\mathbf{R}^2(\mathbf{R})$. Show that $(2, 3)$ belongs to $L(S)$.*

Solution : $(2, 3) \in L(S)$ if it can be put as a linear combination of $(1, 4)$ and $(0, 3)$.

Now $\quad (2, 3) = \alpha(1, 4) + \beta(0, 3)$

$$\Rightarrow (2, 3) = (\alpha + 0, 4\alpha + 3\beta)$$
$$\Rightarrow 2 = \alpha, 4\alpha + 3\beta = 3$$
$$\Rightarrow \alpha = 2, \beta = -\frac{5}{3}$$

Hence $\quad (2, 3) = 2\ (1, 4) - \frac{5}{3}\ (0, 3)$

Showing that $\quad (2, 3) \in L(S)$.

Problem 6 : *Let $V = \mathbf{R}^4(\mathbf{R})$ and let $S = \{(2, 0, 0, 1), (-1, 0, 1, 0)\}$. Find $L(S)$.*

Solution : Any element $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in L(S)$ is a linear combination of members of S.

Let $\quad (\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha(2, 0, 0,1) + \beta(-1, 0, 1, 0), \alpha, \beta \in \mathbf{R}$

Then $\quad (\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (2\alpha - \beta, 0, \beta, \alpha)$

i.e., $\quad L(S) = \{2\alpha - \beta, 0, \beta, \alpha) \mid \alpha, \beta \in \mathbf{R}\}$

Linear Dependence and Independence

Let $V(F)$ be a vector space. Elements $v_1, v_2, \ldots, v_n$ in V are said to be linearly dependent (over F) if $\exists$ scalars $\alpha_1, \alpha_2, \ldots\ldots \alpha_n \in F$, (not all zero) such that

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots \alpha_n v_n = 0$$

($v_1, v_2, \ldots, v_n$ are finite in number, not essentially distinct).

Thus for linear dependence $\Sigma\, \alpha_i v_i = 0$ and at least one $\alpha_i \neq 0$.

If $v_1, v_2, \ldots, v_n$ are not linearly dependent (*L.D.*) these are called linearly independent (*L.I.*).

In other words, $v_1, v_2, \ldots, v_n$ are *L.I.* if

$$\Sigma\alpha_i v_i = 0 \Rightarrow \alpha_i = 0 \text{ for all } i$$

A finite set $X = \{x_1, x_2 \ldots\ldots, x_n\}$ is said to be *L.D.* or *L.I.* according as its n members are *L.D.* or *L.I.*

In general any subset Y of $V(F)$ is called *L.I.* if every finite non empty subset of Y is *L.I., otherwise* it is called *L.D.*

So, if some subsets are *L.I.* and some are *L.D.* then Y is called *L.D.*

Observations :

(*i*) A non zero vector is always *L.I.* as $v \neq 0$, $\alpha v = 0$ would mean $\alpha = 0$.

(*ii*) Zero vector is always *L.D.*

$$1 . 0 = 0 \qquad 1 \neq 0, \ 1 \in F$$

Thus any collection of vectors to which zero belongs is always *L.D.*

In other words, if $v_1, v_2, \ldots, v_n$ are *L.I.*, then none of these can be zero. (But not conversely, see example ahead).

(*iii*) v is *L.I.* iff $v \neq 0$

(*iv*) Empty set φ is *L.I.* since it has no non empty finite subset and consequently it satisfies the condition for linear independence. In other words, whenever $\Sigma\alpha_i v_i = 0$ in φ then as there is no i for which $\alpha_i \neq 0$, set φ is *L.I.* We sometimes express it by saying that empty set is *L.I.* vacuously.

Example 13 : Consider $\mathbf{R}^2(\mathbf{R})$, $\mathbf{R}$ = reals.

$$v_1 = (1, 0), \ v_2 = (0, 1) \in \mathbf{R}^2 \text{ are } L.I.$$

as $\quad \alpha_1 v_1 + \alpha_2 v_2 = 0$ for $\alpha_1, \alpha_2 \in \mathbf{R}$

$$\Rightarrow \alpha_1(1, 0) + \alpha_2(0, 1) = (0, 0)$$

$$\Rightarrow (\alpha_1, \alpha_2) = (0, 0) \Rightarrow \alpha_1 = \alpha_2 = 0.$$

Example 14 : Consider the subset

$$S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1), (2, 3, 4)\}$$

in the vector space $\mathbf{R}^3(\mathbf{R})$.

Since

$$2(1, 0, 0) + 3(0, 1, 0) + 4(0, 0, 1) - 1(2, 3, 4) = (0, 0, 0)$$

we find S is *L.D.*

Example 15 : In the vector space P of polynomials the vectors $f(x) = 1 - x$, $g(x) = x - x^2$, $h(x) = 1 - x^2$ are *L.D.* since $f(x) + g(x) - h(x) = 0$.

Problem 7 : *Show that the vectors* $v_1 = (0, 1, -2)$, $v_2 = (1, -1, 1)$, $v_3 = (1, 2, 1)$ *are L.I. in* $\mathbf{R}^3(\mathbf{R})$.

Solution : Let $\Sigma\alpha_i v_i = 0$ for $\alpha_i \in \mathbf{R}$

Then $\quad \alpha_1(0, 1, -2) + \alpha_2(1, -1, 1) + \alpha_3(1, 2, 1) = (0, 0, 0)$

$$\Rightarrow (0, \alpha_1, -2\alpha_1) + (\alpha_2, -\alpha_2, \alpha_2) + (\alpha_3, 2\alpha_3, \alpha_3) = (0, 0, 0)$$

$$\Rightarrow 0 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1 - \alpha_2 + 2\alpha_3 = 0$$

$$-2\alpha_1 + \alpha_2 + \alpha_3 = 0$$

Since the coefficient determinant $\begin{vmatrix} 0 & 1 & 1 \\ 1 & -1 & 2 \\ -2 & 1 & 1 \end{vmatrix}$ is $-6 \neq 0$ the above equations have only the zero common solution

$$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0 \Rightarrow v_1, v_2, v_3 \text{ are } L.I.$$

Problem 8 : *Show that the vectors*

$v_1 = (1, 1, 2, 4)$, $v_2 = (2, -1, -5, 2)$, $v_3 = (1, -1, -4, 0)$ *and* $v_4 = (2, 1, 1, 6)$ *are L.D. in* $\mathbf{R}^4(\mathbf{R})$.

Solution : Suppose $av_1 + bv_2 + cv_3 + dv_4 = 0$, $a, b, c, d \in \mathbf{R}$

then $a(1, 1, 2, 4) + b(2, -1, -5, 2)$

$+ c(1, -1, -4, 0) + d(2, 1, 1, 6) = (0, 0, 0, 0)$

or $(a, a, 2a, 4a) + (2b, -b, -5b, 2b) + (c, -c, -4c, 0)$

$+ (2d, d, d, 6d) = (0, 0, 0, 0)$

$$\Rightarrow \begin{aligned} a + 2b + c + 2d &= 0 \\ a - b - c + d &= 0 \\ 2a - 5b - 4c + d &= 0 \\ 4a + 2b + 0c + 6d &= 0 \end{aligned}$$

$$\Rightarrow \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & -1 & -1 & 1 \\ 2 & -5 & -4 & 1 \\ 4 & 2 & 0 & 6 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_2 \to R_2 - R_1$, $R_3 \to R_3 - 2R_1$, $R_4 \to R_4 - 4R_1$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to \frac{1}{2} R_4$, $R_3 \to \frac{1}{3} R_3$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -1 & -2/3 & -1/3 \\ 0 & -3/4 & -1 & -1/2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to R_4 - R_2$, $R_3 \to R_3 - R_2$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow \quad a + 2b + c + 2d = 0$$
$$-3b - 2c - d = 0$$
$$3b + 2c + d = 0$$

$a = -1$, $b = -1$, $c = 1$, $d = 1$ satisfy the equations.

Since coefficients are non zero, the given vectors are *L.D.*

Problem 9 : *If two vectors are L.D. then one of them is the scalar multiple of the other.*

Solution : Suppose v_1, v_2 are *L.D.* then $\exists\ \alpha_i \in F$, s.t.,

$$\alpha_1 v_1 + \alpha_2 v_2 = 0 \text{ for some } \alpha_i = 0$$

without loss of generality we can take $\alpha_1 \neq 0$, then α_1^{-1} exists and $\alpha_1 v_1 = (-\alpha_2 v_2)$

$$\Rightarrow \quad v_1 = (-\alpha_1^{-1}\alpha_2)\ v_2 = \beta v_2$$

which proves the result.

Problem 10 : *If x, y, z are L.I. over the field* **C** *of complex nos. then so are* $x + y$, $y + z$ *and* $z + x$ *over* **C**.

Solution : Suppose $\alpha_1(x + y) + \alpha_2(y + z) + \alpha_3\ (z + x) = 0$, $\alpha_i \in \mathbf{C}$

Then $\quad (\alpha_1 + \alpha_3)x + (\alpha_1 + \alpha_2)y + (\alpha_2 + \alpha_3)z = 0$

$$\Rightarrow \quad \alpha_1 + \alpha_3 = \alpha_1 + \alpha_2 = \alpha_2 + \alpha_3 = 0 \text{ as } x,\ y,\ z \text{ are } L.I.$$

Solving we find

$$\alpha_1 = \alpha_2 = \alpha_3 = 0.$$

Hence the result.

Problem 11 : *If* $v_1, v_2, v_3 \in V(F)$ *s.t.,* $v_1 + v_2 + v_3 = 0$ *then show that* $\{v_1, v_2\}$ *spans the same subspace as* $\{v_2, v_3\}$ *i.e., show that* $L(\{v_1, v_2\}) = L(\{v_2, v_3\})$.

Solution : Let $x \in L\ (\{v_1,\ v_2\})$ then $x = \alpha v_1 + \beta_2 v_2 \qquad \alpha,\ \beta \in F$

$$\Rightarrow \quad x = \alpha(-v_2 - v_3) + \beta v_2 \text{ as } v_1 + v_2 + v_3 = 0$$
$$= (\beta - \alpha)v_2 + (-\alpha)\ v_3 \in L(\{v_2,\ v_3\})$$

Showing that $L(\{v_1,\ v_2\}) \subseteq L(\{v_2,\ v_3\})$

Similarly we can show that $L(\{v_2,\ v_3\}) \subseteq L(\{v_1,\ v_2\})$

Hence the result follows.

Note (i) : Linear dependence depends not only upon the vector space, but the field as well.

Consider, for instance, **C(C)**, **C(R)**, **C** = complex, **R** = reals.

Take $1,\ i \in \mathbf{C}$, if $\alpha,\ \beta \in \mathbf{R}$.

then $\qquad \alpha \,.\, 1 + \beta \,.\, i = 0 = 0 + i0$

$$\Rightarrow \alpha = 0, \beta = 0$$

$$\Rightarrow 1, i \text{ are } L.I. \text{ in } \mathbf{C}(\mathbf{R})$$

Now if we take α, β in $\mathbf{C}$, then as we can take $\alpha = i$, $\beta = -1$, so that

$$i \,.\, 1 + (-1)i = 0, \text{ we find } \exists\ \alpha, \beta \neq 0$$

s.t., sums of the type $\Sigma\alpha_i v_i = 0$

i.e., $1, i$ are $L.D.$ in $\mathbf{C}(\mathbf{C})$

Note (ii) : In example 13 above, we showed that (1, 0) and (0, 1) are *L.I.* in $\mathbf{R}^2(\mathbf{R})$

if $v = (a, b) \in \mathbf{R}^2$ be *any* element

then since $(a, b) = a(1, 0) + b(0, 1)$, $a, b \in \mathbf{R}$

We find any element of $\mathbf{R}^2$ can be written as a linear combination of $\{(1, 0), (0, 1)\} = S$

i.e., $v \in \mathbf{R}^2 \Rightarrow v \in L(S)$

$$\Rightarrow \mathbf{R}^2 \subseteq L(S)$$

But $L(S) \subseteq \mathbf{R}^2$

i.e., $\mathbf{R}^2 = L(S)$

or that S spans $\mathbf{R}^2$.

We generalise this through

Definition : Let $V(F)$ be a vector space. A subset S of V is called a *basis* of V if S consists of *L.I.* elements (i.e., any finite number of elements in S are *L.I.*) and $V = L(S)$, i.e., S spans V.

Thus in example 13, $S = \{(1, 0), (0, 1)\}$ is a basis of $\mathbf{R}^2(\mathbf{R})$. It is rather easy to see then that $\{(1, 0, 0)\ (0, 1, 0), (0, 0,1)\}$ will form basis of $\mathbf{R}^3(\mathbf{R})$, and one can trivially extend this to $\boldsymbol{R}^{(n)}$

Again $\{(1, 1, 0), (1, 0, 0), (0, 1, 1)\}$ also forms a basis of $\mathbf{R}^3(\mathbf{R})$. (Show!) Thus a vector space may have more than one basis.

If the elements in a basis are written in a certain specific order, we call it *ordered basis*. Also $\{(1, 0), (0, 1)\}$ $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$ etc. are called *standared basis* of $\mathbf{R}^2$, $\mathbf{R}^3$ etc.

The next few theorems give a concrete shape to the concept of a basis of a vector space.

Theorem16 *If $S = \{v_1, v_2, \ldots\ldots v_n\}$ is a basis of V, then every element of V can be expressed uniquely as a linear combination of $v_1, v_2, \ldots\ldots, v_n$.*

Proof : Since, by definition of basis, $V = L(S)$, each element $v \in V$ can be expressed as a linear combination of $v_1, v_2, \ldots\ldots, v_n$.

Suppose $v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n.$ $\alpha_i \in F$

$v = \beta_1 v_1 + \beta_2 v_2 + \ldots\ldots + \beta_n v_n.$ $\beta_i \in F$

then $\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \ldots\ldots + \beta_n v_n.$

$$\Rightarrow (\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \ldots\ldots + (\alpha_n - \beta_n)v_n = 0$$

$$\Rightarrow \alpha_i - \beta_i = 0 \text{ for all } i \ (v_1, v_2, \ldots\ldots v_n \text{ are } L.I.)$$
$$\Rightarrow \alpha_i = \beta_i \text{ for all } i.$$

Theorem 17 : *Suppose S is a finite subset of a vector space V such that $V = L(S)$ [i.e., V is a F.D.V.S.] then there exists a subset of S which is a basis of V.*

Proof : If S consists of *L.I.* elements then S itself forms basis of V and we've nothing to prove.

Let now T be a subset of S, such that T spans V and T is such minimal subset of S (Existence of T is ensured as S is finte).

Suppose $\quad T = \{v_1, v_2, \ldots\ldots, v_n\}$

we show T is *L.I.*

Let $\quad \Sigma\alpha_i v_i = 0, \ \alpha_i \in F$

Suppose $\alpha_i \neq 0$ for some i. Without any loss of generality we can take $\alpha_1 \neq 0$. then α_1^{-1} exists.

Now
$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n = 0$$
$$\Rightarrow \alpha_1^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n) = 0$$
$$\Rightarrow v_1 = (-\alpha_1^{-1}\alpha_2)v_2 + (-\alpha_1^{-1}\alpha_3)v_3 + \ldots\ldots + (-\alpha_1^{-1}\alpha_n)v_n$$
$$= \beta_2 v_2 + \beta_3 v_3 + \ldots\ldots + \beta_n v_n \quad \beta_i \in F$$

If $v \in V$ be any element then
$$v = \gamma_1 v_1 + \gamma_2 v_2 + \ldots\ldots \gamma_n v_n \qquad \gamma_i \in F \text{ as } V = L(T)$$
$$\Rightarrow v = \gamma_1(\beta_2 v_2 + \ldots\ldots + \beta_n v_n) + \gamma_2 v_2 + \ldots\ldots + \gamma_n v_n$$

i.e., any element of V is a linear combination of $v_2, v_3, \ldots\ldots, v_n$

$\Rightarrow \{v_2, v_3, \ldots\ldots v_n\}$ spans V, which contradicts our choice of T (as T was such minimal)

Hence $\quad \alpha_1 = 0$

or that $\quad \alpha_i = 0$ for all i

$\Rightarrow v_1, v_2, \ldots\ldots v_n$ are *L.I.*

and thus T is a basis of V.

Cor. : A *F.D.V.S.* has a basis.

Theorem 18 : *Any two bases of a F.D.V.S. V have same number of elements.*

Proof : Existence of a basis is ensured by the previous theorem. Suppose
$$S = \{v_1, v_2, \ldots\ldots, v_n\}$$
$$T = \{w_1, w_2, \ldots\ldots, w_m\}$$

are two bases of V. We claim $n = m$.

Suppose $n > m$

Now $v_1 \in V$ and T is basis, we thus get
$$v_1 = a_{11}w_1 + a_{21}w_2 + \ldots\ldots a_{m1}w_m \text{ (coefficients in } F)$$

Similarly we get

$$v_2 = a_{12}w_1 + a_{22}w_2 + \ldots\ldots a_{m2}w_m$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$v_n = a_{1n}w_1 + a_{2n}w_2 + \ldots\ldots a_{mn}w_m \qquad a_{ij} \in F$$

Consider the following system of m equations in n unknowns $x_1, x_2 \ldots\ldots x_n \in F$

$$a_{11}x_1 + a_{12}x_2 + \ldots\ldots a_{1n}x_n = 0$$
$$a_{21}x_1 + a_{22}x_2 + \ldots\ldots a_{2n}x_n = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots\ldots a_{mn}x_n = 0$$

Since $m < n$, the above system of equations has a non zero solution say $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n$ (Here some $\alpha_i \neq 0$).

We thus have

$$a_{11}\alpha_1 + a_{12}\alpha_2 + \ldots\ldots a_{1n}\alpha_n = 0$$
$$a_{21}\alpha_1 + a_{22}\alpha_2 + \ldots\ldots a_{2n}\alpha_n = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{m1}\alpha_1 + a_{m2}\alpha_2 + \ldots\ldots a_{mn}\alpha_n = 0$$

which gives

$$(a_{11}\alpha_1 + a_{12}\alpha_2 + \ldots\ldots a_{1n}\alpha_n)\ w_1 + \ldots\ldots\ldots + (a_{m1}\alpha_1 + a_{m2}\alpha_2 + \ldots\ldots a_{mn}\alpha_n)\ w_m = 0$$

i.e. $\alpha_1(a_{11}w_1 + \ldots\ldots + a_{m1}w_m) + \ldots\ldots + \ldots\ldots + \alpha_n\ (a_{1n}w_1 + \ldots\ldots + a_{mn}w_m) = 0$

Thus $\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n = 0$

$\Rightarrow \alpha_i = 0\ \forall\, i$, a contradiction.

Thus n is not greater than m. Similarly m is not greater than n.

Hence $m = n$.

Aliter : Let $\{v_1, v_2, \ldots\ldots, v_n\}$, $\{w_1, w_2, \ldots\ldots, w_m\}$ be two basis of V.

then $$v_1 = a_{11}w_1 + \ldots\ldots + a_{1m}w_m$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$v_n = a_{n1}w_1 + \ldots\ldots + a_{nm}w_m$$

where $a_J \in F$

$$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} a_{11} & \ldots & a_{1m} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nm} \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}$$

$$= A \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix}, \text{ where } A = (a_{ij}) = n \times m \text{ matrix}$$

Similarly,

$$w_1 = b_{11}v_1 + \ldots\ldots + b_{1n}v_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$w_m = b_{m1}v_1 + \ldots\ldots + b_{mn}v_n \text{ where } b_{ij} \in F$$

$$\therefore \quad \begin{bmatrix} w_1 \\ \vdots \\ w_m \end{bmatrix} = \begin{bmatrix} b_{11} & \ldots & b_{1n} \\ \ldots & \ldots & \ldots \\ b_{m1} & \ldots & b_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$$

$$= B \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}, \text{ where } B = (b_{ij}) = m \times n \text{ matrix.}$$

$$\therefore \quad \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = AB \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \Rightarrow (I - AB) \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = 0$$

$$\Rightarrow \quad C \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = 0, \text{ where } C = I - AB = (c_{ij})$$

$$\Rightarrow \quad \begin{bmatrix} c_{11} & \ldots & c_{1n} \\ \ldots & \ldots & \ldots \\ c_{n1} & \ldots & c_{nn} \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = 0$$

$$\Rightarrow \quad c_{11}v_1 + \ldots\ldots + c_{1n}v_n = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_{n1}v_1 + \ldots\ldots + c_{nn}v_n = 0$$

$$\Rightarrow \quad c_{11} = \ldots\ldots = c_{1n} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$c_{n1} = \ldots\ldots = c_{nn} = 0$$

as $\{v_1, \ldots\ldots, v_n\}$ is a *L.I.* set.

$$\Rightarrow \quad C = 0 \Rightarrow AB = I$$

Similarly, $BA = I$

Let $n > m$.

Define $A_1 = [A \;\; O]$, where O is $n \times (n-m)$ zero matrix.

$$B_1 = \begin{bmatrix} B \\ O \end{bmatrix}, \text{ where } O \text{ is } (n-m) \times n \text{ zero matrix.}$$

$$\therefore \quad A_1B_1 = AB$$
$$\Rightarrow \det A_1B_1 = \det AB$$
$$\Rightarrow \det A_1 \det B_1 = \det I = 1$$
$$\Rightarrow O = 1 \text{ as } \det A_1 = O = \det B_1$$

which is not true as in a field $0 \neq 1$.

$\therefore$ $n \not> m$. Similarly $m \not> n$.

Hence $n = m$.

We can now make

Definition : A F.D.V.S V is said to have *dimension* n if n is the number of elements in any basis of V.

We use the notation $\dim_F V = n$ or simply $\dim V = n$ and say V is n – dimensional vector space.

In view of an example done earlier $\dim \mathbf{R}^2 = 2$.

In fact, $\dim \mathbf{R}^n = n$.

Theorem 19 : *A F.D.V.S. V has dimension n iff n is the maximum number of L.I. vectors in any subset of V.*

Proof : Let $\dim V = n$ and let $\{v_1, v_2, \ldots\ldots v_n\}$ be a basis of V, then these are *L.I.*.

Let $S = \{w_1, w_2, \ldots\ldots w_m\}$ be a subset of V where $m > n$. We show S must be *L.D.* set.

Since $w_1, w_2, \ldots\ldots w_m$ all belong to V and $\{v_1, v_2, \ldots\ldots v_n\}$ is a basis of V; we can write

$$w_1 = a_{11}v_1 + a_{21}v_2 + \ldots\ldots + a_{n1}v_n$$
$$w_2 = a_{12}v_1 + a_{22}v_2 + \ldots\ldots + a_{n2}v_n \qquad a_{ij} \in F$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$w_m = a_{1m}v_1 + a_{2m}v_2 + \ldots\ldots + a_{nm}v_n$$

Consider the following system of n equations in m unknowns

$$a_{11}x_1 + \ldots\ldots + a_{1m}x_m = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{n1}x_1 + \ldots\ldots + a_{nm}x_m = 0$$

Since $n < m$, the above system has a non–zero solution $\alpha_1, \ldots \alpha_m \in F$, (i.e., some $\alpha_i \neq 0$).

$$\therefore \quad a_{11}\alpha_1 + \ldots\ldots + a_{1m}\alpha_m = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{n1}\alpha_1 + \ldots\ldots + a_{nm}\alpha_m = 0$$
$$\Rightarrow a_{11}\alpha_1 v_1 + \ldots\ldots + a_{1m}\alpha_m v_1 = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\alpha_{n1}\alpha_1 v_n + \ldots\ldots + a_{nm}\alpha_m v_n = 0$$

$$\Rightarrow \alpha_1 (a_{11}v_1 + ... + a_{n1}v_n) + ... + \alpha_m (a_{1m}v_1 + ... + a_{nm}v_n) = 0$$
$$\Rightarrow \alpha_1 w_1 + ...\alpha_m w_m = 0, \text{ where some } \alpha_i \neq 0$$
$$\Rightarrow w_1, w_2, ..., w_m \text{ are } L.D.$$

which proves our result.

Conversely, let the maximum number of *L.I.* elements in any subset of V be n then there exists a subset $S = \{v_1, v_2, ...v_n\}$ of V such that S is *L.I.* We claim S forms a basis of V.

Let $v \in V$ be any element.

Let $T = \{v_1, v_2, ...v_n, v\}$ then as it contains $n+1$ elements, it is *L.D.*.

$\Rightarrow \exists\, \alpha_1, \alpha_2, ... \alpha_n, \alpha$ in F such that

$\alpha_1 v_1 + ...\alpha_n v_n + \alpha v = 0$ with some coefficients not zero. Suppose $\alpha = 0$

then $\alpha_1 v_1 + ...\alpha_n v_n = 0$

$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2, ...v_n$ are *L.I.*

i.e. all α_i and α are zero, which is not true. Hence $\alpha \neq 0 \Rightarrow \alpha^{-1}$exists in F.

Now $\alpha v = -\alpha_1 v_1 - \alpha_2 v_2 - .... - \alpha_n v_n$

$\Rightarrow v = (-\alpha^{-1}\alpha_1)\, v_1 + (-\alpha^{-1}\alpha_2)\, v_2 + ... + (-\alpha^{-1}\alpha_n)\, v_n$

or that v is linear combination of $v_1, v_2, ..., v_n$ and v being any element, we find S spans V or that S forms basis of V.

Hence $\dim V = n$.

Cor. 1 : If $\dim V = n$, then any $n+1$ vectors in V are *L.D.*

Proof : Follows from first part of the theorem by taking $m = n+1$

Cor. 2 : If $\dim V = n$ and $\{v_1, v_2, ...v_m\}$ is *L.I.* subset of V then $m \leq n$.

Cor. 3 : In a vector space V, if $\{v_1, v_2, ...v_n\}$ is *L.I.* and $\{w_1, w_2, ...w_m\}$ spans V then $n \leq m$. Follows by converse part of the theorem.

Theorem 20 : *If V is a F.D.V.S. and $\{v_1, v_2, ...v_r\}$ is a L.I. subset of V, then it can be extended to form a basis of V.*

Proof : If $\{v_1, v_2, ...v_r\}$ spans V, then it itself forms a basis of V and there is nothing to prove

Let $S = \{v_1, v_2, ...v_r, v_{r+1}, ...v_n\}$ be the maximal *L.I.* subset of V.

We show S is a basis of V, for which it is enough to prove that S spans V. Let $v \in V$ be any element

then $T = \{v_1, v_2, ...v_n, v\}$ is *L.D.* by choice of S

$\Rightarrow \exists\, \alpha_1, \alpha_2, ..., \alpha_n, \alpha \in F$ (not all zero) such that

$$\alpha_1 v_1 + ... + \alpha_n v_n + \alpha v = 0$$

We claim $\alpha \neq 0$. Suppose $\alpha = 0$

then $\alpha_1 v_1 + ... + \alpha_n v_n = 0$

$\Rightarrow \alpha_i = 0$ for all i as $v_1, v_2, ...v_n$ are *L.I.*

$\therefore\ \alpha = \alpha_i = 0$ for all i which is not true

Hence $\alpha \neq 0$ and so α^{-1} exists.

Since $= (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + \ldots\ldots + (-\alpha^{-1}\alpha_n)v_n$

v is a linear combination of $v_1, v_2, \ldots\ldots v_n$

which proves our assertion.

Theorem 21 : *If dim $V = n$ and $S = \{v_1, v_2, \ldots\ldots, v_n\}$ spans V then S is a basis of V.*

Proof : Since $\dim V = n$, any basis of V has n elements. By theorem 17, a subset of S will be a basis of V but as S contains n elements, it will itself form basis of V.

Theorem 22 : *If dim $V = n$ and $S = \{v_1, v_2, \ldots\ldots, v_n\}$ is L.I. subset of V then S is a basis of V.*

Proof : Since $\{v_1, v_2, \ldots\ldots, v_n\} = S$ is *L.I.* it can be extended to form a basis of V, but $\dim V$ being n, it will itself be a basis of V.

Problem 12 : *If $\{v_1, v_2, \ldots\ldots, v_n\}$ is a basis of F.D.V.S. V of dim n and $v = \Sigma\alpha_i v_i$, $\alpha_r \neq 0$ then prove that $\{v_1, v_2, \ldots\ldots, v_{r-1}, v, v_{r+1} \ldots, v_n\}$ is also a basis of V.*

Solution : We have

$$v = \alpha_1 v_1 + \ldots\ldots + \alpha_r v_r + \ldots\ldots + \alpha_n v_n \qquad \alpha_r \neq 0, \therefore \alpha_r^{-1} \text{ exists}$$

$$\Rightarrow v_r = (-\alpha_r^{-1}\alpha_1)\, v_1 + \ldots\ldots + (-\alpha_r^{-1}\alpha_{r-1})\, v_{r-1} + \alpha_r^{-1} v + \ldots\ldots + (-\alpha_r^{-1}\alpha_n) v_n$$

$$= \beta_1 v_1 + \ldots\ldots + \beta_{r-1} v_{r-1} + \beta_r v + \beta_{r+1}\, v_{r+1} + \ldots\ldots + \beta_n v_n.$$

If $x \in V$ be any element, then

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n \qquad a_i \in F$$

$$\Rightarrow x = a_1 v_1 + \ldots\ldots + a_{r-1} v_{r-1} + a_r(\beta_1 v_1 + \ldots\ldots + \beta_n v_n) + \ldots\ldots + a_n v_n$$

or that x is a linear combination of

$$v_1, \ldots\ldots, v_{r-1}, v, v_{r+1}, \ldots\ldots, v_n$$

and x being any element, we find V is spanned by $\{v_1, \ldots\ldots v_{r-1}, v\ v_{r-1}, \ldots v_n\}$ and it forms a basis of V, using theorem done above.

Theorem 23 : *Two finite dimensional vector spaces over F are isomorphic iff they have the same dimension.*

Proof : Let V and W be two isomorphic vector spaces over F and let $\theta : V \to W$ be the isomorphism.

Let $\dim V = n$ and $\{v_1, v_2, \ldots\ldots, v_n\}$ be a basis of V.

We claim $\{\theta(v_1), \theta(v_2), \ldots\ldots, \theta(v_n)\}$ is a basis of W.

Let $$\sum_{i=1}^{n} \alpha_i\ \theta(v_i) = 0 \qquad \alpha_i \in F,$$

$$\Rightarrow \sum \theta(\alpha_i v_i) = 0 = \theta(0)$$

$$\Rightarrow \sum \alpha_i v_i = 0 \qquad (\theta \text{ is 1-1})$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i \text{ as } v_1, v_2, \ldots\ldots, v_n \text{ are } L.I.$$

$$\Rightarrow \theta(v_1), \theta(v_2), \ldots\ldots, \theta(v_n) \text{ are } L.I.$$

Again, if $w \in W$ is any element, then as θ is onto, $\exists$ some $v \in V$ s.t., $\theta(v) = w$

Now $$v \in V \Rightarrow v = \sum_{i=1}^{n} \alpha_i v_i \quad \text{for some } \alpha_i \in F$$

$$\Rightarrow w = \theta(v) = \theta(\sum \alpha_i v_i)$$

$$\Rightarrow w = \sum \theta(\alpha_i v_i) = \alpha_1\theta(v_1) + \alpha_2\theta(v_2) + \ldots\ldots + \alpha_n\theta(v_n)$$

or that w is a linear combination of $\theta(v_1), \theta(v_2), \ldots\ldots, \theta(v_n)$

Hence $\theta(v_1), \theta(v_2), \ldots\ldots, \theta(v_n)$ span W and therefore, form a basis of W showing that $\dim W = n$.

Conversely, let $\dim V = \dim W = n$ and suppose $\{v_1, v_2, \ldots\ldots, v_n\}$ and $\{w_1, w_2, \ldots\ldots, w_n\}$ are basis of V and W respectively.

Define a map $\theta : V \to W$ s.t.,

$$\theta(v) = \theta(\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_n v_n)$$
$$= \alpha_1 w_1 + \alpha_2 w_2 + \ldots\ldots + \alpha_n w_n$$

then θ is easily seen to be well defined (Indeed any $v \in V$ is a linear combination of members of basis).

If $v, v' \in V$ be any elements then

$$v = \sum \alpha_i v_i, \quad v' = \sum \beta_i v_i \qquad \alpha_i, \beta_i \in F$$

$$\theta(v + v') = \theta(\sum \alpha_i v_i + \sum \beta_i v_i)$$

$$= \theta(\sum (\alpha_i + \beta_i) v_i)$$

$$= \sum (\alpha_i + \beta_i) w_i$$

$$= \sum \alpha_i w_i + \sum \beta_i w_i = \theta(v) + \theta(v')$$

Also $$\theta(\alpha v) = \theta(\alpha \sum \alpha_i v_i) = \theta(\sum \alpha\alpha_i v_i) = \sum (\alpha\alpha_i) w_i$$

$$= \alpha \sum \alpha_i w_i = \alpha\theta(v)$$

Thus θ is a homomorphism.

Now if $v \in \text{Ker } \theta$

then $$\theta(v) = 0$$

$$\Rightarrow \theta(\sum \alpha_i v_i) = 0$$

$$\Rightarrow \sum \alpha_i w_i = 0$$

$\Rightarrow \alpha_i = 0$ for all i $\quad w_1, w_2, \ldots\ldots, w_n$ being *L.I.*

$\Rightarrow v = 0$

$\Rightarrow$ Ker $\theta = \{0\}$

$\Rightarrow \theta$ is one-one.

That θ is onto is obvious. Hence θ is an isomorphism.

Cor. : Under an isomorphism, a basis is mapped onto a basis.

Follows by first part of the theorem.

Problem 13 : *Show that the set of all real valued continuous functions $y = f(x)$ satisfying the differential equation $\frac{d^3y}{dx^3} + 6\frac{d^2y}{dx^2} + 11\frac{dy}{dx} + 6y = 0$ is a vector space over* **R**. *Find a basis of this.*

Solution : One can check that $V = \{f \mid f : \mathbf{R} \to \mathbf{R},\ f \text{ cont.}\}$ is a vector space over **R**, under

$$(f+g)x = f(x) + g(x)$$
$$(\alpha f)x = \alpha(f(x))$$

Let $W = \{f \in V \mid f$ is a solution of given differential equation$\}$

The given differential equation is

$$(D^3 + 6D^2 + 11D + 6)\,y = 0$$
$$(D+1)(D+2)(D+3)\,y = 0$$
$$\Rightarrow \quad D = -1,\ -2,\ -3$$

and this general solution is

$$y = Ae^{-x} + Be^{-2x} + Ce^{-3x}$$

If $S = \{e^{-x},\ e^{-2x},\ e^{-3x}\}$ then clearly S spans W

Let $\quad Ae^{-x} + Be^{-2x} + Ce^{-3x} = 0$

Then $\quad -Ae^{-x} + (-2)Be^{-2x} + (-3C)e^{-3x} = 0$

$$Ae^{-x} + (4B)e^{-2x} + (9C)e^{-3x} = 0 \qquad \forall x$$

Put $\quad x = 0$

$$\begin{bmatrix} 1 & 1 & 1 \\ -1 & -2 & -3 \\ 1 & 4 & 9 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0 \Rightarrow M \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0$$

where $\det M = 1(-18+12) - 1(-9+3) + 1(-4+2) = -2 \neq 0$

Thus M^{-1} exists and so $A = B = C = 0$

$\Rightarrow S$ is L.I. and hence a basis of W.

Note : W is a vector space as it is a subspace of V. $[y_1, y_2 \in W \Rightarrow \alpha_1 y_1 + \alpha_2 y_2$ is a solution of the given differential equation $\Rightarrow \alpha_1 y_1 + \alpha_2 y_2 \in W]$.

Problem 14 : *If $S = \{v_1, v_2, \ldots\ldots, v_r\}$ is a L.I. subset of V and $v \in V$ be such that $v \notin L(S)$, then $S \cup \{v\}$ is a L.I., subset of V.*

Solution : $S \cup \{v\} = \{v_1, v_2, \ldots\ldots, v_r, v\}$

Let $\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots\ldots + \alpha_r v_r + \alpha v = 0 \quad \alpha_i \in F, \ \alpha \in F$

If $\alpha \neq 0$ then α^{-1} exists and we get

$$\alpha^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_r v_r + \alpha v) = 0$$

$$\Rightarrow v = (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + \ldots\ldots + (\alpha^{-1}\alpha_r)v_r$$

$$\Rightarrow v \in L(S), \text{ a contradiction}$$

thus $\alpha = 0$

$$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + a_r v_r = 0$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i \text{ as } v_1, v_2, \ldots\ldots, v_r \text{ are } L.I.$$

$$\Rightarrow \alpha = \alpha_i = 0 \text{ for all } i$$

$$\Rightarrow v_1, v_2, \ldots\ldots, v_r, v \text{ are } L.I.$$

Hence the result follows.

Problem 15 : $(1, 1, 1)$ *is L.I. vector in* $\mathbf{R}^3(\mathbf{R})$. *Extend it to form a basis of* $\mathbf{R}^3$.

Solution : $(1, 1, 1)$ is non zero vector and is therefore *L.I.* in $\mathbf{R}^3$.

Let $S = \{(1, 1, 1)\}$, then $L(S) = \{\alpha(1, 1, 1) \mid \alpha \in \mathbf{R}\}$

Now $(1, 0, 0) \in \mathbf{R}^3$, but $(1, 0, 0) \notin L(S)$

thus by above problem $S_1 = \{(1, 1, 1), (1, 0, 0)\}$ is *L.I.*

Now $L(S_1) = \{\alpha(1, 1, 1) + \beta(1, 0, 0) \mid \alpha, \beta \in \mathbf{R}\}$

$$= \{(\alpha + \beta, \alpha, \alpha) \mid \alpha, \beta \in \mathbf{R}\}$$

Again $(0, 1, 0) \notin L(S_1)$ and by above problem

$$S_2 = \{(1, 1, 1), (1, 0, 0), (0, 1, 0)\} \text{ is } L.I. \text{ subset of } \mathbf{R}^3$$

Since dim $\mathbf{R}^3 = 3$, we find S_2 will be a basis of $\mathbf{R}^3$.

Problem 16 : *A finite set of non zero vectors* $\{v_1, v_2, \ldots\ldots, v_n\}$ *in a vector space* $V(F)$ *is L.D. iff* $\exists\, v_k$, $2 \leq k \leq n$, *s.t.,* v_k *is a linear combination of* $v_1, v_2, \ldots\ldots, v_{k-1}$.

Solution : Let $v_1, v_2, \ldots\ldots, v_n$ be *L.D.* Then $\exists\, \alpha_i \in F$, not all zero s.t., $\sum_{i=1}^{n} \alpha_i v_i = 0$.

Let k be the largest integer s.t., $\alpha_k \neq 0$

then $k \neq 1$ as if $k = 1$,

then $\alpha_1 v_1 = 0$, $\alpha_i \neq 0$ ($\alpha_i = 0$ for all $i \geq 2$)

$$\Rightarrow v_1 = 0, \text{ not true as } v_i \text{ are non zero}$$

Hence $2 \leq k \leq n$

Thus $\alpha_k \neq 0$ and $\alpha_i = 0$ for all $i \geq k+1$. Also then α_k^{-1} exists

$$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_k v_k = 0$$

$$\Rightarrow \alpha_k^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + \ldots\ldots + \alpha_k v_k) = 0$$

$$\Rightarrow v_k = (-\alpha_k^{-1}\alpha_1)v_1 + (-\alpha_k^{-1}\alpha_2)v_2 + \ldots\ldots + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$$

which proves the result.

Conversely, suppose $\exists\, k,\ 2 \le k \le n$ s.t., v_k is a linear combination of $v_1, v_2, \ldots, v_{k-1}$

Let $\quad v_k = a_1 v_1 + a_2 v_2 + \ldots\ldots + a_{k-1} v_{k-1} \qquad a_i \in F$

Then $\quad a_1 v_1 + a_2 v_2 + \ldots\ldots + a_{k-1} v_{k-1} - 1 \,.\, v_k = 0$

$\Rightarrow v_1, v_2, \ldots\ldots, v_k$ are *L.D.* as $(-1) \neq 0$

$\Rightarrow v_1, v_2, \ldots\ldots, v_k, v_{k+1}, \ldots\ldots, v_n$ are *L.D.*

as any super set of a *L.D.* set is *L.D.* (See exercises).

Hence the result follows.

Remark : If $v_1, v_2, \ldots\ldots, v_n$ be in V then either these are *L.I.* or some v_k is a linear combination of the preceeding ones $v_1, v_2, \ldots\ldots, v_{k-1}$.

All this time we've been talking about basis of a F.D.V.S. V. What about a subspace of V, Would it also be finite dimensional? The answer is a natural yes. We formalise it through

Theorem 24 : *Let W be a subspace of a F.D.V.S. V, then W is finite dimensional and $\dim W \le \dim V$. In fact, $\dim V = \dim W$ iff $V = W$.*

Proof : Let $\dim V = n$, then n is the maximum number of *L.I.* elements in any subset of V. Since any subset of W will be a subset of V, n is the maximum number of *L.I.* elements in W.

Let $w_1, w_2, \ldots\ldots, w_m$ be the maximum number of *L.I.* elements in W then $m \le n$.

We show $\{w_1, w_2, \ldots\ldots, w_m\}$ is a basis of W. These are already *L.I.* If $w \in W$ be any element then the set $\{w_1, w_2, \ldots\ldots, w_m, w\}$ is *L.D.*

$\Rightarrow \exists\ \alpha_1, \alpha_2, \ldots\ldots, \alpha_m, \alpha$ in F (not all zero) s.t.,

$$\alpha_1 w_1 + \ldots\ldots + \alpha_m w_m + \alpha w = 0.$$

If $\alpha = 0$, we get $\alpha_i = 0$ for all i as $w_1, \ldots\ldots, w_m$ are *L.I.* which is not true. Thus $\alpha \neq 0$ and so α^{-1} exists.

The above equation then gives us

$$w = (-\alpha^{-1}\ \alpha_1) w_1 + \ldots\ldots + (-\alpha^{-1}\ \alpha_m) w_m$$

Showing that $\{w_1, w_2, \ldots\ldots, w_m\}$ spans W (and thus W is finite dimensional)

$\Rightarrow \{w_1, w_2, \ldots\ldots, w_m\}$ is a basis of W

$\Rightarrow \dim W = m \le n = \dim V$

Finally, if $\dim V = \dim W = n$

and $\{w_1, w_2, \ldots\ldots, w_n\}$ be a basis of W then as $\{w_1, w_2, \ldots\ldots, w_n\}$ is *L.I.* in W, it will be *L.I.* in V.

and as $\dim V = n$, $\{w_1, w_2, \ldots\ldots, w_n\}$ is a basis of V.

Now if $v \in V$ be any element then

$$v = \alpha_1 w_1 + \alpha_2 w_2 + \ldots\ldots + \alpha_n w_n \in W$$

$$\Rightarrow V \subseteq W \Rightarrow V = W.$$

Conversely, of course, $V = W \Rightarrow \dim V = \dim W$.

Remark : If W is a subspace of V where $W = (0)$ then dimension of W is taken to be zero.

Theorem 25 : *Let W be a subspace of a F.D.V.S.V Then*

$$dim \frac{V}{W} = dim\, V - dim\, W.$$

Proof : Let dim $W = m$ and let $\{w_1, w_2, \ldots, w_m\}$ be a basis of W.

$w_1, w_2, \ldots, w_m$ being *L.I.* in W will be *L.I.* in V and thus $\{w_1, w_2, \ldots, w_m\}$ can be extended to form a basis of V.

Let $\{w_1, w_2, \ldots, w_m, v_1, v_2, \ldots, v_n\}$ be this extended basis of V.

then $\qquad \dim V = n + m$

Consider the set $S = \{W + v_1, W + v_2, \ldots, W + v_n\}$, we show it forms a basis of $\frac{V}{W}$.

Let $\qquad \alpha_1(W + v_1) + \ldots + \alpha_n(W + v_n) = W \qquad \alpha_i \in F$

Then $\qquad W + (\alpha_1 v_1 + \ldots + \alpha_n v_n) = W$

$\Rightarrow \alpha_1 v_1 + \ldots + \alpha_n v_n \in W$

$\Rightarrow \alpha_1 v_1 + \ldots + \alpha_n v_n$ is a linear combination of $w_1, \ldots, w_m$

$\Rightarrow \alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 w_1 + \ldots + \beta_m w_m \qquad \beta_j \in F$

$\Rightarrow \alpha_1 v_1 + \ldots + \alpha_n v_n - \beta_1 w_1 - \ldots - \beta_m w_m = 0$

$\Rightarrow \alpha_i = \beta_j = 0$ for all i, j.

$\Rightarrow \{W + v_1, W + v_2, \ldots, W + v_n\}$ is L.I..

Again, for any $W + v \in \frac{V}{W}$, $v \in V$ means v is a linear combination of $w_1, \ldots, w_m, v_1, \ldots, v_n$.

i.e., $v = \alpha_1 w_1 + \ldots + \alpha_m w_m + \beta_1 v_1 + \ldots + \beta_n v_n \qquad \alpha_i, \beta_j \in F$

giving $W + v = W + (\alpha_1 w_1 + \ldots + a_m w_m) + (\beta_1 v_1 + \ldots + \beta_n v_n)$

$= W + (\beta_1 v_1 + \ldots + \beta_n v_n)$

$= (W + \beta_1 v_1) + \ldots + (W + \beta_n v_n)$

$= \beta_1(W + v_1) + \beta_2(W + v_2) + \ldots + \beta_n(W + v_n).$

Hence S spans $\frac{V}{W}$ and is therefore a basis.

$\therefore \qquad \dim \frac{V}{W} = n$

Thus $\qquad \dim \frac{V}{W} = \dim V - \dim W.$

Theorem 26 : *If A and B are two subspaces of a F.D.V.S. V then dim $(A + B)$ = dim A + dim B − dim $(A \cap B)$.*

Proof : We've already proved that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

$$\therefore \qquad \dim \frac{A+B}{A} = \dim \frac{B}{A \cap B}$$

$$\Rightarrow \dim (A+B) - \dim A = \dim B - \dim (A \cap B)$$

or that $\dim (A + B) = \dim A + \dim B - \dim (A \cap B)$.

Remark : The reader should try to give an independent proof of the above theorem as an exercise.

Cor : If $A \cap B = (0)$ then $\dim (A+B) = \dim A + \dim B$

i.e., $\qquad \dim (A \oplus B) = \dim A + \dim B.$

Problem 17 : *Let P_n be the vector space of all polynomials of degree $\leq n$ over* **R**. *Exibit a basis of P_4/P_2. Hence verify that* $\dim \frac{P_4}{P_2} = \dim P_4 - \dim P_2$.

Solution : It is easy to see that $\{1, x, x^2, x^3, x^4\}$ is a basis of P_4 and thus $\dim P_4 = 5$. Similarly $\dim P_2 = 3$ as $\{1, x, x^2\}$ will be a basis of P_2.

Let $S = \{P_2 + x^3,\ P_2 + x^4\}$ then S is a basis of $\frac{P_4}{P_2}$ as

$$P_2 + f \in \frac{P_4}{P_2} \Rightarrow P_2 + \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \alpha_4 x^4 = P_2 + f$$

$$\Rightarrow P_2 + f = \alpha_3 (P_2 + x^3) + \alpha_4 (P_2 + x^4)$$

$$\Rightarrow S \text{ spans } \frac{P_4}{P_2}.$$

Again, $\qquad \alpha (P_2 + x^3) + \beta (P_2 + x^4) = \text{zero} = P_2$

$$\Rightarrow P_2 + \alpha x^3 + \beta x^4 = P_2$$

$$\Rightarrow \alpha x^3 + \beta x^4 = a + bx + cx^2 \in P_2$$

$$\Rightarrow a = b = c = \alpha = \beta = 0 \text{ as polynomial is zero, if each coefficient is zero.}$$

Thus S is a basis of $\frac{P_4}{P_2}$

Hence $\dim \frac{P_4}{P_2} = 2 = 5 - 3 = \dim P_4 - \dim P_2$.

Theorem 27 : *Let W be a subspace of a F.D.V.S. V, then there exists a subspace W' of V such that $V = W \oplus W'$*

Proof : Let $\{w_1, w_2, \ldots\ldots, w_m\}$ be a basis of W, then $w_1, w_2, \ldots\ldots, w_m$ being *L.I.* in W will be *L.I.* in V. We extend these *L.I.* elements to form a basis of V, say $\{w_1, \ldots\ldots, w_m, v_1, \ldots\ldots, v_n\}$

Let $W' = L(\{v_1, v_2, \ldots\ldots, v_n\})$, i.e., W' be the subspace spanned by $\{v_1, v_2, \ldots\ldots, v_n\}$.

We show $\quad W \oplus W' = V$

Let $v \in V$ be any element, then

$v = (\alpha_1 w_1 + \ldots\ldots + \alpha_m w_m) + (\beta_1 v_1 + \ldots\ldots + \beta_n v_n), \ \alpha_i, \beta_j \in F$

where the first bracket term belongs to W and the second to W'

$\therefore \ v \in W + W'$ and thus $V \subseteq W + W'$

$$\Rightarrow V = W + W'$$

Again, if $x \in W \cap W'$ be any element

then $x \in W$ and $x \in W'$

$$\Rightarrow x = a_1 w_1 + \ldots\ldots + a_m w_m \qquad a_i, b_j \in F$$

$$x = b_1 v_1 + \ldots\ldots + b_n v_n$$

$$\Rightarrow a_1 w_1 + \ldots\ldots + a_m w_m + (-b_1) v_1 + \ldots\ldots + (-b_n) v_n = 0$$

$$\Rightarrow a_i = b_j = 0 \text{ for all } i, j \qquad w_1, \ldots\ldots, w_m, v_1, \ldots\ldots, v_n \text{ being } L.I.$$

Hence $\quad x = 0$

$$\Rightarrow W \cap W' = (0)$$

or that $\quad V = W \oplus W'$

Note : W' is called complement of W. Thus we have proved that *every subspace of a F.D.V.S. has a complement.*

Cor. : If W' is any complement of W in V then $\dim W' = \dim V - \dim W$.

Since $V = W \oplus W' \Rightarrow \dim V = \dim (W \oplus W') = \dim W + \dim W'$

$$\Rightarrow \dim W' = \dim V - \dim W.$$

Although every complement of a subspace has same dimension it does not mean that a subspace has a unique complement. Consider

Example 16 : Let $V = \mathbf{R}^2(\mathbf{R})$ and let

$$W = \{(a, 0) \mid a \in \mathbf{R}\}$$

$$W_1 = \{(0, b) \mid b \in \mathbf{R}\}$$

$$W_2 = \{(c, c) \mid c \in \mathbf{R}\}$$

It is easy to see that W, W_1, W_2 are subspaces of V

We show $V = W \oplus W_1$ and $V = W \oplus W_2$

Now $\quad v \in V \Rightarrow v = (x, y) = (x, 0) + (0, y) \in W + W_1$

$$\Rightarrow V \subseteq W + W_1 \Rightarrow V = W + W_1$$

Again $\quad x \in W \cap W_1 \Rightarrow x \in W$ and $x \in W_1$

$$\Rightarrow x = (a, 0), \ x = (0, b)$$

$$\Rightarrow (a, 0) = (0, b) \Rightarrow a = b = 0 \Rightarrow x = 0$$

Hence $\quad W \cap W_1 = (0)$

or that $\quad V = W \oplus W_1$.

Also $\quad v \in V \Rightarrow v = (x, y) = (x - y, 0) + (y, y) \in W + W_2$

$$\Rightarrow V \subseteq W + W_2 \Rightarrow V = W + W_2$$

Now $\quad x \in W \cap W_2 \Rightarrow x \in W$ and $x \in W_2$

$$\Rightarrow x = (a, 0),\ x = (c, c)$$
$$\Rightarrow (a, 0) = (c, c)$$
$$\Rightarrow c = 0,\ a = 0$$
$$\Rightarrow x = (0, 0)$$

Thus $\quad W \cap W_2 = (0)$

or that $\quad V = W \oplus W_2$.

Notice that W, W_1, W_2 are spanned by $\{(1, 0)\}$, $\{(0, 1)\}$, $\{(1, 1)\}$ respectively and as each of these is L.I. (they are non zero). These subsets form bases of W, W_1, W_2 respectively.

Hence $\quad \dim W = \dim W_1 = \dim W_2 = 1$.

Exercises

1. Show that the following vectors are *L.I.*
   (*i*) (1, 0, 0), (1, 1, 1), (1, 2, 3), in $\mathbf{R}^3(\mathbf{R})$
   (*ii*) (1, 1, 0), (1, 0, 1), (0, 1, 1) in $\mathbf{R}^3(\mathbf{R})$
   (*iii*) (1, 0, 0, 0), (1, 1, 0, 0), (0, 0, 1, 1), (1, 1, 1, 1) in $\mathbf{R}^4(\mathbf{R})$
2. Show that the following vectors are *L.D.*
   (*i*) (1, −1, 2, 0), (3, 0, 0, 1), (2, 1, −1, 0), (1, −1, 2, 0) in $\mathbf{R}^4(\mathbf{R})$
   (*ii*) (1, 1, 2), (−3, 1, 0), (1, −1, 1), (1, 2, −3) in $\mathbf{R}^3(\mathbf{R})$
   (*iii*) (1, 2, 3, 4), (0, 1, −1, 2), (1, 5, 1, 8), (3, 7, 8, 14) in $\mathbf{R}^4(\mathbf{R})$
3. Show that vecotrs (v_1, v_2) and (w_1, w_2) in $\mathbf{C}$ are *L.D.* iff $v_1 w_2 = v_2 w_1$.
4. Prove that every subset of a *L.I.* set is *L.I.* whereas every super set of a *L.D.* set is *L.D.* Hence show that in $\mathbf{C}$ the vector space of complex numbers, every set with more than one element is *L.D.* set.
5. Let $\alpha_1 = (1, 1, -2, 1)$, $\alpha_2 = (3, 0, 4, -1)$, $a_3 = (-1, 2, 5, 2)$. Show that the vector $(4, -5, 9, -7)$ is spanned by α_1, α_2, α_3.
6. If S spans V then show that every superset of S spans V.
7. Let $v_1, v_2, \ldots, v_n \in V(F)$, a vector space. Show that $L(\{v_1, v_2, \ldots, v_n\}) = L_1(\{a_1 v_1, a_2 v_2, \ldots, a_n v_n\})$, $a_i \neq 0$ in F and $L(\{v_1, v_2\}) = L(\{v_1 - v_2, v_1 + v_2\})$
8. Show that $\{1, i\}$ forms a basis of $\mathbf{C}(\mathbf{R})$.
9. Show that $\{(1, 1, 0), (1, 0, 1), (0, 1, 1)\}$ and $\{(1, -1, 1), (0, 1, 1), (1, 1, 1)\}$ both form basis of $\mathbf{R}^3(\mathbf{R})$.
10. Show that the identity map $i : V \to V$ s.t., $i(x) = x$ and zero map $O : V \to V$ s.t., $O(x) = 0$ are linear transformations.
11. Show that every set of three vectors in $\mathbf{R}^2(\mathbf{R})$ is *L.D.*

12. Show that $W_1 = \{(a, b, 0, 0) \mid a, b \in F\}$, $W_2 = \{(0, 0, c, d) \mid c, d \in F\}$ are subspaces of $F^4(F)$, F a field such that $F^4 = W_1 \oplus W_2$.
13. Let W be a subspace of a vector space $V(F)$. For $a, b \in V$, define $a \equiv b \bmod W$(a is congruent to b modulo W) iff $a - b \in W$ and $\alpha(a - b) \in W$, for all $\alpha \in F$. Show that this relation is an equivalence relation on V and for any $a \in W$, $cl(a) = W + a$.
14. Extend the set $S = \{(1, 1, 0)\}$ to form two different bases of $\mathbf{R}^3(\mathbf{R})$.
15. Let S be a finite subset of a vector space V such that S is *L.I.* and every proper superset of S in V is *L.D.* Show that S is a basis of V.
16. Find two subspaces A and B of $\mathbf{R}^4(\mathbf{R})$ such that dim $A = 2$, dim $B = 3$ and dim $(A \cap B) = 1$.
17. Let F be a field. Let $A = \{(x, y, 0) \mid x, y \in F\}$, $B = \{(0, y, z) \mid y, z \in F\}$ be subspaces of $F^3(F)$. Find dimension of the subspace $A + B$.
18. Let W be the subspace of $\mathbf{R}^3$ $(\mathbf{R})$, spanned by $\{(1, 0, 0), (0, 1, 0)\}$. Find a complement of W.
19. Let S be a set of four vectors such that any three of them are *L.I.* Does it follow that the four vectors are *L.I.*?

    [No. Consider (1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)].
20. Let W_1 and W_2 be subspaces of $\mathbf{R}^n$ such that every vector in $\mathbf{R}^n$ is the sum of a vector in W_1 and a vector in W_2. Let B_1 and B_2 be basis for W_1 and W_2 respectively. Under what condition is $B_1 \cup B_2$ a basis of $\mathbf{R}^n$?

    $[W_1 \cap W_2 = (0)]$
21. Prove that if $S = \{v_1, v_2, \ldots\ldots, v_n\}$ is a basis of a vector space $V(F)$ and $S' = \{w_1, w_2, \ldots\ldots, w_m\}$ is a *L.I.* subset of V then $m \leq n$.

Inner Product Spaces

In general a vector space is defined over an arbitrary field F and this is what we did earlier. In this section we restrict F to the field of real or complex numbers. In the first case, the vector space is called real vector space and in the second case it is called a complex vector space. We study real vector spaces in analytical geometry and vector analysis. There we discuss the concept of length and orthogonality. We also have dot or scalar product of two vectors which among other things satisfies the following

(*i*) $\vec{v}.\vec{v} \geq 0$ and $(\vec{v}.\vec{v}) = 0 \Leftrightarrow \vec{v} = 0$

(*ii*) $\vec{v}.\vec{w} = \vec{w}.\vec{v}$

(*iii*) $\vec{u}.(\alpha\vec{v} + \beta\vec{w}) = \alpha(\vec{u}.\vec{v}) + \beta(\vec{u}.\vec{w})$

where $\vec{u}, \vec{v}, \vec{w}$ are vectors and α, β real numbers.

We wish to extend the concept of dot product to complex vector spaces also. We define a map on $V \times V$ to F (where V = vector space over F) with same property as dot product, called inner product and study the concept of length and orthogonality.

Definition : Let V be a vector space over field F (where F = field of real or complex numbers). Suppose for any two vectors $u, v \in V \exists$ an element $(u, v) \in F$ s.t., [(u, v) here is just an element of F and should not be confused with the ordered pair.]

$$(i)\ (u, v) = \overline{(v, u)} \text{ (i.e., complex conjugate of } (v, u))$$

$$(ii)\ (u, u) \geq 0 \text{ and } (u, u) = 0 \Leftrightarrow u = 0$$

$$(iii)\ (\alpha u + \beta v, w) = \alpha(u, w) + \beta(v, w)$$

for any $u, v, w \in V$ and $\alpha, \beta \in F$.

Then V is called an *inner product space* and the function satisfying (i), (ii) and (iii) is called an *inner product.*

Thus inner product space is a vector space over the field of real or complex numbers with an inner product function.

Remarks :

1. Property (ii) in the definition of inner product space makes sense in as much as $(u, u) = \overline{(u, u)}$ by $(i) \Rightarrow (u, u)$ = real.
2. Property (iii) can also be described by saying that inner product is a linear map in 1st variable.
3. Can we say that inner product is linear in 2nd variable?

   Let's evaluate

$$(u, \alpha v + \beta w) = \overline{(\alpha v + \beta w, u)} \text{ by } (i)$$

$$= \bar{\alpha}\,\overline{(v, u)} + \bar{\beta}\,\overline{(w, u)}$$

$$= \bar{\alpha}\,(u, v) + \bar{\beta}\,(u, w)$$

So, it need not be linear in 2nd variable.

4. If F = field of real numbers, then the function inner product satisfies same properties as dot product seen earlier.
5. Inner product space over real field is called *Euclidean space* and over complex field is called *Unitary space.*

Example 17 : Let $V = F^{(n)}$, F = field of complex numbers.

Let $\quad u = (\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$

$\quad v = (\beta_1, \beta_2, \ldots\ldots, \beta_n)$ in $F^{(n)}$

define $\quad (u, v) = \alpha_1 \overline{\beta_1} + \ldots\ldots + \alpha_n \overline{\beta_n}$

It can be easily shown that (u, v) defines an inner product, called standard inner product.

Example 18 : Let $V = \mathbf{R}^{(2)}$, $u = (\alpha_1, \alpha_2)$, $v = (\beta_1, \beta_2)$

Define $$(u, v) = \alpha_1\beta_1 - \alpha_2\beta_1 - \alpha_1\beta_2 + 4\alpha_2\beta_2$$

Then

(*i*) $(u, v) = (v, u) = \overline{(v, u)}$

(*ii*) $(u, u) = (\alpha_1 - \alpha_2)^2 + 3\alpha_2^2 \geq 0$

$$(u, u) = 0 \Leftrightarrow \alpha_1 = \alpha_2, \alpha_2 = 0$$
$$\Leftrightarrow \alpha_1 = 0 = \alpha_2$$
$$\Leftrightarrow u = (\alpha_1, \alpha_2) = (0, 0) = 0$$

(*iii*) $(\alpha u + \beta u, w) = \alpha(u, w) + \beta(v, w)$

can be easily verified.

Thus, (u, v) defines an inner product.

Example 19 : One may construct a new inner product from a given one. Let V, W be vector spaces over F and T, a one-one linear transformation from V into W. Suppose $(,)$ is an inner product on W. Then

$$< u, v > = (T(u), T(v))$$

defines an inner product on V as

(*i*) $<\overline{v, u}> = \overline{(T(v), T(u))}$

$$= (T(u), T(v))$$
$$= < u, v >$$

(*ii*) $< u, v > = (T(u), T(u)) \geq 0$

and $< u, u > = 0 \Leftrightarrow (T(u), T(u)) = 0$

$$\Leftrightarrow T(u) = 0 \Leftrightarrow u = 0 \text{ as } T \text{ is } 1-1$$

(*iii*) $< \alpha u + \beta v, w > = (T(\alpha u + \beta v), T(w))$

$$= (\alpha T(u) + \beta T(v), T(w))$$
$$= \alpha(T(u), T(w)) + \beta(T(v), T(w))$$
$$= \alpha < u, w > + \beta < v, w >$$

Problem 18 : *Let V be an inner product space. Show that*

(*i*) $(0, v) = 0$ *for all* $v \in V$

(*ii*) $(u, v) = 0$ *for all* $v \in V \Rightarrow u = 0$

Solution :

(*i*) $(0, v) = (0 . 0, v)$

$$= 0\ (0, v) = 0$$

(*ii*) $(u, v) = 0$ for all $v \in V$

$$\Rightarrow (u, u) = 0 \Rightarrow u = 0.$$

Problem 19 : *Let W_1, W_2 be two subspaces of a vector space V. If W_1, W_2 are inner product spaces, show that $W_1 + W_2$ is also an inner product space.*

Solution : Let $x, y \in W_1 + W_2$.

Then $\quad x = u_1 + u_2$

$y = v_1 + v_2 \qquad u_1, v_1 \in W_1;\ u_2, v_2 \in W_2$

Define $\quad < x, y > = (u_1, v_1) + (u_2, v_2)$

Then

(*i*) $\overline{< y, x >} = \overline{(v_1, u_1) + (v_2, u_2)}$

$= \overline{(v_1, u_1)} + \overline{(v_2, u_2)}$

$= (u_1, v_1) + (u_2, v_2)$

$= < x, y >$

(*ii*) $< x, x > = (u_1, u_1) + (u_2, u_2) \geq 0$

and $< x, x > = 0 \Leftrightarrow (u_1, u_1) = 0 = (u_2, u_2)$

$\Leftrightarrow u_1 = 0 = u_2$

$\Leftrightarrow x = 0$

(*iii*) $< \alpha x + \beta y, z > = \alpha < x, z > + \beta < y, z >$

can be easily verified.

$\therefore$ $< x, y >$ defines an inner product on $W_1 + W_2$

So, $W_1 + W_2$ is an inner product space.

Norm of a vector

Let V be an inner product space. Let $v \in V$. Then *norm* of v (or length of v) is defined as $\sqrt{(v, v)}$ and is denoted by $||v||$.

Problem 20 : $||\alpha v|| = |\alpha|\ ||v||$ *for all* $\alpha \in F,\ v \in V$

Solution : $\quad ||\alpha v||^2 = (\alpha v, \alpha v)$

$= \alpha \bar{\alpha} (v, v)$

$= |\alpha|^2\ ||v||^2$

$\Rightarrow ||\alpha v|| = |\alpha|\ ||v||$

We now prove an important inequality known as *Cauchy Schwarz inequality.*

Theorem 28 : *Let V be an inner product space.*

Then $\quad |(u, v)| \leq ||u||\ ||v||$ *for all* $u, v \in V$.

Proof : If $u = 0$, then $(u, v) = (0, v) = 0$

and $\quad ||u|| = \sqrt{(u, u)} = \sqrt{(0, 0)} = 0$

$\therefore \quad$ L.H.S. = R.H.S.

Let $u \neq 0$. Then $||u|| \neq 0$

(as $||u|| = 0 \Rightarrow \sqrt{(0, 0)} = 0$

$\Rightarrow (u, u) = 0 \Rightarrow u = 0$)

Let $$w = v - \frac{(v, u)}{\|u\|^2} u$$

Then $$(w, w) = \left(v - \frac{(v, u)}{\|u\|^2} u, v - \frac{(v, u)}{\|u\|^2} u \right)$$

$$= (v, v) - \frac{(v, u)}{\|u\|^2} (u, v)$$

$$= \| v \|^2 - \frac{\overline{(u, v)}\,(u, v)}{\|u\|^2} = \| v \|^2 - \frac{|(u, v)|^2}{\|u\|^2}$$

$$= \frac{\|u\|^2 \|v\|^2 - |(u, v)|^2}{\|u\|^2}$$

Since $(w, w) \geq 0$,

$$|(u, v)|^2 \leq \| u \|^2 \| v \|^2$$

$$\Rightarrow |(u, v)| \leq \| u \| \| v \|.$$

Remark : The above inequality will be an equality if and only if u, v are linearly dependent.

Proof : Suppose $|(u, v)| = \| u \| \| v \|$

If $u = 0$, then $u = 0\ v \Rightarrow u$, v are linearly dependent.

Let $u \neq 0$. Then from above

$$(w, w) = 0 \Rightarrow w = 0$$

$$\therefore \quad v - \frac{(v, u)}{\|u\|^2} u = 0$$

$$\Rightarrow v = \frac{(v, u)}{\|u\|^2} u \Rightarrow u, v \text{ are linearly dependent.}$$

Conversely, let $u = \alpha v$, $\alpha \in F$

Then $$|(u, v)| = |\alpha (v, v)| = |\alpha| \| v \|^2$$

$$\| u \| \| v \| = |\alpha| \| v \| \| v \| = |\alpha| \| v \|^2$$

$$\therefore \quad |(u, v)| = \| u \| \| v \|.$$

Theorem 29 : *Let V be an inner product space.*

Then (i) $\| x + y \| \leq \| x \| + \| y \|$ *for all* $x, y \in V$

(Triangle inequality)

(*ii*) $\| x + y \|^2 + \| x - y \|^2 = 2 (\| x \|^2 + \| y \|^2)$

(*Parallelogram Law*)

Proof : (*i*) $\| x + y \|^2 = (x + y, x + y)$

$$= (x, x) + (y, x) + (x, y) + (y, y)$$

$$= \| x \|^2 + \overline{(x, y)} + (x, y) + \| y \|^2$$

$$= \| x \|^2 + 2Re\ (x, y) + \| y \|^2$$

$$\leq \| x \|^2 + 2 \mid (x, y) \mid + \| y \|^2$$

$$\leq \| x \|^2 + 2 \| x \| \| y \| + \| y \|^2$$

$$= (\| x \| + \| y \|)^2$$

Hence, $\| x + y \| \leq \| x \| + \| y \|$

This is called triangle inequality as

$\| x \| + \| y \| =$ sum of the lengths of two sides of a triangle

$\| x + y \| =$ length of the third side of the triangle showing that sum of two side of a triangle is less than its third side.

(*ii*) $\| x + y \|^2 + \| x - y \|^2$

$$= (x + y, x + y) + (x - y, x - y)$$

$$= \| x \|^2 + \| y \|^2 + (x, y) + (y, x) + \| x \|^2 + \| y \|^2 - (x, y) - (y, x)$$

$$= 2 (\| x \|^2 + \| y \|^2)$$

Note : $\| x + y \|^2 + \| x - y \|^2 =$ sum of squares of legnths of diagonals of a parallelogram

$2(\| x \|^2 + \| y \|^2) =$ sum of squares of sides of a parallelogram.

$\therefore$ sum of squares of lengths of diagonals of a parallelogram is equal to sum of squares of lengths of its sides. For this reason (*ii*) is called parallelogram law.

Problem 21 : *Using Cauchy Schwarz inequality, prove that cosine of an angle is of absolute vale at most* 1.

Solution : Let F = field of real numbers and $V = F^{(3)}$

Consider standard inner product on V.

Let $u = (x_1, y_1, z_1),\ v = (x_2, y_2, z_2) \in V$

$O = (0, 0, 0)$

Let θ be an angle between OU and OV.

Then
$$\cos \theta = \frac{x_1x_2 + y_1y_2 + z_1z_2}{\sqrt{x_1^2 + y_1^2 + z_1^2}\ \sqrt{x_2^2 + y_2^2 + z_2^2}} = \frac{(u, v)}{\|u\| \|v\|}$$

$\therefore$
$$| \cos \theta | = \frac{|(u, v)|}{\|u\| \|v\|} \leq \frac{\|u\| \|v\|}{\|u\| \|v\|} = 1$$

Orthogonality

Let V be an inner product space. Two vectors $u, v \in V$ are said to be *orthogonal* if $(u, v) = 0 \Leftrightarrow (v, u) = 0$. So, u is orthogonal to v iff v is orthogonal to u. Since $(0, v) = 0$ for all $v \in V$, 0 is orthogonal to every vector in V.

Conversely, if $u \in V$ is orthogonal to every vector in V, then $(u, u) = 0 \Rightarrow u = 0$.

Let W be a subspace of V.

Define $W^{\perp} = \{v \in V \mid (v, w) = 0 \text{ for all } w \in W\}$ ($W^{\perp}$ is read as W perpendicular). Then $W^{\perp}$ is a subspace of V as $0 \in W^{\perp} \Rightarrow W^{\perp} \neq \varphi$ and $v_1, v_2 \in W^{\perp}$, $\alpha, \beta \in F$

$\Rightarrow (\alpha v_1 + \beta v_2, w) = \alpha(v_1, w) + \beta(v_2, w) = 0$ for all $w \in W$

$\Rightarrow \alpha v_1 + \beta v_2 \in W^{\perp}$.

$W^{\perp}$ is called *orthogonal complement* of W. The reason for calling it thus is because we shall prove later that $V = W \oplus W^{\perp}$.

Problem 22 : *Let V be an inner product space. Let $x, y \in V$ s.t. $x \perp y$ Then show that $\|x+y\|^2 = \|x\|^2 + \|y\|^2$. (This is Pythagoras Theorem when $F = R$ as in triangle ABC with $AB \perp BC$, $AB^2 = \|x\|^2$, $BC^2 = \|y\|^2$, $AC^2 = \|x+y\|^2$)*

Solution :
$$\begin{aligned}\|x+y\|^2 &= (x + y, x + y)\\ &= (x, x) + (y, y) + (x, y) + (y, x)\\ &= \|x\|^2 + \|y\|^2 \text{ as } (x, y) = 0 = (y, x).\end{aligned}$$

Orthonormal Set

A set $\{u_i\}_i$ of vectors in an inner product space V is said to be orthogonal if $(u_i, u_j) = 0$ for $i \neq j$. If further $(u_i, u_i) = 1$ for all i, then the set $\{u_i\}$ is called an *orthonormal set*.

Example 20 : Let V be the real vector space of real polynomials of degree less than or equal to n. Define an inner product on V by

$$\left(\sum_{i=0}^{n} a_i x^i, \sum_{j=1}^{n} b_j x^i\right) = \sum_{1}^{n} a_i b_j$$

Then $\{1, x, \ldots\ldots, x^n\}$ is an orthonormal subset of V.

Theorem 30 : *Let S be an orthogonal set of non zero vectors in an inner product space V. Then S is a linearly independent set.*

Proof : To show S is linearly independent, we have to show that every finite subset of S is linearly independent.

Let $\{v_1, \ldots\ldots, v_n\}$ be a finite subset of S.

Let $\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n = 0$, $\alpha_i \in F$

$\therefore$ $(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n, \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n) = 0$

$$\Rightarrow |\alpha_1|^2 \|v_1\|^2 + \ldots\ldots + |\alpha_n|^2 \|v_n\|^2 = 0$$
$$\Rightarrow |\alpha_i|^2 \|v_i\|^2 = 0 \text{ for all } i = 1, \ldots\ldots, n$$
$$\Rightarrow |\alpha_i|^2 = 0 \text{ for all } i \text{ as } \|v_i\|^2 = 0 \Rightarrow \|v_i\| = 0 \Rightarrow v_i = 0$$

which is not true

$$\Rightarrow \alpha_i = 0 \text{ for all } i = 1, \ldots\ldots, n$$
$$\Rightarrow S \text{ is linearly independent.}$$

Cor. : An orthonormal set in an inner product space is linearly independent.

Proof : Let S be an orthonormal set in an inner product space V. Let $v \in S$. Then $v \neq 0$ as $v = 0 \Rightarrow (v, v) = 0 \neq 1$, a contradiction. Therefore, S is an orthogonal set of non zero vectors and so linearly independent.

Theorem 31 : (Gram-Schmidt Orthogonalisation process)

Let V be a non zero inner product space of dimension n. Then V has an orthonormal basis.

Proof : It is enough to construct an orthogonal basis of V. For let $S \subseteq V$ be an orthogonal set. Then $T = \left\{ \frac{x}{\|x\|} \middle| x \in S \right\}$ is an orthonormal set.

Let $\{v_1, \ldots\ldots, v_n\}$ be a basis of V.

Let $w_1 = v_1$. Define $w_2 = v_2 - \frac{(v_2, w_1)}{(w_1, w_1)} w_1$

$$= v_2 - \frac{(v_2, v_1)}{(v_1, v_1)} v_1$$

Then $\quad (w_2, w_1) = (w_2, v_1)$

$$= (v_2, v_1) - \frac{(v_2, v_1)}{(v_1, v_1)} (v_1, v_1) = 0$$

Also $\quad v_2 = \alpha_1 v_1 + w_2 = \alpha_1 w_1 + w_2$

where $\quad \alpha_1 = \frac{(v_2, v_1)}{(v_1, v_1)} \in F$

(Note v_1, is linearly independent $\Rightarrow v_1 \neq 0 \Rightarrow (v_1, v_1) \neq 0$)

Define $\quad w_3 = v_3 - \frac{(v_3, w_2)}{(w_2, w_2)} w_2 - \frac{(v_3, w_1)}{(w_1, w_1)} w_1$

Then $\quad (w_3, w_2) = 0 = (w_3, w_1)$

Also $\quad v_3 = \alpha_1 w_1 + \alpha_2 w_2 + w_3$, where $\alpha_1, \alpha_2 \in F$

In this way, we can construct an orthogonal set $\{w_1, \ldots\ldots, w_n\}$ where each $v_i = \alpha_1 w_1 + \ldots\ldots + w_i, \quad \alpha_i \in F$

$\therefore \left\{\frac{w_1}{\|w_1\|}, \ldots\ldots, \frac{w_n}{\|w_n\|}\right\}$ is an orthonormal set which is linearly independent by Cor. to Theorem 30 and hence forms a basis of V as $\dim V = n$.

Problem 23 : *Obtain an orthonormal basis, w.r.t. the standard inner product for the subspace of* $\mathbf{R}^3$ *generated by* (1, 0, 3) *and* (2, 1, 1).

Solution : Let $v_1 = (1, 0, 3)$, $v_2 = (2, 1, 1)$

Then $$w_1 = v_1, \quad w_2 = v_2 - \frac{(v_2, w_1)}{(w_1, w_1)} w_1$$

Now $$(v_2, w_1) = (v_2, v_1) = 2 + 0 + 3 = 5$$
$$(w_1, w_1) = (v_1, v_1) = 1 + 0 + 9 = 10$$

$\therefore$ $$\| w_1 \| = \sqrt{10}$$

So, $$w_2 = (2, 1, 1) - \frac{5}{10}(1, 0, 3) = \left(\frac{3}{2}, 1, -\frac{1}{2}\right)$$

$\therefore$ $$\| w_2 \| = \sqrt{\frac{9}{4} + 1 + \frac{1}{4}} = \sqrt{\frac{7}{2}}$$

$\therefore$ required orthonormal basis is

$$\left\{\frac{w_1}{\|w_1\|}, \frac{w_2}{\|w_2\|}\right\} = \left\{\frac{1}{\sqrt{10}}(1, 0, 3), \frac{\sqrt{2}}{7}\left(\frac{\sqrt{3}}{2}, 1, -\frac{1}{2}\right)\right\}$$

Theorem 32 : (Bessel's inequality)

If $\{w_1, \ldots\ldots, w_m\}$ *is an orthonormal set in* V, *then*

$$\sum_{i=1}^{m} |(w_i, v)|^2 \leq \|v\|^2 \text{ for all } v \in V.$$

Proof : Let $x = v - \sum_{i=1}^{m} (v, w_i) w_i$

$\therefore$ $$(x, w_j) = (v, w_j) - (v, w_j) = 0 \text{ for all } j = 1, \ldots\ldots, m$$

Let $$w = \sum_{i=1}^{m} (v, w_i) w_i = \sum_{i=1}^{m} \alpha_i w_i, \quad \alpha_i = (v, w_i)$$

$\therefore$ $$v = x + w$$

Also $$(w, x) = (\alpha_1 w_1 + \ldots\ldots + \alpha_m w_m, x)$$
$$= \alpha_1 (w_1, x) + \ldots\ldots + \alpha_m (w_m, x) = 0$$

Now $\quad \| v \|^2 = (v, v)$

$$= (w + x, w + x)$$
$$= (w, w) + (x, x)$$
$$= \| w \|^2 + \| x \|^2 \geq \| w \|^2$$

But $\quad \| w \|^2 = (w, w)$

$$= (\alpha_1 w_1 + \ldots\ldots + \alpha_m w_m, \alpha_1 w_1 + \ldots\ldots + \alpha_m w_m)$$
$$= \alpha_1 \overline{\alpha_1} (w_1, w_1) + \ldots\ldots + \alpha_m \overline{\alpha_m} (w_m, w_m)$$
$$= | \alpha_1 |^2 + \ldots\ldots + | \alpha_m |^2$$

as $\{w_1, \ldots\ldots, w_m\}$ is an orthonormal set

$$= \sum_{i=1}^{m} | \alpha_i |^2 = \sum_{i=1}^{m} | (v, w_i) |^2 = \sum_{i=1}^{m} \left| \overline{(w_i, v)} \right|^2 = \sum_{i=1}^{m} | (w_i, v) |^2$$

$$\therefore \quad \sum_{i=1}^{m} | (w_i, v) |^2 \leq \| v \|^2 \text{ for all } v \in V.$$

Cor. : Equality holds if and only if $v = w$.

Proof : Suppose $v = w$

Then $\quad \| v \|^2 = \| w \|^2 = \sum_{i=1}^{m} | (w_i, v) |^2.$

Conversely, suppose equality holds

Then $\quad \| v \|^2 = \| w \|^2$

$$\Rightarrow \| x \|^2 = 0 \Rightarrow (x, x) = 0 \Rightarrow x = 0$$
$$\Rightarrow v = w + x = w.$$

Theorem 33 : *If V is a finite dimensional inner product space and W is a subspace of V, then $V = W \oplus W^{\perp}$.*

Proof : Since V is an inner product spare, so is W. By theorem 31, W has an orthonormal basis $\{w_1, \ldots\ldots, w_m\}$.

Let $v \in V$.

Let $w = \sum_{i=1}^{m} (v, w_i)$, $w_i \in W$ and $x = v - w$

Then $(x, w_j) = 0$ as in theorem 32, for all $j = 1, \ldots\ldots, m$

$$\therefore \quad (x, w) = (x, \beta_1 w_1 + \ldots\ldots + \beta_m w_m)$$
$$= \overline{\beta_1} (x, w_1) + \ldots\ldots + \overline{\beta_m} (x, w_m)$$
$$= 0 \text{ for all } w \in W$$

$$\therefore \quad x \in W^{\perp}$$

So, $\quad v = w + x \in W + W^{\perp}$

$\therefore \quad V \subseteq W + W^{\perp}$

$\Rightarrow V = W + W^{\perp}$

Let $\quad y \in W \cap W^{\perp} \Rightarrow (y, w) = 0$ for all $w \in W$, $y \in W$

$\Rightarrow (y, y) = 0$ as $y \in W$

$\Rightarrow y = 0$

$\therefore \quad W \cap W^{\perp} = \{0\}$

Hence $\quad V = W \oplus W^{\perp}$.

Problem 24 : *If W is a subspace of V and $v \in V$ satisfies*

$$(v, w) + (w, v) \leq (w, w) \text{ for all } w \in W$$

prove that $(v, w) = 0$ for all $w \in W$, where V is an inner product space over F.

Solution : Let n be a $+ve$ integer

Then $\quad w \in W \Rightarrow \dfrac{w}{n} \in W$

$$\therefore \quad \left(v, \frac{w}{n}\right) + \left(\frac{w}{n}, v\right) \leq \left(\frac{w}{n}, \frac{w}{n}\right)$$

$$\therefore \quad (v, w) + (w, v) \leq \frac{1}{n}(w, w)$$

Let $\quad n \to \infty$

Then $\quad (v, w) + (w, v) \leq 0 \quad$ for all $w \in W$

$\therefore \quad (v, -w) + (-w, v) \leq 0 \quad$ for all $w \in W$

$\Rightarrow -[(v, w) + (w, v)] \leq 0 \quad$ for all $w \in W$

$\Rightarrow (v, w) + (w, v) \geq 0 \quad$ for all $w \in W$

$\Rightarrow (v, w) + (w, v) = 0 \quad$ for all $w \in W$

If $F \subseteq \mathbf{R}$, then $(w, v) = (v, w)$

$\Rightarrow (v, w) + (v, w) = 0$

$\Rightarrow 2(v, w) = 0 \quad$ for all $w \in W$

$\Rightarrow (v, w) = 0 \quad$ for all $w \in W$

If $F \subseteq \mathbf{C}$, then $(v, iw) + (iw, v) = 0$ for all $w \in W$

$\Rightarrow -i\,(v, w) + i\,(w, v) = 0 \quad$ for all $w \in W$

$\Rightarrow -i\,[z - \bar{z}] = 0,\ z = (v, w) = x + iy$

$\Rightarrow -i\,(2iy) = 0$

$\Rightarrow y = 0$

$\Rightarrow z = (v, w) = \text{real} \quad$ for all $w \in W$

$\Rightarrow (v, w) + (v, w) = 0$

$$\Rightarrow 2(v, w) = 0$$

$$\Rightarrow (v, w) = 0 \text{ for all } w \in W.$$

Problem 25 : *If V is a finite dimensional inner product space and $f \in V$, prove that $\exists\, u_0 \in V$ s.t. $f(v) = (v, u_0)$ for all $v \in V$. Also show that u_0 is uniquely determined.*

Solution : Let $\{v_1, \ldots\ldots, v_n\}$ be an orthonormal basis for V. Let $v \in V$.

Then $\quad v = \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n, \qquad \alpha_i \in F$

Let $\quad f(v_i) = \beta_i,\ i = 1, 2, \ldots\ldots, n$

Define $\quad u_0 = \overline{\beta_1} v_1 + \ldots\ldots + \overline{\beta_n} v_n \in V$

Then $\quad (v, u_0) = (\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n, \overline{\beta_1} v_1 + \ldots\ldots + \overline{\beta_n} v_n)$

$$= \alpha_1\beta_1 + \ldots\ldots + \alpha_n\beta_n \text{ as } (v_i, v_j) = \delta_{ij}$$

$$= f(v) \text{ for all } v \in V$$

Suppose $\quad \exists\, u_0' \in V$ s.t. $f(v) = (v, u_0')$

Then $\quad (v, u_0) = (v, u_0')$ for all $v \in V$

$$\Rightarrow (v, u_0 - u_0') = 0 \text{ for all } v \in V$$

$$\Rightarrow (u_0 - u_0', u_0 - u_0') = 0$$

$$\Rightarrow u_0 = u_0'$$

$\therefore \quad u_0$ is uniquely determined.

Exercises

Throughout these exercises V stands for inner product space with inner product (,).

1. Show that $(x, z) = (y, z)$ for all $z \in V \Rightarrow x = y$.
2. Consider standard inner product on $\mathbf{R}^2$.

   Suppose $\alpha = (1, 2)$, $\beta = (-1, 1) \in \mathbf{R}^2$. If $\gamma \in \mathbf{R}^2$ be s.t. $(\alpha, \gamma) = -1$ and $(\beta, \gamma) = 3$, find γ.
3. Show that for any $\alpha \in \boldsymbol{R}^2$

   $$\alpha = (\alpha, \epsilon_1)\epsilon_1 + (\alpha, \epsilon_2)\epsilon_2$$

   where $\epsilon_1 = (1, 0), \epsilon_2 = (0, 1)$.
4. Let $u = (x_1, x_2)$ and $v = (y_1, y_2) \in \mathbf{R}^2$

   (*i*) Verify that the following is an inner product on $\mathbf{R}^2$

   $$(u, v) = x_1y_1 - 2x_1y_2 - 2x_2y_1 + 5x_2y_2$$

   (*ii*) For what values of k is the following an inner product on $\mathbf{R}^2$

   $$(u, v) = x_1y_1 - 3x_1y_2 - 3x_2y_1 + kx_2\, y_2. \qquad \text{(Ans. } k > 9\text{)}$$

(*iii*) For what values of $a, b, c, d \in \mathbf{R}$ is the following an inner product on $\mathbf{R}^2$.

$$(u, v) = ax_1 y_1 + cx_1 y_2 + dx_2 y_1 + bx_2 y_2$$

(Ans. $c^2 < ab$, $a \geq 0$, $b \geq 0$ $c = d$)

5. Show that $\| x \| - \| y \| \leq \| x - y \|$ for all $x, y \in V$.

6. Obtain an orthonormal basis w.r.t. standard inner product for the subspace of $\mathbf{R}^4$ generated by (1, 0, 2, 0) and (1, 2, 3, 1).

$$\left[\text{Ans.} \left\{\left(\frac{1}{\sqrt{5}}, 0, \frac{2}{\sqrt{5}}, 0\right), \left(\frac{-2\sqrt{26}}{5\sqrt{5}}, \frac{2\sqrt{26}}{\sqrt{5}}, \frac{\sqrt{26}}{5\sqrt{5}}, \frac{\sqrt{26}}{\sqrt{5}}\right)\right\}\right]$$

7. Obtain an orthonormal basis for V, the space of all real polynomials of degree at most 2, the inner product defined by

$$(f, g) = \int_0^1 f(x)\, g(x)\, dx$$

(Ans. $\{1, \sqrt{12}\,(x - \frac{1}{2}), 180\,(x^2 - x + \frac{1}{6})\}$)

8. Let $\{u_1, \ldots\ldots, u_r\}$ be an orthonormal set in V. Show that for any $v \in V$, the vector

$$w = v - (v, u_1)\, u_1 - \ldots\ldots - (v, u_r)\, u_r$$

is orthogonal to each of the u_i.

9. Let W be the set of real valued functions $y = f(x)$ satisfying $\dfrac{d^2y}{dx^2} + 4y = 0$.

Prove that W is two dimensional real vector space.

Define $(y, z) = \int_0^\pi yzdz$ in W. Find an orthonormal basis of W.

$$\left(\text{Ans.} \left\{\frac{\sqrt{2}}{\pi} \sin 2x, \frac{\sqrt{2}}{\pi} \cos 2x\right\}\right)$$

10. Let V be the vector space of real valued functions $y = f(x)$ satisfying

$$\frac{d^3y}{dx^3} - \frac{6d^2y}{dx^2} + 11\frac{dy}{dx} - 6y = 0$$

Prove that V is a 3-dimenisonal vector space over $\mathbf{R}$. Define

$$(f, g) = \int_{-\infty}^0 fgdx \text{ in } V$$

Find an orthonormal basis of V over $\mathbf{R}$.

(Ans. $\sqrt{2}\, e^x$, $2\,(3e^{2x} - 2e^x)$, $(3e^x - 12e^{2x} + 10e^{3x})\sqrt{6}$)

Chapter 10

Linear Transformations

We defined a linear transformation (homomorphism) in the previous chapter and proved a few results pertaining to it, including a few on isomorphisms. We now come back to it and study it in little more detail. To recall the definition, by a linear transformation (*L.T.*) we mean a map $T: V \to W$, s.t., $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ where $x, y \in V$, $\alpha\ \beta \in F$ and V, W are vector spaces over the field F. We urge the reader to go through the definitions and results done earlier, especially on kernel and range of a *L.T.* Also, we'll be dealing with vector spaces that are finite dimensional, unless mentioned otherwise.

Theorem 1 : *A L.T. $T: V \to V$ is one-one iff T is onto.*

Proof : Let $T: V \to V$ be one-one. Let dim $V = n$.

Let $\{v_1, v_2, \ldots\ldots, v_n\}$ be a basis of V, then $\{T(v_1), \ldots\ldots\ldots, T(v_n)\}$ will also be a basis of V as

$$\alpha_1 T(v_1) + \alpha_2 T(v_2) + \ldots\ldots + \alpha_n T(v_n) = 0$$

$$\Rightarrow T(\alpha_1 v_1 + \ldots\ldots\ldots + \alpha_n v_n) = T(0) \qquad (T \text{ a } L.T.)$$

$$\Rightarrow \alpha_1 v_1 + \ldots\ldots\ldots + \alpha_n v_n = 0 \qquad (T \text{ is 1-1})$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i$$

thus $T(v_1), \ldots\ldots\ldots, T(v_n)$ are *L.I.* and as dim $V = n$ the result follows (Theorem done earlier).

Let now $v \in V$ be any element

then
$$v = a_1 T(v_1) + a_2 T(v_2) + \ldots\ldots\ldots + a_n T(v_n) \qquad \alpha_i \in F$$
$$= T(a_1 v_1 + \ldots\ldots\ldots + a_n v_n)$$
$$= T(v') \text{ for some } v'$$

Hence T is onto.

Conversely, let T be onto.

Here again we show that if $\{v_1, v_2, \ldots\ldots\ldots, v_n\}$ is a basis of V then so also is $\{T(v_1), T(v_2), \ldots\ldots, T(v_n)\}$

For any $v \in V$, since T is onto, $\exists$ some $v' \in V$ s.t.,

$$T(v') = v$$

Again $v' \in V$ means $v' = \sum \alpha_i v_i \qquad \alpha_i \in F$

$$\therefore \qquad v = T(v') = T(\sum \alpha_i v_i) = \sum \alpha_i T(v_i)$$

$$\Rightarrow T(v_1), T(v_2), \ldots\ldots, T(v_n) \text{ span } V$$

and as $\dim V = n$, $\{T(v_1), \ldots\ldots, T(v_n)\}$ forms a basis of V.

Now if $v \in \text{Ker } T$ be any element

then $\qquad T(v) = 0$

$$\Rightarrow T(\sum \alpha_i v_i) = 0$$

$$\Rightarrow \sum \alpha_i T(v_i) = 0$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i \text{ as } T(v_1), \ldots\ldots, T(v_n) \text{ are } L.I.$$

$$\Rightarrow v = \sum \alpha_i v_i = 0$$

$$\Rightarrow \text{Ker } T = \{0\} \Rightarrow T \text{ is 1-1.}$$

Theorem 2 : *Let V and W be two vector spaces over F. Let $\{v_1, v_2, \ldots\ldots, v_n\}$ be a basis of V and $w_1, w_2, \ldots\ldots, w_n$ be any vectors in W (not essentially distinct). Then there exists a unique L.T.*

$$T : V \to W \text{ s.t., } T(v_i) = w_i \qquad i = 1, 2, \ldots\ldots, n.$$

Proof : Let $v \in V$ be any element, then $v = \sum_{i=1}^{n} \alpha_i v_i, \qquad \alpha_i \in F$

as $\{v_1, v_2, \ldots\ldots, v_n\}$ is a basis of V.

Define $\qquad T : V \to W$ s.t.,

$$T(v) = \sum \alpha_i w_i$$

Then T is a linear transformation (Verify!).

Clearly here, $T(v_i) = T(ov_1 + \ldots\ldots + 1 \,.\, v_i + \ldots\ldots + ov_n) = 1w_i$ for all i

To show uniqueness let T′ be any other *L.T.* from

$$V \to W \text{ s.t. } T'(v_i) = w_i$$

Let $v \in V$ be any element, then $v = \sum \alpha_i v_i$

$$T'(v) = T'(\sum \alpha_i v_i) = \sum \alpha_i T'(v_i) = \sum \alpha_i w_i = T(v)$$

Hence $\qquad T' = T.$

Thus we notice that a linear transformation is completely determined by its values on the elements of a basis.

Definition : Let $T: V \to W$ be a L.T.

then we define Rank of $T = \dim \text{Range } T = r(T)$

Nullity of $T = \dim \text{Ker } T = \nu(T)$.

Theorem 3 : (Sylvester's Law) : *Let $T: V \to W$ be a L.T., then Rank T + Nullity T = dim V.*

Proof : Let $\{x_1, x_2, \ldots, x_m\}$ be a basis of Ker T then $\{x_1, x_2, \ldots, x_m\}$ being *L.I.* in Ker T will be *L.I.* in V. Thus it can be extended to form a basis of V.

Let $\{x_1, x_2, \ldots, x_m, v_1, v_2, \ldots, v_n\}$ be the extended basis of V.

Then $\dim \text{Ker } T = \text{nullity of } T = m$

$\dim V = m + n$

we show $\{T(v_1), T(v_2), \ldots, T(v_n)\}$ is a basis of Range T

Now $\alpha_1 T(v_1) + \alpha_2 T(v_2) + \ldots + \alpha_n T(v_n) = 0$

$\Rightarrow T(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 \ldots + \alpha_n v_n \in \text{Ker } T$

$\Rightarrow \alpha_1 v_1 + \ldots + \alpha_n v_n = \beta_1 x_1 + \ldots + \beta_m x_m$

or $\alpha_1 v_1 + \ldots + \alpha_n v_n + (-\beta_1) x_1 + \ldots + (-\beta_m) x_m = 0$

$\Rightarrow \alpha_1 = \alpha_2 = \ldots = \beta_1 = \ldots = \beta_m = 0$

$\Rightarrow \alpha_i = 0$ for all i

i.e., $\{T(v_1), T(v_2), \ldots, T(v_n)\}$ is L.I.

Now if $T(v) \in \text{Range } T$ be any element then as $v \in V$

$$v = a_1 x_1 + \ldots + a_m x_m + b_1 v_1 + \ldots + b_n v_n \qquad a_i, b_j \in F$$

$$\therefore \quad T(v) = a_1 T(x_1) + \ldots + a_m T(x_m) + b_1 T(v_1) + \ldots + b_n T(v_n)$$

$$= 0 + \ldots + 0 + b_1 T(v_1) + \ldots + b_n T(v_n) \quad [\text{as } x_i \in \text{Ker } T]$$

or that $T(v)$ is a liner combination of $T(v_1), \ldots, T(v_n)$

which, therefore, form a basis of Range T.

$\therefore$ $\dim \text{Range } T = n = \text{rank } T$

which proves the theorem.

Theorem 4 : *If $T: V \to V$ be a L.T. Show that the following statements are equivalent.*

(*i*) *Range $T \cap$ Ker T = $\{0\}$*

(*ii*) *If $T(T(v)) = 0$ then $T(v) = 0$, $v \in V$*

Proof : (*i*) $\Rightarrow$ (*ii*)

$T(T(v)) = 0 \Rightarrow T(v) \in \text{Ker } T$

Also $T(v) \in \text{Range } T$ (by definition)

$\Rightarrow T(v) = 0.$

(*ii*) $\Rightarrow$ (*i*) Let $x \in \text{Range } T \cap \text{Ker } T$

$\Rightarrow x \in \text{Range } T$ and $x \in \text{Ker } T$

$\Rightarrow x = T(v)$ for some $v \in V$

and $\quad T(x) = 0$

$$x = T(v) \Rightarrow T(x) = T(T(v))$$
$$\Rightarrow 0 = T(T(v))$$
$$\Rightarrow T(v) = 0 \text{ (given condition)}$$
$$\Rightarrow x = 0.$$

Algebra Of Linear Transformations

Let V and W be two vector spaces over the same field F. Let $T: V \to W$ and $S: V \to W$ be two linear transformations. We define $T + S$, the sum of T and S by

$$T + S : V \to W, \text{ s.t.}$$
$$(T + S)v = T(v) + S(v), \quad v \in V$$

Then $T + S$ is also a L.T. from $V \to W$ as

$$(T + S)(\alpha x + \beta y) = T(\alpha x + \beta y) + S(\alpha x + \beta y)$$
$$= \alpha T(x) + \beta T(y) + \alpha S(x) + \beta S(y)$$
$$= \alpha(T + S)\ x + \beta(T + S)y$$

Again for $\alpha \in F$, we define the product of a *L.T.* $T: V \to W$ with α, by $(\alpha T): V \to W$ s.t., $(\alpha T)v = \alpha(T(v))$.

It is easy to see that αT is a also a *L.T.* from $V \to W$. Let Hom (V, W) be the set of all linear transformations from $V \to W$. Then we show Hom (V, W) forms a vector space over F under the addition and scalar multiplication as defined above.

We have already seen that when $T, S \in$ Hom (V, W), $\alpha \in F$ then $T + S$, $\alpha T \in$ Hom (V, W), thus closure holds for these operations. We verify some of the other conditions in the definition.

$$(T + S)\ v = T(v) + S(v) = S(v) + T(v) = (S + T)v \text{ for all } v \in V$$
$$\Rightarrow T + S = S + T \text{ for all } S, T \in \text{Hom}(V, W)$$

The map $O: V \to W$, s.t., $O(v) = 0$ is a L.T. and

$$(T + O)v = T(v) + O(v) = T(v) = (O + T)v \text{ for all } v$$

thus O is zero of Hom (V, W)

For any $T \in$ Hom (V, W), the map $(-T): V \to W$, s.t.,

$$(-T)v = -T(v)$$

willl be additive inverse of T.

Again, $[\alpha(T + S)]\ v = \alpha\ [(T + S)\ v] = \alpha\ [T(v) + S(v)] = \alpha T(v) + \alpha S(v)$

$$= (\alpha T)\ v + (\alpha S)\ v = (\alpha T + \alpha S)v \quad \text{for all } v \in V$$
$$\Rightarrow \alpha(T + S) = \alpha T + \alpha S$$
$$[(\alpha\beta)\ T]\ v = (\alpha\beta)\ T(v) = \alpha\ [\beta T(v)] = [\alpha(\beta T)]v \quad \text{for all } v$$
$$\Rightarrow (\alpha\beta)T = \alpha(\beta T)$$
$$(1T)\ v = 1\ .\ T(v) = T(v) \quad \text{for all } v$$
$$\Rightarrow 1\ .\ T = T$$

Hence one notices that Hom (V, W) forms a vector space over F.

Note : The notation $L(V, W)$ is also used for denoting Hom (V, W)

Definition : Product (composition) of two linear transformations

Let V, W, Z be three vector spaces over a field F

Let $T: V \to W, \quad S: W \to Z$ be $L.T.$

We define $ST: V \to Z$, s.t.,

$$(ST)v = S(T(v))$$

then ST is a linear transformation (verify!), called product of S and T

Note : TS may not be defined and even if it is defined it may not equal ST.

Definition : A $L.T.$ $T: V \to V$ is called a *linear operator* on V, whereas a $L.T.$ $T: V \to F$ is called a *linear functional*. We use notation T^2 for $T.T$ and $T^n = T^{n-1}T$ etc.

Theorem 5 : *Let T, T_1, T_2 be linear operators on V, and let $I: V \to V$ be the identity may $I(v) = v$ for all v (which is clearly a L.T.) then*

(*i*) $IT = TI = T$

(*ii*) $T(T_1 + T_2) = TT_1 + TT_2$

$(T_1 + T_2)T = T_1T + T_2T$

(*iii*) $\alpha(T_1T_2) = (\alpha T_1)T_2 = T_1(\alpha T_2) \qquad \alpha \in F$

(*iv*) $T_1(T_1T_2) = (T_1T_2)T_3$.

Proof : (*i*) Obvious.

(*ii*) $[T(T_1 + T_2)]x = T[(T_1+T_2)x] = T[T_1(x) + T_2(x)]$

$= T(T_1(x)) + T(T_2(x)) = TT_1(x) + TT_2(x)$

$= (TT_1+TT_2)x$

$\Rightarrow T(T_1+T_2) = TT_1+TT_2$

Other result follows similarly.

(*iii*) $[\alpha(T_1T_2)]\ x = \alpha\ [(T_1T_2)x] = \alpha[T_1(T_2(x))]$

$[(\alpha T_1)T_2]\ x = (\alpha T_1)\ [T_2(x)] = \alpha[T_1(T_2(x)]$

$[T_1(\alpha T_2)]x = T_1((\alpha T_2)x = T_1(\alpha T_2(x)) = \alpha T_1(T_2(x))]$

Hence the result follows.

(*iv*) Follows easily by defintion.

See exercises for the generalised version of above theorem.

Theorem 6 : *Let V and W be two vector spaces (over F) of dim m and n respectively. Then Hom (V, W) has dim mn.*

Proof : Let $\{v_1, v_2, \ldots v_m\}$ and $\{w_1, w_2, \ldots, w_n\}$ be basis of V and W respectively. Define mappings $T_{ij}: V \to W$, s.t

$$T_{ij}(v) = \alpha_i w_j \qquad \begin{array}{l} 1 \le i \le m \\ 1 \le j \le n \end{array}$$

where $v \in V$ is any element and therefore,

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots \alpha_m v_m \text{ for some } \alpha_i \in F$$

(Thus we have defined mn mappings)

Note also that $T_{ij}(v_k) = 0$ if $k \neq i$

$= w_j$ if $k = i$

We show T_{ij} are $L.T.$

Let $x, y \in V$ then $x = \sum_1^m \alpha_i v_i$, $y = \sum_1^m \beta_i v_i$ $\quad \alpha_i, \beta_i \in F$

Now
$$\begin{aligned} T_{ij}(x + y) &= T_{ij}[(\alpha_1 v_1 + \ldots + \alpha_m v_m) + (\beta_1 v_1 + \ldots + \beta_m v_m)] \\ &= T_{ij}(\alpha_1 + \beta_1) v_1 + \ldots + (\alpha_m + \beta_m) v_m] \\ &\quad T_{ij}(\gamma_1 v_1 + \ldots + \gamma_m v_m) \\ &= \gamma_i w_j \\ &= (\alpha_i + \beta_i) w_j = \alpha_i w_j + \beta_i w_j = T_{ij}(x) + T_{ij}(y) \end{aligned}$$

Also,
$$\begin{aligned} T_{ij}(\lambda x) &= T_{ij}(\lambda(\alpha_1 v_1 + \ldots + \alpha_m v_m)) \\ &= T_{ij}(\lambda\alpha_1 v_1 + \ldots + \lambda\alpha_m v_m) \\ &= (\lambda\alpha_i) w_j = \lambda(\alpha_i w_j) = \lambda T_{ij}(\sum \alpha_i v_i) \\ &= \lambda T_{ij}(x) \end{aligned}$$

Hence $T_{ij} \in \text{Hom}(V, W)$, and these are mn in number. We claim $S = \{T_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ forms a basis of $\text{Hom}(V, W)$

Suppose

$\beta_{11}T_{11} + \beta_{12}T_{12} + \ldots + \beta_{1n}T_{1n} + \beta_{21}T_{21} + \beta_{22}T_{22} + \ldots\ldots + \beta_{2n}T_{2n} + \ldots + \beta_{m1}T_{m1} + \beta_{m2}T_{m2} + \ldots + \beta_{mn}T_{mn} = 0$, $\beta_{ij} \in F$

[where 0 is, of course, zero of Hom (V, W)]

By operating on v_1, we get

$$\beta_{11}T_{11}(v_1) + \beta_{12}T_{12}(v_1) + \ldots + \beta_{1n}T_{1n}(v_1) + \beta_{21}T_{21}(v_1) + \ldots\ldots = 0$$

$\Rightarrow \beta_{11}w_1 + \beta_{12}w_2 + \ldots\ldots + \beta_{1n}w_n + 0 + \ldots + 0 + \ldots = 0$

But $w_1, w_2, \ldots, w_n$ are $L.I.$

$\Rightarrow \beta_{11} = \beta_{12} = \ldots \beta_{1n} = 0$

Similarly, by operating on v_2 we'll get $\beta_{21} = \beta_{22} = \ldots \beta_{2n} = 0$

Thus by operating on $v_3, v_4 \ldots$ we find that all the coefficients are zero and hence S is $L.I.$

Let Now $T \in \text{Hom}(V, W)$ be any element, then

$T : V \to W$ is a $L.T.$

We show T is a linear combination of T_{ij}

Consider v_1, then $T(v_1) \in W$ and thus is a linear combination of $w_1, w_2, \ldots w_n$

Let $T(v_1) = \alpha_{11}w_1 + \alpha_{12}w_2 + \ldots \alpha_{1n}w_n$

Put $T_0 = \alpha_{11}T_{11} + \alpha_{12}T_{12} + \ldots + \alpha_{1n}T_{1n} + \alpha_{21}T_{21} + \alpha_{22}T_{22} + \ldots + \alpha_{mn}T_{mn}$

(where α_{11}, α_{12}..... are, of course, the same as before)

Then $$T_0(v_1) = \alpha_{11}T_{11}(v_1) + \alpha_{12}T_{12}(v_1) + \ldots$$
$$= \alpha_{11}w_1 + \alpha_{12}w_2 + \alpha_{1n}w_n + 0 + 0 + \ldots\ldots + 0$$
$$\Rightarrow T_0(v_1) = T(v_1)$$

Similarly proceeding with $v_2, v_3, \ldots\ldots v_m$ we get

$$T_0(v_2) = T(v_2)$$
$$\ldots\ldots\ldots$$
$$T_0(v_m) = T(v_m)$$

Thus T_0 and T agree on all elements of the basis of V.

$\Rightarrow$ T_0 and T agree on all elemnts of $V \Rightarrow T_0 = T$

But T_0 is a linear combination of members of S

$\Rightarrow$ T is a linear combination of memebers of S

$\Rightarrow$ S spans Hom (V, W)

or that S forms a basis of Hom (V, W)

Hence $$\dim \text{Hom}(V, W) = mn.$$

Cor : Obviously $\dim \text{Hom}(V, V) = m^2$ where $\dim V = m$ and $\dim \text{Hom}(V, F) = m.1 = m$ as $\dim F(F) = 1$ as F is generated by 1 and thus $\{1\}$ is a basis of $F(F)$.

Problem 1 : *Find the range, rank , Ker and nullity of the following linear transformations*

(*a*) $T: \mathbf{R}^2 \to \mathbf{R}^3$ s.t. $T(x_1, x_2) = (x_1, x_1 + x_2, x_2)$

(*b*) $T: \mathbf{R}^4 \to \mathbf{R}^3$ s.t., $T(x_1, x_2, x_3, x_4) = (x_1 - x_4, x_2 + x_3, x_3 - x_4)$

Solution (*a*) : From definition of T, we notice elements of the type $(x_1, x_1 + x_2, x_2)$ will have pre images in $\mathbf{R}^2$ i.e., elements of this type are in Range T.

Now $$(x_1, x_1 + x_2, x_2) = (x_1 + 0, x_1 + x_2, 0 + x_2)$$
$$= (x_1, x_1, 0) + (0, x_2, x_2)$$
$$= x_1(1, 1, 0) + x_2(0, 1, 1)$$

or that Range T is spanned by $\{(1, 1, 0\}, (0, 1, 1)\}$ and since

$$\alpha_1(1,1, 0) + \alpha_2(0, 1, 1) = (0, 0, 0)$$
$$\Rightarrow \alpha_1 = \alpha_2 = 0$$

these are *L.I.* and thus form a basis of Range T

$$\Rightarrow \text{Rank } T = \dim \text{Range } T = 2.$$

Again $$(x_1, x_2) \in \text{Ker } T \Rightarrow T(x_1, x_2) = (0, 0,0)$$
$$\Rightarrow (x_1, x_1 + x_2, x_2) = (0, 0, 0)$$
$$\Rightarrow x_1 = 0, x_1 + x_2 = 0, x_2 = 0$$
$$\Rightarrow x_1 = x_2 = 0$$
$$\Rightarrow \text{Ker } T = \{(0, 0)\}$$

Also then $$\text{nullity } T = \dim \text{Ker } T = 0.$$

(*b*) : From definiton of T. we find elements of the type $(x_1-x_4, x_2+x_3, x_3-x_4)$ have pre image in $\mathbf{R}^4$.

Now

$(x_1- x_4,\ x_2+x_3,\ x_3 - x_4) = (x_1+0+0-x_4,\ 0+x_2+x_3+0,\ 0+0+x_3-x_4)$

$= x_1(1,0,0) + x_2\ (0,1,0) + x_3(0,1,1) + x_4(-1,0,-1)$

or that Range T is spanned by

$\{(1,0,0),\ (0,1,0),\ (0,1,1),\ (-1,0,-1)\}$

Since Range T is a subspace of $\mathbf{R}^3$ which has dim 3 these four elements cannot form basis of Range T.

In fact these are *L.D.*, elements as

$$(-1,0,-1) + (1,0,0) + (0,1,0) + (0,1,1) = (0,0,0)$$

If we consider three members

$$(1,0,0),\ (0,1,0),\ (0,1,1)$$

we notice $\quad \alpha_1(1,0,0) + \alpha_2(0,1,0) + \alpha_3(0,1,1) = (0,0,0)$

$\Rightarrow \alpha_i = 0$ for all i

or that $(1,0,0)$, $(0,1,0)$ $(0,1,1)$ are *L.I* and hence form basis of Range T

$\Rightarrow$ dim Range $T = 3 = 3$ rank of T

one might notice here that as

$$(-1,0,-1) = -1\ (1,0,0)\ -1\ (0,1,0)\ -1\ (0,1,1)$$

the elements $(1,0,0)$, $(0,1,0)$, $(0,1,1)$ span Range T

Also then $\quad$ Range $T = \mathbf{R}^3$

Again $\quad (x_1,\ x_2,\ x_3,\ x_4) \in \text{Ker}\, T \Rightarrow T(x_1,\ x_2,\ x_3,\ x_4) = (0,0,0)$

$\Rightarrow x_1 - x_4 = 0$

$x_2 + x_3 = 0$

$x_3 - x_4 = 0$

if we fix x_4, we get $x_1 = x_4$, $x_2 = -x_3 = -x_4$, $x_3 = x_4$

or that elements of the type $(x_4, -x_4, x_4, x_4)$ are in the Ker T

i.e., Ker T is spanned by $(1,-1,1,1)$

this being *L.I.* forms basis of Ker T

$\Rightarrow$ dim Ker $T = 1$

$\Rightarrow$ nullity of $T = 1$.

Problem 2 : *Let F be a subfield of complex numbers and T a function from $F^3 \to F^3$ defined by*

$$T(x_1,\ x_2,\ x_3) = (x_1 - x_2 + 2x_3,\ 2x_1 + x_2, -x_1 - 2x_2 + 2x_3)$$

(*i*) *Shows that T is a L.T.*

(*ii*) *What are the conditions on a, b, c such that (a, b, c) be in the null space of T? Find nullity of T.*

Solution :

$$T[(x_1, x_2, x_3) + (y_1, y_2, y_3)] = T(x_1+y_1, x_2+y_2, x_3+y_3)$$
$$= (x_1+y_1-x_2-y_2+2x_3+2y_3,\ 2x_1+2y_1+x_2+y_2,$$
$$-x_1-y_1-2x_2-y_2+2x_3+2y_3)$$

Also

$$T(x_1, x_2, x_3) + T(y_1, y_2, y_3) = (x_1-x_2+2x_3, 2x_1+x_2, -x_1-2x_2+2x_3)$$
$$+ (y_1-y_2+2y_3,\ 2y_1+y_2, -y_1-2y_2+2y_3)$$
$$= (x_1-x_2+2x_3+y_1-y_2+2y_3,\ 2x_1+x_2+2y_1+y_2$$
$$-x_1-2x_2+2x_3-y_1-2y_2+2y_3)$$
$$= (x_1+y_1-x_2-y_2+2x_3+2y_3,\ 2x_1+2y_1+x_2+y_2,$$
$$-x_1-y_1-2x_2-y_2+2x_3+2y_3)$$

Thus $\quad T((x_1, x_2, x_3) + (y_1, y_2, y_3)) = T(x_1, x_2, x_3) + T(y_1, y_2, y_3)$

It is easy to see that for any α

$$T(\alpha(x_1, x_2, x_3)) = \alpha T(x_1, x_2, x_3)$$

Thus T is a *L.T.*

Now if $(a, b, c) \in \text{Ker}\, T$ then $T(a, b, c) = (0, 0, 0)$

$$\Rightarrow (a-b+2c,\ 2a+b, -a-2b+2c) = (0, 0, 0)$$
$$\Rightarrow a-b+2c=0$$
$$2a+b = 0$$
$$-a-2b+2c = 0$$

Since
$$\begin{vmatrix} 1 & -1 & 2 \\ 2 & 1 & 0 \\ -1 & -2 & 2 \end{vmatrix} = 0$$

The above equations have a non zero solution.

Solving the equiations, we find

$$\begin{bmatrix} 1 & -1 & 2 \\ 2 & 1 & 0 \\ -1 & -2 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$R_2 \to R_2 - 2R_1,\ R_3 \to R_3 + R_1$$

$$\begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -4 \\ 0 & -3 & 4 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$R_3 \to R_3 + R_2$$

$$\begin{bmatrix} 1 & -1 & 2 \\ 0 & 3 & -4 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

$$\Rightarrow \quad a - b + 2c = 0$$
$$3b - 4c = 0$$

Since rank of coefficeint matrix is 2, the number of *L.I.* solutions is $3 - 2T = 1$.

If we take $c = k$, we get $a = -\frac{2k}{3}$, $b = \frac{4k}{3}$, $c = k$ as solution of the given equations. In other words a, b, c should satisfy the relation $\frac{a}{-2} = \frac{b}{4} = \frac{c}{3}$ for (a, b, c) to be in Ker T.

Now $(-2, 4, 3)$ is one memeber of Ker T and all other memebers would be multiples of this, i.e., $\{(-2, 4, 3)\}$ generates Ker T. Since $(-2, 4, 3)$ being non zero is *L.I.* $\{(-2, 4, 3\}$ forms a basis of Ker T or that dim Ker T = nullity T = 1

In fact, the result $\dim V = \dim \text{Range } T + \dim \ker T$ will then give us $\dim \text{Range } T = \text{rank } T = 2$ as $\dim V = \dim F^3 = 3$. (See exercises).

Problem 3 : *If $T_1, T_2 \in Hom\ (V, W)$ then show that*

(*i*) $r(\alpha(T_1)) = r(T_1)$ *for all* $\alpha \in F$, $\alpha \neq 0$

(*ii*) $|r(T_1) - r(T_2)| \leq r(T_1 + T_2) \leq r(T_1) + r(T_2)$

where $r(T)$ means rank of T.

Solution (i) : $T_1 : V \to W$

thus $T_1(V) = \text{range } T_1$, is a subspace of W

Now $\quad (\alpha T_1)v = \alpha(T_1(v)) \in T_1(V) \quad$ for all $v \in V$

$$\Rightarrow (\alpha T_1)V \subseteq T_1(V) \qquad \ldots (1)$$

Again as $\alpha \neq 0$, α^{-1} exists and thus

$$(\alpha^{-1}T_1)\ V \subseteq T_1(V)$$
$$\alpha(\alpha^{-1}T_1)V \subseteq \alpha T_1(V)$$
$$\Rightarrow T_1(V) \subseteq \alpha T_1(V) \Rightarrow T_1(V) = \alpha T_1(V) \quad \text{by (1)}$$
$$\Rightarrow \dim T_1(V) = \dim \alpha T_1(V)$$

or $\quad r(T_1) = r(\alpha T_1)$.

(ii) : Since $\quad (T_1 + T_2)x = T_1(x) + T_2(x) \quad$ for all $x \in V$

$$(T_1 + T_2)V \subseteq T_1(V) + T_2(V)$$
$$\Rightarrow \dim [(T_1+T_2)V] \leq \dim [T_1(V) + T_2(V)]$$
$$\leq \dim T_1(V) + \dim T_2(V)$$
$$\Rightarrow r(T_1 + T_2) \leq r(T_1) + r(T_2)$$

Again $\quad T_1 = (T_1 + T_2) - T_2 = (T_1 + T_2) + (-T_2)$

$$\Rightarrow r(T_1) = r(T_1 + T_2) + (-T_2))$$
$$\leq r(T_1 + T_2) + r(-T_2) = r(T_1 + T_2) + r(T_2)$$
(using (1) $\alpha = -1$)

$$\Rightarrow r(T_1) - r(T_2) \leq r(T_1 + T_2)$$

Similarly $\quad r(T_2) - r(T_1) \leq r(T_1 + T_2)$

$$\Rightarrow |r(T_1) - r(T_2)| \leq r(T_1 + T_2) \leq r(T_1) + r(T_2)$$

Problem 4 : *Let T be a linear operator on V. If $T^2 = 0$, what can you say about the relation of the range of T to the null space of T? Give an example of linear operator T of $\mathbf{R}^2$ such that $T^2 = 0$, but $T \neq 0$.*

Solution : $T^2 = 0 \Rightarrow T^2(v) = 0$ for all $v \in V$

$$\Rightarrow T(T(V)) = 0$$
$$\Rightarrow T(v) \in \text{Ker } T \quad \text{for all } v \in V$$
$$\Rightarrow \text{range } T \subseteq \text{Ker } T.$$

Define $T : \mathbf{R}^2 \to \mathbf{R}^2$, such that

$$T(x_1, x_2) = (x_2, 0)$$

then T is a linear operator (Verify!)

Since $\quad T(2, 2) = (2, 0) \neq (0, 0)$

$$T \neq 0$$

But $\quad T^2(x_1, x_2) = T(T(x_1, x_2)) = T(x_2, 0) = (0, 0)$

$$\Rightarrow T^2 = 0.$$

Problem 5 : *Let T be a linear operator on V and let Rank T^2 = Rank T then show that Range $T \subseteq$ Ker T = $\{0\}$.*

Solution : $T : V \to V$, $T^2 : V \to V$

$$\text{Rank } T^2 = \dim V - \dim \text{ Ker } T^2$$
$$\Rightarrow \dim \text{ Ker } T = \dim \text{ Ker } T^2$$

we claim $\quad \text{Ker } T = \text{Ker } T^2$

$$x \in \text{Ker } T \Rightarrow T(x) = 0 \Rightarrow T^2(x) = T(0) = 0$$
$$\Rightarrow x \in \text{Ker } T^2 \Rightarrow \text{Ker } T \subseteq \text{Ker } T^2$$
$$\Rightarrow \text{Ker } T = \text{Ker } T^2 \text{ (as they have same dim)}$$

Now $\quad x \in \text{Range } T \cap \text{Ker } T \Rightarrow x \in \text{Range } T$ and $x \in \text{Ker } T$

$$\Rightarrow T(x) = 0, \; x = T(y) \text{ for some } y \in V$$
$$\Rightarrow T(T(y)) = 0$$
$$\Rightarrow T^2(y) = 0$$
$$\Rightarrow y \in \text{Ker } T^2 = \text{Ker } T$$
$$\Rightarrow T(y) = 0 \Rightarrow x = 0$$
$$\Rightarrow \text{Ker } T \cap \text{Range } T = \{0\}.$$

Invertible Linear Transformations

We recall that a map $T: V \to W$ is invertible iff it is 1-1 onto, and inverse of T is the map $T^{-1}: W \to V$ such that

$$T^{-1}(y) = x \Leftrightarrow T(x) = y$$

We show that inverse of a (1–1 onto) *L.T.* is also a *L.T.* Let $T: V \to W$ be a 1-1 onto *L.T.* and $T^{-1}: W \to V$ be its inverse.

We have to prove

$$T^{-1}(\alpha w_1 + \beta w_2) = \alpha T^{-1}(w_1) + \beta T^{-1}(w_2) \qquad \alpha, \beta \in F, w_1, w_2 \in W$$

Since T is onto, for $w_1, w_2 \in W$, $\exists\, v_1, v_2 \in V$ such that $T(v_1) = w_1$, $T(v_2) = w_2$

$$\Leftrightarrow v_1 = T^{-1}(w_1),\ v_2 = T^{-1}(w_2)$$

Now
$$\begin{aligned} T^{-1}(\alpha w_1 + \beta w_2) &= T^{-1}(\alpha T(v_1) + \beta T(v_2)) \\ &= T^{-1}(T(\alpha v_1) + T(\beta v_2)) \\ &= T^{-1}(T(\alpha v_1 + \beta v_2)) \\ &= \alpha v_1 + \beta v_2 \\ &= \alpha T^{-1}(w_1) + \beta T^{-1}(w_2). \end{aligned}$$

Definition : A *L.T.* $T: V \to W$ is called *non-singular* if Ker $T = \{0\}$ i.e. if T is 1-1.

Theorem 7 : *A linear transforamtion $T: V \to W$ is non singular iff T carries each L.I. subset of V onto a L.I. subset of W.*

Proof : Let T be non-singluar and $\{v_1, v_2 ..., v_n\}$ be a L.I. subset of V. we show $\{T(v_1), T(v_2) ....., T(v_n)\}$ is *L.I* subset of W.

Now
$$\alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0 \qquad a_i \in F$$
$$\Rightarrow T(\alpha_1 v_1 + ... + \alpha_n v_n) = 0$$
$$\Rightarrow \alpha_1 v_1 + ... \alpha_n v_n = \text{Ker}\, T = \{0\}$$
$$\Rightarrow \alpha_1 v_1 + ... \alpha_n v_n = 0$$
$$\Rightarrow \alpha_i = 0 \text{ for all } i \text{ as } v_1, v_2 ....., v_n \text{ are } L.I.$$

Conversely, let $v \in \text{Ker}\, T$ be any element

Then
$$T(v) = 0$$
$$\Rightarrow \{T(v)\} \text{ is not } L.I \text{ in } W$$
$$\Rightarrow v \text{ is not } L.I \text{ in } V.$$
$$\Rightarrow v = 0 \Rightarrow \text{Ker}\, T = \{0\}$$
$$\Rightarrow T \text{ is non singular.}$$

Theorem 8 : *Let $T: V \to W$ be a L.T. where V and W are two F.D.V.S. with same dimension. Then the following are equivalent*

(*i*) *T is invertible*

(*ii*) *T is non singular (i.e. T is 1-1)*

(*iii*) *T is onto (i.e., Range $T = W$)*

(*iv*) *If* $\{v_1, v_2, \ldots, v_n\}$ *is a basis of* V *then* $\{T(v_1), T(v_2), \ldots, T(v_n)\}$ *is a basis of* W.

Proof : (*i*) $\Rightarrow$ (*ii*) follows by definition.

(*ii*) $\Rightarrow$ (*iii*) T is non - singular

$$\Rightarrow \text{Ker } T = \{0\}$$

$$\Rightarrow \dim \text{Ker } T = 0$$

Since $\dim \text{Range } T + \dim \text{Ker } T = \dim V$, we get

$$\dim \text{Range } T = \dim V$$

$$\Rightarrow \dim \text{Range } T = \dim W \text{ (given condition)}$$

But Range T being a subspace of W, we find

$$\text{Range } T = W$$

(*iii*) $\Rightarrow$ (*i*) T onto means Range $T = W$

$$\Rightarrow \dim \text{Range } T = \dim W = \dim V$$

and as $\dim \text{Range } T + \dim \text{Ker } T = \dim V$, we get

$$\dim \text{Ker } T = 0$$

$$\Rightarrow \text{Ker } T = \{0\}$$

or that T is 1-1 and as it is onto T will be invertible.

(*i*) $\Rightarrow$ (*iv*) T is invertible $\Rightarrow$ T is 1-1 onto

i.e, T is an isomorphism, so result follows as done in theorem 23, chapter 9.

(*iv*) $\Rightarrow$ (*i*)

Let $\{T(v_1), \ldots, T(v_n)\}$ be basis of W where $\{v_1, \ldots v_n\}$ is basis of V. Any $w \in W$ can be put as

$$w = \alpha_1 T(v_1) + \ldots + \alpha_n T(v_n)$$

$$= T(\alpha_1 v_1 + \ldots + \alpha_n v_n) = T(v) \text{ for some } v \in V$$

$\therefore$ T is onto. Thus (*iii*) holds.

Hence (*i*) holds.

Problem 6 : *Let* T *be a linear operator on* $\mathbf{R}^3$, *defined by*

$$T(x_1, x_2, x_3) = (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3)$$

show that T *is invertible and find the rule by which* T^{-1} *is defined.*

Solution : $T : \mathbf{R}^3 \to \mathbf{R}^3$

Let $(x_1, x_2, x_3) \in \text{Ker } T$ be any element

Then $T(x_1, x_2, x_3) = (0, 0, 0)$

$$\Rightarrow (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3) = (0, 0, 0)$$

$$\Rightarrow 3x_1 = 0, \; x_1 - x_2 = 0, \; 2x_1 + x_2 + x_3 = 0$$

$$\Rightarrow x_1 = x_2 = x_3 = 0 \text{ or that Ker } T = \{(0, 0, 0)\}$$

$\Rightarrow$ T is non singular and thus invertible (See theorem 8)

Now if (z_1, z_2, z_3) be any element of $\mathbf{R}^3$, then (x_1, x_2, x_3) will be its image under T if

$$T(x_1, x_2, x_3) = (z_1, z_2, z_3)$$
$$\Rightarrow 2x_1 = z_1$$
$$x_1 - x_2 = z_2$$
$$2x_1 + x_2 + x_3 = z_3$$

which give $x_1 = \frac{z_1}{3}$, $x_2 = \frac{z_1}{3} - z_2$, $z_3 = z_3 - z_1 + z_2$

Hence $T^{-1} : \mathbf{R}^3 \to \mathbf{R}^3$ is defined by

$$T^{-1}(z_1, z_2, z_3) = \left(\frac{z_1}{3}, \frac{z_1}{3} - z_2, z_3 - z_1 + z_2\right).$$

Problem 7 : *If $T : V \to V$ is a L.T., such that T is not onto, then show that there exists some $0 \neq v$ in V s.t., $T(v) = 0$.*

Solution : Since T is not onto, it is not 1–1 (theorem done)

Suppose $\exists$ no $0 \neq v \in V$ s.t., $T(v) = 0$

Then $T(v) = 0$ only when $v = 0$

$\Rightarrow$ Ker $T = \{0\} \Rightarrow T$ is 1-1, a contradiction.

Theorem 9 : *Let $T : V \to W$ and $S : W \to U$ be two linear transformations. Then*

(*i*) *If S and T are one-one onto then ST is one-one onto and $(ST)^{-1} = T^{-1} S^{-1}$.*

(*ii*) *If ST is one-one then T is one-one*

(*iii*) *If ST is onto then S is onto.*

Proof (i) : Since S and T are 1-1 onto, S^{-1} and T^{-1} exist.

Let $\quad ST(x) = ST(y)$

Then $\quad S(T(x)) = S(T(y))$

$\Rightarrow T(x) = T(y)$ as S is 1-1

$\Rightarrow x = y$ as T is 1-1

$\Rightarrow ST$ is 1-1.

Again $ST : V \to U$, let $u \in U$ be any element then as S in onto, $\exists\ w \in W$ s.t., $S(w) = u$ and as $T : V \to W$ is onto $\exists\ v \in V$ s.t., $T(v) = w$

Now $\quad T(v) = w \Rightarrow S(T(v)) = S(w) \Rightarrow ST(v) = u$

or that ST is onto.

Also $\quad (ST)(T^{-1}S^{-1}) = S(T(T^{-1}S^{-1})) = S(TT^{-1})S^{-1} = S(IS^{-1}) = SS^{-1} = I$

Similarly $\quad (T^{-1}S^{-1})(ST) = T^{-1}(S^{-1}(ST)) = T^{-1}(S^{-1}S)T = T^{-1}(IT) = T^{-1}T = I$

Showing that $\quad (ST)^{-1} = T^{-1} S^{-1}$.

(ii) : Let $v \in$ Ker T be any element

Then $\quad T(v) = 0$

$$\Rightarrow S(T(v) = S(0)$$
$$\Rightarrow ST(v) = 0$$
$$\Rightarrow v \in \text{Ker}\, ST \text{ and } \text{Ker}\, ST = (0) \text{ as } ST \text{ is 1-1}$$
$$\Rightarrow v = 0 \Rightarrow \text{Ker}\, T = (0) \Rightarrow T \text{ is 1-1.}$$

(iii) : Let $u \in U$ be any element. Since $ST : V \to U$ is onto, some $v \in V$ s.t., $ST(v) = u$

i.e., $$S(T(v)) = u$$

Let $T(v) = w$ and $w \in W$ such that

$$S(w) = u$$

Then S is onto.

Problem 8 : *In the above theorem show that if ST is* 1-1 *onto then T is* 1-1 *and S is onto. Again, if V, W, U are of same dimension and ST is one-one onto then so are S and T.*

Solution : First part of the problem follows by (*ii*) and (*iii*) of theorem 9.

Let now $$\dim V = \dim W = \dim U$$

The result then follows by using theorem 8 we proved earlier that if $T : V \to W$ is a *L.T.* where $\dim V = \dim W$ then T is 1-1 iff T is onto.

Problem 9 : *Let T be a linear operator on F.D.V.S. V. Suppose there is a linear operator U on V such that TU = I. Show that T is invertible and* $T^{-1} = U$.

Solution : We have $T : V \to V$, $U : V \to V$ s.t., $TU = I$ we claim U is 1-1.

Let $$U(x) = U(y)$$

Then $$T(U(x) = T(U(y))$$
$$\Rightarrow I(x) = I(y) \ (TU = I)$$
$$\Rightarrow x = y$$

or that U is 1-1 and, therefore, onto also.

Hence U is invertible.

Now $U^{-1} : V \to V$ s.t., $UU^{-1} = 1$

Thus $UT = (UT)\, I = UT(UU^{-1}) = U(TU)U^{-1} = UIU^{-1} = I$

$$\Rightarrow UT = I = TU$$
$$\Rightarrow T \text{ is invertible and } T^{-1} = U.$$

Problem 10 : *Show that the conclusion of the previous problem fails if V is not finite dimensional.*

Solution : Let V be the vector space of all polynomials in x over a field F.

Let T = differential operator on V.

i.e., $$T : V \to V, \text{ s.t.,}$$

$$T(f(x)) = \frac{d}{dx} f(x)$$

Notice this T is a linear transformation (example 11, chapter 9).

Let $U : V \to V$

$$U(f) = \int_0^x f(t)\, dt$$

Then U is a linear transformation.

Again $TU(f) = T \int_0^x f(t)\ dt = f = I(f)$

$\Rightarrow TU = 1$

Now $T(2x) = 2,\ T(2x+3) = 2$

and as $2x \neq 2x + 3$, T is not 1-1 and hence T is not invertible. Thus $UT \neq I$.

Exercises

1. Let $T : F^3 \to F^3$ be defined by
$$T(x_1, x_2, x_3) = (x_1 - x_2 + 2x_3,\ 2x_1 + x_2,\ -x_1 - 2x_2 + 2x_3)$$
then T is a *L.T.* Find the conditions on a,b,c such that (a, b, c) is in Range T. Show that rank T is 2. $[a = b + c]$
2. Show that image of a *L.I.* set by a *L.T,* need not be *L.I.* (consider zero *L.T.*).
3. Let dim $V = n$, $T : V \to V$ be a *L.T.* such that Range T = Ker T. Show that n is even. Prove that $T : \mathbf{R}^2 \to \mathbf{R}^2$, s.t., $T(x_1, x_2) = (x_2, 0)$ is such a *L.T.*
4. Find a *L.T.* $T : \mathbf{R}^3 \to \mathbf{R}^3$ such that the set of all vectors (x_1, x_2, x_3) satisfying the equation $4x_1 - 3x_2 + x_3 = 0$ is Ker T.
$[T(x_1, x_2, x_3) = (4x_1 - 3x_2 + x_3,\ 8x_1 - 6x_2 + 2x_3, 0)]$
5. Show that $f : \mathbf{R}^4 \to \mathbf{R}^4$, s.t., $f(x, y, z, t) = (2x, 3y, 0, 0)$ is a *L.T.* Find its rank and nullity.
6. Find range, rank, Ker and nullity of the *L.T.* defined by
   (*i*) $T : \mathbf{R}^2 \to \mathbf{R}^2$ s.t., $T(x_1, x_2) = (x_1 + x_2, x_1)$ $[\mathbf{R}^2, 2, (0), 0]$
   (*ii*) $T : \mathbf{R}^2 \to \mathbf{R}^3$ s.t., $T(x_1, x_2) = (x_1 + x_2, x_1 - x_2, x_2)$
   (*iii*) $T : \mathbf{R}^3 \to \mathbf{R}^2$ s.t., $T(x_1, x_2, x_3) = (x_1 - x_2, x_1 + x_3)$
   $[(1, 1, 0)\ (1, -1, 1), 2, (0), 0]$
   (*iv*) The zero and the identity linear transformations.
   (*v*) $T : \mathbf{R}^3 \to \mathbf{R}^2$, s.t., $T(x_1, x_2, x_3) = (x_1 + x_2, 2x_3 - x_1)$
7. Find the *L.T.* from $\mathbf{R}^3 \to \mathbf{R}^3$ which has its range the subspace spanned by $(1, 0, -1), (1, 2, 2)$.
8. Let G be the set of all invertible linear transformations from $V \to V$ then show that G forms a group under product of linear trnaformations.

9. Let T, T_1, T_2 be linear transformations from $V \to W$, S, S_1, S_2 from $W \to U$ and K, K_1, K_2 from $U \to Z$ where V, W, U, Z are vector spaces over a field F then show that

   (*i*) $S(T_1 + T_2) = ST_1 + ST_2$

   (*ii*) $(S_1 + S_2)T = S_1T + S_2T$

   (*iii*) $K(ST) = (KS)T$

   (*iv*) $(\alpha S)T = \alpha(ST) = S(\alpha T)$ $\alpha \in F$.

10. Let $T : \mathbf{R}^3 \to \mathbf{R}^2$, $S : \mathbf{R}^2 \to \mathbf{R}^2$ be linear transformations. Show that ST is not invertible.

11. Show that it is possible to find two linear operators T, U on $\mathbf{R}^2$ such that $TU = 0$ but $UT \neq 0$.

    (Consider $(x_1, x_2) \to (x_1, 0)$ and $(x_1, x_2) \to (0, x_1)$)

12. A linear transformation $T : V \to V$ is called *idempotent* or a *projection* if $T^2 = T$.Show that if S, T are idempotent and $ST = TS$ then ST and $S + T - ST$ are idempotent and if $ST + TS = 0$ then $S + T$ is idempotent.

13. A linear transformation $T : V \to V$ is called *nilpotent* on V if $T^n = 0$ for some integer $n > 1$. The smallest integer (> 1) for which $T^n = 0$ is called degree of nilpotence of T. Show that $T : \mathbf{R}^4 \to \mathbf{R}^4$, defined b y

    $T(x_1, x_2, x_3, x_4) = (0, 2x_1, 3x_1 + 2x_2, x_2 + 4x_3)$ is nilpotent of degree 4.

14. Show that a necessary and sufficient condition for the map $T : F^2 \to F^2$ s.t., $T(x_1, x_2) = (\alpha x_1 + \beta x_2, \gamma x_1 + \delta x_2)$, $(\alpha, \beta, \gamma, \delta)$ some fixed elements of F) to be an isomorphism is that $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0$.

15. If $O \neq T \in \text{Hom}(V, V)$ then show that there exists some $S \in \text{Hom}(V, V)$ such that TS is an idempotent.

16. Show that the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$ defined by $T(x_1, x_2, x_3) = (2x_1, x_1 - x_2, 5x_1 + 4x_2 + x_3)$ is invertible.

17. If the *L.T.* $T : \mathbf{R}^3 \to \mathbf{R}^3$ has a four dimensional Kernel, show that range of T has dimension three.

18. Let T be a *L.T.* from $\mathbf{R}^7$ onto a 3-dimensional subsapce of $\mathbf{R}^5$. Show that dim Ker $T = 4$.

Matrix of a Linear Transformation

Let $U(F)$, $V(F)$ be vector spaces of dimension n and m respectively. Let $\beta = \{u_1, \ldots, u_n\}$. $\beta' = \{v_1, \ldots v_m\}$ be their ordered basis respectively. Suppose $T : U \to V$ is a linear transformation. Since $T(u_1), \ldots, T(u_n) \in V$ and $\{v_1, \ldots, v_m\}$ span V, each $T(u_i)$ is a linear combination of vectors $v_1, \ldots, v_m$.

Let
$$T(u_1) = \alpha_{11}v_1 + \ldots \alpha_{m1}v_m$$
$$T(u_2) = \alpha_{12}\ v_1 + \ldots + \alpha_{m2}v_m$$
$$\ldots\ldots\ldots$$
$$T(u_n) = \alpha_{1n}v_1 + \ldots + \alpha_{mn}v_m$$

where each $a_{ij} \in F$. Then the $m \times n$ matrix

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \ldots & \ldots & \alpha_{1n} \\ \vdots & \vdots & \ldots & \ldots & \vdots \\ \vdots & \vdots & \ldots & \ldots & \vdots \\ \vdots & \vdots & \ldots & \ldots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \ldots & \alpha_{mn} \end{bmatrix}$$

is called matrix of T with respect to ordered basis β, β' respectively. A is uniquely determined by T as each $\alpha_{ij} \in F$ is uniquely determined. We write

$$A = [T]_{\beta,\ \beta'}$$

The word *ordered basis is very significant, for as the order of basis is changed, the entries α_{ij} will change their positions and so the corresponding matrix will be different.*

In particular if $U = V$, $\beta = \beta'$, then instead of writing $[T]_{\beta,\ \beta'}$, we write $[T]_\beta$.

Let $M_{m \times n}(F)$ denoted the vector space of all $m \times n$ matrices over F. Let Hom (U, V) denote the vector space of all linear transformations from $U(F)$ into $V(F)$. We prove

Theorem 10 : *Hom $(U, V) \cong M_{m \times n}(F)$.*

Proof : Define $\theta : \text{Hom}\ (U, V) \to M_{m \times n}(F)$, s.t.,

$$\theta(T) = [T]_{\beta,\ \beta'}$$

Where $\beta = \{u_1, \ldots u_n\}$, $\beta' = \{v_1, \ldots v_m\}$ are ordered basis of U, V respectively. θ is well defined as $[T]_{\beta,\beta'}$ is uniquely determined by T.

It is not difficult to verify that θ is a linear transformation.

Let $\qquad \theta(S) = \theta(T), \qquad S, T \in \text{Hom}\ (U, V)$

Then $\qquad [S]_{\beta,\beta'} = [T]_{\beta,\beta'}$

$$\Rightarrow (a_{ij}) = (b_{ij})$$
$$\Rightarrow a_{ij} = b_{ij} \text{ for all } i, j$$
$$\Rightarrow S(u_j) = \sum_{i=1}^{m} a_{ij}v_i = \sum_{i=1}^{m} b_{ij}v_i = T(u_j) \text{ for all } j = 1, \ldots n$$
$$\Rightarrow S = T \Rightarrow \theta \text{ is 1-1.}$$

Let $A = (a_{ij})_{m \times n} \in M_{m \times n}(F)$. Then $\exists$ a linear transformation $T \in \text{Hom}\ (U, V)$ s.t.,

$$T(u_j) = \sum_{i=1}^{m} a_{ij}v_i \qquad \text{for } j = 1, \ldots, n$$

$\therefore\ A = [T]_{\beta,\beta'} = \theta(T) \Rightarrow \theta$ is onto

$\therefore$ θ is an isomorphism and so Hom $(U, V) \cong M_{m \times n}(F)$.

Cor. : dim Hom $(U, V) = mn$.

Proof : S = set of all $m \times n$ matrices with only one entry 1 and all other entries zero, is a basis of $M_{m \times n}(F)$.

Clealy, $o(S) = mn \Rightarrow$ dim $M_{m \times n}(F) = mn$

$\therefore$ dim Hom $(U, V) = mn$.

Theorem 11 : *Let S, T be two linear transformations from V(F) into V(F). Let* β *be an ordered basis of V. Then*

$$[ST]_\beta = [S]_\beta \; [T]_\beta.$$

Proof : Let $\beta = \{v_1, \ldots, v_n\}$

Let $S(v_1) = a_{11}v_1 + \ldots a_{n1}v_1$

.....

$S(v_n) = a_{1n}v_1 + \ldots\ldots + a_{nn}v_n$

where $a_{ij} \in F$

In general, $S(v_j) = \sum_{i=1}^{n} a_{ij}v_i$ for all $j = 1, \ldots, n$

$\therefore$ $[S]_\beta = (a_{ij})$

Similarly,

$T(v_1) = b_{11}v_1 + \ldots + b_{n1}v_n$

.....

$T(v_n) = b_{1n}v_1 + \ldots\ldots + b_{nn}v_n$ where $b_{ij} \in F$

In general $T(v_k) = \sum_{j=1}^{n} b_{jk}v_j$, for all $k = 1, \ldots, n$

$\therefore$ $[T]_\beta = (b_{jk})$

$\therefore$ $ST(v_k) = S(\sum_{j=1}^{n} b_{jk}v_j) = \sum_{j=1}^{n} b_{jk} \; S(v_j)$

$$= \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij}b_{jk}) \, v_i$$

$$[ST]_\beta = (c_{ik}), \text{ where } c_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk}$$

Also, (i, k)th entry in $[S]_\beta \; [T]_\beta$

$$= \sum_{j=1}^{n} a_{ij}b_{jk} = c_{ik} = (i, k)\text{th entry in } [ST]_\beta$$

$\therefore \qquad [ST]_\beta = [S]_\beta\ [T]_\beta$

Cor. : If S is an invertible linear transformation form $V(F)$ into $V(F)$, then so is $[S]_\beta$ with respect to any basis β of V and conversely.

Proof : Since S is invertible, $\exists\ T: V \to V$ s.t., $ST = I = TS$. Let β be an ordered basis of V. Then by above theorem,

$$[ST]_\beta = [I]_\beta = I, \text{ where } T = S^{-1}$$
$$\Rightarrow [S]_\beta\ [T]_\beta = I$$
$$\Rightarrow [S]_\beta\ [S^{-1}]_\beta = I$$
$$\Rightarrow [S]^{-1}{}_\beta = [S]^{-1}{}_\beta \text{ for any basis } \beta \text{ of } V$$

Conversely, let $[S]_\beta$ be invertible. Then $\exists$ a matrix $A = (a_{ij})$ over F s.t., $[S]_\beta A = I$

Let $T: V \to V$ be a linear transformation s.t.,

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i \qquad \text{for all } j = 1,....n$$

$$\therefore \qquad [T]_\beta = A$$
$$\therefore \qquad [S]_\beta\ [T]_\beta = I$$
$$\Rightarrow [ST]_\beta = I$$
$$\Rightarrow (ST)\ (v_j) = v_j \text{ for all } j = 1,....,n$$
$$\Rightarrow (ST)\ (x) = (ST)\ (\alpha_1 v_1 + ... + \alpha_n v_n)$$
$$= \alpha_1 v_1 + ... + \alpha_n v_n$$
$$= x \text{ for all } x \in V$$
$$\Rightarrow ST = I \Rightarrow S \text{ isinvertible.}$$

We now give a relation between matrices of a linear transformation with respect to two different basis of a vector space.

Theorem 12 : *Let $T : V(F) \to V(F)$ be a linear transformation. Let $\beta = \{u_1,....u_n\}$, $\beta' = \{v_1,....v_n\}$ be two ordered basis of V. Then $\exists$ a non singular matrix P over F such that*

$$[T]_{\beta'} = P^{-1}\ [T]_\beta P.$$

Proof : Let $S: V \to V$ be a linear transformation such that $S(u_i) = v_i$ for all $i = 1,....n$.

Now $x \in \text{Ker } S \Rightarrow S(x) = 0,\ x = \alpha_1 u_1 + ... + \alpha_n u_n, \qquad \alpha_i \in F$

$$\Rightarrow S(\alpha_1 u_1 + ... + \alpha_n u_n) = 0$$
$$\Rightarrow \alpha_1 S(u_1) + ... + \alpha_n S(u_n) = 0$$
$$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = 0$$
$$\Rightarrow \alpha_i = 0 \text{ for all } i$$
$$\Rightarrow x = 0$$
$$\Rightarrow \text{Ker } S = \{0\}$$
$$\Rightarrow S \text{ is 1–1 and so onto}$$

$\therefore$ S is an isomorphism. Let $[T]_\beta = (a_{ij})$

Then $$T(u_j) = \sum_{i=1}^{n} a_{ij} u_i$$

$\therefore$ $$(STS^{-1})(v_j) = ST(u_j)$$

$$= S(\sum_{i=1}^{n} a_{ij} u_i) = \sum_{i=1}^{n} a_{ij} v_i$$

$\therefore$ $$[STS^{-1}]_{\beta'} = (a_{ij}) = [T]_\beta$$

$$\Rightarrow [S]_{\beta'} [T]_{\beta'} [S^{-1}]_{\beta'} = [T]_\beta$$

$$\Rightarrow [S]_{\beta'} [T]_{\beta'} [S]_\beta^{-1} = [T]_\beta$$

$$\Rightarrow [T]_\beta = [S]_{\beta'}^{-1} [T]_\beta [S]_{\beta'}$$

$$= P^{-1} [T]_\beta P, \text{ where } P = [S]_{\beta'}$$

Problem 11 : *Let T be a linear operator on $\mathbf{C}^2$ defined by $T(x_1, x_2) = (x_1, 0)$ Let $\beta = \{\epsilon_1 = (1, 0), \epsilon_2 = (0, 1)\}$, $\beta' = \{\alpha_1 = (1, i), \alpha_2 = (-i, 2)\}$ be ordered basis for $\mathbf{C}^2$. What is the matrix of T relative to the pair β, β'?*

Solution : Now $T(\epsilon_1) = T(1, 0)$

$$= (1, 0)$$

$$= a(1, i) + b(-i, 2)$$

$$\Rightarrow a - bi = 1 \text{ where } a, b \in \mathbf{C}$$

$$ai + 2b = 0$$

$$\Rightarrow a = 2, \ b = -i$$

$$\Rightarrow T(\epsilon_1) = 2\alpha_1 - i\alpha_2$$

Also $T(\epsilon_2) = T(0, 1) = (0, 0) = 0\alpha_1 + 0\alpha_2$

$\therefore$ $$[T]_{\beta\,\beta'} = \begin{bmatrix} 2 & 0 \\ -i & 0 \end{bmatrix}.$$

Problem 12 : *Let T be the linear operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (-x_2, x_1)$*

(*i*) *Prove that for all real numbers c, the operator $(T - cI)$ is invertible.*

(*ii*) *Prove that if β is any ordered basis for $\mathbf{R}^2$ and $[T]_\beta = A$, then $a_{12}a_{21} \neq 0$, where $A = (a_{ij})$.*

Solution (i) : Let $\beta = \{\epsilon_1 = (1, 0), \epsilon_2 = (0, 1)\}$ be an ordered basis for $\mathbf{R}^2$.

Then $$T(\epsilon_1) = T(1, 0) = (0, 1) = 0\epsilon_1 + 1\epsilon_2$$

$$T(\epsilon_2) = T(0, 1) = (-1, 0) = -1\epsilon_1 + 0\epsilon_2$$

$\therefore$ $$[T]_\beta = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ [cI]_\beta = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix}$$

$\therefore$ $$[T - cI]_\beta = \begin{bmatrix} -c & -1 \\ 1 & -c \end{bmatrix}$$

$$\det [T - cI]_\beta = c^2 + 1 \neq 0 \text{ for all real numbers } c$$

$\therefore$ $[T - cI]_\beta$ is invertible.

$\Rightarrow$ $T - cI$ is invertible for all real numbers c.

(ii) : Let β be any ordered basis for $\mathbf{R}^2$ s.t.

$$[T]_\beta = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = A, \ a_{ij} \in \mathbf{R}$$

By (*i*) $T - a_{11}I$ is Invertible

$$\Rightarrow [T - a_{11}I]_\beta \text{ is invertible}$$

$$\Rightarrow \begin{bmatrix} 0 & a_{12} \\ a_{21} & a_{22} - a_{11} \end{bmatrix} \text{ is invertible}$$

$$\Rightarrow -a_{12}a_{21} \neq 0 \text{ as det of above matrix} \neq 0$$

$$\Rightarrow a_{12}a_{21} \neq 0.$$

Problem 13 : *Let T be the linear operator on $\mathbf{R}^3$ defined by*

$$T(x_1, x_2, x_3) = (3x_1 + x_3, -2x_1 + x_2, -x_1 + 2x_2 + 4x_3)$$

Show that T is invertible.

Solution : Let $\beta = \{\epsilon_1 = (1, 0, 0), \epsilon_2 = (0, 1, 0), \epsilon_3 = (0, 0, 1)\}$ be an ordered basis of $\mathbf{R}^3$. Then $[T]_\beta = \begin{bmatrix} 3 & 0 & 1 \\ -2 & 1 & 0 \\ -1 & 2 & 4 \end{bmatrix} = A.$

$$\det A = 3(4) + 1(-4 + 1) = 12 - 3 = 9 \neq 0$$

So, A is invertible

$\Rightarrow$ T is invertible.

Problem 14 : *Let A be an $n \times n$ matrix over F. Show that A is invertible if and only if columns of A are linearly independent over F.*

Solution : Let $V(F)$ be a vector space of dimension n. Let $\beta = \{v_1, \ldots, v_n\}$ be an ordered basis of V. Let $A = (a_{ij})$. Then $\exists$ a linear transformation $T : V \to V$ such that

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i$$

$\therefore$ $[T]_\beta = A.$

Let $M_n(F)$ denote the vector space of all $n \times n$ matrices over F.

Let $A \in M_n(F)$ be invertible. Then T is also invertible (by Cor. to Theorem 11) and so T is 1-1, onto.

Let $$\alpha_1 \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \ldots + \alpha_n \begin{bmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{bmatrix} = 0, \ \alpha_i \in F$$

$$\Rightarrow \begin{bmatrix} \alpha_1 a_{11} & \ldots\ldots & +\alpha_n a_{1n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \alpha_1 a_{n1} + & \ldots\ldots & +\alpha_n a_{nn} \end{bmatrix} = 0$$

$$\Rightarrow \alpha_1 a_{11} + \ldots\ldots + \alpha_n a_{1n} = 0$$

$$\ldots\ldots\ldots$$

$$\alpha_1 a_{n1} + \ldots\ldots + \alpha_n a_{nn} = 0$$

$$\Rightarrow \alpha_1 a_{11} v_1 + \ldots\ldots + \alpha_n a_{1n} v_1 = 0$$

$$\ldots\ldots\ldots$$

$$\alpha_1 a_{n1} v_n + \ldots\ldots + \alpha_n a_{nn} v_n = 0$$

$$\Rightarrow \alpha_1 (a_{11} v_1 + \ldots\ldots + a_{n1} v_n) + \ldots\ldots + \alpha_n (a_{1n} v_1 + \ldots\ldots + \alpha_{nn} v_n) = 0$$

$$\Rightarrow \alpha_1 T(v_1) + \ldots\ldots + \alpha_n T(v_n) = 0$$

$$\Rightarrow T(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n) = 0$$

$$\Rightarrow \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n = 0 \text{ as } T \text{ is 1-1}$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i$$

$\Rightarrow$ columns of A are linearly independent.

Conversely, let columns of A be linearly independent over F.

Now $\quad x \in \text{Ker } T$

$$\Rightarrow T(x) = 0, \quad x \in V$$

$$\Rightarrow T(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n) = 0$$

$$\Rightarrow \alpha_1 T(v_1) + \ldots\ldots + \alpha_n T(v_n) = 0$$

$$\Rightarrow \sum_{j=1}^{n} \alpha_j T(v_j) = 0 \Rightarrow \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{n} a_{ij} v_i \right) = 0$$

$$\Rightarrow \sum_{i=1}^{n} \left(\sum_{j=}^{n} (\alpha_j a_{ij}) \right) v_i = 0$$

$$\Rightarrow \sum_{j=1}^{n} \alpha_j a_{ij} = 0 \text{ for all } i = 1, \ldots\ldots, n$$

$$\Rightarrow \alpha_1 \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \ldots\ldots + \alpha_n \begin{bmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{bmatrix} = 0$$

$\Rightarrow$ each $\alpha_i = 0$ as columns are linearly independent

$\Rightarrow x = 0 \qquad \Rightarrow \text{Ker } T = \{0\}$

$\Rightarrow T$ is 1-1 and so onto

$\Rightarrow T$ is invertible.

Problem 15 : *Let T be the linear operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (-x_2, x_1)$. Let*

$$\beta = \{\epsilon_1 = (1, 0),\ \ \epsilon_2 = (0, 1)\}$$

$$\beta' = \{\alpha_1 = (1, 2),\ \ \alpha_2 = (1, -1)\}$$

be ordered basis for $\mathbf{R}^2$. Find a matrix P such

$$[T]_{\beta'} = P^{-1}\ [T]_\beta P.$$

Proof :

$$T(\epsilon_1) = T(1, 0) = (0, 1) = 0\epsilon_1 + 1\epsilon_2$$

$$T(\epsilon_2) = T(0, 1) = (-1, 0) = -1\epsilon_1 + 0\epsilon_2$$

$$\therefore \qquad [T]_\beta = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Define $\quad S : \mathbf{R}^2 \to \mathbf{R}^2$

s.t., $\quad S(\epsilon_i) = \alpha_i \quad i = 1, 2$

Now $\quad \alpha_1 = (1, 2) = 1\epsilon_1 + 2\epsilon_2$

$$\alpha_2 = (1,\ -1) = 1\epsilon_1 + (-1)\epsilon_2$$

$$\Rightarrow \quad S(\alpha_1) = 1\alpha_1 + 2\alpha_2$$

$$S(\alpha_2) = 1\alpha_1 + (-1)\alpha_2$$

$$\Rightarrow \quad [S]_{\beta'} = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}$$

$$\Rightarrow \quad P = \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix} \text{ and } P^{-1} = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{bmatrix}$$

$$\Rightarrow \quad P^{-1}\,[T]_\beta P = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{3} & -\frac{1}{3} \\ -\frac{1}{3} & -\frac{2}{3} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} -\frac{1}{3} & \frac{2}{3} \\ -\frac{5}{3} & -\frac{1}{3} \end{bmatrix}$$

$$= [T]_{\beta'}.$$

Problem 16 : *Let T be the linear operator on $\mathbf{R}^3$, the matrix of which in the standard ordered basis is*

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ -1 & 3 & 4 \end{bmatrix}$$

Find a basis for the range of T and a basis for the null space of T.

Solution : $\text{Det}\, A = 1(4-3) - 2(1) + 1(1)$

$$= 1 - 2 + 1 = 0$$

$\therefore$ A is not invertible and so T is not invertible.

Let $\{\in_1 = (1,\ 0,\ 0),\ \in_2 = (0,\ 1,\ 0),\ \in_3 = (0,\ 0,\ 1)\}$

be standard ordered basis of $\mathbf{R}^3$.

Let $(x_1, x_2, x_3) \in \text{Ker}\ T$

Then $T(x_1, x_2, x_3) = 0$

$$\Rightarrow T(x_1(1,\ 0,\ 0) + x_2(0,\ 1,\ 0) + x_3(0,\ 0,\ 1)) = 0$$

$$\Rightarrow T(x_1 \in_1 + x_2 \in_2 + x_3 \in_3) = 0$$

$$\Rightarrow x_1 T(\in_1) + x_2 T(\in_2) + x_3 T(\in_3) = 0$$

$$\Rightarrow x_1(1,\ 0,\ -1) + x_2(2,\ 1,\ 3) + x_3(1,\ 1,\ 4) = 0$$

$$\Rightarrow (x_1 + 2x_2 + x_3,\ x_2 + x_3,\ -x_1 + 3x_2 + 4x_3) = 0$$

$$\Rightarrow x_1 + 2x_2 + x_3 = 0$$

$$x_2 + x_3 = 0,\ -x_1 + 3x_2 + 4x_3 = 0$$

$$\Rightarrow x_1 + x_2 = 0,\ x_2 + x_3 = 0$$

$$\Rightarrow (x_1, x_2, x_3) = (-x_2, x_2, -x_3)$$

$$= x_2(-1,\ 1,\ -1)$$

$\Rightarrow$ every element in Ker T is multiple of $(-1,\ 1,\ -1)$

$\Rightarrow$ Ker T is spanned by $(-1,\ 1,\ -1)$

Since $(-1, 1, -1) \neq 0$, $\{(-1,\ 1, -1)\}$ is a basis of Ker T. $\therefore$ dim Ker $T = 1 \Rightarrow$ dim Range $T = 2$

Since $T\in_1 = (1, 0, -1)$

$T\in_2 = (2, 1, 3)$

belong to Range T and $aT\in_1 + bT\in_2 = 0$

we find $a(1, 0, -1) + b(2, 1, 3) = 0$

$$\Rightarrow b = 0,\ a = 0$$

$\Rightarrow \{T\in_1,\ T\in_2\}$ is a linearly independent set in Range T. As dim Range $T = 2$, $\{(1, 0, -1),\ (2, 1, 3)\}$ is a basis of Range T.

Problem 17 : *Let T be a linear operator on F^n and let A be the matrix of T in the standard ordered basis for F^n. Let W be the subspace of F^n spanned by the column vectors of A. Find a relation between W and T.*

Solution : $T : F^n \to F^n$

Let $\beta = \{e_1 = (1,\ 0,\ 0, \ldots\ldots 0), \ldots\ldots, e_n = (0,\ 0, \ldots\ldots, 1)\}$ be the standard ordered basis of F^n and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

thus
$$T(e_1) = a_{11}e_1 + a_{21}e_2 + \ldots\ldots + a_{n1}e_n$$
$$T(e_2) = a_{12}e_1 + a_{22}e_2 + \ldots\ldots + a_{n2}e_2$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$T(e_n) = a_{1n}e_1 + a_{2n}e_2 + \ldots\ldots + a_{nn}e_n$$

and also W is spanned by
$$\{(a_{11}, a_{21}, \ldots\ldots, a_{n1}), (a_{12}, a_{22}, \ldots\ldots, a_{n2}), \ldots\ldots, (a_{1n}, a_{2n}, \ldots\ldots, a_{nn})\}$$

We claim $T : F^n \to W$ is onto $L.T.$

For any $x \in F^n$, $x = \alpha_1 e_1 + \alpha_2 e_2 + \ldots\ldots + \alpha_n e_n$

$\Rightarrow T(x) = \alpha_1 T(e_1) + \alpha_2 T(e_2) + \ldots\ldots + \alpha_n T(e_n)$

$\Rightarrow T(x) \in W$ as $T(e_1), T(e_2), \ldots\ldots, T(e_n) \in W$

Again, for any $w \in W$, $w = \beta_1 T(e_1) + \beta_2 T(e_2) + \ldots\ldots + \beta_n T(e_n)$
$$= T(\beta_1 e_1 + \beta_2 e_2 + \ldots\ldots + \beta_n e_n)$$

showing that T is onto.

$\Rightarrow$ Range $T = W \Rightarrow$ dim Range $T =$ dim W

or that rank of $T =$ dim W

which is the required relation betwen T and W.

Exercises

1. Let V be the space of all polynomial functions from $\mathbf{R}$ into $\mathbf{R}$ of the form
$$f(x) = c_o + c_1 x + c_2 x^2 + c_3 x^3$$
Let $\beta = \{1, x, x^2, x^3\}$ be an ordered basis of V. Let D be the differential operator on V. Show
$$[D]_\beta = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

2. Let T be the operator on $\mathbf{C}^2$ defined by $T(x_1, x_2) = (x_1, 0)$. Let β be the standard ordered basis for $\mathbf{C}^2$ and $\beta' = \{\alpha_1 = (1, i), \alpha_2 = (-i, 2)\}$ be an ordered basis for $\mathbf{C}^2$.
   (*i*) what is $[T]_{\beta', \beta}$?
   (*ii*) what is $[T]_{\beta'}$? Find P such that $[T]_{\beta'} = P^{-1}[T]_\beta P$.

3. Let T be the linear transformation from $\mathbf{R}^3$ into $\mathbf{R}^2$ defined by
$$T(x_1, x_2, x_3) = (x_1 + x_2, 2x_3 - x_1)$$
   (*i*) If β, β' are standard ordered basis for $\mathbf{R}^3$ and $\mathbf{R}^2$ respectively, find $[T]_{\beta, \beta'}$.

(*ii*) If $\beta = \{\alpha_1 = (1, 0, -1), \alpha_2 = (1, 1, 1), \alpha_3 = (1, 0, 0)\}$
$\beta' = \{\beta_1 = (0, 1), \beta_2 = (1, 0)\}$
are ordered basis for $\mathbf{R}^3$ and $\mathbf{R}^2$ respectively, find $[T]_{\beta, \beta'}$

4. Let V be a two dimensional vector space over the field F and β be an ordered basis for V. If T is a linear operator on V and $[T]_\beta = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, prove that
$$T^2 - (a+d)T + (ad - bc)\ I = 0$$

5. Let T be the operator on $\mathbf{R}^2$ defined by $T(x_1, x_2) = (x_1, 0)$. Let β be the standard ordered basis for $\mathbf{R}^2$ and $\beta' = \{\alpha_1 = (1, 1), \alpha_2 = (2, 1)\}$ be an ordered basis for $\mathbf{R}^2$. Find P s.t.,
$$[T]_{\beta'} = P^{-1}[T]_\beta P$$

6. Let A be $n \times n$ matrix over F. Show that A is invertible if and only if rows of A are linearly independent over F.

7. Let T be the linear operator on $\mathbf{R}^3$, the matrix of which in the standard ordered basis is $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

   Find a basis of Range T and Ker T.

8. Show that $T : \mathbf{R}^3 \to \mathbf{R}^2$ s.t., $T(x, y, z) = (y, x)$ is a *L.T.* Find the matrix representation of T for the standard ordered basis of $\mathbf{R}^3$ and $\{(0, 1), (2, 3)\}$ of $\mathbf{R}^2$.

Dual Spaces

Earlier we saw that Hom (V, W), the set of all linear transformations from vector space V over F into vector space W over F, is also a vector space over F. Further, if dim $V = m$, dim $W = n$, then dim Hom $(V, W) = mn$. In particular, if $W = F$, then Hom (V, F) is called dual space of V over F. It is denoted by $\hat{V}$ and read as V dual. In this section we study these dual spaces.

Our first job will be to construct a basis of $\hat{V}$, from a given basis of V.

Theorem 13 : *Let $\{v_1, \ldots\ldots, v_n\}$ be a basis of V.*

Define $\hat{v}_i : V \to F$ *s.t.,*
$$\hat{v}_i(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n) = \alpha_i \qquad i = 1, 2, \ldots\ldots, n$$

Then $\hat{v}_i$ is a linear transformation for all $i = 1, \ldots\ldots, n$ and $\{\hat{v}_1, \ldots\ldots, \hat{v}_n\}$ is a basis of $\hat{V}$. Hence dim V = dim $\hat{V}$.

Proof : Let $v,\ v' \in V$

Suppose $\quad v = \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n$

$\quad v' = \beta_1 v_1 + \ldots\ldots + \beta_n v_n, \qquad \alpha_i, \beta_i \in F$

If $v = v'$, then $\alpha_j = \beta_j$ for all $j = 1, \ldots\ldots, n$

$\therefore \qquad \hat{v}_i(v) = \alpha_i = \hat{v}_i(v')$

$\therefore$ $\hat{v}_i$ is well defined for all $i = 1, \ldots\ldots, n$

Also $\qquad \hat{v}_i(v + v') = \hat{v}_i(\overline{\alpha_1 + \beta_1} v_1 + \ldots\ldots + \overline{\alpha_n + \beta_n} v_n)$

$$= \alpha_i + \beta_i$$

$$= \hat{v}_i(v) + \hat{v}_i(v')$$

and $\qquad \hat{v}_i(\alpha v) = \hat{v}_i(\alpha\alpha_1 v_1 + \ldots\ldots + \alpha\alpha_n v_n)$

$$= \alpha\alpha_i = \alpha\hat{v}_i(v)$$

$\therefore$ $\hat{v}_i$ is a *L.T.* for all $i = 1, \ldots\ldots, n$

By def., $\qquad \hat{v}_i(v_j) = \hat{v}_i(0v_1 + \ldots\ldots + 1v_j + \ldots\ldots + 0v_n) = 0$ if $j \neq i$

$= 1$ if $j = i$

$\therefore \qquad \hat{v}_i(v_j) = \delta_{ij} \qquad$ for all $i, j = 1, \ldots\ldots, n$

Let $\qquad \alpha_1 \hat{v}_1 + \ldots\ldots + \alpha_n \hat{v}_n = 0 \qquad \alpha_i \in F$

Then $\qquad (\alpha_1 \hat{v}_1 + \ldots\ldots + \alpha_n \hat{v}_n)(v_j) = 0(v_j) = 0$

$\Rightarrow \alpha_j \hat{v}_j(v_j) = 0$

$\Rightarrow \alpha_j = 0 \qquad$ for all $j = 1, \ldots\ldots, n$

$\therefore$ $\{\hat{v}_1, \ldots\ldots, \hat{v}_n\}$ is *L.I.* over F.

Let $f \in \hat{V}$. Let $f(v_i) = \alpha_i \quad i = 1, \ldots\ldots, n$

Then $\qquad (\alpha_1 \hat{v}_1 + \ldots\ldots + \alpha_n \hat{v}_n)(v_i)$

$$= \alpha_i \hat{v}_i(v_i)$$

$$= \alpha_i \quad i = 1, \ldots\ldots, n$$

$\therefore$ f and $\alpha_1 \hat{v}_1 + \ldots\ldots + \alpha_n \hat{v}_n$ agree on all bases elements of V.

So, $\qquad f = \alpha_1 \hat{v}_1 + \ldots\ldots + \alpha_n \hat{v}_n$

$\therefore$ $\{\hat{v}_1, \ldots\ldots, \hat{v}_n\}$ spans $\hat{V}$.

Hence, $\{\hat{v}_1, \ldots\ldots, \hat{v}_n\}$ is a basis of $\hat{V}$, called *dual basis* of $\{v_1, \ldots\ldots, v_n\}$ s.t., $\hat{v}_i(v_j) = \delta_{ij}$.

Cor. : Let V be a finite dimensional vector space over F. Let $0 \neq v \in V$. Then $\exists f \in \hat{V}$ s.t., $f(v) \neq 0$.

Proof : Since $v \neq 0$, $\{v\}$ is *L.I.* set. So, it can be extended to form a basis of V.

Let $\{v = v_1, v_2, \ldots\ldots, v_n\}$ be a basis of V.

Let $\{\hat{v}_1, \ldots\ldots, \hat{v}_n\}$ be corresponding dual basis. Then $\hat{v}_i(v_j) = \delta_{ij}$

$\therefore \qquad \hat{v}_1(v_1) = 1$

Let $\qquad f = \hat{v}_1 \in \hat{V}$

Then $\qquad f(v) = f(v_1) = \hat{v}_1(v_1) = 1 \neq 0.$

Theorem 14 : *Let V be a finite dimensional vector space over F.*

Define $\qquad \theta : V \to \hat{\hat{V}}$, *s.t.,*

$\theta(v) = T_v$ *for all* $v \in V$

where $\qquad T_v : \hat{V} \to F$ *s.t.,*

$T_v(f) = f(v)$ *for all* $f \in \hat{V}$

Then θ is an isomorphism from V onto $\hat{\hat{V}}$. (Here $\hat{\hat{V}}$ = dual of $\hat{V}$, called double dual of V).

Proof : Let $f, g \in \hat{V}$

Then
$$\begin{aligned} T_v(f+g) &= (f+g)(v) \\ &= f(v) + g(v) \\ &= T_v(f) + T_v(g) \end{aligned}$$

Let $\alpha \in F$

Then
$$\begin{aligned} T_v(\alpha f) &= (\alpha f)(v) \\ &= \alpha f(v) \\ &= \alpha T_v(f) \end{aligned}$$

$\therefore \qquad T_v \in \hat{\hat{V}}$

θ is well defined as $v = v' \Rightarrow T_v(f) = f(v)$

$= f(v') = T_{v'}(f)$ for all $f \in \hat{V} \Rightarrow T_v = T_{v'}$

θ is a *L.T.* as

$$\theta(v + v') = T_{v+v'} = T_v + T_{v'} = \theta(v) + \theta(v')$$

as
$$\begin{aligned} T_{v+v'}(f) &= f(v + v') \\ &= f(v) + f(v') \\ &= T_v(f) + T_{v'}(f) \\ &= (T_v + T_{v'}) \text{ for all } f \in \hat{V} \end{aligned}$$

$\therefore \qquad T_{v+v'} = T_v + T_{v'}$

Also $\qquad \theta(\alpha v) = T_{\alpha v} = \alpha T_v = \alpha\theta(v)$

as $\qquad T_{\alpha v}(f) = f(\alpha v)$

$$= \alpha f(v)$$

$$= \alpha T_v(f) \text{ for all } f \in \hat{V}$$

$\therefore \qquad T_{\alpha v} = \alpha T_v$

Let $0 \neq v \in \operatorname{Ker}\theta \Rightarrow \theta(v) = 0 \Rightarrow T_v = 0$

By Cor. to Theorem 13 $\exists f \in \hat{V}$ s.t., $f(v) \neq 0$

$\therefore \qquad T_v(f) \neq 0$

a contradiction as $T_v = 0 \Rightarrow T_v(f) = 0$

$\therefore \qquad \operatorname{Ker}\theta = \{0\} \Rightarrow \theta$ is 1-1

$\therefore \qquad V \cong \theta(V) \subseteq \hat{\hat{V}}$

$\Rightarrow \qquad \dim \theta(V) = \dim V = \dim \hat{V} = \dim \hat{\hat{V}}$ (by Theorem 13)

$\therefore \qquad \theta(V) = \hat{\hat{V}}$ as $\theta(V)$ is a subspace of $\hat{\hat{V}}$

$\therefore$ θ is onto from V to $\hat{\hat{V}}$

Thus θ is an isomorphism.

Cor. 1 : Let V be a finite dimensional vector space over F. If L is a linear functional on $\hat{V}$, then $\exists$ a unique $v \in V$ s.t., $L(f) = f(v)$ for all $f \in \hat{V}$.

Proof : L is a linear functional on $\hat{V}$

$\Rightarrow L \in \hat{\hat{V}} \Rightarrow \exists$ unique $v \in V$ s.t.,

$\theta(v) = L$ as θ is 1-1 onto

$\therefore \qquad T_v = L$

$\Rightarrow L(f) = T_v(f) = f(v)$ for all $f \in \hat{V}$.

Cor. 2 : Let V be a finite dimensional vector space over the field F. Then each basis for $\hat{V}$ is the dual of some basis for V.

Proof : Let $\{f_1, \ldots\ldots, f_n\}$ be a basis for $\hat{V}$.

By theorem 13, $\exists$ a basis $\{L_1, \ldots\ldots, L_n\}$ for $\hat{\hat{V}}$ s.t., $L_i(f_j) = \delta_{ij}$. As in Cor. 1 $\exists$ unique $v_i \in V$ for each i

s.t., $\qquad L_i = T_{v_i} = \theta(v_i)$

Since $\{L_1, L_2, \ldots\ldots, L_n\}$ is a basis for $\hat{\hat{V}}$, $\{\theta^{-1} L_1, \ldots\ldots, \theta^{-1} L_n\} = \{v_1, \ldots\ldots, v_n\}$ is basis for V as θ is an isomorphism.

Also $\delta_{ij} = L_i(f_j) = T_{v_i}(f_j) = f_j(v_i)$

$\therefore$ $\{f_1, \ldots\ldots, f_n\}$ is dual of basis $\{v_1, \ldots\ldots, v_n\}$ for V.

Problem 18 : *Let V be the vector space of all polynomial functions from* **R** *to* **R** *which have degree less than or equal to 2. Let t_1, t_2, t_3 be three distinct real numbers and let $L_i : V \to F$ be s.t., $L_i(p(x)) = p(t_i)$, $i = 1, 2, 3$. Show that $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$. Determine a basis for V s.t., $\{L_1, L_2, L_3\}$ is its dual.*

Solution : $L_i(p(x) + q(x))$

$$= L_i(r(x)), \quad r(x) = p(x) + q(x)$$
$$= r(t_i) = p(t_i) + q(t_i)$$
$$= L_i(p(x)) + L_i(q(x))$$

Also $L_i(\alpha p(x))$, $\alpha \in F$

$$= L_i(q(x)), \quad q(x) = \alpha p(x)$$
$$= q(t_i)$$
$$= \alpha p(t_i) = \alpha L_i p(x) \text{ for all } i = 1, 2, 3$$

$\therefore$ $L_i \in \hat{V}$ for all $i = 1, 2, 3$

Let $\alpha_1 L_1 + \alpha_2 L_2 + \alpha_3 L_3 = 0$

Apply it on polynomials 1, x, x^2 to get

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$
$$\alpha_1 t_1 + \alpha_2 t_2 + \alpha_3 t_3 = 0$$
$$\alpha_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 = 0$$

$$\therefore \quad \begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\therefore \quad A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0, \quad A = \begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix}$$

$$\det A = (t_1 - t_2)\ (t_2 - t_3)\ (t_3 - t_1)$$
$$\neq 0 \text{ as } t_1, t_2, t_3 \text{ are distinct}$$

Thus A^{-1} exists

$$\therefore \quad \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

Hence $\{L_1, L_2, L_3\}$ is a *L.I.* set.

Since $\dim V = 3$, $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$.

Let $\{p_1(x), p_2(x), p_3(x)\}$ be a basis of V s.t., $\{L_1, L_2, L_3\}$ is its dual basis.

Then $L_1(p_1) = 1,\ L_2(p_1) = 0,\ L_3(p_1) = 0$

$$L_2(p_1) = 0 \Rightarrow p_1(t_2) = 0$$
$$\Rightarrow t_2 \text{ is a root of } p_1(x)$$
$$L_3(p_1) = 0 \Rightarrow p_1(t_3) = 0$$
$$\Rightarrow t_3 \text{ is a root of } p_1(x)$$

Since $\deg\ p_1(x) \le 2$,

$$p_1(x) = \alpha(x - t_2)\ (x - t_3),\ \alpha = \text{constant}$$
$$L_1(p_1) = 1 \Rightarrow p_1(t_1) = 1$$
$$\Rightarrow \alpha(t_1 - t_2)\ (t_1 - t_3) = 1$$
$$\Rightarrow \alpha = \frac{1}{(t_1 - t_2)(t_1 - t_3)}$$

$$\therefore \quad p_1(x) = \frac{(x - t_2)(x - t_3)}{(t_1 - t_2)(t_1 - t_3)}$$

Similarly, $$p_2(x) = \frac{(x - t_1)(x - t_3)}{(t_2 - t_1)(t_2 - t_3)},\ p_3(x) = \frac{(x - t_1)(x - t_2)}{(t_3 - t_1)(t_3 - t_2)}.$$

Problem 19 : *Let V be the vector space of all polynomial functions p from* **R** *into* **R** *which have degree 2 or less. Define three linear functionals on V by*

$$f_1(p) = \int_0^1 p(x)\,dx,\ f_2(p) = \int_0^2 p(x)\,dx,$$

$$f_3(p) = \int_0^{-1} p(x)\,dx$$

Show that $\{f_1, f_2, f_3\}$ is basis of $\hat{V}$. Determine a basis for V s.t., $\{f_1, f_2, f_3\}$ is its dual basis.

Solution : It can be easily seen that $f_1, f_2, f_3 \in \hat{V}$.

Let $\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 = 0,\ \alpha_i \in \mathbf{R}$

Apply it on $1, x, x^2$ to get

$$\alpha_1 + 2\alpha_2 - \alpha_3 = 0$$

$$\frac{\alpha_1}{2} + \frac{4}{2}\alpha_2 + \frac{\alpha_3}{2} = 0$$

$$\frac{\alpha_1}{3} + \frac{8}{3}\alpha_2 - \frac{\alpha_3}{3} = 0$$

Let $$A = \begin{bmatrix} 1 & 2 & -1 \\ 1 & 4 & 1 \\ 1 & 8 & -1 \end{bmatrix}$$

Then $$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0, \quad \det A \neq 0$$

$\therefore$ $$A^{-1}A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

$\therefore$ $\{f_1, f_2, f_3\}$ is a *L.I.* set.

Since $\dim V = 3$, $\{f_1, f_2, f_3\}$ is a basis of $\hat{V}$.

Let $\{p_1(x), p_2(x), p_3(x)\}$ be a basis of V s.t., $\{f_1, f_2, f_3\}$ is its dual basis.

$\therefore$ $$f_1(p_1) = 1, \; f_2(p_1) = 0, \; f_3(p_1) = 0$$

Let $$p_1(x) = c_o + c_1 x + c_2 x^2$$

$$f_2(p_1) = 0 \Rightarrow c_o x + c_1 \frac{x^2}{2} + c_2 \frac{x^3}{3}\Big|_0^2 = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 = 0 \text{ when } x = 2$$

$$f_3(p_1) = 0 \Rightarrow c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 \Big|_0^{-1} = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 = 0 \text{ when } x = -1$$

$\therefore$ $$c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 = \alpha x(x-2)(x+1)$$

$$f_1(p_1) = 1 \Rightarrow c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 = 1 \text{ when } x = 1$$

$$\Rightarrow \alpha \,.\, 1\,(-1)\,(2) = 1 \Rightarrow \alpha = -\frac{1}{2}$$

$$c_o x + \frac{c_1}{2} x^2 + \frac{c_2}{3} x^3 = -\frac{1}{2} x\,(x-2)\,(x+1)$$

$$= -\frac{1}{2} x^3 + \frac{1}{2} x^2 + x$$

$$\therefore \qquad \frac{c_2}{3} = -\frac{1}{2}, \ \frac{c_1}{2} = \frac{1}{2}, \ c_o = 1$$

$$\therefore \qquad c_o = 1, \ c_1 = 1, \ c_2 = -\frac{3}{2}$$

$$\therefore \qquad p_1(x) = 1 + x - \frac{3}{2}x^2$$

Similarly, we can find $p_2(x)$, $p_3(x)$.

Definition : Let W be a sub-set of V.

Define $\qquad A(W) = \{f \in \hat{V} \mid f(W) = 0 \text{ for all } w \in W\}$

Then $A(W)$ is a sub-space of $\hat{V}$ as $\alpha, \beta \in F$,

$$\begin{aligned} f, g \in A(W) &\Rightarrow f(w) = 0 = g(w) && \text{for all } w \in W \\ &\Rightarrow \alpha f(w) + \beta g(w) = 0 && \text{for all } w \in W \\ &\Rightarrow (\alpha f + \beta g)(w) = 0 && \text{for all } w \in W \\ &\Rightarrow \alpha f + \beta g \in A(W) \end{aligned}$$

$A(W)$ is called *annihilator* of W.

Problem 20 : *Let U, W be sub-sets of V. If $U \subseteq W$, show that $A(U) \supseteq A(W)$.*

Solution : Let $f \in A(W)$ then, $f(w) = 0$ for all $w \in W$

$$\Rightarrow f(u) = 0 \text{ for all } u \in U \text{ as } U \subseteq W$$

$$\Rightarrow f \in A(U).$$

Theorem 15 : *Let V be a finite dimensional vector space and W, a subspace of V. Then $\dim A(W) = \dim V - \dim W$.*

Proof : Let $\{w_1, \ldots\ldots, w_m\}$ be a basis of W.

It can be extended to form a basis of V.

Let $\{w_1, \ldots\ldots, w_m, v_{m+1}, \ldots\ldots, v_n\}$ be a basis of V.

Let $\{f_1, \ldots\ldots, f_m, f_{m+1}, \ldots\ldots, f_n\}$ be corresponding dual basis.

Then $\qquad f_i(w_j) = 0 \quad i = m+1, \ldots\ldots, n$

$$j = 1, \ldots\ldots, m$$

$$\therefore \qquad f_i \in A(W) \text{ for all } i = m+1, \ldots\ldots, n$$

We show $\{f_{m+1}, \ldots\ldots, f_n\}$ is a basis of $A(W)$.

Let $\qquad \alpha_{m+1} f_{m+1} + \ldots\ldots + \alpha_n f_n = 0$

$$\therefore \qquad (\alpha_{m+1} f_{m+1} + \ldots\ldots + \alpha_n f_n)(v_k) = 0 \text{ for all } k = m+1, \ldots\ldots, n$$

$$\therefore \qquad \alpha_k f_k (v_k) = 0$$

$$\therefore \qquad \alpha_k = 0 \text{ for all } k = m+1, \ldots\ldots, n$$

So, $\{f_{m+1}, \ldots\ldots, f_n\}$ is a *L.I.* set.

Let $f \in A(W)$ then $f(w) = 0$ for all $w \in W$, $f \in \hat{V}$

$$f \in \hat{V} \Rightarrow f = \beta_1 f_1 + \ldots\ldots + \beta_m f_m + \ldots\ldots + \beta_n f_n$$
$$\Rightarrow 0 = f(w_j) = \beta_j f_j(w_j) = \beta_j \text{ for all } j = 1, \ldots, m$$
$$\Rightarrow f = \beta_{m+1} f_{m+1} + \ldots\ldots + \beta_n f_n$$
$$\Rightarrow \{f_{m+1}, \ldots\ldots, f_n\} \text{ spans } A(W)$$

$\therefore$ $\{f_{m+1}, \ldots\ldots, f_n\}$ is a basis of $A(W)$.

Hence $\dim A(W) = n - m = \dim V - \dim W$.

Cor. 1 : $$\frac{\hat{V}}{A(W)} \cong \hat{W}$$

Proof : Since $$\dim \frac{\hat{V}}{A(W)} = \dim \hat{V} - \dim A(W)$$
$$= \dim V - \dim V + \dim W$$
$$= \dim W = \dim \hat{W}.$$

Hence $$\frac{\hat{V}}{A(W)} \cong \hat{W}.$$

Cor. 2 : If V is a finite dimensional vector space and W, a subspace of V, then

$$A(A(W)) \cong W.$$

Proof : Define $\theta : W \to A(A(W))$ s.t.,

$$\theta(w) = T_w$$

where $T_w : \hat{W} \to F$ s.t.,

$$T_w(f) = f(w)$$

$$T_w \in A(A(W)) \text{ as } T_w(f) = f(w) = 0 \text{ for all } f \in A(W)$$

Then as in Theorem 14, θ is well defined 1-1 linear transformation.

$\therefore$ $$W \cong \theta(W) \subseteq A(A(W))$$

Since $$\dim A(A(W))$$
$$= \dim \hat{V} - \dim A(W)$$
$$= \dim V - \dim A(W)$$
$$= \dim W \quad \text{by Theorem 15}$$

and $$\dim \theta(W) = \dim W$$
$$A(A(W)) = \theta(W)$$

$\therefore$ θ is onto from W to $A(A(W))$

Hence $$W \cong A(A(W)).$$

For sake of convenience, we shall write $A(A(W)) = W$.

Consider for example, $V = \mathbf{R}^2$, $W = \{(x, 0) \mid x \in R\}$

Then $A(W)$ is a subspace of $\hat{V}$ spanned by f

where $\quad f(x_1, x_2) = x_2$

In fact, $\quad \{f\}$ is a basis of $A(W)$ as dim $W = 1$.

Also, $A(A(W))$ is spanned by T_w where $w = (1, 0)$

Since dim $A(A(W)) = 1$, $\{T_w\}$ is a basis of $A(A(W))$

Then $\quad \theta : W \to A(A(W))$ s.t.,

$$\theta(w) = T_w$$

is an isomorphism as basis of W is mapped to basis of $A(A(W))$.

Problem 21 : *Let W_1, W_2 be subspaces of finite dimensional vector space V. Determine $A(W_1 + W_2)$.*

Solution : $f \in A\ (W_1 + W_2)$

$$\Leftrightarrow f(x) = 0 \text{ for all } x \in W_1 + W_2$$

$$\Leftrightarrow f(w_1) = 0 = f(w_2) \text{ for all } w_1 \in W_1,\ w_2 \in W_2$$

$$\Leftrightarrow f \in A(W_1) \cap A(W_2)$$

$$\therefore \quad A(W_1 + W_2) = A(W_1) \cap A(W_2)$$

Problem 22 : *Let f_1, f_2, f_3 be three linear functionals on $\mathbf{R}^4$ defined as follows :*

$$f_1(x_1, x_2, x_3, x_4) = x_1 + 2x_2 + 2x_3 + x_4$$

$$f_2(x_1, x_2, x_3, x_4) = 2x_2 + x_4$$

$$f_3(x_1, x_2, x_3, x_4) = -2x_1 - 4x_3 + 3x_4$$

Determine the subspace W of $\mathbf{R}^4$ s.t.,

$$f_i(w) = 0,\ w \in W \quad i = 1, 2, 3.$$

Solution : Let $(x_1, x_2, x_3, x_4) \in W$

Then $\quad f_i(x_1, x_2, x_3, x_4) = 0 \qquad i = 1, 2, 3$

$$\therefore \quad x_1 + 2x_2 + 2x_3 + x_4 = 0$$

$$2x_2 + x_4 = 0$$

$$-2x_1 - 4x_3 + 3x_4 = 0$$

$$\therefore \quad \begin{bmatrix} 1 & 2 & 2 & 1 \\ 0 & 2 & 0 & 1 \\ -2 & 0 & -4 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0$$

By elementary row tranformations, we get

$$\begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = 0$$

$\therefore \qquad x_1 + 2x_3 = 0, \; x_2 = 0, \; x_4 = 0$

$\therefore \qquad (x_1, x_2, x_3, x_4) = (-2x_3, 0, x_3, 0), = x_3(-2, 0, 1, 0)$

$\therefore$ W is spanned by $(-2, 0, 1, 0)$.

Problem 23 : *Let W be the subspace of $\mathbf{R}^5$ spanned by the vectors*

$$\alpha_1 = (2, -2, 3, 4, -1), \; \alpha_3 = (0, 0, -1, -2, 3)$$
$$\alpha_2 = (-1, 1, 2, 5, 2), \; \alpha_4 = (1, -1, 2, 3, 0)$$

Describe $A(W)$.

Solution : Let $f \in A(W)$

Then $\qquad f(w) = 0$ for all $w \in W$

$\Rightarrow f(\alpha_i) = 0$ for all $i = 1, 2, 3, 4$

Let $\qquad f(x_1, x_2, x_3, x_4, x_5) = c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$

(Note $v_1 = (1, 0, 0, 0, 0)$, $v_2 = (0, 1, 0, 0, 0)$, $v_3 = (0, 0, 1, 0, 0)$, $v_4 = (0, 0, 0, 1, 0)$, $v_5 = (0, 0, 0, 0, 1)$ form a basis of $\mathbf{R}^5$).

Let $\{\hat{v}_1, \hat{v}_2, \hat{v}_3, \hat{v}_4, \hat{v}_5\}$ be its dual basis.

Then $\qquad f = c_1\hat{v}_1 + c_2\hat{v}_2 + c_3\hat{v}_3 + c_4\hat{v}_4 + c_5\hat{v}_5$

$$\Rightarrow f(x_1, x_2, x_3, x_4, x_5) = \sum_1^5 c_i\hat{v}_i\,(x_1, x_2, x_3, x_4, x_5)$$

$$= \sum_1^5 c_i\hat{v}_i\,(x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4 + x_5v_5)$$

$$= c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$$

as $\qquad \hat{v}_i\,(v_j) = \delta_{ij}$

$\therefore \qquad f\,(\alpha_i) = 0$ for all $i = 1, 2, 3, 4$

$$\Rightarrow \begin{bmatrix} 2 & -2 & 3 & 4 & -1 \\ -1 & 1 & 2 & 5 & 2 \\ 0 & 0 & 1 & -2 & 3 \\ 1 & -1 & 2 & 3 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 0$$

By elementary row transformations, we get

$$\begin{bmatrix} 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = 0$$

$$\Rightarrow \quad c_1 - c_2 - c_4 = 0, \quad c_3 + 2c_4 = 0, \quad c_5 = 0$$

$$\Rightarrow \quad 2c_1 - 2c_2 + c_3 = 0, \quad c_5 = 0, \quad c_3 = -2c_4$$

Let $\quad c_2 = a, \quad c_4 = b$

Then $\quad c_3 = -2b$

$$2c_1 - 2a - 2b = 0 \Rightarrow c_1 = a + b$$

$$\Rightarrow f(x_1, x_2, x_3, x_4, x_5) = (a+b)\, x_1 + ax_2 - 2bx_3 + bx_4$$

Take $\quad a = 1, \quad b = 0$

Then $\quad f_1(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2$

Take $\quad a = 0, \quad b = 1$

Then $\quad f_2(x_1, x_2, x_3, x_4, x_5) = x_1 - 2x_3 + x_4$

$\therefore \quad f = af_1 + bf_2$

$\therefore \{f_1, f_2\}$ spans $A(W)$

Let $\alpha f_1 + \beta f_2 = 0$. Apply it on v_1, v_2 respectively. We get $\alpha + \beta = 0, \alpha = 0 \Rightarrow \beta = 0$.

$\therefore \{f_1, f_2\}$ is *L.I.* So, $\{f_1, f_2\}$ is a basis of $A(W)$

Hence $\quad \dim A(W) = 2.$

Problem 24 : *Let V be a finite dimensional vector space. Suppose $V = W_1 \oplus W_2$, where W_1, W_2 are subspaces of V. Show that $\hat{V} = A(W_1) \oplus A(W_2)$.*

Solution : $\dim V = \dim (W_1 \oplus W_2)$

$$= \dim W_1 + \dim W_2$$

Also $\dim (A(W_1) \oplus A(W_2))$

$$= \dim A(W_1) + \dim A(W_2))$$

$$= \dim V - \dim W_1 + \dim V - \dim W_2$$

$$= 2 \dim V - (\dim W_1 + \dim W_2)$$

$$= 2 \dim V - \dim V = \dim V = \dim \hat{V}$$

Since $A(W_1) \oplus A(W_2)$ is a subspace of $\hat{V}$

and $\dim \hat{V} = \dim (A(W_1) \oplus A(W_2))$,

$$\hat{V} = A(W_1) \oplus A(W_2).$$

Problem 25 : *If f and g are in $\hat{V}$ s.t., $f(v) = 0$ implies $g(v) = 0$, prove that $g = cf$ for some $c \in F$.*

Solution : If $f = 0$, then $g = 0 = cf$ where $c = 0 \in F$.

Let $f \neq 0$ then $\exists\, v \neq 0$ in V s.t., $f(v) \neq 0$

Let $\quad c = \dfrac{g(v)}{f(v)}$

$$h = g - cf \text{ and } x \in V$$

and $\quad \alpha = \dfrac{f(x)}{f(v)}.$

Then $$f(x-\alpha v) = f(x) - \alpha f(v) = 0$$
$$\Rightarrow x - \alpha v \in \operatorname{Ker} f$$
$$\Rightarrow x - \alpha v = y \in \operatorname{Ker} f$$
$$\Rightarrow x = y + \alpha v$$
$$\therefore \quad h(x) = g(x) - cf(x)$$
$$= g(y) + \alpha g(v) - cf(y) - c\alpha f(v)$$
$$= \alpha g(v) - c\alpha f(v) \text{ as } y \in \operatorname{Ker} f \Rightarrow y \in \operatorname{Ker} g$$
$$= \alpha g(v) - \alpha g(v) = 0 \text{ for all } x \in V$$
$$\therefore \quad h = 0 \Rightarrow g = cf$$

Consider the system of m equations

$$a_{11}x_1 + \ldots\ldots + a_{1n}x_n = 0$$
$$\ldots\ldots\ldots\ldots$$
$$a_{m1}x_1 + \ldots\ldots\ldots + a_{mn}x_n = 0, \text{ where } a_{ij} \in F$$

in n unknows.

Let U be the subspace of $F^{(n)}$ generated by m vectors

$u_1 = (a_{11}, \ldots\ldots, a_{1n}), \ldots\ldots\ldots, u_m = (a_{m1}, \ldots\ldots, a_{mn})$

If $\dim U = r$, we say the system of equations has rank r.

We wish to determine the number of linearly independent solutions to the system of equations in $F^{(n)}$.

Theorem 16 : *If the system of homogeneous linear equations*

$$a_{11}x_1 + \ldots\ldots\ldots + a_{1n}x_n = 0$$
$$\ldots\ldots\ldots\ldots$$
$$a_{m1}x_1 + \ldots\ldots\ldots + a_{mn}x_n = 0$$

where $a_{ij} \in F$ is of rank r, then there are $n-r$ linearly independent solutions in $F^{(n)}$.

Proof : Let $V = F^{(n)}$. Then $v_1 = (1, 0, \ldots\ldots, 0), \ldots\ldots v_n = (0, 0, \ldots\ldots, 0, 1)$ is a basis of V.

Let $\{\hat{v}_1, \ldots\ldots\ldots, \hat{v}_n\}$ be its dual basis.

Let U be the subspace of V described as above.

Let $f \in A(U)$ then $f(u_i) = 0$ for all $i = 1, \ldots\ldots, m$, $f \in \hat{V}$

Let $$f = c_1\hat{v}_1 + \ldots\ldots\ldots + c_n\hat{v}_n$$

$$\therefore \quad 0 = f(u_1) = (c_1\hat{v}_1 + \ldots\ldots\ldots + c_n\hat{v}_n)\ (a_{11}v_1 + \ldots\ldots + a_{1n}v_n)$$
$$= c_1a_{11} + c_2a_{12} + \ldots\ldots + c_na_{1n}$$

$\therefore (c_1, \ldots\ldots, c_n) \in F^{(n)}$ is a solution of first equation. Similarly, we get $(c_1, \ldots\ldots, c_n)$ to be solution of all m equations.

Conversely, let $(c_1, \ldots\ldots, c_n) \in F^{(n)}$ be a solution of system of given equations.

Let $\quad f = c_1\hat{v}_1 + \ldots\ldots\ldots + c_n\hat{v}_n$

Then
$$f(u_1) = (c_1\hat{v}_1 + \ldots\ldots\ldots + c_n\hat{v}_n)\ (a_{11}v_1 + \ldots\ldots + a_{1n}v_n)$$
$$= c_1a_{11} + \ldots\ldots + c_na_{1n}$$
$$= 0$$

Similarly, $\quad f(u_2) = 0, \ldots\ldots, f(u_m) = 0$

$\therefore \quad f \in A(U)$

Now

$\dim A(U)$ = maximum number of linearly independent vectors in $A(U)$

= maximum number of linearly independent solutions

But $\quad \dim A(U) = \dim V - \dim U = n - r$

$\therefore$ number of linearly independent solutions of given system is $n - r$.

Cor. : If $n > m$, that is, if the number of unknowns exceed the number of equations, then the system of equations has a non zero solution.

Proof : Since U is generated by m vectors, $r = \dim U \leq m < n \Rightarrow n - r > 0$ $\Rightarrow$ system of equations has a linearly independent solution, which is non zero (as zero vector is not linearly independent).

Problem 26 : *Let m and n be positive integers. Let $f_1, \ldots\ldots, f_m$ be linear functionals on $F^{(n)}$. For α in $F^{(n)}$ define $T(\alpha) = (f_1(\alpha), \ldots\ldots, f_m(\alpha))$.*

Show that T is a linear transformation from $F^{(n)}$ into $F^{(m)}$. Then show that every linear transformation from $F^{(n)}$ into $F^{(m)}$ is of the above form, for some $f_1, \ldots, f_m$.

Solution : Since $f_1, \ldots\ldots, f_m$ are linear transformations, so is T. Let $\{e_1, \ldots\ldots, e_n\}$ be the standard basis of $F^{(n)}$.

Then $\quad T(e_i) \in F^{(m)} \qquad \forall\ i = 1, \ldots\ldots, n.$

So, $\quad T(e_i) = (\beta_{i1}, \ldots\ldots, \beta_{im}) \qquad \forall\ i = 1, \ldots\ldots, n.$

$\therefore$
$$T(\alpha) = T(\alpha_1e_1 + \ldots\ldots + \alpha_ne_n),\ \alpha = \alpha_1e_1 + \ldots\ldots + \alpha_ne_n$$
$$= \alpha_1T(e_1) + \ldots\ldots + \alpha_nT(e_n)$$
$$= \alpha_1(\beta_{11}, \ldots\ldots, \beta_{1m}) + \ldots\ldots + \alpha_n(\beta_{n1}, \ldots\ldots, \beta_{nm})$$
$$= (\alpha_1\beta_{11} + \ldots\ldots + \alpha_n\beta_{n1}, \ldots\ldots, \alpha_1\beta_{1m} + \ldots\ldots + \alpha_n\beta_{nm})$$

For each i $(1 \leq i \leq m)$, $\exists$ a linear transformation
$$f_i : F^{(n)} \to F \text{ s.t.,}$$
$$f_i(e_1) = \beta_{1i}, \ldots\ldots\ldots, f_i(e_n) = \beta_{ni}$$

$\therefore$
$$f_1(\alpha) = f_1(\alpha_1e_1 + \ldots\ldots + \alpha_ne_n)$$
$$= \alpha_1\beta_{11} + \ldots\ldots + \alpha_n\beta_{n1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_m(\alpha) = f_m(\alpha_1e_1 + \ldots\ldots + \alpha_ne_n)$$
$$= \alpha_1\beta_{1m} + \ldots\ldots + \alpha_n\beta_{nm}$$

So, $$T(\alpha) = (f_1(\alpha), \ldots\ldots, f_m(\alpha)).$$

Problem 27 : *Let V be the vector space of all 2×2 matrices over the field of real numbers, and let*

$$B = \begin{bmatrix} 2 & -2 \\ -1 & 1 \end{bmatrix}$$

Let W be the subspace of V consisting of all A such that $AB = 0$. Let f be a linear functional on V which is in the annihilator of W. Suppose that $f(I) = 0$ and $f(C) = 3$, where I is the 2×2 identity matrix and

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Find $f(B)$.

Solution : Now $W = \{A \mid AB = 0\}$

Let $$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{221} \end{bmatrix} \in V$$

Then $$A = a_{11}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{12}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{21}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{22}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore$ $$f(A) = a_{11} f\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + a_{12} f\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + a_{21} f\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + a_{22} f\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= a_{11}\alpha + a_{12}\beta + a_{21}\gamma + a_{22}\delta \text{ (say).}$$

$\therefore$ $$0 = f(I) = \alpha + \delta$$

$$3 = f(C) = \delta$$

So, $$\alpha = -3, \ \delta = 3$$

Let $D = \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$. Then $DB = 0$

So, $D \in W$

$$\Rightarrow f(D) = 0 \text{ as } f \in A(W).$$

$\therefore$ $$0 = \alpha + 2\beta \Rightarrow \beta = \tfrac{3}{2}$$

Also, let $$E = \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix}.$$

Then $EB = 0$.

So, $E \in W$.

$$\Rightarrow f(E) = 0 \text{ as } f \in A(W)$$

$\therefore \qquad \gamma + 2\delta = 0 \Rightarrow \gamma = -6$

So, $\qquad f(B) = 2 \times (-3) + (-2)\ (\frac{3}{2}) + (-1)(-6) + (3)(1)$

$$= -6 - 3 + 6 + 3 = 0.$$

Problem 28 : *Let F be a subfield of complex numbers. We define n linear functionals on $F^{(n)}$ $(n \geq 2)$ by*

$$f_k\ (x_1, \ldots\ldots, x_n) = \sum_{j=1}^{n} (k-j)\ x_j, \quad 1 \leq k \leq m.$$

What is the dimension of the subspace annihilated by $f_1, \ldots\ldots, f_n$?

Solution : Now $f_1(x_1, \ldots\ldots, x_n) = ox_1 - x_2 - 2x_3 \ldots\ldots -(n-1)\, x_n$

$$f_2(x_1, \ldots\ldots, x_n) = x_1 + ox_2 - x_3 \ldots\ldots -(n-2)\, x_n$$

$$f_3(x_1, \ldots\ldots, x_n) = 2x_1 + x_2 + ox_3 \ldots\ldots -(n-3)\, x_n$$

.....

$$f_n(x_1, \ldots\ldots, x_n) = (n-1)\, x_1 + (n-2)\, x_2 + (n-3)\, x_3 + \ldots\ldots + 1\, x_{n-1} + ox_n$$

Let W be the subspace of $F^{(n)}$ annihilated by $f_1, \ldots\ldots, f_n$.

Then $\qquad (x_1, \ldots\ldots, x_n) \in W$

$$\Rightarrow f_k(x_1, \ldots\ldots, x_n) = 0 \qquad \forall\, k = 1, 2, \ldots\ldots, n.$$

$$\begin{bmatrix} 0 & -1 & -2 & \ldots & \ldots & -(n-1) \\ 1 & 0 & -1 & \ldots & \ldots & -(n-2) \\ 2 & 1 & 0 & \ldots & \ldots & -(n-3) \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ n-1 & n-2 & n-3 & \ldots & \ldots & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = 0$$

i.e., $AX = 0$, where A is the matrix on the left and $X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$.

It can be easily seen that Rank $A = 2$.

$\therefore$ number of linear independent solutions in W is $n-2$.

$\therefore$ dim $W = n-2$.

Transpose of a linear transformation

Let V, W be vector spaces over F.

Let T be a linear transformation from V into W.

Define $\qquad T^t : \hat{W} \to \hat{V}$ s.t.,

$$T^t(g) = gT$$

Then T^t is a linear transformation called the *transpose* of T.

It can be easily shown that

(*i*) $(T_1 + T_2)^t = T_1^t + T_2^t$, whee T_1, T_2 are linear transformations from V into W.

(*ii*) $(T_1 T_2)^t = T_2^t \; T_1^t$, where $T_1 : W \to V$ and $T_2 : V \to W$ are inear transformations

(*iii*) $(\alpha T)^t = \alpha T^t$, $\alpha \in F$, $T : V \to W$ is a linear transformation

(*iv*) $I^t = I$, $I : V \to V$ is the identity map.

Theorem 17 : *Let $T : V \to W$ be a linear transformation. Then*

(*a*) *The null space of T^t = the annihilator of range of T.*

(*b*) *If V, W are finite dimensional,*

then (*i*) *rank of T = rank of T^t*

(*ii*) *range of T^t = annihilator of the null space of T.*

Proof (*a*) : Now $g \in$ Null space of T^t

$$\Leftrightarrow T^t(g) = 0$$

$$\Leftrightarrow gT = 0 \Leftrightarrow gTV = 0 \Leftrightarrow g(\text{Range } T) = 0$$

$$\Leftrightarrow g \in A(R_T)$$

where $A(R_T)$ denotes the annihilator of range T.

(*b*) Let $\dim V = n$, $\dim W = m$,

Let r = rank of T = $\dim R_T = \dim T(V)$

where R_T denotes the range of T.

Now $\dim A(R_T) = \dim A(TV)$

$$= \dim W - \dim T(V) = m - r$$

Nullity of T^t = dimension of the null space of T^t

$$= \dim A(R_T) = m - r$$

But nullity of $T^t = \dim W - \text{rank } T^t$

$$= \dim W - \text{rank } T^t$$

$$\Rightarrow m - r = m - \text{rank } T^t$$

$$\Rightarrow \text{rank } T^t = r = \text{rank } T$$

This proves (*i*)

Let N denote the null space of T.

Then $A(N) = \{ f \in \hat{V} \mid f(n) = 0 \;\; \forall\, n \in N \}$ = Annihilator of the null space of T.

Now $f \in$ Range T^t

$$\Rightarrow f = T^t g, \; g \in W$$

$$= gT$$

$$\Rightarrow f(n) = gT(n) = g(0) = 0 \qquad \forall\, n \in N$$

$$\Rightarrow f \in A(N)$$

$$\Rightarrow \text{Range } T^t \subseteq A(N)$$

So, $\dim A(N) = \dim V - \dim N$

$$= \dim V - \text{nullity } T = \text{rank } T$$

$$= \text{rank } T^t = \dim \text{ Range } T^t$$

Therefore, $A(N) = \text{Range } T^t$

This proves (*ii*)

Lemma : *Let $T: V \to W$ be a linear transformation. Let $\beta = \{v_1, \ldots\ldots, v_n\}$, $\beta' = \{w_1, \ldots\ldots, w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, \ldots\ldots, f_n\}$ be the dual basis of V such that $f_i(v_j) = \delta_{ij}$.* Let $f \in \hat{V}$. *Then*

$$f = \sum_1^n f(v_i)\ f_i.$$

Proof : Suppose $f = \sum_1^n c_i f_i, \qquad c_i \in F$

Then $$f(v_j) = \sum c_i f_i(v_j) = \sum c_i \delta_{ij} = c_j$$

So, $$f = \sum_1^n f(v_i)\ f_i.$$

Theorem 18 : *Let $T: V \to W$ be a linear transformation. Let $\beta = \{v_1, \ldots\ldots, v_n\}$, $\beta' = \{w_1, \ldots\ldots, w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, \ldots\ldots, f_n\}$, $\hat{\beta}' = \{g_1, \ldots\ldots, g_m\}$ be the dual basis of V, W respectively.*

Let $A = (a_{ij})$ be the matrix of T w.r.t. β, β' and $B = (b_{ij})$ be the matrix of T^t w.r.t., $\hat{\beta}'$, $\hat{\beta}$.

Then $a_{ij} = b_{ji}\ \forall\ i, j$.

(This shows that the matrix of T^t is the transpose of the matrix of T. For this reason T^t is called the transpose of T).

Proof : Now $T^t: \hat{W} \to \hat{V}$ s.t.,

$$T^t(g_j) = g_j T = f \text{ (say)}$$

Then $$f(v_i) = (T^t g_j)(v_i)$$

$$= (g_j T)(v_i)$$

$$= g_j T(v_i) = g_j\left(\sum_1^m a_{ki} w_k\right)$$

$$= \sum a_{ki}\, g_j(w_k) = \sum a_{ki}\, \delta_{jk} = a_{ji}$$

By above lemma,

$$f = \sum_1^n f(v_i) f_i = \sum_1^n a_{ji} f_i$$

But $$f = T^t g_j = \sum_1^n b_{ij} f_i$$

So, $$\sum_1^n b_{ij} f_i = \sum_1^n a_{ji} f_i$$

$$\Rightarrow \sum_1^n (b_{ij} - a_{ji})\ f_i = 0$$

$\Rightarrow b_{ij} = a_{ji}\ \forall\ i, j$. This proves the theorem.

Let $A = (a_{ij})$ be the $m \times n$ matrix over F. Then *row rank* of A is defined as the dimension of the subspace of $F^{(n)}$ spanned by $(a_{11}, \ldots\ldots, a_{1n}), \ldots\ldots, (a_{m1}, \ldots\ldots, a_{mn})$.

Similarly, *column rank* of A is defined as the dimension of the subspace of $F^{(m)}$ spanned by $(a_{11}, a_{21}, \ldots\ldots, a_{m1}), \ldots\ldots, (a_{1n}, \ldots\ldots, a_{mn})$.

Theorem 19 : *Let A be an $m \times n$ matrix over F. Then*

Row rank of A = column rank of A.

Proof : Define $T : F^{(n)} \to F^{(m)}$ s.t.,

$$T((x_1, \ldots\ldots\ldots, x_n)) = (y_1, \ldots\ldots\ldots, y_m)$$

where $$y_i = \sum_{j=1}^n a_{ij} x_j$$

Then T is a linear transformation.

$$\begin{aligned}
\text{Range } T &= \{T(x_1, \ldots\ldots, x_n) \mid x_i \in F\} \\
&= \{T(x_1(1, \ldots\ldots, 0) + \ldots\ldots\ldots + x_n(0, \ldots 0, 1)) \mid x_i \in F\} \\
&= \{x_1 T(e_1) + \ldots\ldots\ldots + x_n T(e_n) \mid x_i \in F\}
\end{aligned}$$

e_i = nth-tuple with ith co-ordinate 1 and zero elsewhere

$= \{$linear combination of columns of $A\}$

$\subseteq$ subspace generated by columns of A and vice-versa

Thus, Range T = subspace of $F^{(n)}$ generated by columns of A

So, Rank T = column rank of A

Also, Rank T^t = column rank of A^t

= dimension of subspace of $F^{(m)}$ generated by columns of A^t

= dimension of subspace generated by rows of A

= Row rank of A

Thus, column rank of A

$$= \text{Row rank of } A \text{ (as Rank } T^t = \text{Rank } T)$$

$$= \text{Rank } T.$$

Problem 29 : *Let V be a finite dimensional vector space over F. Let T be a linear operator on V. Let $c \in F$. Suppose $\exists\, 0 \neq v \in V$ such that $T(v) = cv$. Prove that there is a non zero linear functional f on v s.t., $T^t f = cf$.*

Solution : Now $(T - cI)v = 0,\ v \neq 0$

$$\Rightarrow v \in \text{Ker}\,(T - cI)$$

$$\Rightarrow \text{Ker}\,(T - cI) \neq \{0\}$$

$$\Rightarrow \dim \text{Ker}\,(T - cI) \geq 1$$

$$\Rightarrow \text{nullity of } (T - cI) \geq 1$$

$$\Rightarrow \text{rank of } (T - cI) < n$$

$$\Rightarrow \text{rank of } (T - cI)^t < n$$

$$\Rightarrow \text{nullity of } (T - cI)^t \geq 1$$

$$\Rightarrow \exists\, f \in \hat{v} \text{ such that } f \neq 0 \text{ and } (T - cI)^t f = 0$$

$$\Rightarrow T^t f = cf,\ f \neq 0.$$

Problem 30 : *Let A be $m \times n$ matrix with real entries. Prove that $A = 0 \Leftrightarrow$ Trace $(A^t A) = 0$*

Solution : Let $A^t = B = (b_{ij})_{n \times m}$

$$A = (a_{jk})_{m \times n}$$

$$A^t A = BA = C = (c_{ik}),\ c_{ik} = \sum_{j=1}^{m} b_{ij} c_{jk}$$

$$\text{Trace } (A^t A) = 0$$

$$\Rightarrow \sum_{1}^{n} C_{ii} = 0$$

$$\Rightarrow C_{11} + \ldots\ldots + C_{nn} = 0$$

$$\Rightarrow \sum_{1}^{m} b_{ij}\, a_{ji} + \ldots\ldots + \sum_{1}^{m} b_{nj}\, a_{jn} = 0$$

$$\Rightarrow \sum (a_{ji})^2 + \ldots\ldots + \sum (a_{jn})^2 = 0$$

$$\Rightarrow a_{ji} = 0\ \forall\ i, j$$

$$\Rightarrow A = 0.$$

Converse is obvious.

Exercises

1. Let $S = \{\alpha_1, \alpha_2, \alpha_3\}$ be the basis of $\mathbf{C}^3$ defined by
$$\alpha_1 = (1, 0, -1),\ \alpha_2 = (1, 1, 1),\ \alpha_3 = (2, 2, 0)$$
Find the dual basis of S.

$$\{f_1(\alpha) = a - b,\ f_2(\alpha) = a - b + c,\ f_3(\alpha) = -\frac{a}{2} + b - \frac{c}{2},\ \alpha = (a, b, c)\})$$

2. Let $\{e_1, \ldots\ldots, e_n\}$ be the standard basis of $F^{(n)}$ (F = field). Define
$$\pi_i : F^{(n)} \to F \text{ s.t.,}$$
$$\pi_i(a_1, \ldots\ldots, a_n) = a_i$$
Show that π_i is a linear functional for all i and $\{\pi_1, \ldots\ldots, \pi_n\}$ is a dual basis of $\{e_1, \ldots\ldots, e_n\}$.

3. Let F be a subfield of the field of complex numbers and V a vector space over F. Suppose that f and g are linear functionals on V such that the function h defined by $h(v) = f(v)\, g(v)$ is also a linear functional on V. Prove that

   (*i*) $h(v) = 0$ for all $v \in V$

   (*ii*) $f = 0$ or $g = 0$

   (Hint (*ii*) suppose $g \neq 0$, $\exists\, v \in V$ s.t., $g(v) \neq 0 \Rightarrow f(v) = 0$
   $\therefore f(x - v)\ g(x - v) = 0$ for all $x \in V \Rightarrow f(x)\ g(v) = 0$ for all $x \in V$)

4. Let V be the vector space of polynomials over $\mathbf{R}$ of degree ≤ 1. Let $\varphi_1 : V \to \mathbf{R}$, $\varphi_2 : V \to \mathbf{R}$ be defined by
$$\varphi_1(f(x)) = \int_0^1 f(x)\, dx, \qquad \varphi_2(f(x)) = \int_0^2 f(x)\, dx$$
Show that $\{\varphi_1, \varphi_2\}$ is a basis of $\hat{V}$. Find a basis $\{v_1, v_2\}$ of V which is dual to $\{\varphi_1, \varphi_2\}$. $\quad [\{2 - 2x,\ -\frac{1}{2} + x\}]$

5. Suppose $u, v \in V$ and that $\varphi(u) = 0 \Rightarrow \varphi(v) = 0$ for all $\varphi \in \hat{V}$. Show that $v = \alpha u$ for some scalar α.

6. Let W be the subspace of $\mathbf{R}^3$ spanned by $(1, 1, 0)$ and $(0, 1, 1)$. Find a basis of the annihilator of W.
$$[\varphi(x, y, z) = x - y + z]$$

7. Let W be the subspace of $\mathbf{R}^4$ spanned by $(1, 2, -3, 4)$, $(1, 3, -2, 6)$ and $(1, 4, -1, 8)$. Find a basis of the annihilator of W.
$$[\varphi_1(x, y, z, t) = 5x - y + z,\ \varphi_2(x, y, z, t) = 2y - t]$$

8. Let W_1, W_2 be subspaces of a finite dimensional vector space. Show that
$$A(W_1 \cap W_2) = A(W_1) + A(W_2)$$
(Hint : apply problem (4) on $A(W_1)$ and $A(W_2)$)

9. Let n be a + ve integer and F, a field. Let

$$W = \{(x_1, \ldots\ldots, x_n) \in F^{(n)} \mid x_1 + \ldots\ldots + x_n = 0\}$$

Prove that $A(W) = \{f \mid f(x_1, \ldots\ldots, x_n) = c \sum_{j=1}^{n} x_j\}$

10. Let W be a subspace of a finite dimensional vector space. Define

$$\theta : \hat{V} \to \hat{W}$$

$$\theta(f) = f \mid W = \bar{f} \; (\bar{f}(w) = f(w) \text{ for all } w \in W)$$

Show that θ is onto linear transformation and $\operatorname{Ker} \theta = A(W)$.

(Thus $\dfrac{\hat{V}}{A(W)} \cong \hat{W}$).

Chapter 11

Eigen Values and Eigen Vectors

In this chapter we will be dealing with linear operators T on a finite dimensional vector space V. The main idea is to find an ordered basis β of V s.t., matrix of T w.r.t. β is a diagonal matrix. We can know a lot about T through this. The question that arises is "Can we find such an ordered basis for all linear operators?" and if not then for which operators such a basis would exist? We shall attempt to answer it in this chapter. If $\beta = \{v_1, \ldots, v_n\}$ s.t. $[T]_\beta = \text{diag}\ (c_1, \ldots, c_n)$, then $T(v_i) = cv_i$, $i = 1, \ldots, n$. This leads us to the concept of eigen values c_i and eigen vectors v_i of T. We start with

Definition : Let V be a vector space over F. Let T be a linear operator on V. If $\exists\ 0 \neq v \in V$ s.t., $T(v) = cv$ for some $c \in F$, then v is called an *eigen vector or characteristic vector* of T and c is called an *eigen value or characteristic value* of T.

Example 1 : Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be a linear operator defined by $T(x, y) = (x, 0)$. If $c \in \mathbf{R}$ is an eigen value of T, then $\exists\ (x, y) \neq (0, 0)$ in $\mathbf{R}^2$ s.t. $T(x, y) = c(x, y)$

$$\therefore \qquad (x,\ 0) = c(x,\ y) = (cx,\ cy) \Rightarrow cx = x,\ cy = 0$$

$$\Rightarrow x(c-1) = 0,\ cy = 0$$

Now $\qquad x(c-1) = 0 \Rightarrow x = 0$ or $c = 1$

If $x = 0$, then $y \neq 0$. $\therefore\ cy = 0 \Rightarrow c = 0$

If $c = 0$, then $(0, 1)$ is an eigen value of T as $T(0, 1) = (0, 0) = c(0, 1)$. $\therefore 0$ is an eigen value of T. If $c \neq 0$, then $y = 0$ and $c = 1$. $\therefore\ T(1, 0) = (1, 0) = 1\ (1, 0) \Rightarrow (1,0)$ is an eigen vector of T and 1 is an eigen value of T.

Example 2 : Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be a linear operator defined by $T(x, y) = (x + y, x + y)$.

Then $T(1, -1) = (0, 0) = 0(1, -1) \Rightarrow 0$ is an eigen value of T and $(1, -1)$ is an eigen value of T.

Also $T(1,\ 1) = (2,\ 2) = 2(1,\ 1) \Rightarrow 2$ is an eigen value of T and $(1, 1)$ is an eigen vector of T.

Remark : If 0 is an eigen value of T, then $\exists\ 0 \neq v \in V$ s.t. $T(v) = 0v = 0$ $\Rightarrow\ 0 \neq v \in \text{Ker}\ T$

$\Rightarrow$ Ker $T \neq \{0\} \Rightarrow T$ is not 1-1 $\Rightarrow T$ is singular.

Eigen Space : Let c be an eigen value of T.

Define $$W_c = \{v \in V \mid T(v) = cv\}$$

$$0 \in W_c \text{ as } T(0) = 0 = c.0 \Rightarrow W_c \neq \varphi$$

Let $\alpha, \beta \in F$, $v_1, v_2 \in V$. Then

$$\begin{aligned} T(\alpha v_1 + \beta v_2) &= \alpha T(v_1) + \beta T(v_2) \\ &= \alpha c v_1 + \beta c v_2 \\ &= c(\alpha v_1 + \beta v_2) \end{aligned}$$

$$\therefore \quad \alpha v_1 + \beta v_2 \in W_c$$

$\therefore$ W_c is a subspace of V.

W_c is called an *eigen space of* T associated with an eigen value c of T.

Example 3 : Let $T : \mathbf{R}^2 \to \mathbf{R}^2$ be defined by $T(x, y) = (x, 0)$.

As seen before, 1 is an eigen value of T.

$\therefore$ Eigen space of T associated with eigen value 1 is given by

$$\begin{aligned} W_1 &= \{(x, y) \mid T(x, y) = (x, y)\} \\ &= \{(x, y) \mid (x, 0) = (x, y)\} \\ &= \{(x, 0) \in \mathbf{R}^2 \mid x \in \mathbf{R}\} \\ &= x\text{-axis} \end{aligned}$$

Note : Eigen space $$\begin{aligned} W_c &= \{v \in V \mid T(v) = cv\} \\ &= \{v \in V \mid (T - cI)\, v = 0\} \\ &= \operatorname{Ker}(T - cI) \end{aligned}$$

i.e., W_c is the null space of $T - cI$.

Theorem 1 : *Let T be a linear operator on a finite dimensional vector space V over F. Then $c \in F$ is an eigen value of T if and only if $T - cI$ is singular (not invertible).*

Proof : Let c be an eigen value of T.

Then $$\exists\, 0 \neq v \in V \text{ s.t. } T(v) = cv$$

$$\therefore \quad (T - cI)\, v = 0$$

$$\Rightarrow 0 \neq v \in \operatorname{Ker} T - cI$$

$$\Rightarrow T - cI \text{ is not one-one}$$

$$\Rightarrow T - cI \text{ is singular.}$$

Conversely, $T - cI$ is singular $\Rightarrow$ $T - cI$ is not one-one (as $\dim V$ = finite $\Rightarrow$ $T - cI$ is one-one if and only if $T - cI$ is onto)

$$\Rightarrow \exists\, 0 \neq v \in \operatorname{Ker}(T - cI)$$

$$\Rightarrow (T - cI)\, v = 0,\ v \neq 0 \Rightarrow T(v) = cv,\ v \neq 0$$

$$\Rightarrow c \text{ is eigen value of } T.$$

Let A be an $n \times n$ matrix over a field F. $c \in F$ is eigen value of A if $A - cI$ is singular (not invertible), i.e. $\det(A - cI) = 0$.

Now, $\det(A - cI) = 0 \Leftrightarrow \det(cI - A) = 0$.

Let $$f(x) = \det(xI - A)$$

Then c is an eigen value of A if and only if $f(c) = 0$. For this reason $f(x)$ is called *characteristic polynomial* of A. Clearly deg $f(x) = n$ and coefficient of highest degree term x^n in $f(x)$ is 1 (i.e. $f(x)$ is monic).

Theorem 2 : *Similar matrices have same characteristic polynomial.*

Proof : Let A, B be similar matrices.

Then $\exists$ non singular matrix P s.t.

$$B = P^{-1}AP$$

$$\begin{aligned} \therefore \quad & \det(xI - B) \\ &= \det(xI - P^{-1}AP) \\ &= \det(P^{-1}(xI - A)P) \\ &= \det(xI - A). \end{aligned}$$

If β, β' are two ordered basis of V s.t. $[T]_\beta = A$, $[T]_{\beta'} = B$, then $B = P^{-1}AP$ for some matrix P.

$c \in F$ is an eigen value of operator T on a finite dimensional vector space V.

$$\begin{aligned} &\Leftrightarrow T - cI \text{ is singular by Theorem 1} \\ &\Leftrightarrow \det[T - cI]_\beta = 0 \\ &\Leftrightarrow \det\{[T]_\beta - cI\} = 0 \\ &\Leftrightarrow \det(A - cI) = 0 \\ &\Leftrightarrow c \text{ is an eigen value of } A. \end{aligned}$$

By theorem 2, A and B have same characteristic polynomial. So, c is an eigen value of $A \Leftrightarrow c$ is an eigen value of B.

Hence $c \in F$ is an eigen value of T if and only if c is an eigen value of corresponding matrix of T w.r.t. any basis of V.

If $[T]_\beta = A$, we say characteristic polynomial of T is $\det(A - xI)$, which does not depend on the basis of V by theorem 2.

Remarks :

1. If $T : V \to V$ is a linear operator s.t. $\dim V = n$, then $[T]_\beta$ is $n \times n$ matrix. Let $A = [T]_\beta$. Then $\det(A - xI)$ is a polynomial of degree n. So, A (or T) can't have more than n distinct eigen values.
2. T may not have any eigen value (See Problem 1).
3. Let $A = (a_{ij})$. Then
$$\det(xI - A) = x^n - (a_{11} + a_{12} + \ldots\ldots + a_{nn})x^{n-1} + \ldots\ldots$$
$\Rightarrow$ sum of eigen values of A (or T) is sum of diagonal elements of A
$\Rightarrow$ sum of eigen values of A (or T) is trace of A.
4. Put $x = 0$ in
$$\det(xI - A) = x^n - (a_{11} + \ldots\ldots + a_{nn})\, x^{n-1} \ldots\ldots + \text{constant term}$$

then $\det(-A)$ = constant term

$\Rightarrow (-1)^n \det A$ = constant term of characteristic polynomial of A or T.

5. If A is a matrix over $\mathbf{C}$, the field of complex numbers, then by fundamental theorem of algebra, characteristic polynomial of A must have a root in $\mathbf{C}$. In other words A (or T) has at least one eigen value in $\mathbf{C}$.

6. Let $c \in F$ be an eigen value of $n \times n$ matrix A over F.

Then $\det(cI - A) = 0$.

So, columns of $cI - A$ are linearly dependent over F.

$\therefore \exists\, \alpha_1, \alpha_2, \ldots\ldots, \alpha_n \in F$ such that $\alpha_1 c_1 + \ldots\ldots + \alpha_n c_n = 0$, $\alpha_i \neq 0$ for some i, where $c_1, \ldots\ldots, c_n$ are columns of $cI - A$.

$$\text{Thus, } [c_1,\ c_2, \ldots\ldots, c_n] \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

$$\therefore\ (cI - A) \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0$$

$$\text{So, } A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = c \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

$$\text{Hence } AX = cX, \text{ where } X = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} \neq 0$$

X is called an eigen vector of A.

Conversely, let $AX = cX$, $X \neq 0$ is an $n \times 1$ matrix over F.

$\therefore\ (cI - A)X = 0$

So, $\det(cI - A) = 0$ as $X \neq 0$.

Thus, c is an eigen value of A.

7. We now give a method of determining eigen vector of $A = [T]_\beta$, given an eigen vector of T and conversely.

Let $\{v_1, v_2, \ldots\ldots, v_n\} = \beta$ be an ordered basis of V. Let $A = (a_{ij}) = [T]_\beta$.

Now $0 \neq v \in V$ is an eigen vector of T

$\Leftrightarrow T(v) = cv$, for some $c \in F$

$\Leftrightarrow T(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n) = c(\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n)$, $\alpha_i \in F$

$$\Leftrightarrow \alpha_1 T(v_1) + \ldots\ldots + \alpha_n T(v_n) = c\alpha_1 v_1 + \ldots\ldots + c\alpha_n v_n$$

$$\Leftrightarrow \alpha_1(a_{11}v_1 + \ldots\ldots + a_{n1}v_n) + \ldots\ldots + \alpha_n(a_{1n}v_1 + \ldots\ldots + a_{nn}v_n) = c\alpha_1 v_1 + \ldots\ldots + c\alpha_n v_n$$

$$\Leftrightarrow \alpha_1 a_{11} + \ldots\ldots + \alpha_n a_{1n} = c\alpha_1$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\alpha_1 a_{n1} + \ldots\ldots + \alpha_n a_{nn} = c\alpha_n$$

$$\Leftrightarrow A\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix} = c\begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix}$$

$$\Leftrightarrow AX = cX, \text{ where } X = \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix} \neq 0.$$

So, if $v = \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n$ is an eigen vector of T, then $X = \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix}$ is an eigen vector of A and conversely.

8. Let c be an eigen value of $n \times n$ matrix A over F.

Then $W'_c = \{X \mid X = n \times 1$ matrix over F $AX = CX\}$, is a subspace of $n \times 1$ matrices over F. W'_c is called an eigen space of A w.r.t. eigen value c of A.

Let $A = [T]_\beta$, where T is a linear operator on V and β, an ordered basis of V. We show that dim W'_c = dim W_c, where W_c = eigen space of T w.r.t. eigen value c of T.

Define $\theta : W_c \to W'_c$ s.t.,

$$\theta(v) = \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{bmatrix} \text{ where } v = \alpha_1 v_1 + \ldots\ldots + \alpha_n v_n$$

Then θ is an isomorphism. (Verify !)

So, dim W_c = dim W'_c

9. Let $[T]_\beta = A$ = diagonal matrix

$$= \begin{bmatrix} c_1 & & O \\ & \ddots & \\ O & & c_n \end{bmatrix}$$

Suppose Rank $A = r$. So, r entries in diagonal of A are non-zeros and all other entries are zeros. Let first r entries $c_1, \ldots\ldots, c_r$ be all non-zero and $c_{r+1} = \ldots\ldots = c_n = 0$. Let $\beta = \{v_1, \ldots\ldots, v_r, v_{r+1}, \ldots\ldots, v_n\}$ = ordered basis of V. Then, $T(v_i) = c_i v_i$, $i = 1, 2, \ldots\ldots, r$. Now

$\{T(v_1), \ldots\ldots, T(v_r)\} \subseteq$ Range T. Let $\alpha_1 T(v_1) + \ldots\ldots + \alpha_r T(v_r) = 0, \alpha_i \in F$.

Then $\alpha_1 c_1 v_1 + \ldots\ldots + \alpha_r c_r v_r = 0$

$\Rightarrow \alpha_i c_i = 0 \ \forall i = 1, 2, \ldots\ldots, r$

$\Rightarrow \alpha_i = 0 \ \forall i = 1, 2, \ldots\ldots, r$ as $c_i \neq 0$

$\therefore S = \{T(v_1), \ldots\ldots, T(v_r)\}$ is a *L.I.* set.

Let $T(v) \in$ Range T.

Now $v \in V \Rightarrow v = \beta_1 v_1 + \ldots\ldots + \beta_r v_r + \beta_{r+1} v_{r+1} + \ldots\ldots$

$\Rightarrow T(v) = \beta_1 T(v_1) + \ldots\ldots + \beta_r T(v_r)$

$\Rightarrow S$ spans Range T

$\Rightarrow S$ = basis of Range T

$\Rightarrow$ dim Range $T = r$

$\Rightarrow$ Rank $T = r$

So, Rank A = Rank T, where $[T]_\beta = A$ = diagonal matrix.

Infact, Rank A = Rank T, even when A is not diagonal matrix.

Problem 1 : *Let T be a linear operator on $\mathbf{R}^2$ which is represented in the standard ordered basis by the matrix*

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Show that T has no eigen values in **R**.

Solution : The characteristic polynomial of A (or T) is given by

$$\det(xI - A) = \begin{vmatrix} x & 1 \\ -1 & x \end{vmatrix} = x^2 + 1$$

which has no real roots. So T has no eigen values in **R**. However $\pm i$ are eigen values of T in **C**.

Problem 2 : *Let $c \neq 0$ be an eigen value of an invertible operator T. Show that c^{-1} is an eigen value of T^{-1}.*

Solution : Since c is an eigen value of T, $\exists\, 0 \neq v \in V$ s.t.

$$T(v) = cv$$

$$\Rightarrow v = T^{-1}(cv) = c(T^{-1}(v))$$

$$\Rightarrow c^{-1} v = T^{-1}(v)$$

$\Rightarrow c^{-1}$ is an eigen value of T^{-1}.

Problem 3 : *Obtain the eigen values, eigen vectors and eigen spaces of*

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Solution : The characteristic polynomial of A is

$$\det(xI - A) = \begin{vmatrix} x & -1 & 0 \\ -1 & x & 0 \\ 0 & 0 & x-1 \end{vmatrix} = (x+1)(x-1)^2$$

$\therefore$ eigen values of A are 1, –1.

The eigen vector corresponding to eigen value 1 is given by

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$\therefore \qquad \begin{aligned} x_2 &= x_1 \\ x_1 &= x_2 \\ x_3 &= x_3 \end{aligned}$$

Thus eigen vectors are

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + x_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

So, eigen space W_1 corresponding to eigen value 1 is spanned by $\left\{ \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$

which is linearly independent.

$$\therefore \qquad \dim W_1 = 2$$

Also eigen vectors corresponding to eigen value –1 are given by

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = (-1) \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

giving $\qquad x_1 = -x_1,\ x_1 = -x_2,\ x_3 = -x_3$

$$\therefore \qquad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_1 \\ 0 \end{bmatrix} = x_1 \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$$

i.e., eigen space W_{-1} corresponding to eigen value –1 is spanned by $\begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$

$$\therefore \qquad \dim W_{-1} = 1$$

$\therefore$ eigen values are ± 1 and eigen vectors are $\begin{bmatrix}1\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\-1\\0\end{bmatrix}$.

Problem 4 : *Let A be a real $n \times n$ matrix. Let λ be a real eigen value of A. Show that there exists an eigen vector X of A corresponding to eigen value λ such that X is also real.*

Solution : Suppose $Ay = \lambda y$, $y \neq 0$. Then y is eigen vector of A corresponding to eigen value λ of A. If y is real, then result follows. Suppose y is not real. Let $y = u + iv$ where u and v real column matrices.

Then
$$\begin{aligned} Ay &= \lambda y \\ \Rightarrow A(u+iv) &= \lambda(u+iv) \\ \Rightarrow Au + iAv &= \lambda u + i\lambda v \\ \Rightarrow Au &= \lambda u, \; Av = \lambda v \end{aligned}$$

Since $y \neq 0$, either $u \neq 0$ or $v \neq 0$. If $u \neq 0$, then u is real eigen vector of A and $v \neq 0 \Rightarrow v$ is real eigen vector of A corresponding to eigen value λ of A.

Problem 5 : *Let A be $n \times n$ matrix given by*

$$A = \begin{bmatrix} k & 1 & 0 & \dots & \dots & 0 \\ 1 & k & 1 & \dots & \dots & 0 \\ 0 & 1 & k & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & k \end{bmatrix}$$

(i.e. diagonal entries of A are k and entries above and below the diagonal are 1 and zero elsewhere).

Show that $X_i (i = 1, \dots\dots, n)$ where X_is are column matrices with jth entry $\{\sin \frac{ij\pi}{n+1}\}$ are eigen vectors of A. Find corresponding eigen values of A.

Solution : Now

$$AX_i = \begin{bmatrix} k & 1 & 0 & \dots & \dots & 0 \\ 1 & k & 1 & \dots & \dots & 0 \\ 0 & 1 & k & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & k \end{bmatrix} \begin{bmatrix} \sin \frac{i\pi}{n+1} \\ \sin \frac{2i\pi}{n+1} \\ \sin \frac{3i\pi}{n+1} \\ \dots\dots\dots \\ \sin \frac{ni\pi}{n+1} \end{bmatrix} = \begin{bmatrix} k \sin \frac{i\pi}{n+1} + \sin \frac{2i\pi}{n+1} \\ \sin \frac{i\pi}{n+1} + k \sin \frac{2i\pi}{n+1} + \sin \frac{3i\pi}{n+1} \\ \sin \frac{2i\pi}{n+1} + k \sin \frac{3i\pi}{n+1} + \sin \frac{4i\pi}{n+1} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \sin \frac{(n-1)\, i\pi}{n+1} + k \sin \frac{ni\pi}{n+1} \end{bmatrix}$$

$$= \begin{bmatrix} k\sin\frac{i\pi}{n+1} + 2\sin\frac{2i\pi}{n+1}\cos\frac{i\pi}{n+1} \\ k\sin\frac{2i\pi}{n+1} + 2\sin\frac{2i\pi}{n+1}\cos\frac{i\pi}{n+1} \\ k\sin\frac{3i\pi}{n+1} + 2\sin\frac{3i\pi}{n+1}\cos\frac{i\pi}{n+1} \\ \cdots\cdots\cdots\cdots \\ k\sin\frac{ni\pi}{n+1} + 2\sin\frac{ni\pi}{n+1}\cos\frac{i\pi}{n+1} \end{bmatrix}$$

$$= \begin{bmatrix} (k + 2\cos\frac{i\pi}{n+1}\sin\frac{i\pi}{n+1} \\ (k + 2\cos\frac{i\pi}{n+1}\sin\frac{2i\pi}{n+1} \\ (k + 2\cos\frac{i\pi}{n+1}\sin\frac{3\pi}{n+1} \\ \cdots\cdots\cdots\cdots \\ (k + 2\cos\frac{i\pi}{n+1}\sin\frac{n\pi}{n+1} \end{bmatrix}$$

$$= (k + 2\cos\frac{i\pi}{n+1}) \begin{bmatrix} \sin\frac{i\pi}{n+1} \\ \sin\frac{2i\pi}{n+1} \\ \sin\frac{3i\pi}{n+1} \\ \cdots\cdots \\ \sin\frac{ni\pi}{n+1} \end{bmatrix}$$

$$= (k + 2\cos\frac{i\pi}{n+1})X_i$$

$\therefore$ X_i are eigen vectors of A for each $i = 1, \ldots\ldots, n$ and $k + 2\cos\frac{i\pi}{n+1}$ are corresponding eigen values of A.

Definition : A linear operator T on a finite dimensional vector space V is called *diagonalizable* if $\exists$ an ordered basis $\beta = \{v_1, \ldots\ldots, v_n\}$ of V s.t. matrix of T w.r.t. β is a diagonal matrix.

i.e., $$[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & c_2 & \\ & & \ldots \\ 0 & & c_n \end{bmatrix}$$

Cor. : *A* linear operator T on the finite dimensional vector space V is diagonisable if and only if $\exists$ a basis β of V consisting of eigen vectors of T.

Proof : Let T be diagonisable.

Then $\exists$ a basis $\beta = \{v_1, \ldots\ldots, v_n\}$ of V s.t.,

$$[T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & c_2 & \\ & & \cdots \\ 0 & & c_n \end{bmatrix}$$

i.e. $\qquad T(v_i) = c_i v_i$ for all $i = 1, \ldots\ldots, n$.

$\therefore$ $v_1, \ldots\ldots, v_n$ are eigen vectors of T.

Conversely, let $\beta = \{v_1, \ldots\ldots, v_n\}$ be a basis of V s.t. each v_i is an eigen vector of T.

Then $\qquad [T]_\beta = \begin{bmatrix} c_1 & & 0 \\ & \ldots\ldots & \\ 0 & & c_n \end{bmatrix}$ is a diagonal matrix

$\therefore$ T is diagonisable.

We now discuss conditions under which opertor T is diagonisable.

Theorem 3 : *Let T be a linear operator on a finite dimensional vector space V. Let $c_1, \ldots\ldots, c_k$ be the distinct eigen values of T and W_i be the eigen space of T corresponding to eigen value c_i. Then the following are equivalent.*

(*i*) *T is diagonisable.*

(*ii*) *The characteristic polynomial for T is*

$$f(x) = (x - c_1)^{d_1} \ldots\ldots (x - c_k)^{d_k}$$

where $\dim W_i = d_i$, $d_1 + \ldots\ldots + d_k = n = \dim V$

(*iii*) $\dim W_1 + \ldots\ldots + \dim W_k = \dim V$

Proof : (*i*) $\Rightarrow$ (*ii*)

Since T is diagonisable, $\exists$ an ordered basis $\beta = \{v_1, \ldots\ldots, v_n\}$ s.t. $[T]_\beta = \begin{bmatrix} c_1 & \ddots & 0 \\ 0 & \ddots & c_n \end{bmatrix}$

Suppose c_1 appears d_1 times, ..., c_k appears d_k times, then

$$[T]_\beta = \begin{bmatrix} c_1 & & & & & O \\ & \vdots & & & & \\ & & c_1 & & & \\ & & & \cdots & & \\ & & & & c_k & \\ & & & & & \vdots \\ O & & & & & c_k \end{bmatrix}$$

$\therefore$ characteristic polynomial for T is given by

$$f(x) = (x-c_1)^{d_1} \ldots\ldots (x-c_k)^{d_k}, \quad d_1 + \ldots\ldots + d_k = n$$

$\therefore$ $[T-c_iI]_\beta$ has only d_i zeros on the diagonal for all $i = 1, \ldots\ldots, k$

$\therefore$ Rank $[T-c_iI] = n-d_i$ for all $i = 1, \ldots\ldots, k$ (See Remark 9)

$\Rightarrow$ nullity $(T-c_iI) = d_i$ for all $i = i, \ldots\ldots, k$

$\Rightarrow$ dim $W_i = d_i$ for all $i = 1, \ldots\ldots, k$. (W_i = Ker $(T-c_iI)$)

$(ii) \Rightarrow (iii)$ obvious

$(iii) \Rightarrow (i)$

We first prove three lemmas

Lemma 1 : *Let* $f(x) = a_o + a_1x + \ldots\ldots + a_m x^m \qquad a_i \in F$

Let c be an eigen value of linear operator T on a finite dimensional vector space V over F. Then $f(T)v = f(c)v$, *where* $T(v) = cv$.

Proof : Now $T(v) = cv$

$$\Rightarrow T^2(v) = T(cv) = cT(v) = c^2v$$

In general, $T^r(v) = c^rv$

$$\therefore \quad f(T) = a_oI + a_1T + \ldots\ldots + a_mT^m$$

$$\Rightarrow f(T)v = a_ov + a_1Tv + \ldots\ldots + a_mT^mv$$

$$= a_ov + a_1cv + \ldots\ldots + a_mc^mv$$

$$= (a_o + a_1c + \ldots\ldots + a_mc^m)v$$

$$= f(c)v.$$

Lemma 2 : *If* $x_1 + \ldots\ldots + x_k = 0$, $x_i \in W_i$, *then* $x_i = 0$ *for all i.*

Proof : Now $0 = f(T)0$

$$= f(T)(x_1 + \ldots\ldots + x_k)$$

$$= f(T)x_1 + \ldots\ldots + f(T)x_k$$

$$= f(c_1)x_1 + \ldots\ldots + f(c_k)x_k \text{ (by lemma 1) (as } T(x_i) = c_ix_i)$$

$$\therefore \quad f(c_1)x_1 + \ldots\ldots + f(c_k)x_k = 0$$

for any polynomial $f(x) \in F[x]$

Define $\quad f_i(x) = (x-c_1) \ldots\ldots (x-c_{i-1})(x-c_{i+1})$

$$\ldots\ldots (x-c_k)(c_i-c_1)^{-1} \ldots\ldots (c_i-c_k)^{-1}$$

for all $i = 1, \ldots\ldots, k$

Then $\quad f_i(c_i) = 1$ for all $i = 1, \ldots\ldots, k$

and $\quad f_i(c_j) = 0$ for all $i \neq j$

$$\therefore \quad f_i(c_1)x_1 + \ldots\ldots + f_i(c_i)x_i + \ldots\ldots + f_i(c_k)x_k = 0 \text{ for all } i$$

$$\Rightarrow f_i(c_i)x_i = 0 \text{ for all } i$$

$$\Rightarrow x_i = 0 \text{ for all } i = 1, \ldots\ldots, k.$$

Lemma 3 : *Suppose* $\beta_1, \ldots\ldots, \beta_k$ *are basis of* $W_1, \ldots\ldots, W_k$ *respectively. Then* $\beta = \{\beta_1, \ldots\ldots, \beta_k\}$ *is a basis of* $W = W_1 + \ldots\ldots + W_k$. *Hence* $\dim W = \dim W_1 + \ldots\ldots + \dim W_k$.

Proof : Let $x \in W$. Then $x = x_1 + \ldots\ldots + x_k$, $x_i \in W_i$ as $W = W_1 + \ldots\ldots + W_k$

Now $\beta_1 = \{v_1, \ldots\ldots v_{d_1}\}$ spans W_1

In this way, since $\beta_k = \{v'_1, \ldots\ldots, v'_{d_k}\}$ spans W_k

we find $x_k = \beta_1 v_1 + \ldots\ldots + \beta_{d_k} v'_{d_k}$

So, $x = \alpha_1 v_1 + \ldots\ldots + \alpha_{d_1} v_{d_1} + \ldots\ldots + \beta_1 v_1' + \ldots\ldots + \beta_{d_k} v'_{d_k}$

$= $ linear combination of $v_1, \ldots\ldots, v_{d_1}, \ldots\ldots, v'_{d_1}, \ldots, v'_{d_k}$

$\Rightarrow \{\beta_1, \beta_2, \ldots\ldots, \beta_k\} = \beta$ spans W.

Suppose $(\alpha_1 v_1 + \ldots\ldots + \alpha_{d_1} v_{d_1}) + \ldots\ldots + (\beta_1 v_1' + \ldots\ldots + \beta_{d_k} v'_{d_k}) = 0$

$\Rightarrow x_1 + \ldots\ldots + x_k = 0$

where $x_1 = \alpha_1 v_1 + \ldots\ldots + \alpha_{d_1} v_{d_1} \in W_1$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$x_k = \beta_1 v_1' + \ldots\ldots + \beta_{d_k} v'_{d_k} \in W_k$

Then $x_i = 0$ for all i by lemma 2

$\Rightarrow \alpha_1 = \ldots\ldots = \alpha_{d_1} = \ldots\ldots = \beta_1 = \ldots\ldots = \beta_{d_k} = 0$

as each β_i is basis of W_i

$\Rightarrow \beta = \{\beta_1, \ldots\ldots, \beta_k\}$ is linearly independent and so forms a basis of W.

Now $\dim W = o(\beta_1) + \ldots\ldots + o(\beta_k)$

$= \dim W_1 + \ldots\ldots + \dim W_k$

This proves lemma 3.

Proof of (*iii*) $\Rightarrow$ (*i*). Since $\dim V = \dim W_1 + \ldots\ldots + \dim W_k$ by (*iii*) and by lemma 3, $\dim W = \dim W_1 + \ldots\ldots + \dim W_k$, we have $\dim V = \dim W$. So, $V = W$.

Hence $V = W_1 + \ldots\ldots\ldots + W_k$. Thus $\beta = \{\beta_1, \ldots\ldots, \beta_k\}$ is a basis of V (by lemma 3) consisting of eigen vectors of T.

$\therefore$ T is diagonisable.

This proves (*i*).

Cor. : Let T be a linear operator on an n-dimensional vector space V, and suppose that T has n distinct characteristic values. Then T is diagonalisable.

Proof : Let $c_1, \ldots\ldots, c_n$ be distinct eigen values of T and $v_1, \ldots\ldots, v_n$ be corresponding eigen vectors of T.

$\therefore$ $T(v_i) = c_i v_i$ for all $i = 1, \ldots\ldots, n$

$\Rightarrow (T - cI)v_i = 0$ for all i, $v_i \neq 0$

$$\Rightarrow \; 0 \neq v_i \in \text{Ker}\,(T - c_i I)$$
$$\Rightarrow \; \dim \; (\text{Ker}\,(T - c_i I) \geq 1$$
$$\Rightarrow \; \dim W_i \geq 1, \text{ where } W_i = \text{Ker}\,(T - c_i I) = \text{ eigen space of } T$$
$$\Rightarrow \; \dim W_1 + \ldots\ldots + \dim W_n \geq n = \dim V$$
$$\Rightarrow \; \dim (W_1 + \ldots\ldots + W_n) \geq \dim V$$
$$\Rightarrow \; \dim (W_1 + \ldots\ldots + W_n) = \dim V \text{ as } W_1 + \ldots\ldots + W_n \subseteq V$$
$$\Rightarrow \; \dim W_1 + \ldots\ldots + \dim W_n = \dim V$$
$$\Rightarrow \; T \text{ is diagonalisable by Theorem 3.}$$

Note : If T is diagonalisable operator, then $\exists$ a basis β of V s.t. $[T]_\beta$ = diagonal matrix = A. If β' is any other basis of V, then $\exists$ matrix P s.t. $[T]_{\beta'} = P^{-1}AP$. We say that $[T]_{\beta'}$ is similar to diagonal matrix. So if T is diagonalisable, then matrix of T w.r.t. any basis is similar to a diagonal matrix. This leads us to the following definition.

Let A be $n \times n$ matrix. We say A is diagonalisable if A is similar to a diagonal matrix, i.e. $A = P^{-1}BP$, B = diagonal matrix.

Remark : Let $A = [T]_\beta$. Suppose A is diagonalisable. Then T is diagonalisable.

Proof : Since A is diagonalisable, $\exists$ matrix P s.t. $A = P^{-1}BP$, where B = diagonal matrix $(c_1, \ldots\ldots, c_1, \ldots\ldots, c_k, \ldots\ldots, c_k)$

$\therefore$ $f(x)$ = characteristic polynomial of T

$$= (x - c_1)^{d_1} \ldots\ldots (x - c_k)^{d_k}, \text{ where}$$

c_is are distinct and $d_1 + \ldots\ldots + d_k = n = \dim V$.

Now
$$B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = c_1 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

$\therefore$
$$X_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \text{ eigen vector of } B \text{ w.r.t. eigen value } c_1 \text{ of } B$$

So,
$$\begin{aligned} A(P^{-1}X_1) &= (P^{-1}BP)(P^{-1}X_1) \\ &= P^{-1}BX_1 \\ &= P^{-1}c_1X_1 \\ &= c_1(P^{-1}X_1) \end{aligned}$$

$\therefore$ $P^{-1}X_1$ = eigen vector of A w.r.t. eigen value c_1 of A. Similarly,

$$X_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \text{eigen vector of } B.$$

$$\Rightarrow P^{-1}X_2 = \text{eigen vector of } A.$$

In this way, $X_1, X_2, \ldots, X_{d_1}$ are eigen vectors of B

$\Rightarrow P^{-1}X_1, P^{-1}X_2, \ldots\ldots P^{-1}X_{d_1}$ are eigen vectors of A w.r.t. eigen value c_1.

Let $$\sum_{i=1}^{d_1} \alpha_i P^{-1} X_i = 0, \quad \alpha_i \in F$$

Then $$P^{-1}\sum_{i=1}^{d_1} \alpha_i X_i = 0 \Rightarrow \sum_{i=1}^{d_1} \alpha_i X_i = 0 \Rightarrow \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{d_1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$$

$\therefore \quad \alpha_i = 0 \quad \forall\, i = 1, \ldots\ldots, d_1$

So, $P^{-1}X_1, \ldots\ldots, P^{-1}X_{d_1}$ are *L.I.* vectors.

$\therefore$ dim $W'_{c_1} \geq d_1$, where W'_{c_1} = eigen space of A w.r.t. eigen value c_1 of A.

So, dim $W_{c_1} \geq d_1$, where W_{c_1} = eigen space of T w.r.t. eigen value c_1 of T.

Similarly,

$$\dim W_{c_i} \geq d_i \quad \forall\, i = 1, 2, \ldots\ldots, k.$$

Suppose dim $W_{c_i} > d_i$ for some i. Let $W = W_{c_1} + \ldots\ldots + W_{c_k}$.

Then $\dim W = \sum_{i=1}^{k} \dim W_{c_i} > d_1 + \ldots\ldots + d_i + \ldots\ldots + d_k = n.$

$\therefore$ dim $W >$ dim V, a contradiction.

So, dim $W_{c_i} = d_i \;\forall\; i$.

Hence T is diagonalisable by theorem 3

Theorem 4 : *Let T be a linear operator on a finite dimensional vector space V over F. Let $c_1, \ldots\ldots, c_k$ be distinct eigen values of T and $v_1, \ldots\ldots, v_k$ be corresponding eigen values of T. then $v_1, \ldots\ldots, v_k$ are linearly independent.*

Proof : Let W_i be eigen space of T corresponding to eigen value c_i. By lemma 3 in Theorem 3, $\{\beta_1, \ldots\ldots, \beta_k\}$ is a basis of $W_1 + \ldots\ldots + W_k$ where each β_i is a basis of W_i. Since $v_i \neq 0$, $(v_i \in W_i)$ it is linearly independent and can be extended to form a basis β_i of W_i. $\therefore$ $v_i \in \beta_i$ for all i.

$\therefore$ $\{v_1, \ldots\ldots, v_k\} \subseteq \{\beta_1, \ldots\ldots, \beta_k\}$ = linearly independent

$\Rightarrow$ $\{v_1, \ldots\ldots, v_k\}$ is linearly independent.

Remark : Let $X_1, \ldots\ldots, X_k$ be eigen vectors corresponding to eigen values $c_1, c_2, \ldots\ldots, c_k$ of an $n \times n$ matrix A over F. Then $\{X_1, \ldots\ldots, X_k\}$ is a *L.I.* set.

Let $$X_1 = \begin{bmatrix} \alpha_{11} \\ \cdots \\ \cdots \\ \alpha_{n1} \end{bmatrix}, \ldots\ldots\ldots, X_k = \begin{bmatrix} \alpha_{1k} \\ \cdots \\ \cdots \\ \alpha_{nk} \end{bmatrix}$$

Then $$AX_i = c_i X_i$$

Let $\beta = \{e_1, e_2, \ldots\ldots, e_n\}$ be a basis of some vector space V, then $\exists$ a linear transformation $T : V \to V$, s.t.,

$$T(e_1) = a_{11}e_1 + \ldots\ldots + a_{n1}e_n$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$T(e_n) = a_{1n}e_1 + \ldots\ldots\ldots + a_{nn}e_n$$

where $A = (a_{ij})$.

Then $A = [T]_\beta$

Let $v_1 = \alpha_{11}e_1 + \ldots\ldots + \alpha_{n1}e_n$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$v_k = \alpha_{1k}e_1 + \ldots\ldots\ldots + \alpha_{nk}e_n$$

Then $v_1, \ldots\ldots, v_k$ are eigen vectors of T s.t.,

$T(v_i) = c_i v_i$, $i = 1, 2, \ldots\ldots, k$ (See Remark 7, page 450)

$\therefore$ By theorem 4, $\{v_1, v_2, \ldots\ldots, v_k\}$ is L.I.

Let $$\beta_1 X_1 + \ldots\ldots + \beta_k X_k = 0, \ \beta_i \in F$$

Then $$\beta_1 \begin{bmatrix} \alpha_{11} \\ \cdots \\ \cdots \\ \alpha_{n1} \end{bmatrix} + \ldots\ldots + \beta_k \begin{bmatrix} \alpha_{1k} \\ \cdots \\ \cdots \\ \alpha_{nk} \end{bmatrix} = 0$$

Thus $$\beta_1\alpha_{11} + \ldots\ldots + \beta_k\alpha_{1k} = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\beta_1\alpha_{n1} + \ldots\ldots + \beta_k\alpha_{nk} = 0$$

So, $$\beta_1(\alpha_{11}e_1 + \ldots\ldots + \alpha_{n1}e_n) + \ldots\ldots + \beta_k(\alpha_{1k}e_1 + \ldots\ldots + \alpha_{nk}e_n) = 0$$
$$\Rightarrow \beta_1 v_1 + \ldots\ldots + \beta_k v_k = 0$$
$$\Rightarrow \beta_i = 0 \ \forall i$$
$$\Rightarrow \{X_1, X_2, \ldots\ldots, X_k\} \text{ is a } L.I. \text{ set.}$$

Theorem 5 : *Let A be $n \times n$ matrix s.t. $c_1, \ldots\ldots, c_n$ are distinct eigen values of A. Let $X_1, \ldots\ldots, X_n$ be corresponding eigen vectors of A. Let $P = (X_1, \ldots\ldots, X_n)$ be $n \times n$ matrix. Then A is diagonalisable and $P^{-1}AP = diag\,(c_1, \ldots\ldots, c_n)$.*

Proof : Now $AP = A(X_1, \ldots\ldots, X_n)$
$$= (AX_1, \ldots\ldots, AX_n)$$
$$= (c_1X_1, \ldots\ldots, c_nX_n)$$
$$= (X_1, \ldots\ldots, X_n)\begin{bmatrix} c_1 & & 0 \\ & \ldots & \\ 0 & & c_n \end{bmatrix}$$
$$= P \text{ diag } (c_1, \ldots\ldots, c_n)$$

Since $X_1, \ldots\ldots, X_n$ are linearly independent (by Theorem 4), P is invertible.

$\therefore$ $$P^{-1}AP = \text{diag}\,(c_1, \ldots\ldots, c_n)$$

Theorem 5 provides us with a method of diagonalising a matrix.

Problem 6 : *Let A be $n \times n$ triangular matrix over F. Prove that the eigen values of A are diagonal entries.*

Solution :

Let $$A = \begin{bmatrix} a_{11} & & & \\ & a_{22} & & \\ & & \ldots & \\ 0 & & & a_{nn} \end{bmatrix}, \quad a_{ij} = 0 \text{ for all } i > j$$

Characteristic polynomial of A is
$$(x - a_{11}) \ \ldots\ldots \ (x - a_{nn})$$

$\therefore$ $a_{11}, \ldots\ldots, a_{nn}$ are eigen values of A.

Problem 7 : *Let*
$$A = \begin{bmatrix} 6 & -3 & -2 \\ 4 & -1 & -2 \\ 10 & -5 & -3 \end{bmatrix}$$

Show that A is not similar over **R** *to a diagonal matrix whereas A is similar over* **C** *to a diagonal matrix.*

Solution : Characteristic polynomial of A is $(x-2)(x^2+1)$

If A is similar to a diagonal matrix over **R**, then $\exists$ matrix P s.t.

$P^{-1}AP$ = diag (a, b, c), a, b, c are real. Eigen values of $P^{-1}AP$ are eigen values of $A = 2, \pm i$. But eigen values of diag (a, b, c) are a, b, c by (problem 6) where a, b, c are all real, a contradiction.

$\therefore$ A is not similar over $\mathbf{R}$ to a diagonal matrix.

Since eigen values of A are distinct, by Theorem 5, A is similar over $\mathbf{C}$ to a diagonal matrix.

Problem 8 : *Let V be the space of $n \times n$ matrices over F. Let A be a fixed $n \times n$ matrix over F. Let T be a linear operator "left multiplication by A" on V. Is it true that A, T have the same characteristic values?*

Solution : Let c be an eigen value of A.

Then $AX = cX$ for some $0 \neq X$ ($X = n \times 1$ matrix).

Now $T(XX^t) = AXX^t = cXX^t$ (X^t means transpose of X)

If $XX^t = 0$, then

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} [x_1, \ldots\ldots, x_n] = 0$$

$$\Rightarrow x_1^2 + \ldots\ldots + x_n^2 = 0$$

$$\Rightarrow x_i = 0 \text{ for all } i \Rightarrow X = 0, \text{ a contradiction}$$

$$\therefore \quad XX^t \neq 0$$

So, c is also an eigen value of T.

Conversely, let c be an eigen value of T.

Then $\exists\, 0 \neq B \in V$ s.t. $T(B) = cB$

$$\Rightarrow AB = cB$$

$$\Rightarrow ABX = cBX \text{ for all column matrices } X$$

If $BX = 0$ for all X, then $B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0$

$\Rightarrow$ Ist column of B is zero.

Similarly, $B \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = 0 \Rightarrow$ 2nd column of B is zero.

In this way, all columns of B are zero.

$\therefore$ $BX \neq 0$ for some X

$\therefore$ c is also an eigen value of A.

Thus T and A have same eigen values.

Problem 9 : *Let V be the space of all real valued continuous functions. Define*

$$T : V \to V \text{ by } (Tf)(x) = \int_0^x f(t)\, dt$$

Show that T has no eigen values.

Solution : Let c be an eigen value of T.

$\therefore$ $\exists\, 0 \neq f \in V$ s.t.

$$Tf = cf$$

$\therefore$ $$Tf(x) = cf(x)$$

$\therefore$ $$\int_0^x f(t)\, dt = cf(x)$$

$$f(x) = cf'(x)$$

$$y = c\frac{dy}{dx}$$

$c \neq 0$ (as $c = 0 \Rightarrow y = 0 \Rightarrow f(x) = 0 \Rightarrow f = 0$)

$\therefore$ $$\frac{dy}{y} = \frac{dx}{c}$$

$$\Rightarrow \log y = \frac{x}{c} + \log a \Rightarrow y = ae^{x/c}$$

$$\Rightarrow y(0) = a$$

$$\Rightarrow f(x) = y = f(0)\, e^{x/c}$$

$$\Rightarrow \int_0^x f(0)\, e^{t/c}\, dt = \int_0^x f(t)\, dt = cf(x) = cf(0)\, e^{x/c}$$

$f(0) \neq 0$ (as $f(0) = 0 \Rightarrow a = 0 \Rightarrow y = 0 \Rightarrow f(x) = 0 \Rightarrow f = 0$)

$\therefore$ $$f(0)\left[ce^{t/c}\right]_0^x = cf(0)\, e^{x/c}$$

$\therefore$ $$c(e^{x/c} - 1) = ce^{x/c}$$

$$\Rightarrow e^{x/c} - 1 = e^{x/c}$$

$$\Rightarrow 1 = 0, \text{ a contradiction}$$

$\therefore$ T has no eigen value.

Problem 10 : *Let T be the linear operator on $\mathbf{R}^4$ which is represented in the standard ordered basis by* $\begin{bmatrix} 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \end{bmatrix}$. *Under what conditions on a, b, c is T diagonalisable?*

Solution : Clearly 0 is only eigen value of T. Let W be corresponding eigen space. Then T is diagonisable $\Leftrightarrow$ $\dim W = 4$. $W = \{v \in V \mid Tv = 0\} = \operatorname{Ker} T$.
$\therefore$ $\dim W = 4 \Leftrightarrow \dim \operatorname{Ker} T = 4$.

But $\dim \operatorname{Ker} T = 4 \Leftrightarrow \operatorname{Rank} T = 0 \Leftrightarrow T = 0$, i.e., $a = b = c = 0$.

Problem 11 : *Let N be 2×2 complex matrix such that $N^2 = 0$. Prove that either $N = 0$ or N is similar over $\mathbf{C}$ to* $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

Solution : Let $T : V \to V$ be a linear operator such that

$$[T]_\beta = N, \ \beta = \{v_1, v_2\} \text{ is a basis of } V.$$

Now $\quad 0 = N^2 = N.N = [T]_\beta \, [T]_\beta = [T^2]_\beta$

$$\Rightarrow T^2 = 0.$$

Suppose $N \neq 0$, i.e., $T \neq 0$.

Let λ be an eigen value of T.

Then there exists $0 \neq v \in V$ s.t.

$$T(v) = \lambda v$$
$$\Rightarrow T^2(v) = \lambda(T(v)) = \lambda^2 v$$
$$\Rightarrow 0 = \lambda^2 v$$
$$\Rightarrow \lambda^2 = 0 \text{ as } v \neq 0$$
$$\Rightarrow \lambda = 0$$
$$\Rightarrow 0 \text{ is the only eigen value of } T.$$

Let W_o be the eigen space of T w.r.t. eigen value 0.

Then $\quad W_o = \{x \in V \mid T(x) = 0\} = \operatorname{Ker} T$

Since $\quad 0 \neq v \in W_o, \ W_o \neq \{0\}$

So, $\dim W_o = 1$ or 2.

If $\dim W_o = 2$, then $\dim W_o = \dim V$

$\Rightarrow W_o = V \Rightarrow \operatorname{Ker} T = V \Rightarrow T = 0$, which is not true.

Therefore, $\dim W_o = 1$.

Let $\quad W_o = \langle w_2 \rangle$

There exists a subspace W' of V s.t.

$$V = W' \oplus W_o$$

Since $\dim V = 2$, $\dim W_o = 1$, $\dim W' = 1$.

Let $\quad W' = \langle w_1 \rangle$

Then $\{w_1, w_2\}$ is a basis of V.

Let $\quad T(w_1) = \alpha_1 w_1 + \alpha_2 w_2$

$\quad T(w_2) = 0w_1 + 0w_2$ as $w_2 \in \text{Ker } T$.

But
$$\begin{aligned} T^2 = 0 \Rightarrow 0 &= T^2(w_1) \\ &= \alpha_1 T(w_1) + \alpha_2 T(w_2) \\ &= \alpha_1 T(w_1) \\ &= \alpha_1(\alpha_1 w_1 + \alpha_2 w_2) \\ &= \alpha_1^2 w_1 + \alpha_1\alpha_2 w_2 \end{aligned}$$

$\Rightarrow \alpha_1 = 0$ ($\alpha_2 \neq 0$ as $\alpha_2 = 0 \Rightarrow w_1 \in \text{Ker } T$

$\Rightarrow w_1 \in W_o \cap W' = \{0\}$

$\Rightarrow w_1 = 0$ which is not true)

So, $\quad T(w_1) = \alpha_2 w_2$.

Now $\{\alpha_2^{-1} w_1, w_2\} = \beta'$ is also a basis of V

as $\quad a\alpha_2^{-1} w_1 + bw_2 = 0$

$\Rightarrow a\alpha_2^{-1} = 0, \; b = 0$

$\Rightarrow a = 0 = b$.

$\Rightarrow \{\alpha_2^{-1} w_1, w_2\} = \beta'$ is a *L.I.* set

$\Rightarrow \beta'$ is a basis of V as $\dim V = 2$

Therefore,
$$\begin{aligned} T(\alpha_2^{-1} w_1) &= \alpha_2^{-1} T(w_1) \\ &= \alpha_2^{-1}\alpha_2 w_2 = w_2 \\ &= 0\alpha_2^{-1} w_1 + 1w_2 \end{aligned}$$

$$\Rightarrow [T]_{\beta'} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Also $\quad [T]_\beta = N$

$\Rightarrow N$ is similar to $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ over $\mathbf{C}$.

Problem 12 : *Use the result of problem* 11 *to prove the following :*

If A is 2×2 matrix with complex entries, then A is similar over $\mathbf{C}$ *to a matrix of one of the type* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $\begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}$.

Solution : Let $f(x)$ be the characteristic polynomial of A. If the roots of $f(x)$ are distinct, then A is diagonalisable.

So, $\quad A = P^{-1}BP, \; B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \; a, b \in \mathbf{C}$.

$\Rightarrow A$ is similar over $\mathbf{C}$ to $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$

If the roots of $f(x)$ are same, let $f(x) = (x - \alpha)^2$

Then $\quad 0 = f(A) = (A - \alpha I)^2$

Let $\quad N = A - \alpha I$

By problem 11, either $N = 0$ or N is similar over $\mathbf{C}$ to $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$.

If $N = 0$, then $A = \alpha I = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$

$\Rightarrow A$ is similar over $\mathbf{C}$ to $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}$

If $\quad N = Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$

Then $\quad A - \alpha I = Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$

$$\Rightarrow A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} + Q^{-1}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}Q$$

$$= Q^{-1}\left\{\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\right\}Q$$

$$= Q^{-1}\begin{bmatrix} \alpha & 0 \\ 1 & \alpha \end{bmatrix}Q$$

$\Rightarrow A$ is similar over $\mathbf{C}$ to the matrix of the type $\begin{bmatrix} \alpha & 0 \\ 1 & \alpha \end{bmatrix}$.

Annihilating Polynomials

In order to determine a linear operator T, it is very useful to determine the class of polynomials which annihilate T.

If T is a linear operator on the n - dimensional space V, then dim Hom $(V, V) = n^2$ $\Rightarrow$ any $n^2 + 1$ vectors in Hom (V, V) are linearly dependent.

$\Rightarrow I, T, T^2, \ldots\ldots, T^{n^2}$ are linearly dependent.

$\Rightarrow \exists\, c_o, c_1, c_2, \ldots\ldots, c_{n^2} \in F$ s.t.

$$c_o I + c_1 T + \ldots\ldots + c_{n^2} T^{n^2} = 0 \text{ where some } c_i \neq 0$$

$\therefore$ T satisfies a polynomial $p(x) \in F[x]$,

$$p(x) = c_o + c_1 x + \ldots\ldots + c_{n^2} T^{n^2}, \; p(x) \neq 0 \text{ s.t. } p(T) = 0$$

Among all such polynomials satisfied by T, choose a polynomial of least degree.

Definition : Let T be a linear operator on a finite dimensional space V over F. The *minimal polynomial* for T is the unique polynomial $p(x) \in F[x]$ s.t.

(*i*) $p(x)$ is monic polynomial

(*ii*) $p(T) = 0$

(*iii*) No polynomial over F which annihilates T has smaller degree than $p(x)$.

We have similar definition for minimal polynomial for square matrix A.

Theorem 6 : *Let T be a linear operator on an n-dimensional space V. The characteristic and minimal polynomials for T have the same roots.*

Proof : Let $p(x)$ be the minimal polynomial for T. Let c be a root of $p(x)$ i.e., $p(c) = 0$.

Then $p(x) = (x - c)\, q(x)$ for some $q(x) \in F[x]$.

Since $\deg q(x) < \deg p(x)$, $q(T) \neq 0$

$\exists\, v \in V$ s.t. $q(T)\, v \neq 0$, $v \neq 0$

Let $\quad x = q(T)\, v \neq 0$

Then $\quad 0 = p(T)\, v$

$$= (T - cI)\, q(T)\, v$$

$$= T(x) - cx$$

$$\Rightarrow T(x) = cx, \; x \neq 0$$

$\Rightarrow$ c is an eigen value of T.

Conversely, let c be an eigen value of T.

Then $\quad \exists\, 0 \neq v \in V$ s.t. $Tv = cv$

$\therefore \quad p(T)\, v = p(c)\, v$

Since $\quad p(T) = 0$, $p(c)\, v = 0$, $v \neq 0$

$$p(c) = 0$$

$\therefore$ c is a root of minimal polynomial for T.

Note : Although minimal polynomial and, characteristic polynomial have same roots, they may not be same. For example, the characteristic polynomial of

$A = \begin{bmatrix} 3 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$ is $(x-1)(x-2)^2$ while $(A - I)(A - 2I) = 0 \Rightarrow$ minimal polynomial of A is $(x-1)(x-2)$.

A natural question arises. When would these two polynomials be same? If eigen values of linear operator T are all distinct, the characteristic polynomial of T is $f(x) = (x - c_1) \ldots\ldots (x - c_n)$. Since roots of minimal polynomial $p(x)$ of T are same as of $f(x)$ and $\deg\ p(x) \leq f(x) = n$

$$p(x) = (x - c_1) \ldots\ldots (x - c_n) = f(x)$$

There is well known result in matrices called "*Cayley Hamilton Theorem*" which says "Every square matrix satisfies its characteristic polynomial". Since characteristic polynomial of a linear operator T is same as characteristic polynomial of $[T]_\beta$. w.r.t. any basis β of V, Cayley Hamilton Theorem is true for linear operators also i.e. if $f(x)$ is the characteristic polynomial of T, then $f(T) = 0$.

A simple consequence of the above is

Theorem 7 : *The minimal polynomial of a linear operator T divides its characteristic polynomial.*

Proof : Let $p(x), f(x)$ be the minimal and characteristic polynomials respectively of T.

Then $f(x) = g(x)\,p(x) + q(x)$ where either $q(x) = 0$ or $\deg q(x) < \deg p(x)$

Let $q(x) \neq 0$. Now $0 = f(T) = g(T)\,p(T) + q(T)$

$\Rightarrow\ q(T) = 0$ ($f(T) = 0$ by Cayley Hamilton Theorem)

$\therefore\ q(x)$ is a non zero monic polynomial of degree less than $\deg p(x)$ and $q(T) = 0$, contradicting $p(x)$ is minimal. $\therefore\ q(x) = 0$

$\therefore\ p(x)$ divides $f(x)$.

Remarks (1) : Let $A = [T]_\beta$ and $p(x)$ = minimal polynomial of T. Then $p(x)$ is also minimal polynomial of A.

Proof : Now $\quad [T^r]_\beta = [T]_\beta \ldots\ldots [T]_\beta = A^r$

$\therefore \quad [p(T)]_\beta = p(A)$

$\therefore \quad p(A) = 0$ as $p(T) = 0$

Let $\quad q(x)$ = minimal polynomial of A.

Let $\quad p(x) = q(x)\,r(x) + s(x)$, where

$r(x) = 0$ or $\deg s(x) < \deg q(x)$

Now $\quad 0 = p(A) = q(A)\,r(A) + s(A)$

$\Rightarrow\ s(A) = 0$

If $s(x) \neq 0$, then A satisfies a non-zero polynomial of degree less than $\deg q(x)$, a contradiction.

$\therefore\ s(x) = 0$. So, $q(x) \mid p(x)$

Again $\quad [q(T)]_\beta = q(A) = 0 \Rightarrow q(T) = 0$

Let $\quad q(x) = p(x)\,g(x) + h(x)$

where $h(x) = 0$ or $\deg h(x) < \deg p(x)$

$\therefore \quad q(T) = p(T)\,g(T) + h(T)$

$\Rightarrow\ 0 = h(T)$

If $h(x) \neq 0$, then T satisfies a non-zero polynomial of degree less than $\deg p(x)$, a contradiction.

$\therefore \qquad h(x) = 0 \Rightarrow p(x) \mid q(x)$

Hence $p(x) = q(x) =$ minimal polynomial of A.

(2) Similar matrices have same minimal polynomial.

Proof : Let A, B be similar matrices

Then $\qquad B = P^{-1}AP$

Let $\qquad p(x) =$ minimal polynomial of A.

$\qquad q(x) =$ minimal polynomial of B.

Now $\qquad 0 = q(B) = q(P^{-1}AP) = P^{-1}\, q(A)P$

$\therefore \qquad q(A) = 0$

As before $\qquad p(x) \mid q(x)$

Similarly, $\qquad 0 = p(A) = p(PBP^{-1}) = Pp(B)P^{-1}$

$\therefore \qquad p(B) = 0$

So, $\qquad q(x) \mid p(x)$

Thus, $\qquad p(x) = q(x)$.

Problem 13 : *Let a, b, c be elements of a field F and*

$$A = \begin{bmatrix} 0 & 0 & c \\ 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$$

Prove that the characteristic polynomial of A is same as that of its minimal polynomial.

Solution : The characteristic polynomial of A is given by

$$f(x) = |xI - A| = x^3 - ax^2 - bx - c$$

Let $p(x)$ be its minimal polynomial.

Then $\deg p(x) \leq \deg f(x) = 3$.

If $\deg p(x) = 1$, then $p(x) = x - \alpha$, $\alpha \in F$

$$\therefore \qquad O = p(A) = A - \alpha I = \begin{bmatrix} -\alpha & 0 & c \\ 1 & -\alpha & b \\ 0 & 1 & a-\alpha \end{bmatrix}$$

which is not true as $1 \neq 0$.

If $\deg p(x) = 2$, then $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$

$$\Rightarrow O = p(A) = A^2 + \alpha A + \beta I$$

$$\Rightarrow \begin{bmatrix} - & - & - \\ - & - & - \\ 1 & - & - \end{bmatrix} + \begin{bmatrix} - & - & - \\ - & - & - \\ 0 & - & - \end{bmatrix} + \begin{bmatrix} - & - & - \\ - & - & - \\ 0 & - & - \end{bmatrix} = 0$$

$\Rightarrow$ 1 = 0, which is not true.

$\therefore$ deg $p(x) = 3$. $\therefore$ $p(x) = f(x)$.

Problem 14 : *Let V be the space of $n \times n$ matrices over F. Let A be $n \times n$ matrix in V. Define $T : V \to V$ s.t. $T(B) = AB$ for all $B \in V$. Show that the minimal polynomial of T is the minimal polynomial of A.*

Solution : Let $p(x) = x^n + \ldots\ldots + \alpha_{n-1} x + \alpha_n$

$$q(x) = x^m + \ldots\ldots + \beta_{m-1} x + \beta_m$$

be minimal polynomials of T and A respectively

Now
$$\begin{aligned} O &= p(T)I \\ &= (T^n + \ldots\ldots + \alpha_n I)I \\ &= A^n + \ldots\ldots + \alpha_n I \text{ as } T(I) = A \Rightarrow T^r(I) = A^r \\ &= p(A). \end{aligned}$$

$\therefore$ A satisfies $p(x)$.

Let $p(x) = (x - c)\ q(x) + r(x)$, $r(x) = 0$ or deg $r(x) <$ deg $q(x)$, c is root of $p(x)$.

Then
$$O = p(A) = (A - cI)\, q(A) + r(A)$$
$$\Rightarrow r(A) = 0$$

If $r(x) \neq 0$, then $r(x)$ is non zero monic polynomial of degree less than deg $q(x)$ s.t. $r(A) = 0$, a contradiction. $\therefore$ $r(x) = 0$.

$\therefore$ $q(x)$ divides $p(x)$

Also
$$\begin{aligned} 0 &= q(A)B \\ &= (A^m + \ldots\ldots + \beta_m I)B \\ &= A^m B + \ldots\ldots + \beta_m B \\ &= T^m B + \ldots\ldots + \beta_m B \\ &= (T^m + \ldots\ldots + \beta_m I)B \\ &= q(T)B \text{ for all } B \in V \end{aligned}$$
$$\Rightarrow q(T) = 0$$

As before, $p(x)$ divides $q(x)$ and thus $p(x) = q(x)$.

Exercises

1. Find the characteristic polynomial for identity and zero operator on n - dimensional space.
2. Let T be the linear operator on $\mathbf{R}^3$ which is represented in the standard ordered by the matrix

$$\begin{bmatrix} -9 & 4 & 4 \\ -8 & 3 & 4 \\ 16 & 8 & 7 \end{bmatrix}$$

Prove that T is diagonisable, by finding a basis for $\mathbf{R}^3$, each vector of which is an eigen value of T.

3. Let A, B be $n \times n$ matrix over the field F. Prove that if $(I - AB)$ is invertible, then $I - BA$ is invertible and

$$(I - BA)^{-1} = I + B(I - AB)^{-1}A.$$

4. Using problem 3, show that AB and BA have same eigen values.

5. Let A be 2×2 real matrix s.t. $A^t = A$. Prove that A is similar over $\mathbf{R}$ to a diagonal matrix.

6. Give an example of a 2×2 matrix A such that A and transpose of A do not have same eigen values.

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

7. Find the eigen values and bases for the eigen spaces of the matrix

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ 0 & 2 & 4 \end{bmatrix}$$

Is A diagonisable?

$$2,\ 3 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ -2 \end{bmatrix}$$

8. Find eigen values, eigen vectors and eigen spaces of the matrix

$$A = \begin{bmatrix} 2 & 2 & -6 \\ 2 & -1 & -3 \\ 2 & -1 & 1 \end{bmatrix}$$

Show A is diagonisable.

$$-2,\ -2,\ 6,\ \begin{bmatrix} x_1 \\ -2x_1 + 3x_2 \\ x_2 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$$

Eigen space corresponding to eigen value -2 is spanned by $\begin{bmatrix} 1 \\ -2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 3 \\ 1 \end{bmatrix}$

and corresponding to eigen value 3 is spanned by $\begin{bmatrix} 2 \\ 1 \\ -1 \end{bmatrix}$.

9. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\Delta = (a - d)^2 + 4bd$. Show that

(*i*) If $\Delta > 0$ then A is diagonalisable.

(*ii*) If $\Delta < 0$ then A is not diagonalisable and

(*iii*) If $\Delta = 0$ then A many or may not be diagonalisable.

10. Let A be an $n \times n$ matrix with characteristic polynomial $f(x) = (x - c_1)^{d_1} \ldots\ldots\ldots (x - c_k)^{d_k}$.

Show that trace $A = c_1 d_1 + c_2 d_2 + \ldots\ldots + c_k d_k$.

11. Let λ be an eigen value of $n \times n$ matrix A. Prove that

(*i*) transpose of A has the same eigen value as that of A

(*ii*) kA has eigen value $k\lambda$ for any scalar k

(*iii*) A^r(r is a positive integer) has the eigen value λ^r

(*iv*) If A is invertible, A^{-1} has the eigen value $\frac{1}{\lambda}$.

(*v*) the matrix $A + kI$ has the eigen value $\lambda + k$.

12. For the matrix $A = \begin{bmatrix} 1 & 2 & 0 \\ 2 & 1 & -6 \\ 2 & -2 & 3 \end{bmatrix}$ find P such that $P^{-1}AP$ is a diagonal matrix.

$$\begin{bmatrix} 1 & 1 & -1 \\ 2 & 1 & 2 \\ -1 & 0 & 1 \end{bmatrix}.$$

Invariant Subspaces

Definition : Let T be a linear operator on a vector space V. If W is a subspace of V s.t. $T(W) \subseteq W$, we say W is *invariant under T or is T-invariant.*

Example 1 : Since $T(0) = 0$ and $T(V) = V$, both zero subspace and V are invariant subspaces of V.

Example 2 : Let $v \in \text{Ker } T$ then $T(v) = 0 \in \text{Ker } T \Rightarrow \text{Ker } T$ is invariant subspace of V. Also $w \in ImT \Rightarrow w = T(v) \Rightarrow Tw = T(Tv)$, $Tv \in V \Rightarrow Tw \in ImT$. $\therefore$ ImT is an invariant subspace of V.

Example 3 : Let $f(t)$ be any polynomial. Let $v \in \text{Ker}(f(T))$ then $f(T)\ v = 0$

Since $\quad f(t) \cdot t = tf(t)$

$$f(T)\,T = Tf(T)$$

Thus, $\quad f(T)\,Tv = Tf(T)\,v = 0$

$$\Rightarrow Tv \in \text{Ker } f(T)$$

$$\Rightarrow \text{Ker } f(T) \text{ is invariant under } T.$$

Problem 13 : *Let T be a linear operator on $\mathbf{R}^2$, the matrix of which in the standard ordered basis is*

$$A = \begin{bmatrix} 1 & -1 \\ 2 & 2 \end{bmatrix}$$

Prove that the only subspaces of $\mathbf{R}^2$ invariant under T are $\mathbf{R}^2$ and zero subspaces.

Solution : Characteristic polynomial of A (or T) is $\begin{vmatrix} x-1 & 1 \\ -2 & x-2 \end{vmatrix} = x^2 - 3x + 4$, whose roots are not real. Thus eigen values of A(or T) do not exist in $\mathbf{R}$. If W is an invariant subspace of $\mathbf{R}^2$ s.t. $W \neq 0$, then $\dim W = 1$. Let W be spanned by v. Then $Tv \in W \Rightarrow Tv = \alpha v$, $v \neq 0 \Rightarrow \alpha$ is an eigen value of $T(\alpha \in \mathbf{R})$, a contradiction. Hence O and $\mathbf{R}^2$ are only invariant subspaces of $\mathbf{R}^2$.

Theorem 8 : *Let W be an invariant subspace of linear operator T on V. Then T has a matrix representation $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$, where A is matrix of restriction T_w of T on W.*

Proof : Let $\{w_1, \ldots\ldots, w_r\}$ be a basis of W. Let $\beta = \{w_1, \ldots\ldots, w_r, v_1, \ldots\ldots, v_s\}$ be a basis of V, obtained by extending basis of W.

Since $T(w) \in W$ for all $w \in W$, we define $T_w : W \to W$ by $T_w(x) = T(x)$ for all $x \in W$.

Then T_w is operator on W.

$$T_w(w_1) = T(w_1) = a_{11}w_1 + \ldots\ldots + a_{r1}w_r$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$T_w(w_r) = T(w_r) = a_{1r}w_1 + \ldots\ldots + a_{rr}w_r$$

$$T(v_1) = b_{11}w_1 + \ldots\ldots + b_{r1}w_r + c_{11}v_1 + \ldots + c_{s1}v_s$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$T(v_s) = b_{1s}w_1 + \ldots\ldots + b_{rs}w_r + c_{1s}v_1 + \ldots\ldots + c_{ss}v_s$$

Thus matrix of T w.r.t. basis β is

$$\begin{bmatrix} a_{11} & \ldots & a_{1r} & b_{11} & \ldots & b_{1s} \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ a_{r1} & \ldots & a_{rr} & b_{r1} & \ldots & b_{rs} \\ 0 & \ldots & 0 & c_{11} & \ldots & c_{1s} \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & c_{s1} & \ldots & c_{ss} \end{bmatrix}$$

$$= \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} \text{ where } A = (a_{ij}),\ B = (b_{ij}),\ C = (c_{ij})$$

are of order $r \times r$, $r \times s$, $s \times s$ respectively

Clearly, A is matrix of T_w w.r.t. $\{w_1, \ldots\ldots, w_r\}$ = basis of W. T_w is called restriction of T on W.

We now show that the matrix C obtained in theorem 8 is the matrix of some linear operator on $\frac{V}{W}$ induced by T.

Define $\hat{T}: \frac{V}{W} \to \frac{V}{W}$ s.t.,

$$\hat{T}(W+v) = W + T(v), \qquad v \in V$$

Then $\hat{T}$ is well defined as $W + v = W + v'$

$$\Rightarrow v - v' \in W$$
$$\Rightarrow T(v - v') \in W$$
$$\Rightarrow T(v) - T(v') \in W$$
$$\Rightarrow W + T(v) = W + T(v')$$

Since T is linear transformation, so is $\hat{T}$, Let $\{w_1, \ldots\ldots, w_r\}$ be a basis of W. Then it can be extended to form a basis of V. Let $\{w_1, \ldots\ldots, w_r, v_1, \ldots\ldots, v_s\}$ be a basis of V. Then $\{W + v_1, \ldots\ldots, W + v_s\}$ is a basis of $\frac{V}{W}$.

Now
$$\begin{aligned}\hat{T}(w+v_1) &= W + T(v_1)\\ &= W + b_{11}w_1 + \ldots\ldots + b_{r1}w_r + c_{11}v_1 + \ldots\ldots\ldots + c_{s1}v_s\\ &= W + c_{11}v_1 + \ldots\ldots + c_{s1}v_s\\ &\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

$$\begin{aligned}\hat{T}(W + v_s) &= W + T(v_s) = W + b_{1s}w_1 + \ldots\ldots + b_{rs}w_r + c_{1s}w_1 + \ldots\ldots + c_{ss}v_s\\ &= W + c_{1s}v_1 + \ldots\ldots + c_{ss}v_s \qquad \text{(as in theorem 8)}\end{aligned}$$

$\therefore$ matrix of $\hat{T}$ w.r.t. basis $\{W + v_1, \ldots\ldots, W + v_s\}$ of $\frac{V}{W}$ is

$$\begin{bmatrix} c_{11} & \cdots & \cdots & c_{1s} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ c_{s1} & \cdots & \cdots & c_{ss} \end{bmatrix} = C$$

A special situation where $B = 0$ in theorem is obtained when V is a direct sum of two invariant subspaces under T.

Problem 14 : *If W and U are invariant subspaces of a linear operator on a F.D.V.S. V over F and $V = U \oplus W$, then $\exists$ a basis β of V such that the matrix of T w.r.t. β is $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$, where A is the matrix of T_w on W and C is the matrix of T_u on U.*

Solution : Let $\{w_1, \ldots\ldots, w_r\}$ be a basis of W and $\{u_1, \ldots\ldots, u_s\}$ be a basis of U. Then $\{w_1, \ldots\ldots, w_r, u_1, \ldots\ldots, u_s\}$ is a basis of $W \oplus U = V$.

Now
$$T_w(w_1) = T(w_1) = a_{11}w_1 + \ldots\ldots + a_{r1}w_r$$
$$T_w(w_2) = T(w_2) = a_{12}w_1 + \ldots\ldots + a_{r2}w_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$T_w(w_r) = T(w_r) = a_{1r}w_1 + \ldots\ldots + a_{rr}w_r$$
as $\quad T(w_i) \in W$ for all $i = 1, \ldots\ldots, r$

Similarly,
$$T_u(u_1) = T(u_1) = c_{11}u_1 + \ldots\ldots + c_{s1}u_s$$
$$T_u(u_2) = T(u_2) = c_{12}u_1 + \ldots\ldots + c_{s2}u_s$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$T_u(u_s) = T(u_s) = c_{1s}u_1 + \ldots\ldots + c_{ss}u_s$$
as $\quad T(u_j) \in U$ for all $j = 1, \ldots\ldots, s$

So matrix of T w.r.t. $\beta = \{w_1, \ldots\ldots, w_r, u_1, \ldots\ldots, u_r\}$ of V is given by

$$\begin{bmatrix} a_{11} & \ldots & a_{1r} & 0 & \ldots & 0 \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ a_{r1} & \ldots & a_{rr} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & c_{11} & \ldots & c_{1s} \\ \vdots & \ldots & \vdots & \vdots & \ldots & \vdots \\ 0 & \ldots & 0 & c_{s1} & \ldots & c_{ss} \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$$

where $A = (a_{ij})$, $C = (c_{ij})$ are $r \times r$ and $s \times s$ matrices respectively. Clearly A is the matrix of T_w on W and C is the matrix of T_u on U.

Problem 15 : *Let V be the vector space of all polynomials in x over F, of degree ≤ 5. Let $T: V \to V$ be defined by $T(1) = x^2 + x^4$, $T(x) = x + 1$, $T(x^2) = 1$, $T(x^3) = x^3 + x^2 + 1$, $T(x^4) = x^4$, $T(x^5) = 0$. If W is the linear span of $\{1, x^2, x^4\}$,*

(*a*) *Show that W is invariant under T.*

(*b*) *Find the matrix of T_w in a suitable basis of W.*

(*c*) *Find the matrix of $\hat{T}$ in a suitable basis of $\dfrac{V}{W}$.*

(*d*) *Find the matrix of T in a suitable basis of V.*

Solution (*a*) : Let $w \in W$. Then $w = a + bx^2 + cx^4$ where $a, b, c \in F$.

$$\therefore \quad T(w) = a \,.\, T(1) + bT(x^2) + cT(x^4)$$
$$= a(x^2 + x^4) + b + cx^4$$
$$= b + ax^2 + (a + c)\,x^4$$
$$\in W \text{ for all } w \in W$$

$\therefore$ W is invariant under T.

(b) : Notice that $\{1, x^2, x^4\}$ is linearly independent set over F and so forms a basis of W, and it can be extended to form a basis, namely $\{1, x^2, x^4, x, x^3, x^5\}$ of V.

Now
$$T_w(1) = T(1) = x^2 + x^4 = 0 \,.\, 1 + 1 \,.\, x^2 + 1 \,.\, x^4$$
$$T_w(x^2) = T(x^2) = 1 = 1 \,.\, 1 + 0 \,.\, x^2 + + 0 \,.\, x^4$$
$$T_w(x^4) = T(x^4) = x^4 = 0 \,.\, 1 + x^2 + 1 \,.\, x^4$$

$\therefore$ matrix of T_w w.r.t. basis $\{1, x^2, x^4\}$ of W is given by $A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$.

(c) : Now $\{W + x,\ W + x^3,\ W + x^5\}$ is basis of $\dfrac{V}{W}$.

$\therefore$
$$\begin{aligned} \hat{T}(W + x) &= W + T(x) = W + x + 1 \\ &= W + x = 1 \,.\, (W + x) + 0(W + x^3) + 0(W + x^5) \\ \hat{T}(W + x^3) &= W + T(x^3) \\ &= W + x^3 + x^2 + 1 \\ &= W + x^3 \\ &= 0(W + x) + 1\ \ (W + x^3) + 0(W + x^5) \\ \hat{T}\ (W + x^5) &= W + T(x^5) \\ &= W + 0 = W = \text{zero of } \frac{V}{W} \\ &= 0(W + x) + 0(W + x^3) + 0(W + x^5) \end{aligned}$$

$\therefore$ matrix of $\hat{T}$ w.r.t. basis $\{W + x,\ W + x^3,\ W + x^5\}$ of $\dfrac{V}{W}$ is given by

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

(d) :
$$T(x) = x + 1 = 1 \,.\, 1 + 0 \,.\, x^2 + 0 \,.\, x^4 + 1 \,.\, x + 0 \,.\, x^3 + 0 \,.\, x^5$$
$$T(x^3) = x^3 + x^2 + 1 = 1 \,.\, 1 + 1 \,.\, x^2 + 0 \,.\, x^4 + 0 \,.\, x + 1 \,.\, x^3 + 0 \,.\, x^5$$
$$T(x^5) = 0 = 0 \,.\, 1 + 0 \,.\, x^2 + 0 \,.\, x^4 + 0 \,.\, x + 0 \,.\, x^3 + 0 \,.\, x^5$$

$\therefore$ matrix of T w.r.t basis $\{1, x^2, x^4, x, x^3, x^5\}$ of V is given by

$$\begin{bmatrix} 0 & 1 & 0 & : & 1 & 1 & 0 \\ 1 & 0 & 0 & : & 0 & 1 & 0 \\ 1 & 0 & 1 & : & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & : & 1 & 0 & 0 \\ 0 & 0 & 0 & : & 0 & 1 & 0 \\ 0 & 0 & 0 & : & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}, \text{ where } B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Problem 16 : *Let T be a linear operator on a F.D.V.S. V over F. Let W be an invariant subspace of T. Show that the characteristic polynomial $p_T(x)$ of T is given by*

$p_T(x) = p_{T_w}(x)\, p_{\hat{T}}(x)$, *where $p_{T_w}(x)$, $p_{\hat{T}}(x)$ are the characteristic polynomials of T_w and $\hat{T}$ respectively.*

Solution : Characteristic polynomial $p_T(x)$ of T is given by

$$\left| \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} - xI \right|$$

$$= \left| \begin{bmatrix} A - xI & B \\ 0 & C - xI \end{bmatrix} \right| \quad \left(\begin{array}{l} \text{Here } A = \text{ matrix of } T_w \text{ on } W \\ \qquad C = \text{ matrix of } \hat{T} \text{ on } \dfrac{V}{W} \end{array} \right)$$

$$= |A - xI|\,|C - xI|$$

$$= (\text{characteristic polynomial of } T_w)$$

$$\times\ (\text{characteristic polynomial of } \hat{T})$$

$$= p_{T_w}(x)\, p_{\hat{T}}(x).$$

A natural question arises "what is the minimal polynomial for T in terms of minimal polynomial for T_w"? As we saw in above problem that the characteristic polynomial of T_w divides the characteristic polynomial of T, we have a similar result about minimal polynomial of T. We prove

Theorem 9 : *The minimal polynomial of T_w divides the minimal polynomial for T, where W is an invariant subspace of V and T is a linear operator of W.*

Proof : Let $p(x)$ be the minimal polynomial for T.

Let $\quad p(x) = \alpha_0 + \alpha_1 x + \ldots\ldots + \alpha_{n-1}x^{n-1} + x^n$

Since $\quad T(w) = T_w(w)$ for all $w \in W$

$$T^2(w) = T(T_w(w))$$

$$= T_w(T_w(w)) \text{ as } T_w(w) \in W$$

In this way $\quad T^r(w) = T_w^r(w)$ for all $w \in W$

$\therefore \quad p(T_w)(w) = p(T)(w)$ for all $w \in W$)

$$= 0 \text{ as } p(T) = 0 \text{ for all } w \in W$$

$\therefore \quad p(T_w) = 0$

Let $q(x)$ be the minimal polynomial for T_w. Then $p(x) = q(x)\, r(x) + h(x)$ where $h(x) = 0$ or $\deg h(x) < \deg q(x)$

$\therefore \qquad 0 = p(T_w) = q(T_w)\ r(T_w) + h(T_w)$

$\therefore \qquad h(T_w) = 0$

If $h(x) \neq 0$, then $h(x)$ is non zero polynomial satisfied by T_w of degree less than deg $q(x)$, a contradiction as $q(x)$ is minimal.

$\therefore \qquad h(x) = 0 \Rightarrow q(x)$ divides $p(x)$.

Definition : Let T be a linear operator on V. Let $v \in V$. Define $S(v, W) = \{f(x) \mid f(T)\ v \in W\}$. It is called the *T-conductor of* v into W.

The unique monic polynomial $g(x)$ of least degree s.t. $g(T)\ v \in W$ is also called the T-conductor of v into W.

If $p(x)$ is the minimal polynomial for T, then $p(T)\ v = 0v = 0 \in W \Rightarrow p(T)\ v$ belongs to W.

Let $\qquad p(x) = q(x)\, g(x) + r(x)$

where $\qquad r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore \qquad 0 = p(T)\ v = q(T)\, g(T)\ v + r(T)\ v$

Let $\qquad g(T)\ v = w \in W$

$\therefore \qquad r(T)\ v = -q(T)\ w \in W$ as W is T invariant.

If $r(x) \neq 0$, then $r(x)$ is non zero polynomial of degree less than $\deg g(x)$ s.t. $r(T)\ v \in W$, a contradiction.

$\therefore \qquad r(x) = 0$

Hence $\qquad g(x)$ divides $p(x)$.

Lemma : *Let V be a finite dimensional vector space over F. Let T be a linear operator on V s.t. minimal polynomial for T has $c_1, \ldots\ldots, c_k$ as its distinct roots in F. Let $W \neq V$ be an invariant subspace of T. Then $\exists\, v \in V$ s.t. $v \notin W$ $(Tv - cv) \in W$, for some eigen value c of T.*

Proof : Let $p(x)$ be the minimal polynomial for T. Let $v_1 \in V$ s.t. $v_1 \notin W$. Let $g(x)$ be the T-conductor of v_1 into W. If $g(x)$ = constant, then $g(x) = 1$ (as $g(x)$ is monic). So, $g(T)v_1 \in W \Rightarrow v_1 \in W$, a contradiction.

$\therefore\ g(x) \neq$ constant. From above $g(x)$ divides $p(x)$.

Let $\qquad g(x) = (x - c_1)^{e_1} \ldots\ldots (x - c_k)^{e_k}$

Since $g(x) \neq$ constant, some $e_i > 0$.

Choose j s.t. $e_j > 0$. Then

$$g(x) = (x - c_j)\ h(x)$$

By definition of $g(x)$, $v = h(T)\, v_1 \notin W$, as $\deg h(x) < \deg g(x)$

But $\qquad (T - c_j I)v = (T - c_j I)\, h(T)\, v_1$

$$= g(T)\, v_1 \in W$$

$\therefore\ Tv - c_j\, v \in W$ where c_j is a root of $p(x) \Rightarrow c_j$ is also an eigen value of T.

Theorem 10 : *Let V be a finite dimensional space over F and let T be a linear operator on V. Then T is diagonalisable if and only if the minimal polynomial for T has the form*

$$p(x) = (x - c_1) \ldots\ldots (x - c_k)$$

where $c_1, \ldots\ldots, c_k$ *are distinct elements of* F.

Proof : Let T be diagonalisable. Let $c_1, \ldots\ldots, c_k$ be distinct eigen values of T. Let v be any eigen vector of T.

Then $(T - c_1 I) \ldots\ldots (T - c_k I)\, v = 0$ for all eigen vectors v of T.

Since T is diagonalisable $\exists$ a basis $\beta = \{v_1, \ldots\ldots, v_n\}$ consisting of eigen vectors of T.

$$\therefore \qquad p(T) = (T - c_1 I) \ldots\ldots (T - c_k I) = 0 \quad \text{on} \quad \beta'$$

$$\Rightarrow \; p(T) = 0 \quad \text{on} \quad V$$

$\Rightarrow$ $p(x) = (x - c_1) \ldots\ldots (x - c_k)$ is the minimal polynomial for T as $c_1, \ldots\ldots, c_k$ are also roots of $p(x)$.

Conversely, let $p(x) = (x - c_1) \ldots\ldots (x - c_k)$ be the minimal polynomial for T. Then $c_1, \ldots\ldots, c_k$ are also distinct eigen values of T and there are no more.

Let W_is be corresponding eigen spaces

i.e. $\qquad W_i = \{v \in V \mid Tv = c_i v\}$

Let $\qquad W = W_1 + \ldots\ldots + W_k$

If $\beta_1, \ldots\ldots, \beta_k$ are basis of $W_1, \ldots\ldots, W_k$ resp., then we have seen before that $\{\beta_1, \ldots\ldots, \beta_k\}$ is a basis of W.

If we show $W = V$, then $\exists$ a basis of V consisting of eigen vectors of T and so T is diagonalisable. Let $W \neq V$.

Let $x \in W$. Then $x = w_1 + \ldots\ldots + w_k, \; w_i \in W_i$

$$\Rightarrow \; T(x) = T(w_1) + \ldots\ldots + T(w_k)$$

$$= c_1 w_1 + \ldots\ldots + c_k w_k \in W_1 + \ldots\ldots + W_k = W$$

$\Rightarrow$ W is T-invariant

By previous lemma $\exists\, v \in V$ s.t. $v \notin W$ and

$v_1 = Tv - c_j v \in W$ for some eigen values c_j of T.

Now $v_1 \in W$

$$\Rightarrow \; v_1 = x_1 + \ldots\ldots + x_k, \; x_i \in W$$

$$\therefore \qquad h(T)\, v_1 = h(c_1)\, x_1 + \ldots\ldots + h(c_k)\, x_k \quad \text{as} \quad T(x_i) = c_i x_i$$

for any polynomial $h(x)$.

Now $p(x) = (x - c_j)\, q(x)$ for some polynomial $q(x)$.

Let $q(x) = (x - c_j)\, h(x) + \alpha, \; \alpha =$ constant

$$\Rightarrow \; q(c_j) = \alpha$$

$$\Rightarrow \; q(x) = (x - c_j)\, h(x) + q(c_j)$$

$$\Rightarrow \; q(x) - q(c_j) = (x - c_j)\, h(x)$$

$$\Rightarrow \; q(T)\, v - q(c_j)\, v = h(T)\, (T - c_j I) v$$

$$= h(T)\, v_1 \in W$$

Also $O = p(T)\, v = (T - c_j I)\, q(T) v$

$$\Rightarrow T(y) = c_j y, \text{ where } y = q(T)v$$
$$\Rightarrow y \in W_j \subseteq W \Rightarrow q(c_j)\ v \in W \Rightarrow q(c_j) = 0 \text{ as } v \notin W$$
$$\Rightarrow p(x) \text{ has } (x - c_j) \text{ appearing twice, a contradiction}$$
$$\Rightarrow V = W \Rightarrow \text{result.}$$

Problem 17 : *Let T be a linear operator on a finite dimensional vector space V. Then T is triangular if and only if the minimal polynomial for T is of form* $p(x) = (x - c_1)^{r_1} \ldots\ldots (x - c_k)^{r_k}$.

Proof : Let $p(x) = (x - c_1)^{r_1} \ldots\ldots (x - c_k)^{r_k}$.

We apply lemma before Theorem 10 repeatedly. Applying it to $W = 0$, take $v_1 \neq 0$ then $\exists\, v = T(v_1) - c_{11}v_1 \in W$ for some $c_{11} \in F$.

$$\therefore \qquad T(v_1) - c_{11}v_1 = 0$$
$$\Rightarrow T(v_1) = c_{11}v_1$$

Let W_1 = subspace spanned by v_1.

Then W_1 is T-invariant.

Applying lemma to W_1, we get $v_2 \in V$ s.t. $v_2 \notin W_1$ and $T(v_2) - c_{22}v_2 \in W_1$ for some $c_{22} \in F$.

$$\Rightarrow T(v_2) = c_{12}v_1 + c_{22}v_2$$

Let W_2 = subspace spanned by v_1, v_2

Let $x \in W_2$ then $x = \alpha_1 v_1 + \alpha_2 v_2$

$$\Rightarrow T(x) = \alpha_1 c_{11} v_1 + \alpha_2(c_{12}v_1 + c_{22}v_2) \in W_2$$
$$\Rightarrow W_2 \text{ is } T\text{-invariant}$$

Applying lemma to W_2, we get $v_3 \in V$ s.t. $v_3 \notin W_2$ and $T(v_3) - c_{33}v_3 \in W_2$ for some $c_{33} \in F$

$$\therefore \qquad T(v_3) = c_{13}v_1 + c_{23}v_2 + c_{33}v_3$$

In this way, we get T-invariant subspace W_{n-1} spanned by $v_1, \ldots\ldots, v_{n-1}$ s.t. $v_n \notin W_{n-1}$ and

$$T(v_n) = c_{1n}v_1 + \ldots\ldots + c_{nn}v_n$$

Then $\{v_1, \ldots\ldots, v_n\}$ are linearly independent over F as $\alpha_1 v_1 + \ldots\ldots + \alpha_n v_n = 0$

$$\Rightarrow \alpha_n v_n = -(\alpha_1 v_1 + \ldots\ldots + \alpha_{n-1}v_{n-1}) \in W_{n-1}$$

If $\alpha_n \neq 0$, then $v_n \in W_{n-1}$, a contradiction

$\therefore\ \alpha_n = 0$, similarly $\alpha_{n-1} = \ldots\ldots = \alpha_1 = 0$

Since $\dim V = n$, $\beta = \{v_1, \ldots\ldots, v_n\}$ is a basis of V.

$$\therefore \qquad [T]_\beta = \begin{bmatrix} c_{11} & c_{12} & \vdots & c_{1n} \\ 0 & c_{22} & \vdots & c_{2n} \\ \vdots & 0 & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \vdots & c_{nn} \end{bmatrix} = \text{triangular matrix}$$

$\therefore$ T is triangulable.

Conversely, if T is triangulable, then the characteristic polynomial of T has the form

$$f(x) = (x-c_1)^{d_1} \ldots\ldots (x-c_k)^{d_k}$$

Therefore, the minimal polynomial $p(x)$ which divides $f(x)$, is of the form

$$p(x) = (x-c_1)^{r_1} \ldots\ldots (x-c_k)^{r_k}.$$

Problem 18 : *Prove that every matrix A s.t. $A^2 = A$ is similar to a diagonal matrix.*

Solution : Clearly A satisfies

$$f(x) = x^2 - x = x(x-1)$$

Let $p(x)$ be the minimal polynomial for A. Then $p(x)$ divides $f(x)$.

$$\therefore \qquad p(x) = x,\ x-1 \text{ or } x(x-1)$$

By theorem 10, A is diagonalisable.

Problem 19 : *Let T be a linear operator on V. If every subspace of V is invariant under T, show that T is a scalar multiple of the identity operator.*

Solution : Let $0 \neq v \in V$. Let W be a subspace of V spanned by V. Since W is invariant under T, $v \in W \Rightarrow T(v) \in W \Rightarrow T(v) = \alpha v$. $w \in W \Rightarrow w = av \Rightarrow T(w) = aT(v) = a\alpha v = \alpha av = \alpha w$. Let $v' \notin W$, $v' \in V$. Then, v, v' are linearly independent. Let W' be the subspace spanned by v'. Since W' is invariant under T, $T(v') \in W'$.

$\therefore$ $T(v') = \alpha' v'$. Let V' be the subspace spanned by $v - v'$. Then as before $T(v-v') = \beta(v-v')$

$$\Rightarrow T(v) - T(v') = \beta v - \beta v' \Rightarrow \alpha v - \alpha' v' = \beta v - \beta v'$$

$$\Rightarrow (\alpha-\beta)\, v = (\alpha'-\beta)\, v' \Rightarrow \alpha = \beta = \alpha' \text{ as } v, v' \text{ are linearly independent}$$

$$\Rightarrow T(v') = \alpha(v').$$

$\therefore$ for all $v \in V$, $T(v) = \alpha v$

$$\Rightarrow T = \alpha I.$$

Problem 20 : *Is it true "if the triangular matrix A is similar to a diagonal matrix, then A is already diagonal ?"*

Solution : No, for example $A = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ has distinct eigen values 1 and 2. So, A is similar to a diagonal matrix but A is not a diagonal matrix.

Problem 21 : *Let T be a linear operator on a finite dimensional vector space over the field of complex numbers. Prove that T is diagonalisable, if and only if T is annihilated by some polynomial over* **C** *which has distinct roots.*

Solution : Suppose T is a diagonisable. Let $p(x)$ be the minimal polynomial for T. By theorem 3, $p(x)$ has distinct roots and $p(T) = 0$.

Conversely, let $q(x)$ be a polynomial over **C** s.t. $q(T) = 0$ and roots of $q(x)$ are distinct.

$\therefore$ $p(x)$ divides $q(x)$

and thus roots of $p(x)$ are distinct.

By theorem 10 then T is diagonalisable.

Problem 22 : *Let V be the space of $n \times n$ matrices over F. Let A be a fixed $n \times n$ matrix over F. Let T be linear operator on V defined by $T(A) = AB$. Is it true that 'A is diagonalisable over $F \Rightarrow T$ is diagonalisable'.*

Solution : We saw before that the minimal polynomial for A = minimal polynomial for $T = p(x)$. If A is diagonalisable, then $p(x)$ has distinct roots. This means T is diagonalisable.

Direct Sum Decomposition

In this section, we study linear operators in terms of subspaces. The underlying space V is decomposed into direct sum of invariant subspaces s.t. restriction of operator T on these subspaces has a *simple form.*

Definition : Let $W_1, \ldots\ldots, W_k$ be subspaces of space V then $W_1, \ldots\ldots, W_k$ are said to be independent if

$$x_1 + \ldots\ldots + x_k = 0, \Rightarrow x_i = 0 \text{ for all } i,\ x_i \in W_i$$

Theorem 11 : *Let V be a finite dimensional space. Let $W_1, \ldots\ldots, W_k$ be subspaces of V and $W = W_1 + \ldots\ldots + W_k$. Then the following are equivalent*

(*i*) $W_1, \ldots\ldots, W_k$ *are independent.*

(*ii*) $W_j \cap (W_1 + \ldots\ldots + W_{j-1}) = \{0\}$ *for all* j, $2 \le j \le k$

(*iii*) *If* β_i *is an ordered basis of* W_i, $1 \le i \le k$ *then* $\beta = \{\beta_i, \ldots\ldots, \beta_k\}$ *is an ordered basis of* W.

Proof : (*i*) $\Rightarrow$ (*ii*)

Let $x \in W_j \cap (W_1 + \ldots\ldots + W_{j-1})$

Then $x_1 + \ldots\ldots + x_{j-1} + (-x) = 0,\ x_i \in W_i$

$\Rightarrow x_i = 0 = x$ for all $i = 1, \ldots\ldots, j-1$ by (*i*)

$\Rightarrow W_j \cap (W_1 + \ldots\ldots + W_{j-1}) = \{0\}$

(*ii*) $\Rightarrow$ (*iii*)

Let $\beta_i = \{x_{i_1}, \ldots\ldots\ldots, x_{i_{d_i}}\}$ be basis of W_i.

Let $\sum_{i=1}^{k} \alpha_{i_1} x_{i_1} + \alpha_{i_2} x_{i_2} + \ldots\ldots\ldots + \alpha_{i_{d_1}} x_{i_{d_1}} = 0$

Then $\sum_{i=1}^{k} w_i = 0 \Rightarrow w_i = 0$ for all i (since, if j is the largest integer s.t. $w_j \neq 0$, then $w_1 + \ldots\ldots + w_j = 0 \Rightarrow w_j \in W_j \cap (W_1 + \ldots\ldots + W_{j-1}) = \{0\} \Rightarrow w_j = 0$, a contradiction).

$\therefore$ $\beta = \{\beta_1, \ldots\ldots, \beta_k\}$ is an independent set in W. Since β_i spans W_i for all i, β spans W.

$\therefore$ β is a basis of W.

$(iii) \Rightarrow (i)$

Let $\quad x_1 + \ldots\ldots + x_k = 0, \; x_i \in W_i$

Then $\quad \alpha_{1_1} x_{1_1} + \ldots\ldots + \alpha_{1_{d_1}} x_{1_{d_1}} + \ldots\ldots + \alpha_{k_1} x_{k_1} + \ldots\ldots + x_{k_{d_k}} = 0$

$\Rightarrow$ each coefficient $\alpha_{ij} = 0$ as β is linearly independent

$\Rightarrow$ each $x_i = 0$

$\Rightarrow$ $W_1, \ldots\ldots, W_k$ are independent.

Problem 23 : *Let V be a finite dimensional space and $W_1, \ldots\ldots, W_k$ be subspaces of V s.t.*

$$V = W_1 + \ldots\ldots + W_k \text{ and } \dim V = \dim W_1 + \ldots\ldots + \dim W_k$$

Prove that $V = W_1 \oplus \ldots\ldots \oplus W_k$.

Solution : Let β_i be an ordered basis of W_i for all i. Let $\dim W_i = d_i$. Let $x \in V$. Then $x = x_1 + \ldots\ldots + x_k$, $x_i \in W_i$, $x_i \in W_i \Rightarrow x_i$ is a linear combination of vectors in β_i.

$\Rightarrow$ x is a linear combination of vectors in $\beta = \{\beta_1, \ldots\ldots, \beta_k\}$

$\Rightarrow$ β spans V

$\Rightarrow$ β is a basis of V (for if β is not a basis of V, then some subset of β is a basis of V

$\Rightarrow$ $\dim V < o(\beta_1) + \ldots\ldots + o(\beta_k) = \dim W_1 + \ldots\ldots + \dim W_k = \dim V$, a contradiction)

$\Rightarrow$ $W_1, \ldots\ldots, W_k$ are independent by Theorem 11

$\Rightarrow$ $W_j \cap (W_1 + \ldots\ldots + W_{j-1}) = \{0\}$ for all j, $2 \le j \le k$

$\Rightarrow$ $V = W_1 \oplus \ldots\ldots \oplus W_k$.

Projection : We recall, by a projection E of a space V we mean a linear operator on V s.t. $E^2 = E$. Let R be the range of E and N, its null space. Then we can show that $V = R \oplus N$.

as $x \in R \cap N \Rightarrow x = Ey, \; Ex = 0, \; y \in V$

$\Rightarrow Ex = E^2 y = Ey$

$\Rightarrow 0 = Ey \Rightarrow x = 0$

and $\quad x \in V \Rightarrow Ex \in R$ and $E(x - Ex) = Ex - E^2 x = Ex - Ex = 0$

$\Rightarrow Ex \in R$ and $x - Ex \in N$

$\Rightarrow x = (x - Ex) + Ex \in N + R = R + N.$

Conversely, if R, N are subspaces of V s.t. $V = R \oplus N$, define $E : V \to V$ s.t., $E(r + n) = r$ (each $v \in V$ can be uniquely written as $v = r + n$, $r \in R$, $n \in N$) then E is a linear operator on V s.t.

$$E^2(v) = E^2(r + n) = E(r) = r = E(v) \text{ for all } v \in V \Rightarrow E^2 = E$$

$\therefore$ E is a projection s.t., range E is R. Let $v \in$ null space of E then $E(v) = 0$ $\Rightarrow$ $E(r+n) = 0$ $\Rightarrow$ $r = 0$ $\Rightarrow$ $v = n \in N$

$\therefore$ null space of E is N.

Any projection E on V is diagonalisable as $\{v_1, \ldots\ldots, v_r\}$ is a basis of range space R of E and $\{v_{r+1}, \ldots\ldots, v_n\}$, a basis of null space N of E.

$\Rightarrow$ $\{v_1, \ldots\ldots, v_r, v_{r+1}, \ldots\ldots, v_n\}$, is a basis of $R \oplus N = V$

Now $\quad E(v_1) = (x_1 + x_2),\ x_1 \in R,\ x_2 \in N$

$\therefore \quad E^2(v_1) = E(v_1) = E(x_1 + x_2) = E(x_1) + E(x_2) = E(x_1)$

$\Rightarrow \quad E(v_1) = E(x_1)$

$\Rightarrow \quad v_1 - x_1 \in \text{Ker}\, E = N$

Also $\quad v_1 \in R,\ x_1 \in R \Rightarrow v_1 - x_1 \in R$

So, $\quad v_1 - x_1 \in R \cap N = \{0\} \Rightarrow v_1 = x_1$

Again $\quad x_2 = E(v_1) - x_1 \in R \cap N = \{0\} \Rightarrow x_2 = 0$

$\therefore$ $E(v_1) = v_1$. Similarly, $E(v_i) = 0\ \forall\ i = 1, 2, \ldots\ldots, r$. Also $E(v_j) = 0\ \forall\ j = r+1, \ldots\ldots, n$.

$\Rightarrow$ matrix of E w.r.t this basis is $\begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}$, which is clearly a diagonal matrix.

Theorem 12 : *If $V = W_1 \oplus \ldots\ldots \oplus W_k$, then $\exists$ k linear operators $E_1, \ldots\ldots, E_k$ on V s.t.*

(*i*) *Each E_i is a projection* $(E_i^2 = E_i)$

(*ii*) $E_i E_j = 0$ *for all* $i \neq j$

(*iii*) $I = E_1 + \ldots\ldots + E_k$

(*iv*) *the range of E_i is W_i*

and conversely.

Proof : Define $\quad E_i : V \to V$, s.t.,

$$E_i(x_1 + \ldots\ldots + x_k) = x_i \text{ for all } i \text{ where } x_i \in W_i$$

Then E_i is linear operator s.t.

$$E_i^2(x_1 + \ldots\ldots + x_k) = E_i(x_i) = x_i = E_i(x_1 + \ldots\ldots + x_k)$$

$$\Rightarrow \quad E_i^2 = E_i \text{ for all } i$$

This proves (*i*)

Let $i \neq j$. Then $E_i E_j(x_1 + \ldots\ldots + x_k) = E_i(x_j) = 0$

$\therefore \quad E_i E_j = 0$ for all $i \neq j$.

This proves (*ii*).

Let $v \in V$. Then $v = x_1 + \ldots\ldots + x_k,\ x_i \in W_i$

$$\begin{aligned} \therefore \quad (E_1 + \ldots\ldots + E_k)v &= E_1 v + \ldots\ldots + E_k v \\ &= x_1 + \ldots\ldots + x_k \\ &= v = I(v) \end{aligned}$$

$\therefore \qquad E_1 + \ldots\ldots + E_k = I$

This proves (*iii*).

By definition of E_i, range of E_i is W_i which proves (*iv*).

Conversely, let $v \in V$. By (*iii*) $I = E_1 + \ldots\ldots + E_k \Rightarrow$

$$v = I(v) = E_1 v + \ldots\ldots + E_k v = x_1 + \ldots\ldots + x_k,\ x_i \in W_i\ (x_i = E_i v)$$

$\therefore \qquad V = W_1 + \ldots\ldots + W_k$

Let $\qquad v = y_1 + \ldots\ldots + y_k,\ y_i \in W_i$ = Range of E_i

$\Rightarrow \quad y_i = E_i z_i$

$$\therefore \qquad E_j(v) = E_j y_1 + \ldots\ldots + E_j y_k$$
$$= E_j E_1 z_1 + \ldots\ldots + E_j E_k z_k$$
$$= E_j^2 z_j = E_j z_j = y_j$$

$\therefore \qquad x_j = y_j$ for all $j = 1, \ldots\ldots, k$

$\therefore$ each $v \in V$ can be uniquely written as sum of elements of $W_1, \ldots\ldots, W_k$

$\therefore \qquad V = W_1 \oplus \ldots\ldots \oplus W_k.$

Problem 24 : *Let V be a real vector space and E an idempotent linear operator. Prove that $I + E$ is invertible.*

Solution : $\qquad (I+E)(I - \frac{1}{2}E) = I + E - \frac{1}{2}E - \frac{1}{2}E^2$

$$= I + E - \frac{1}{2}E - \frac{1}{2}E$$
$$= I + E - E = I$$

$\therefore$ $I + E$ is invertible.

and $\qquad (I+E)^{-1} = I - \dfrac{1}{2}E.$

Problem 25 : *Prove that if E is the projection on R along N, then $I - E$ is the projection on N along R.*

Solution : When we say E is the projection on R along N, we mean $V = R \oplus N$ where R = range space of E and N = null space of E.

Let $x \in R$ then $x = Ey,\ y \in V$

$$\Rightarrow (I - E)x = x - Ex = Ey - Ey = 0$$
$$\Rightarrow x \in \text{null space of } I - E$$

Also $\quad x \in N \Rightarrow Ex = 0$

$$\Rightarrow (I - E)x = x \text{ for all } x \in N$$

$\therefore \qquad v \in V \Rightarrow v = r + n,\ r + R,\ n \in N$

$$\Rightarrow (I - E)v = (I - E)r + (I - E)n$$
$$= 0 + n = n$$

$\therefore$ Range space of $I-E$ is N

Also $\qquad (I-E)^2 = I + E^2 - 2E = I - E$

$\therefore$ $I-E$ is the projection on N along R.

Problem 26 : *If diagonal operator has only the eigen values* 0 *and* 1, *is it a projection* ?

Solution : Since T is diagonal operator, $\exists$ a basis $\beta = \{v_1, \ldots\ldots, v_n\}$ of V s.t. $[T]_\beta$ = diagonal. Since eigen values of T are 0 and 1, let first m entries in diagonal be 1 and others be 0.

Let $v \in V$. Then $v = \alpha_1 v_1 + \ldots\ldots + \alpha_m v_m + \alpha_{m+1} v_{m+1} + \ldots\ldots + \alpha_n v_n$

$$\therefore \qquad T^2(v) = T(Tv)$$

$$= T(\alpha_1 v_1 + \ldots\ldots + \alpha_m v_m) \text{ as } Tv_i = v_i \text{ for all } i,\ 1 \le i \le m$$

$$Tv_j = 0 \text{ for all } j > m$$

$$= T(\alpha_1 v_1 + \ldots\ldots + \alpha_m v_m + \alpha_{m+1} v_{m+1} + + \alpha_n v_n)$$

$$= T(v) \text{ for all } v \in V$$

$$\therefore \qquad T^2 = T$$

Hence T is a projection.

Invariant Direct Sums

In this section we study direct sum decomposition where each subspace is T-invariant and then conclude the behaviour of T and conversely.

Theorem 13 : *Let T be a linear operator on the space V and $V = W_1 \oplus \ldots\ldots \oplus W_k$. Define $E_i(v) = E_i(x_1 + \ldots\ldots + x_k) = x_i \in W_i$. Then each E_i is a projection on V s.t. $E_i E_j = 0$ for all $i \neq j$ and $I = E_1 + \ldots\ldots + E_k$. A necessary and sufficient condition that each W_i is invariant under T is that $TE_i = E_i T$ for all $i = 1, \ldots\ldots, k$.*

Proof : Let $TE_i = E_i T$

Let $x_i \in W_i$. Then by def., $E_i(x_i) = x_i$

$$\therefore \qquad T(x_i) = T(E_i x_i)$$

$$= E_i(Tx_i)$$

$$\Rightarrow T(x_i) \in \text{Range of } E_i = W_i$$

$\therefore$ W_i is invariant under T for all $i = 1, \ldots\ldots, k$

Conversely, let W_i be invariant under T. Then $v \in V$

$$\Rightarrow I(v) = (E_1 + \ldots\ldots + E_k)v$$

$$\Rightarrow v = E_1(v) + \ldots\ldots + E_k(v)$$

$$\Rightarrow T(v) = TE_1(v) + \ldots\ldots + TE_k(v)$$

Since $E_i(v) \in W_i$ and W_i is T-invariant $\Rightarrow (E_i(v)) \in W_i$.

So, $\qquad E_j[T(E_i(v)] = T(E_i(v)) \text{ if } j = i$

$$= 0 \text{ if } j \neq i$$

$$\therefore \qquad E_j(T(v)) = T(E_j(v)) \text{ for all } v \in V$$
$$\Rightarrow E_jT = TE_j \text{ for all } j$$

Theorem 14 : *Let T be a linear operator on a finite dimensional space V. If T is diagonalisable and $c_1, \ldots\ldots, c_k$ are distinct eigen values of T, then $\exists$ linear operators $E_1, \ldots\ldots, E_k$ on V s.t.*

(*i*) $T = c_1E_1 + \ldots\ldots + c_kE_k$

(*ii*) $I = E_1 + \ldots\ldots + E_k$

(*iii*) $E_iE_j = 0$ *for all* $i \neq j$

(*iv*) $E_i^2 = E_i$

(*v*) *Range of E_i is the eigen space of T associated with eigen value c_i of T.*

Conversely, if $\exists$ distinct scalars $c_1, \ldots\ldots, c_k$ and k non-zero linear operators $E_1, \ldots\ldots, E_k$ satisfying (i), (ii), (iii), then T is diagonalisable, $c_1, \ldots\ldots, c_k$ are eigen values of T and (iv) and (v) are also satisfied.

Proof : Let T be diagonalisable and $c_1, \ldots\ldots, c_k$ be distinct eigen values of T. Let W_i be eigen spaces of T corresponding to eigen values c_i. Then $\dim V = \dim W_1 + \ldots\ldots + \dim W_k$

and $\qquad V = W_1 + \ldots\ldots + W_k$ by Theorem 3 and lemma 3.

By problem 23

$$V = W_1 \oplus \ldots\ldots \oplus W_k$$

As in theorem 12, let $E_1, \ldots\ldots, E_k$ be the projections associated with this decomposition. Then (*ii*) to (*v*) are satisfied. Let $v \in V$

Then
$$\begin{aligned} I(v) = v &= (E_1 + \ldots\ldots + E_k)v \\ &= E_1(v) + \ldots\ldots + E_k(v) \\ \Rightarrow T(v) &= TE_1(v) + \ldots\ldots + TE_k(v) \\ &= c_1E_1(v) + \ldots\ldots + c_kE_k(v) \text{ as } E_i(v) \in \text{Range of } E_i = W_i \\ &= (c_1E_1 + \ldots\ldots + c_kE_k)\, v \\ \Rightarrow T &= c_1E_1 + \ldots\ldots + c_kE_k \end{aligned}$$

This proves (*i*)

Conversely, suppose T along with distinct scalars c_i and non zero operators E_i satisfy (*i*), (*ii*) and (*iii*). Also $T = c_1E_1 + \ldots\ldots + c_kE_k$

Then $\qquad TE_i = c_iE_i$ for all i

$$\Rightarrow (T - c_iI)\, E_i = 0 \text{ for all } i$$

Since $\qquad E_i \neq 0 \;\; \exists\, v_i \in V$ s.t. $E_i(v_i) \neq 0$

$$\therefore \qquad (T - c_iI)\,(E_i(v_i)) = 0 \text{ for all } i$$
$$\Rightarrow T(E_i(v_i)) = c_i(E_i(v_i)),\; E_i(v_i)) \neq 0 \text{ for all } i$$

$\Rightarrow c_i$ is an eigen value of T for all i, (E_iv_i is an eigen vector).

If c is any scalar, then

$$(T - cI) = (c_1E_1 + \ldots\ldots + c_kE_k) - c(E_1 + \ldots\ldots + E_k)$$
$$= (c_1 - c)E_1 + \ldots\ldots + (c_k - c)E_k$$

If c is an eigen value of T, then $\exists\, 0 \neq v \in V$ s.t.

$$Tv = cv \Rightarrow (T - cI)v = 0$$

$$\therefore \quad (c_1 - c)\ E_jE_1(v) + \ldots\ldots + (c_k - c)\ E_jE_k(v) = 0$$

$$\Rightarrow (c_j - c)\ E_j(v) = 0 \text{ for all } j = 1, \ldots\ldots, k$$

If $E_j(v) = 0$ for all j, then $I = E_1 + \ldots\ldots + E_k$

$$\Rightarrow v = Iv = E_1v + \ldots\ldots + E_kv = 0$$

$$\therefore \quad E_j(v) \neq 0 \text{ for some } j$$

$$\therefore \quad c_j = c \text{ for some } j$$

$\therefore$ $c_1, \ldots\ldots, c_k$ are only eigen values of T.

Let W_i = range of E_i, $i = 1, \ldots\ldots, k$.

By (*ii*) $\quad I = E_1 + \ldots\ldots + E_k$

$$\Rightarrow v = Iv = E_1v + \ldots\ldots + E_kv \in W_1 + \ldots\ldots + W_k \text{ for all } v \in V$$

$$\Rightarrow V = W_1 + \ldots\ldots + W_k$$

As in theorem 12, $V = W_1 \oplus \ldots\ldots \oplus W_k$

$$\therefore \quad \dim V = \dim W_1 + \ldots\ldots + \dim W_k$$

$\Rightarrow$ T is diagonalisable if W_i = eigen space of T corresponding to c_i.

Let $x \in$ eigen space of T. Then $Tx = c_ix$, $1 \leq i \leq k$

$$\Rightarrow (c_1E_1 + \ldots\ldots + c_kE_k)\,x = c_iI(x) = c_i(E_1 + \ldots\ldots + E_k)\,x$$

$$\Rightarrow c_1E_1(x) + \ldots\ldots + c_kE_k(x) = c_iE_1(x) + \ldots\ldots + c_iE_k(x)$$

$$\Rightarrow (c_1 - c_i)\ E_1(x) + \ldots\ldots + (c_k - c_i)\,E_k(x) = 0$$

$$\Rightarrow (c_j - c_i)\ E_j(x) = 0 \text{ for all } j = 1, \ldots\ldots, k$$

as $\quad E_j(x) \in$ Range of $E_j = W_j$

and $\quad W_1, \ldots\ldots, W_k$ are independent

we get $\quad E_j(x) = 0,\ j \neq i$ as $c_j - c_i \neq 0$ for all $j \neq i$

Since $\quad I = E_1 + \ldots\ldots + E_k$,

$$x = E_1(x) + \ldots\ldots + E_k(x) = E_i(x)$$

$$\Rightarrow x \in \text{Range of } E_i = W_i$$

$\therefore$ eigen space corresponding to c_i is contained in W_i.

Also $\quad 0 \neq x \in W_i \Rightarrow x = E_i(y_i) \neq 0$

But $\quad (T - c_iI)E_i = 0$

$$\Rightarrow TE_i(y_i) = c_iE_i(y_i)$$

$$\Rightarrow T(x) = c_ix \Rightarrow x \in \text{ eigen space corresponding to } c_i$$

$$\therefore \quad W_i = \text{ eigen space corresponding to } c_i.$$

Using above theorem, we give another proof of Theorem 10 i.e. suppose T is a linear operator with minimal polynomial $p(x) = (x - c_1) \ldots\ldots (x - c_k)$ s.t. $c_1, \ldots\ldots, c_k \in F$ are distinct. To show T is diagonalisable.

Proof : Let $p_j(x) = \underset{i \neq j}{\pi} \dfrac{(x-c_i)}{(c_j-c_i)}$, $j = 1, \ldots\ldots, k$

Then $\qquad p_j(c_i) = \delta_{ij}$

Let V = space of all polynomials over F of degree less than k.

Then $p_1, \ldots\ldots, p_k \in V$ and are linearly independent as $\alpha_1 p_1 + \ldots\ldots + \alpha_k p_k = 0$

$$\Rightarrow \alpha_1 p_1(c_i) + \ldots\ldots + \alpha_k p_k(c_i) = 0$$

$$\Rightarrow \alpha_i = 0 \text{ for all } i$$

Since $\dim V = k$, $\{p_1, \ldots\ldots, p_k\}$ is a basis of V.

Now $\qquad 1 \in V \Rightarrow 1 = \alpha_1 p_1 + \ldots\ldots + \alpha_k p_k$

Put $x = c_i$ on both sides to get

$$1 = \alpha_i \text{ for all } i$$

$$\Rightarrow 1 = p_1 + \ldots\ldots + p_k \qquad \ldots (i)$$

$$x \in V \Rightarrow x = \beta_1 p_1 + \ldots\ldots + \beta_k p_k$$

Put $\qquad x = c_i$

Then $\qquad c_i = \beta_i$ for all i

$$\Rightarrow x = c_1 p_1 + \quad + c_k p_k \qquad \ldots (ii)$$

Let $\qquad p_j(T) = E_j$

Put $x = T$ in (i) and (ii) above to get

$$I = p_1(T) + \ldots\ldots + p_k(T) = E_1 + \ldots\ldots + E_k$$

$$T = c_1 E_1 + \ldots\ldots + c_k E_k$$

Since $p(x)$ divides $p_i(x)\, p_j(x)$ for all $i \neq j$

$$p_i(T)\, p_j(T) = p(T)\, q(T) \text{ for all } i \neq j$$

$$\Rightarrow E_i E_j = 0 \text{ for all } i \neq j$$

If $E_j = 0$ for some j, then $p_j(T) = 0$ and

degree of $p_j(x) < \deg p(x)$, a contradiction

$\therefore \qquad E_j \neq 0$ for all $j = 1, \ldots\ldots, k$

$\therefore$ By Theorem 7, T is diagonalisable.

Problem 27 : *Let E be a projection of V and let T be a linear operator on V. Prove that the range of E is invariant under T if and only if $ETE = TE$. Prove that both the range and null space of E are invariant under T if and only if $ET = TE$.*

Solution : Let $\quad R$ = range of E

N = null space of E

Then $\qquad V = R \oplus N$

Also we have shown before that $I - E$ is also a projection. $x \in N \Rightarrow Ex = 0$ $\Rightarrow (I-E)x = x \Rightarrow x \in$ range of $I - E$. $\therefore$ Range of $E = R$, Range of $(I-E) = N$.

Also $E(I-E) = E - E^2 = E - E = 0$. Suppose R is invariant under T then $\Rightarrow T(EV) \subseteq EV \Rightarrow T(I-E)V = T(V-EV) \subseteq V - EV = (I-E)V \Rightarrow N = (I-E)V$ is invariant under T.

$\therefore$ By Theorem 13, $TE = ET$

$$\Rightarrow ETE = E^2T = ET = TE.$$

Conversely, suppose $ETE = TE$

Let $\quad E(v) \in R$ = range of E

Then $\quad E(TE(v)) \in R$ as $T: V \to V,\ E: V \to V$

$\Rightarrow TE(v) \in R$ since $ETE = TE$

$\Rightarrow R$ is invariant under T.

Further, if both R and N are invariant under T, then by Theorem 13, $TE = ET$.

Conversely, suppose $TE = ET \Rightarrow ETE = TE$

From above then, R is invariant under T.

Also $n \in N \Rightarrow E(n) = 0 \Rightarrow (ET)(n) = (TE)(n)$

$$= T(E(n))$$

$$= T(0) = 0$$

$\therefore \quad E(T(n)) = 0$ for all $n \in N$

$\Rightarrow T(n) \in$ null space of E for all $n \in N$

$\Rightarrow N$ is invariant under T.

Problem 28 : *Let T be a linear operator on $\mathbf{R}^2$, the matrix of which in the standard ordered basis is* $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$.

Let W_1 be the subspace of $\mathbf{R}^2$ spanned by $E_1 = (1, 0)$. (a) Prove that W_1 is invariant under T. (b) Prove that $\exists$ no T-invariant subspace W_2 of $\mathbf{R}^2$ s.t. $\mathbf{R}^2 = W_1 \oplus W_2$.

Solution (a) : $\quad W_1 = \{(x, 0) \mid x \in R\}$

$$T W_1 = \{2(x, 0) \mid x \in R\} \subseteq W_1$$

$\therefore W_1$ is invariant under T.

(b) : Suppose W_2 is T-invariant subspace of $\mathbf{R}^2$ s.t. $\mathbf{R}^2 = W_1 \oplus W_2$. Since dim $W_1 = 1$, dim W_2 must be 1.

Define : $\quad E: \mathbf{R}^2 \to \mathbf{R}^2$ s.t.

$$E(x, y) = (x, 0)$$

Then E is a projection of $\mathbf{R}^2$ onto W_1.

By Theorem 13, $TE = ET$

But $\quad TE(1, 1) = T(1, 0) = (2, 0)$

$$ET(1, 1) = E(3, 2) = (3, 0)$$

$\therefore \quad TE \neq ET$, a contradiction

Thus there does not exist T-invariant subspace W_2 s.t. $\mathbf{R}^2 = W_1 \oplus W_2$.

Primary Decomposition Theorem

Theorem 15 : *Let T be a linear operator on a finite dimensional space V over F. Let $p(x)$ be the minimal polynomial for T s.t.*

$$p(x) = p_1(x)^{r_1} \ldots\ldots p_k(x)^{r_k}$$

where the $p_i(x)$ are distinct irreducible monic polynomials over F and r_i are +ve integers. Let W_i be the null spaces of $p_i(T)^{r_i}$, $i = 1, \ldots\ldots, k$. Then

(i) $V = W_1 \oplus \ldots\ldots \oplus W_k$

(ii) each W_i is invariant under T

(iii) if T_i is operator induced on W_i by T, then the minimal polynomial for T_i is $p_i(x)^{r_i}$.

Proof : Let $f_i(x) = \dfrac{p(x)}{p_i(x)^{r_i}} = \prod_{j \neq 1} p_j(x)^{r_i}, i = 1, \ldots\ldots, k$

Then, clearly $f_1(x), \ldots\ldots, f_k(x)$ are relatively prime. Thus $\exists$ polynomials $g_1(x), \ldots\ldots, g_k(x)$ s.t.

$$f_1(x)\ g_1(x) + \ldots\ldots + f_k(x)\ g_k(x) = 1$$

By def. $p(x)$ divides $f_i(x)\ f_j(x)$ for all $i \neq j$

Let $\quad h_i(x) = f_i(x)\, g_i(x)$

and $\quad E_i = h_i(T) = f_i(T)\, g_i(T)$

Since $\quad h_1(x) + \ldots\ldots + h_k(x) = I$

$$h_1(T) + \ldots\ldots + h_k(T) = I$$

we get $\quad E_1 + \ldots\ldots + E_k = I$

Also $\quad f_i(x) f_j(x) = p(x)\, q(x)$ for all $i \neq j$ for some $q(x)$

$$f_i(T) f_j(T) = p(T)\, q(T) = 0$$

$$\Rightarrow f_i(T)\, g_i(T) f_j(T)\, g_j(T) = 0 \text{ for all } i \neq j$$

$$\Rightarrow E_i E_j = 0 \text{ for all } i \neq j$$

$\therefore\ E_1 + \ldots\ldots + E_k = I$ and $E_i E_j = 0$ for all $i \neq j$

$$\Rightarrow E_i^2 = E_i \text{ for all } i$$

$\Rightarrow E_1, \ldots\ldots, E_k$ are projections of V

Let W_i = null space of $p_i(T)^{r_i}$. Let $v \in$ range of E_i

Then $\quad v = E_i(x)$

$$\Rightarrow E_i(v) = E_i^2(x) = E_i(x) = v$$

and so $p_i(T)^{r_i} v = p_i(T)^{r1} E_i(v))$

$$= p_i(T)^{r_i} f_i(T) \; g_i(T) v$$
$$= p(T) \; g_i(T) v$$
$$= 0 \text{ for all } i = 1, \ldots\ldots, k$$

$\therefore$ $v \in$ null space of $p_i(T)^{r_i}$

$$\Rightarrow v \in W_i$$
$$\Rightarrow \text{range of } E_i \subseteq W_i.$$

Let $v \in W_i$. Then for all $j \neq i$, $p_i(x)^{r_i}$ divides $f_j(x)$

$\therefore$ $$f_j(x) v = q(x) \; p_i(x)^{r_i}$$

$$\Rightarrow f_j(T) v = q(T) \; p_i(T)^{r_i} \; v = 0 \text{ as } v \in W_i$$
$$\Rightarrow f_j(T) \; g_j(T) \; v = 0 \text{ for all } j \neq 1$$
$$\Rightarrow E_j(v) = 0 \text{ for all } j \neq 1$$

Also $$I = E_1 + \ldots\ldots + E_k$$
$$\Rightarrow v = I(v) = E_1(v) + \ldots\ldots + E_k(v) \text{ as } E_j(v) = 0 \text{ for all } j \neq i$$
$$\Rightarrow v \in \text{range of } E_i$$
$$\Rightarrow W_i \subseteq \text{range of } E_i$$

$\therefore$ $$\text{range of } E_i = W_i$$

By theorem 12, $V = W_1 \oplus \ldots\ldots \oplus W_k$. Since $TE_i = Tf_i(T) g_i(T) = f_i(T) g_i(T) T = EiT$ for all i, each W_i is invariant under T by Theorem 13. Let T_i be the restriction of T on W_i.

Since $p_i(T)^{r_i}(v) = 0$ for all $v \in W_i = \text{Ker } p_i(T)^{r_i}$,

$p_i(T_i)^{r_i} = 0$. $\therefore$ $q_i(x)$ divides $p_i(x)^{r_i}$ where $q_i(x) =$ minimal polynomial of T_i.

Now $q_i(T_i) = 0$

$\Rightarrow q_i(T) \; f_i(T) = 0 \Rightarrow p(x)$ divides $q_i(x) \; f_i(x) \Rightarrow p_i^{r_i}(x) \; f_i(x) \mid q_i(x) f_i(x)$

$\Rightarrow p_i^{r_i}(x)$ divides $q_i(x)$.

$\therefore$ $q_i(x) = p_i^{r_i}(x)$ for all i

This proves (*iii*) and the theorem.

Cor : If T is a linear operator on a finite dimensional space V over F and minimal polynomial $p(x)$ of T is a product of distinct linear factors, then T is diagonalisable.

Proof : Let $p(x) = (x-c_1) \ldots\ldots (x-c_k)$, where c_i are distinct roots of $p(x)$ in F. By primary decomposition theorem

$V = W_1 \oplus \ldots\ldots \oplus W_r$, where each W_i = Null space of $(T-c_iI)$

$$\therefore \qquad v \in W_i \Rightarrow (T-c_iI) = 0$$
$$\Rightarrow T(v) = c_iv$$

$\therefore$ every non zero vector in W_i is an eigen vector of T corresponding to eigen value c_i of T. If β_i is a basis of W_i, then $\{\beta_i, \ldots\ldots, \beta_r\}$ is a basis of V. β_i consists of eigen vectors of $T \Rightarrow \{\beta_1, \ldots\ldots, \beta_r\} = \beta$ consists of eigen vectors of T and is a basis of $V \Rightarrow T$ is a diagonalisable.

Theorem 16 : *Let T be a linear operator on the finite dimensional space V over F. Suppose that the minimal polynomial for T decomposes over F into a product of linear polynomials. Then $\exists$ a diagonalisable operator D on V and a nilpotent operator N on V s.t. (i) $T = D+N$ (ii) $DN = ND$.*

Proof : Let $p(x) = (x-c_1)^{r_1} \ldots\ldots\ldots (x-c_k)^{r_k}$ be the minimal polynomial for T where $c_1, \ldots\ldots, c_k$ are distinct scalars in F.

By theorem 15, $V = W_1 \oplus \ldots\ldots \oplus W_k$, where W_i = null space of $(T-c_iI)^{r_i}$. Let $E_1, \ldots\ldots, E_k$ be the corresponding projections. Then W_i = range of E_i.

Let $D = c_1E_1 + \ldots\ldots + c_kE_k$

By theorem 14, D is diagonalisable.

Since $\qquad I = E_1 + \ldots\ldots + E_k$

$$T = TE_1 + \ldots\ldots + TE_k, \quad D = c_1E_1 + \ldots\ldots + c_kE_k$$

Let $\qquad N = T - D = (T-c_1I)\ E_1 + \ldots\ldots + (T-c_kI)\,E_k$

Then $\qquad N^2 = (T-c_1I)^2\ E_1 + \ldots\ldots + (T-c_kI)^2\,E_k$

and in general that

$$N^r = (T-c_1I)^r\ E_1 + \ldots\ldots + (T-c_kI)^r\,E_k$$

Since $(x-c_i)^{r_i}$ is the minimal polynomial of T on W_i, $(T-c_iI)^{r_i} = 0$ on W_i for all i.

$$\Rightarrow (T-c_iI)^r = 0 \text{ on } W_i \text{ for all } r \geq r_i$$

$$\therefore \qquad N^r = 0 \text{ for all } r \geq r_i \text{ for each } i$$

$\therefore$ N is nilpotent operator.

$\therefore$ $T = D+N$, D is diagonalisable and N, nilpotent operator.

Now $\qquad DT = (c_1E_1 + \ldots\ldots + c_kE_k)\ (TE_1 + \ldots\ldots + TE_k)$

$$= c_1TE_1 + \ldots\ldots + c_kTE_k$$

as W_is are invariant under $T \Rightarrow TE_i = E_iT$ for all i

$$= T(c_1E_1) + \ldots\ldots + (c_kE_k)$$
$$= (TE_1)\ (c_1E_1) + \ldots\ldots + (TE_k)\ (c_kE_k)$$
$$= (TE_1 + \ldots\ldots + TE_k)\ (c_1E_1 + \ldots\ldots + c_kE_k)$$
$$= TD$$

$$\therefore \qquad D(D+N) = (D+N)D$$
$$\Rightarrow \quad DN = ND.$$

Exercises

1. Let V be the vector space of all polynomials of degree ≤ 6 over F. Let W be the subspace of V spanned by $\{1, x^2, x^4, x^6\}$. Let D be the differential operator on V. (i.e. $D(f(x)) = \frac{d}{dx} f(x)$). Show that W is not invariant under D.

2. In Exercise 1, show that W is invariant under D^2 where $D^2(f(x)) = \frac{d^2}{dx^2} f(x)$. Let $T = D^2$. Find

   (*i*) the matrix of T_w in a suitable basis of W.

   (*ii*) the matrix of $\hat{T}$ in a suitable basis of $\frac{V}{W}$

   (*iii*) the matrix of T in a suitable basis of V.

   (*i*) $A = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 30 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ (*ii*) $C = \begin{bmatrix} 0 & 6 & 0 \\ 0 & 0 & 20 \\ 0 & 0 & 0 \end{bmatrix}$ (*iii*) $\begin{bmatrix} A & 0 \\ 0 & C \end{bmatrix}$

3. Let V be the vector space of all polynomials over the field of real numbers $\mathbf{R}$. Let W be the subspace of V spanned by $\{1, x, x^2\}$. Let T be the linear operator on V defined by $T(f(x)) = xf(x)$. Show that W is not invariant under T.

4. Let T be a linear operator on a vector space V over F. If $W_1, \ldots\ldots, W_k$ are T-invariant subspaces of V, prove that $\sum_{i=1}^{k} W_i$ and $\bigcap_{i=1}^{k} W_i$ are T-invariant subspaces of V.

5. Let c be a characteristic value of T and W be the space of characteristic vectors associated with the characteristic value c. What is the restriction operator T_w?

   $(T_w = cI)$

6. Let T be a linear operator on a finite dimensional vector space V. Prove that T is diagonalisable if and only if V is a direct sum of one dimensional T-invariant subspaces.

7. Let T be a linear operator on a finite dimensional vector space V and let W be a T-invariant subspace of V.

(*i*) Show that if λ is an eigen value of T_w, then λ is an eigen value of T.

(*ii*) Show that the eigen space of T_w corresponding to eigen value λ of T_w is $W_\lambda \cap W$, where W_λ denotes the eigen space of T corresponding to λ.

(*iii*) Prove that if T is diagonalisable, then so is T_w.

(Hint : T is diagonalisable $\Leftrightarrow$ $V = W_1 + \ldots\ldots + W_k$ where W_i denotes eigen space corresponding to eigen value λ_i of T. Use (*ii*)).

8. Let W be a proper T-invariant subspace of V, where T is a linear operator on a finite dimensional vector space V.

Let $\eta : V \to \dfrac{V}{W}$ s.t.,

$\eta(v) = W + v$ be a linear transformation. Show that $\eta T = \hat{T}\eta$ where $\hat{T}$ is a linear operator on $\dfrac{V}{W}$ defined by $\hat{T}(W + v) = W + T(v)$.

Further, if T is diagonalisable, show that $\hat{T}$ is also diagonalisable.

(Hint : T is diagonalisable $\Rightarrow \exists$ a basis $\{x_1, \ldots\ldots, x_n\}$ of V consisting of eigen vectors of T. Also $\eta T = \hat{T}\eta \Rightarrow \{\eta x_1, \ldots\ldots, \eta x_n\}$ are eigen vectors of $\hat{T} \Rightarrow \{W + x_1, \ldots\ldots, W + x_n\}$ are eigen vectors of $\hat{T}$. If $\{W + v_1, \ldots\ldots, W + v_r\}$ is a basis of $\dfrac{V}{W}$, then it can be replaced by $\{W + x_1, \ldots\ldots, W + x_r\}$ such that it forms a basis of $\dfrac{V}{W}$ consisting of eigen vectors of $\dfrac{V}{W}$).

9. Let T be a linear operator on a finite dimensional vector space and suppose that $V = W_1 \oplus \ldots\ldots \oplus W_k$, where W_i is a T-invariant subspace of V for each $i = 1, \ldots\ldots, k$. If $f(t)$ denotes the characteristic polynomial of T and $f_i(t)$ denotes the characteristic polynomial of T_{w_i} $(1 \le i \le k)$, then show that

$$f(t) = f_1(t) \cdot f_2(t) \ldots\ldots f_k(t)$$

(Hint : Use induction on k).

10. If E_1, E_2 are projections onto independent subspaces, show that $E_1 + E_2$ is also a projection.

11. Let T be a linear operator on a finite dimensional vector space V. Let R be the range of T and let N be the null space of T. Prove that R and N are independent if and only if $V = R \oplus N$.

Chapter 12

Fields

In earlier chapters we defined a field, a subfield and proved a few results regarding these. We now come back to fields and study them in some more details. Fields play an important role in algebra with applications to Number Theory, theory of equations and geometry.

Definition : Let K be a field and suppose F is a subfield of K, then K is called an *extension* of F.

Suppose S is a non empty subset of K,. Let $F(S)$ denote the smallest subfield of K which contains both F and S. (In fact $F(S)$ would be the intersection of all subfields of K that contain F and S). The following theorem is then an easy consequence.

Theorem 1 : *If S, T are non empty subsets of a field K and K is an extension of a field F then $F(S \cup T) = F(S)(T)$ (where, of course, if $F(S) = E$, then by $F(S)(T)$ we mean $E(T)$).*

Proof : $F(S \cup T)$ is the smallest subfield of K containing $S \cup T, F$

i.e., $S, T, F \subseteq F(S \cup T)$

$\Rightarrow F(S) \subseteq F(S \cup T), \quad T \subseteq F(S \cup T)$

$\Rightarrow F(S)(T) \subseteq F(S \cup T)$

Again, $F, S, T \subseteq F(S)(T)$

$\Rightarrow F, S \cup T \subseteq F(S)(T)$

$\Rightarrow F(S \cup T) \subseteq F(S)(T)$

or that $F(S \cup T) = F(S)(T)$

Cor. : $F(S \cup T) = F(T \cup S) = F(S)(T)$ follows clearly as $S \cup T = T \cup S$.

Note : If S is a finite subset $\{a_1, a_2, \ldots, a_n\}$ of K we write $F(S) = F(a_1, a_2, \ldots, a_n)$. The order in which a_i appear is immaterial in view of the above corollary as

$$F(a_1, a_2 \ldots, a_n) = F(\{a_1\}\{a_2, a_3, \ldots, a_n\})$$
$$= F(\{a_2, a_3, \ldots, a_n\} \cup \{a_1\})$$
$$= F(a_2, a_3, \ldots, a_n, a_1).$$

Also then,

$$F(a)(b) = F(a, b) = F(b, a) = F(b)(a)$$

Again, if $K = F(a)$, K is called *simple extension* of F and we say K is got by adjoining the element a to F.

Problem 1 : *Let* $\mathbf{Q}$ *be the field of rationals then show that* $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Solution : By definition

$$\sqrt{2}, \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

$$\Rightarrow \sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2}, \sqrt{3}) \quad \text{(closure)}$$

$$\Rightarrow \mathbf{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

Now $\quad \sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow (\sqrt{2} + \sqrt{3})^2 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Also $\quad 5 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$5 + 2\sqrt{2}\sqrt{3} - 5 = 2\sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Also $\quad 2 \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\therefore \quad 2 \times \frac{1}{2}\sqrt{2}\sqrt{3} = \sqrt{2}\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow (\sqrt{2} + \sqrt{3})\sqrt{2}\sqrt{3} = 2\sqrt{3} + 3\sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Also $\quad \sqrt{2} + \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow 3\sqrt{2} + 3\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\Rightarrow 3\sqrt{2} + 3\sqrt{3} - 2\sqrt{3} - 3\sqrt{2} = \sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

Also $\quad 2\sqrt{2} + 2\sqrt{3} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$

$$\Rightarrow 2\sqrt{3} + 3\sqrt{2} - 2\sqrt{2} - 2\sqrt{3} = \sqrt{2} \in \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\therefore \quad \mathbf{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

$$\therefore \quad \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$$

If K is an extension of F, then we know that K can be regarded as a vector space over F. In that case dimension of K over F is called *degree of K over F* and we denote it by $[K : F]$. Our next theorem is about the degree of extension fields. If $[K : F]$ is finite, we say K is finite extension of F.

Theorem 2 : *Let K be a finite extension of F and L, a finite extension of K. Then L is a finite extension of F and*

$$[L : F] = [L : K]\,[K : F].$$

Proof : Let $[L : K] = m$, $[K : F] = n$

Let $\{a_1, \ldots, a_m\}$ be a basis of L over K and $\{b_1, \ldots, b_n\}$ be a basis of K over F. We show that $\{a_i b_j \mid 1 \le i, j \le n\}$ is a basis of L over F.

$$a_i \in L,\ b_j \in K \Rightarrow b_j \in L. \ \therefore\ a_i b_j \in L \text{ for all } i, j$$

Let $$\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} a_i b_j = 0, \quad \alpha_{ij} \in F$$

Then $$\sum_{i=1}^{m}\sum_{j=1}^{n}(\alpha_{ij}b_j)\ a_i = 0,\quad \sum_{j=1}^{n}\alpha_{ij}b_j \in K$$

Since $\{a_1,\ldots,a_m\}$ are linearly independent over K,

$$\sum_{j=1}^{n}\alpha_{ij}b_j = 0 \text{ for all } i = 1,\ldots, m$$

Also $\{b_1,\ldots,b_n\}$ are linearly independent over F.

$$\alpha_{ij} = 0 \text{ for all } i = 1,\ldots,m \quad j = 1,\ldots,n$$

$\therefore$ $\{a_ib_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ is a linearly independent subset of L over F.

Let $a \in L$. Since $\{a_1,\ldots,a_m\}$ is a basis of L over K, $a = \alpha_1a_1+\ldots+\alpha_ma_m$, $\alpha_i \in K$

$\alpha_i \in K$ and $\{b_1,\ldots,b_n\}$ is a basis of K over F

$$\Rightarrow \alpha_i = \beta_{i1}b_1+\ldots+\beta_{in}b_n, \qquad \beta_{ij} \in F$$

$$\therefore \qquad a = \sum_{i=1}^{m}\alpha_ia_i = \sum_{i=1}^{m}(\beta_{i1}b_1\ldots\ldots+\beta_{in}b_n)a_i$$

$$= \sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}a_ib_j, \qquad \beta_{ij} \in F$$

$\therefore$ $\{a_ib_j \mid 1 \le i \le m,\ 1 \le j \le n\}$ spans L over F and so forms a basis of L over F.

$$\therefore \qquad [L:F] = mn = [L:K]\,[K:F]$$

Remark : If $[L:K]$ is infinite, then $[L:F]$ is also infinite because $[L:F] = r$ $\Rightarrow$ every subset of L having $r+1$ elements is linearly dependent over F. Since $[L:K]$ is infinite, $\exists$ $a_1,\ldots, a_{r+1} \in L$ which are linearly independent over K. Now $1 \in K$ and 1 is linearly independent over F as $1 \ne 0$. As in Theorem 2, $a_1.1,\ a_2.1,\ldots a_{r+1}.1$ are linearly independent over F. We find $a_1,\ldots,a_{r+1} \in L$ are linearly independent over F, a contradiction.

$\therefore$ $[L:F]$ is infinite. Similarly, $[K:F]$ is infinite.

Cor. 1 : If L is a finite extension of F and K is a subfield of L which contains F, then $[K:F]$ divides $[L:F]$.

Proof : By remark above $[K:F]$ is finite as $[L:F]$ = finite. Also $[L:K]$ is finite.

By Theorem 2,

$$[L:F] = [L:K]\,[K:F]$$

$$\therefore \qquad [K:F] \text{ divides } [L:F]$$

Cor. 2 : If K is an extension of F, then $K = F$ if and only if $[K:F] = 1$.

Proof : If $K = F$, then $[K:F] = [K:K] = 1$

If $[K:F] = 1$, let $\{a\}$ be a basis of K over F.

$\therefore \quad 1 \in K \Rightarrow 1 = \alpha a, \ \alpha \in F, \ \alpha \neq 0$ as $1 \neq 0$

$\Rightarrow a = \alpha^{-1} \in F$

Let $\quad b \in K \Rightarrow b = \beta a, \ \beta \in F, \ a \in F$

$\Rightarrow b \in F \Rightarrow K \subseteq F \Rightarrow K = F.$

Cor. 3 : If L is an extension of F and $[L:F]$ is a prime number p, then there is no field K s.t. $F \subset K \subset L$.

Proof : Suppose $\exists$ a field K s.t., $F \subset K \subset L$.

Then $\quad p = [L:F] = [L:K]\,[K:F]$ by Theorem 2

$\Rightarrow [L:K] = 1$ or $[K:F] = 1$

$\Rightarrow K = L$ or $K = F$ by Cor. 2,

a contradiction.

Hence the result.

Trivially then, if K is an extension of F of prime degree then for every $a \in K$, $F(a) = F$ or $F(a) = K$.

Problem 2 : *Let D be an integral domain. Let F be a field s.t. $F \subseteq D$. Suppose unity 1 of F is also unity of D. Then D can be regarded as a vector space over F. Show that D is a field if $[D:F]$ = finite.*

Solution : Let $[D:F] = r$. Let $\{a_1, \ldots, a_r\}$ be a basis of D over F.

Let $0 \neq a \in D$. We show that a is invertible. Consider $\{aa_1, \ldots, aa_r\}$.

Let $\quad \alpha_1(aa_1) + \ldots + \alpha_r(aa_r) = 0, \ \alpha_i \in F.$

Then $\quad a(\alpha_1 a_1 + \ldots + \alpha_r a_r) = 0$

$\Rightarrow \alpha_1 a_1 + \ldots + \alpha_r a_r = 0$, as $a \neq 0$ and D is an integral domain.

$\Rightarrow \alpha_i = 0$ for all $i = 1, \ldots, r$ as $\{a_1, \ldots, a_r\}$ is linearly independent over F.

$\Rightarrow \{aa_1, \ldots, aa_r\}$ is linearly independent over F.

But $[D:F] = r \Rightarrow \{aa_1, \ldots, aa_r\}$ is a basis of D over F.

$\therefore \quad 1 \in D \Rightarrow 1 = \beta_1 aa_1 + \ldots + \beta_r aa_r, \quad \beta_i \in F$

$= a(\beta_1 a_1 + \ldots \beta_r a_r)$

$= ab, \ b = \beta_1 a_1 + \ldots + \beta_r a_r \in D$

$\Rightarrow a$ is invertible.

$\Rightarrow D$ is a field.

Let K be an extension of F. Let $a \in K$.

Define $\quad F[a] = \{f(a) \mid f(x) \in F[x]\} \subseteq K.$

Then it can be shown that $F[a]$ is an integral domain. Let E be the quotient field of $F[a]$. Then $F[a] \subseteq E$ and E is the smallest field containing $F[a]$. Since $x \in F[x]$ as coefficient $1 \in F$, $a \in F[a]$ by definition of $F[a]$. Also $\alpha \in F[x]$, $\alpha \in F$ $\Rightarrow \alpha \in F[a] \Rightarrow F \subseteq F[a]$.

$\therefore\ a, F \subseteq F[a] \subseteq E$. But $F(a)$ is the smallest subfield of K containing F and a.

$\therefore\ F(a) \subseteq E$. Since $a \in F(a)$, $f(a) \in F(a)$ for all $f(x) \in F[x]$ as $F(a)$ is a field. Thus $F[a] \subseteq F(a) \subseteq E$.

But E is the smallest field containing $F[a]$.

$\therefore\ E \subseteq F(a)$. Hence $F(a) = E$.

So, we have explicitly determined the field $F(a)$. It is the field of quotients of $F[a]$.

We write, $F(a) = \left\{ \dfrac{f(a)}{g(a)} \mid g(a) \neq 0, f(x), g(x) \in F[x] \right\}$

In general, one can show that

$$F(a_1,....,a_n) = \left\{ \frac{f(a_1,.....,a_n)}{g(a_1,.....,a_n)} \mid g(a_1,.....,a_n) \neq 0,\ \begin{array}{r} f(x_1,.....,x_n) \in F[x] \\ g(x_1,.....,x_n) \in F[x] \end{array} \right\}$$

A natural question arises. When is $F[a] = F(a)$? To answer this, we first define what is an algebraic element. Let K be an extension of F. $a \in K$ is said to be *algebraic* over F if $\exists$ non-zero polynomial $f(x) \in F[x]$ s.t. $f(a) = 0$. Otherwise, it is called transcendental element. For example, $\sqrt{2} \in \mathbf{R}$ = real field, is algebraic over $\mathbf{Q}$ = rational field as $\sqrt{2}$ satisfies non zero polynomial $f(x) = x^2 - 2 \in \mathbf{Q}[x]$. However, $\pi, e \in \mathbf{R}$ are not algebraic over $\mathbf{Q}$. An extension K of F is called an *algebraic extension* if every $a \in K$ is algebraic over F.

If for some $a \in K$, a is not algebraic over F, then K is called transcendental extension of F. For example, $\mathbf{R}$ is transcendental extension of $\mathbf{Q}$. We shall see in the following theorem that finite extensions are algebraic. So, $\mathbf{C}$ = the field of complex numbers is algebraic over $\mathbf{R}$ as $[\mathbf{C} : \mathbf{R}] = 2$, $\{1, i\}$ being a basis of $\mathbf{C}$ over $\mathbf{R}$.

We sometimes use the notation K/F to express the fact that K is an extension of F. Similarly, K/F is algebraic would mean K is an algebraic extension of F.

Theorem 3 : *A finite extension is algebraic.*

Proof : Let K be a finite extension of F. Let $[K : F] = n$. Let $a \in K$. Then $1, a,.....,a^n$ are linearly dependent over F. Thus $\exists\ \alpha_0, \alpha_1,.....,\alpha_n \in F$ s.t. $\alpha_0 . 1 + \alpha_1 a +..... + \alpha_n a^n = 0$ for some $\alpha_i \neq 0$.

Let $f(x) = \alpha_0 + \alpha_1 x +.....+ \alpha_n x^n$. Then $f(x)$ is non zero polynomial in $F[x]$ as some $\alpha_i \neq 0$. Also $f(a) = \alpha_0 + \alpha_1 a +.....+ \alpha_n a^n = 0$

$\therefore\ a$ is algebraic over F.

$\therefore\ K$ is algebraic over F.

Note : Converse of Theorem 3 is not true. We shall give an example later to prove this.

Cor. : $a \in K$ is algebraic over F if $[F(a) : F]$ = finite.

Department of Mathematics
P380

Proof : By theorem 3, $F(a)$ is algebraic over F.

$\therefore$ $a \in F(a)$ is algebraic over F.

Converse of the above corollary is also true. But we'll prove it after the next theorem.

Theorem 4 : *Let $a \in K$ be algebraic over F. Then*

(*i*) $\exists$ *a unique monic irreducible polynomial* $p(x) \in F[x]$ *s.t.* $p(a) = 0$

(*ii*) *If* $\exists$ *non zero polynomial* $q(x) \in F[x]$ *s.t.* $q(a) = 0$, *then* $p(x)$ *divides* $q(x)$

(*iii*) $F(a) = F[a]$.

Proof : (*i*) Since a is algebraic over F, $\exists$ a non zero polynomial $f(x) \in F[x]$, s.t., $f(a) = 0$

Let $t(x)$ be the non zero polynomial of smallest degree over F s.t., $t(a) = 0$ and suppose

$$t(x) = a_0 + a_1x + \ldots + a_nx^n, \qquad a_i \in F$$

If $t(x)$ is not monic [By monic polynomial, we mean a polynomial in which coefficient of highest degree term is 1], then put

$$p(x) = a_n^{-1}a_0 + a_n^{-1}a_1x + \ldots + x^n = a_n^{-1}t(x)$$

Now deg $p(x) = n =$ deg $t(x)$ and $p(a) = 0$ and $p(x)$ is a monic polynomial. Thus $\exists$ a monic polynomial $p(x)$ of least degree s.t., $p(a) = 0$.

Suppose $p(x) = p_1(x)p_2(x)$, where p_1 and p_2 are polynomials with lesser degree than deg p.

Then $\qquad 0 = p(a) = p_1(a)p_2(a)$

$\Rightarrow$ $p_1(a) = 0$ or $p_2(a) = 0$ [as $F[a]$ is an I.D.]

But that would lead to a contradiction as $p(x)$ is such polynomial with least degree.

Hence $p(x)$ is irreducible polynomial.

To show uniqueness of $p(x)$, suppose $q(x)$ is any irreducible monic polynomial over F s.t., $q(a) = 0$. Since $F[x]$ is a Euclidean domain, $\exists$ $h(x)$ and $r(x)$ s.t., $q(x) = p(x)h(x) + r(x)$

where either $\qquad r(x) = 0$ or deg $r <$ deg p

Now $\qquad 0 = q(a) = p(a)h(a) + r(a)$

$\Rightarrow$ $r(a) = 0$ as $p(a) = 0$

Since $p(x)$ is of least degree s.t., $p(a) = 0$, we find deg $r <$ deg p is not possible. Hence $r(x) = 0$

i.e., $\qquad q(x) = p(x)h(x) \qquad \ldots (1)$

Since $q(x)$ is irreducible, $h(x)$ must be a constant polynomial, say $h(x) = c$

Then $\qquad q(x) = cp(x)$

Since $q(x)$ is monic, coefficient of highest degree term in L.H.S. is 1 and therefore it is 1 on R.H.S. also

R.H.S. being $cp(x) = ca_n^{-1}a_0 + ca_n^{-1}a_1x + \ldots + cx^n$ gives $c = 1$

Hence $q(x) = p(x)$, proving the uniqueness of $p(x)$

(*ii*) Follows by (1)

(*iii*) Define a mapping $\theta : F[x] \to F[a]$, s.t.,

$$\theta(f(x)) = f(a)$$

then θ is an onto homomorphism (verify !)

By fundamental theorem then

$$F[a] \cong \frac{F[x]}{\text{Ker}\,\theta}$$

Since $F[a]$ is an integral domain, so would be $\dfrac{F[x]}{\text{Ker}\,\theta}$ which implies $\text{Ker}\,\theta$ is a prime ideal. Since a is algebraic over K, $\exists$ a *non zero polynomial* $f(x) \in F[x]$ s.t. $f(a) = 0$.

$$\Rightarrow \theta(f(x)) = f(a) = 0$$

$$\Rightarrow f(x) \in \text{Ker}\,\theta \Rightarrow \text{Ker}\,\theta \neq (0)$$

i.e., $\text{Ker}\,\theta$ is a non zero prime ideal of $F[x]$ which being a Euclidean domain is a PID.

Thus $\text{Ker}\,\theta$ is a maximal ideal. (See Problem 3 on Page 292)

$\Rightarrow \dfrac{F[x]}{\text{Ker}\,\theta}$ is a field.

$\Rightarrow F[a]$ is a field.

But $F(a)$ is the smallest field containing F and a and thus $F(a) \subseteq F[a]$

But $\quad F[a] \subseteq F(a)$

Hence $\quad F(a) = F[a]$.

Note $F(a)$ is field of quotients of $F[a]$ and when $F(a)$ is itself a field, $F[a] = F(a)$.

Note : $p(x)$ determined in Theorem 4 is denoted by $p(x) = Irr\,(F, a)$. It is the unique monic irreducible polynomial over F satisfied by a. Since $p(x)$ is of least degree s.t. $p(a) = 0$, $p(x)$ is called the minimal polynomial for a.

where $F(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f, g \in K[x],\ g \neq 0 \right\}$.

Remark : If $a \in K$ is transcendental over F than $F(x) \cong F(a)$.

Proof : Define $\varphi : F(x) \to F(a)$ s.t.,

$$\varphi\left(\frac{f(x)}{g(x)}\right) = \frac{f(a)}{g(a)},$$

Then φ is well defined onto homomorphisim.

Also $$\varphi\left(\frac{f(x)}{g(x)}\right) = 0$$

$$\Rightarrow \frac{f(a)}{g(a)} = 0$$

$$\Rightarrow f(a) = 0$$

$\Rightarrow f(x) = 0$, for otherwise a would be algebraic over F.

$$\Rightarrow \frac{f(x)}{g(x)} = 0$$

$\Rightarrow \varphi$ is 1-1.

Hence $F(x) \cong F(a)$.

Cor. 1 : Let $a \in K$ be algebraic over F. Then $[F(a) : F] = \deg Irr\,(F, a) =$ finite and so $F(a)$ is an algebraic extension of F.

Proof : Let $p(x) = Irr\,(F, a)$. Let $n = \deg p(x)$.

Let $0 \neq f(a) \in F[a] = F(a)$. Then $f(x) \in F[x]$.

Now for $f(x), p(x) \in F[x]$, $\exists\, q(x), r(x) \in F[x]$ s.t., $f(x) = p(x)\,q(x) + r(x)$ where either $r(x) = 0$ or $\deg r < \deg p$.

But $r(x) = 0 \Rightarrow f(x) = p(x)\,q(x)$

$\Rightarrow f(a) = p(a)\,q(a) = 0$ as $p(a) = 0$

which is not possible as $f(a) \neq 0$

Thus $r(x) \neq 0$. Hence $\deg r < \deg p$.

Suppose $r(x) = \alpha_0 + \alpha_1 x + ... + \alpha_m x^m$ where $m < n$, $\alpha_i \in F$

Again as $f(a) = p(a)\,q(a) + r(a)$ and $p(a) = 0$

we find $f(a) = r(a)$

Thus $f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_m a^m$

$= \beta_0 + \beta_1 a + \beta_2 a^2 + ... + \beta_{n-1} a^{n-1}$ (by suitably choosing $\beta_i \in F$)

i.e., $\{1, a, a^2, ..., a^{n-1}\}$ spans $F[a] = F(a)$ over F.

We show these are *L.I.*

Suppose these are *L.D.*, then $\exists\, \gamma_i$, not all zero, s.t.,

$$\gamma_0 + \gamma_1 a + \gamma_2 a^2 + ... + \gamma_{n-1} a^n = 0$$

$\Rightarrow t(x) = \gamma_0 + \gamma_1 x + ... + \gamma_{n-1} x^{n-1}$ is non zero polynomial (some $\gamma_i \neq 0$) with $t(a) = 0$.

A contradiction to the fact that $p(x)$ is such polynomial with least degree. Hence $1, a, ..., a^{n-1}$ are *L.I.* and thus form a basis of $F(a)$.

Hence $[F(a) : F] = n$.

Remark : Using cor. on page 501 we conclude $a \in K$ is algebraic over F iff $[F(a) : F]$ = finite.

Definition : An element $a \in K$ is said to be *algebraic of degree n* over F if it satisfies a polynomial of degree n over F and does not satisfy any polynomial of lesser degree (than n).

Thus a is algebraic of degree n over F if deg $Irr(F, a) = n$. Also in that case, $[F(a) : F] = n$ and $\{1, a, a^2, \ldots, a^{n-1}\}$ is a basis of $F(a)$ over F.

Cor. 2 : If $a_1, \ldots, a_n \in K$ are algebraic over F then $F(a_1, \ldots, a_n)$ is finite extension of F and so is algebraic over F.

Proof : We prove the result by induction on n. If $n = 1$, result follows from Cor. 1. Assume it to be true for naturals less than n. Let $a_1, \ldots, a_n \in K$ be algebraic over F. Now a_n is algebraic over $F \Rightarrow a_n$ is algebraic over $F(a_1, \ldots, a_{n-1})$.

$\therefore$ By Cor. 1, $[F(a_1, \ldots, a_{n-1})(a_n) : F(a_1, \ldots, a_{n-1})]$ is finite. By induction hypothesis, $[F(a_1, \ldots, a_{n-1}) : F]$ is finite.

$\therefore$ $[F(a_1, \ldots, a_n) : F] = [F(a_1, \ldots, a_n) : F(a_1, \ldots, a_{n-1})]\,[F(a_1, \ldots, a_{n-1}) : F] =$ finite

$\therefore$ result is true for n also.

By induction, result is true for all $n \geq 1$.

Cor. 3 : If $a, b \in K$ are algebraic over F, then $a \pm b$, ab, ab^{-1} (if $b \neq 0$) are algebraic over F. In other words, the elements of K which are algebraic over F from a subfield of K (and this subfield is called the *algebraic closure* of F over K).

Proof : By Cor. 2, $F(a, b)$ is algebraic over F.

$\therefore$ $a \pm b$, ab, $ab^{-1} \in F(a, b)$ are algebraic over F.

Remarks (1) : If K is an extension field of a field F and $S \subseteq K$, then

$$F(S) = \left\{ \frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} \;\middle|\; \begin{array}{l} f, g \in F[x_1, \ldots, x_n] \\ g(u_1, \ldots, u_n) \neq 0, n \in \mathbf{N} \\ u_1, \ldots, u_n \in S \end{array} \right\}$$

Proof : Let L denote the R.H.S. We first show that L is a subfield of K.

Let $$\frac{f(u_1, \ldots, u_m)}{g(u_1, \ldots, u_m)} \in L, \quad \frac{f_1(v_1, \ldots, v_n)}{g_1(v_1, \ldots, v_n)} \in L$$

Let $$Y = \frac{f(u_1, \ldots, u_m)}{g(u_1, \ldots, u_m)} - \frac{f_1(v_1, \ldots, v_n)}{g_1(v_1, \ldots, v_n)}$$

$$= \frac{f(u_1, \ldots, u_m)\, g_1(v_1, \ldots, v_n) - f_1(v_1, \ldots, v_n)\, g(u_1, \ldots, u_n)}{g(u_1, \ldots, u_m)\, g_1(v_1, \ldots, v_n)}$$

Define

$$h(x_1, \ldots, x_{m+n})$$
$$= f(x_1, \ldots, x_m)\, g_1(x_{m+1}, \ldots, x_{m+n}) - g(x_1, \ldots, x_m)\, f_1(x_{m+1}, \ldots, x_{m+n})$$
$$r(x_1, \ldots, x_{m+n}) = g(x_1, \ldots, x_m)\, g_1(x_{m+1}, \ldots, x_{m+n})$$

Then

$$Y = \frac{h(u_1, \ldots\ldots, u_m, v_1, \ldots\ldots, v_n)}{r(u_1, \ldots\ldots, u_m, v_1, \ldots\ldots, v_n)} \in L$$

Suppose $$\frac{f_1(v_1, \ldots\ldots, v_n)}{g_1(v_1, \ldots\ldots, v_n)} \neq 0$$

Let $$Z = \frac{f(u_1, \ldots\ldots, u_m)}{g(u_1, \ldots\ldots, u_m)} \cdot \frac{g_1(v_1, \ldots\ldots, v_n)}{f_1(v_1, \ldots\ldots, v_n)}$$

Define $$h_1(x_1, \ldots, x_{m+n}) = f(x_1, \ldots\ldots, x_m)\ g_1(x_{m+1}, \ldots\ldots, x_{m+n});$$
$$r_1(x_1, \ldots, x_{m+n}) = g(x_1, \ldots\ldots, x_m)\ f_1(x_{m+1}, \ldots\ldots, x_{m+n}).$$

Then

$$Z = \frac{h_1(u_1, \ldots\ldots, u_m, v_1, \ldots\ldots, v_n)}{r_1(u_1, \ldots\ldots, u_m, v_1, \ldots\ldots, v_n)} \in L$$

So, L is subfield of K.

Let $u_1 \in S$. Define $f(x) = x$, $g(x) = 1$.

Then $$f(u_1) = u_1,\ g(u_1) = 1$$

$$\Rightarrow \frac{f(u_1)}{g(u_1)} \in L \Rightarrow \frac{u_1}{1} \in L \Rightarrow u_1 \in L$$

So, $S \subseteq L$.

Let $\alpha \in F$. Define $f(x) = \alpha$, $g(x) = 1$.

Let $u \in S$. Then $f(u) = \alpha$, $g(u) = 1$.

Now $$\frac{f(u)}{g(u)} \in L \Rightarrow \frac{\alpha}{1} = \alpha \in L.$$

So, $F \subseteq L$.

But $F(S)$ is the smallest field containing F and S, $F(S) \subseteq L$.

Let $Y \in L$. Then $Y = \dfrac{f(u_1, \ldots\ldots, u_n)}{g(u_1, \ldots\ldots, u_n)}$, $u_i \in S$.

Since $u_i \in S$ and coefficients in f, g belong to F, $f(u_1, \ldots, u_n) \in F(S)$ and $g(u_1, \ldots\ldots, u_n) \in F(S)$.

So, $Y \in F(S)$.

then $L \subseteq F(S)$.

Hence $F(S) = L$.

(2) If K is an extension field of F, and K is generated by algebraic elements (i.e. $K = F(S)$, where $S \subseteq K$ is a set of algebraic elements over K), then K is an algebraic extension of F.

Proof : Let $C \in K$, then $C = \dfrac{f(u_1, \ldots\ldots, u_n)}{g(u_1, \ldots\ldots, u_n)}$, $u_i \in S$.

where $f(x_1, \ldots\ldots, x_n)$, $g(x_1, \ldots\ldots, x_n) \in F\ [x_1, \ldots\ldots, x_n]$.

Clearly $C \in F(u_1, \ldots\ldots, u_n)$. But $u_1, \ldots, u_n$ are algebraic over $F \Rightarrow F(u_i, \ldots, u_n)$ is an algebraic extension of $F \Rightarrow C$ is algebraic over F.

Hence K/F is algebraic.

Theorem 5 : *If L is an algebraic extension of K and K, an algebraic extension of F, then L is an algebraic extension of F.*

Proof : Let $a \in L$. Since L is algebraic over K, a is algebraic over K. $\therefore\ \exists\, 0 \neq f(x) \in K[x]$ s.t. $f(a) = 0$. Let $f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$, $\alpha_i \in K$.

Since K is algebraic over F, each $\alpha_i \in K$ is algebraic over F. By Cor. 2. Theorem 4, $[F(\alpha_0, \alpha_1, \ldots, \alpha_n) : F]$ = finite.

Let $$M = F(\alpha_0, \alpha_1, \ldots\ldots, \alpha_n)$$

Then $[M : F]$ is finite and so M is algebraic over F. Clearly, each $\alpha_i \in M$. Thus, $f(x) \in M[x]$.

i.e., a is algebraic over M.

By Cor. 1, $M(a)$ is finite extension of M.

$\Rightarrow\ [M(a) : F] = [M(a) : M]\,[M : F]$ = finite.

$\Rightarrow\ M(a)$ is algebraic over F.

$\Rightarrow\ a \in M(a)$ is algebraic over F.

Since a is an arbitrary element of L, L is an algebraic extension of F.

Definition : A complex number is said to be an *algebraic number* if it is algebraic over the field of rational numbers.

An algebraic number is said to be an *algebraic integer* if it satisfies an equation of the form $x^n + \alpha_1 x^{n-1} + \ldots\ldots + \alpha_n$ where $\alpha_1, \ldots\ldots, \alpha_n$ are integers (i.e. a monic polynomial over integers.)

Problem 3 : *If a is any algebraic number, prove that $\exists$ a + ve integer n such that na is an algebraic integer.*

Solution : Since a is an algebraic number, a is algebraic over the field of rationals. Thus $\exists$ a non-zero monic polynomial $f(x) \in \mathbf{Q}[x]$ s.t. $f(a) = 0$, where $\mathbf{Q}$ = field of rationals.

Let $$f(x) = x^m + \alpha_1 x^{m-1} + \ldots\ldots + \alpha_{m-1} x + \alpha_m, \qquad \alpha_i \in \mathbf{Q}$$

Let $\alpha_i = \dfrac{p_i}{q_i}$ where p_i, q_i are integers, $q_i > 0$

$$\therefore \qquad a^m + \frac{p_1}{q_1} a^{m-1} + \ldots\ldots + \frac{p_{m-1}}{q_{m-1}} a + \frac{p_m}{q_m} = 0$$

Let $n = q_1 \ldots\ldots q_m$. Then n is a + ve integer

and $na^m + p_1q_2.....q_m a^{m-1} + ... + p_m q_1 .....q_{m-1} = 0$

$\Rightarrow \quad n^m a^m + p_1 q_2 .....q_m a^{m-1} n^{m-1} + ... + p_m q_1 ....q_{m-1} n^{m-1} = 0$

$\Rightarrow$ na satisfies the polynomial

$$x^m + p_1 q_2 ....q_m x^{m-1} + ... + p_m q_1 ....q_{m-1} \quad n^{m-1} = 0$$

where coefficients are integers.

$\therefore$ na is an algebraic integer.

Probelm 4 : *If the rational number r is also an algebraic integer, prove that r must be an ordinary integer.*

Solution : Let $r = \dfrac{p}{q}$, where $q > 0$, $(p, q) = 1$

Since r is an algebraic integer

$$r^m + \alpha_1 r^{m-1} + ... + \alpha_{m-1} r + \alpha_m = 0$$

α_is are integers.

$$\therefore \qquad \frac{p^m}{q^m} + \alpha_1 \frac{p^{m-1}}{q^{m-1}} + ... + \alpha_{m-1} \frac{p}{q} + \alpha_m = 0$$

$\therefore$ $p^m + q \times$ an integer $= 0$

$\Rightarrow$ q divides p^m. But $(p, q) = 1$.

$\therefore \qquad q \mid 1 \Rightarrow q = 1 \Rightarrow r = p =$ integer.

Probelm 5 : *Proves that $\sin m^o$ is an algebraic number for every integer m.*

Solution : Now $e^{\pi m i/180} = \cos \dfrac{\pi m}{180} + i \sin \dfrac{\pi m}{180}$

$$\therefore \qquad \left(e^{\pi m i/180}\right)^{180} = \cos m\pi + i \sin m\pi = \pm 1$$

$\therefore$ $e^{\pi m i/180}$ is a root of $x^{180} = \pm 1$

$\therefore$ $e^{\pi m i/180}$ is an algebraic number for all integers m.

$\therefore$ $\cos \dfrac{m\pi}{180} + i \sin \dfrac{m\pi}{180}$ is an algebraic number.

Also $\cos \dfrac{m\pi}{180} - i \sin \dfrac{m\pi}{180}$ is algebraic number (by putting m as $-m$).

$\therefore$ $2 \cos \dfrac{m\pi}{180}$ is algebraic number for all integers m.

$\therefore$ $\cos \dfrac{m\pi}{180}$ is algebraic number for all integers m

$\therefore$ $\cos m^\circ$ is algebraic number for all integers m.

Also $\cos \frac{m\pi}{180}$ and $\cos \frac{m\pi}{180} + i \sin \frac{m\pi}{180}$ is algebraic number $\Rightarrow i \sin \frac{m\pi}{180}$ is algebraic number $\Rightarrow \sin \frac{m\pi}{180}$ is algebraic number as i is also algebraic number $\Rightarrow \sin m^\circ$ is algebraic number.

Problem 6 : *Find a basis of* $\mathbf{Q}(\sqrt{3},\sqrt{5})$ *over* $\mathbf{Q}$.

Solution : We have

$$\begin{aligned}
[\mathbf{Q}(\sqrt{3}, \sqrt{5}) : \mathbf{Q}] &= [\mathbf{Q}(\sqrt{3})(\sqrt{5}) : \mathbf{Q}] \\
&= [\mathbf{Q}(\sqrt{3})(\sqrt{5}) : \mathbf{Q}(\sqrt{3})]\ [\mathbf{Q}\sqrt{3} : \mathbf{Q}] \\
&= [L(\sqrt{5}) : L]\,[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \text{ where } L = \mathbf{Q}(\sqrt{3}) \\
&= \deg Irr\,(L, \sqrt{5}) \times \deg Irr\,(\mathbf{Q}, \sqrt{3}) \\
&= \deg\,(x^2 - 5) \times \deg\,(x^2 - 3) \\
&= 2 \times 2 = 4.
\end{aligned}$$

Thus basis has 4 elements.

Also if $[(F(a) : F)] = n$ then $1, a, a^2,\ldots,a^{n-1}$ is basis of $F(a)$ over F, and thus

Basis of $L(\sqrt{5})$ over L is $\{1, \sqrt{5}\}$

Basis of $\mathbf{Q}(\sqrt{3})$ over $\mathbf{Q}$ is $\{1, \sqrt{3}\}$

Thus basis of $[L(\sqrt{5}) : L]\,[\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = [(\mathbf{Q}(\sqrt{3}, \sqrt{5}) : \mathbf{Q}]$

is $1.1,\ 1.\sqrt{3},\ 1.\sqrt{5},\ \sqrt{3}\sqrt{5}$ [see theorem 2 page 498]

i.e. $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$.

Problem 7 : *Find the minimal polynomial for* $\sqrt{2} + \sqrt{3}$ *and use it to show that* $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$. *Find a basis for* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Solution : Now $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$;

$$(\sqrt{2} + \sqrt{3})^4 = 49 + 20\sqrt{6}.$$

So,

$$(\sqrt{2} + \sqrt{3})^4 - 10\,(\sqrt{2} + \sqrt{3})^2 + 1 = 0$$

Therefore, $a = \sqrt{2} + \sqrt{3}$ satisfies

$f(x) = x^4 - 10x^2 + 1$ over $\mathbf{Q}$.

Let $\quad p(x) = Irr\,(\mathbf{Q}, a)$

Then $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$ are also roots of $p(x)$. So, degree of $p(x)$ is at least 4. But $f(a) = 0$ and $f(x) \in \mathbf{Q}[x]$

$$\Rightarrow p(x) \text{ divides } f(x)$$

$$\Rightarrow p(x) = f(x).$$

So, $f(x)$ is the minimal polynomial for $\sqrt{2} + \sqrt{3}$.

Therefore, $\quad [\mathbf{Q}(\sqrt{2} + \sqrt{3})] : \mathbf{Q}] = 4$

Also, $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = \deg \; Irr\,(\mathbf{Q}, \sqrt{2})$

$= \deg\,(x^2 - 2) = 2$.

Now $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

Consider $g(x) = x^2 - 3 \in \mathbf{Q}(\sqrt{2})\,[x]$.

Then $g(\sqrt{3}) = 0$

$\therefore$ $\deg \; Irr\,(\mathbf{Q}(\sqrt{2}), \sqrt{3}) \leq \deg g(x) = 2$

$\Rightarrow$ $[(\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})] \leq 2$.

So, $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] \leq 4$.

Clearly, $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbf{Q}(\sqrt{2}, \sqrt{3})$.

$\therefore$ $[\mathbf{Q}(\sqrt{2}, \sqrt{3})] : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2} + \sqrt{3})] \times [\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}]$

$\Rightarrow$ $[\mathbf{Q}(\sqrt{2}, \sqrt{3})] : \mathbf{Q}(\sqrt{2} + \sqrt{3})] = 1$

$\Rightarrow$ $\mathbf{Q}(\sqrt{2},\sqrt{3}) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$

Since $[\mathbf{Q}(\sqrt{2} + \sqrt{3}) : \mathbf{Q}] = 4$

$\{1, \sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3\}$ is a basis for $\mathbf{Q}(\sqrt{2} + \sqrt{3}) = \mathbf{Q}(\sqrt{2},\sqrt{3})$ over $\mathbf{Q}$.

Problem 8 : *Let $F(x)$ be the field of rational functions in an indeterminate x. Show that every element of $F(x)$ which is not in F is transcendental over F.*

Solution : Let $0 \neq \dfrac{f}{g} \in F(x)$, $\dfrac{f}{g} \notin F$, $(f, g) = 1$.

Suppose $\dfrac{f}{g}$ is not transcendental over F.

Then $\dfrac{f}{g}$ is algebraic over F.

So, $F(\dfrac{f}{g}) = F[\dfrac{f}{g}]$.

Consider $\dfrac{g}{f} \in F[\dfrac{f}{g}] = F(\dfrac{f}{g})$.

(Note $0 \neq \dfrac{f}{g} \in F[\dfrac{f}{g}]$ and $F[\dfrac{f}{g}]$ is a field, $\dfrac{g}{f} \in F(\dfrac{f}{g}) = F[\dfrac{f}{g}]$)

Therefore, $\dfrac{g}{f} = \alpha_0 + \alpha_1 (\dfrac{f}{g}) + \ldots\ldots + \alpha_n \; (\dfrac{f}{g})^n$, $\alpha_i \in F$.

So, $g^{n+1} = (\alpha_0 g^n + \alpha_1 f g^{n-1} + \ldots\ldots \alpha_n f^n) \; f$.

Since $(f, g) = 1$, $f \mid g^{n+1} \Rightarrow f \mid g \Rightarrow f =$ unit.

$\Rightarrow g =$ unit $\Rightarrow \dfrac{f}{g} =$ unit $\in F$, a contradiction.

So, $\dfrac{f}{g}$ is transcendental over F.

Exercises

1. If $a, b \in K$ are algebraic over F of degrees m and n respectively and if m and n are relatively prime, prove that $F(a, b)$ is of degree mn over F.
2. If $a \in K$ is algebraic over F of odd degree. Show that $F(a) = F(a^2)$.
3. Show that degree of $\sqrt{2} + \sqrt{3}$ over $\mathbf{Q}$ is 4 and degree of $\sqrt{2} + \sqrt{5}$ over $\mathbf{Q}$ is 6.
4. If a is an algebraic integer and m is an ordinary integer, prove
   (*i*) $a + m$ is an algebraic integer.
   (*ii*) ma is an algebraic integer.
5. Prove that sum and product of two algebraic integers is an algebraic integer.
6. Find a basis of $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$. $[1, \sqrt{2}, \sqrt{3}, \sqrt{6}]$
7. Let K be an extension of F. Suppose E_1, E_2 are contained in K and are extensions of F. If $[E_1 : F]$ and $[E_2 : F]$ are primes, show that either $E_1 \cap E_2 = F$ or $E_1 = E_2$.
8. If K is an extension of F, $c \in K$, $a, b \in F$, $a \neq 0$ then show that $F(c) = F(ac + b)$.
9. Suppose that a field F has finite number of elements q. Show that
   (*i*) $q = p^n$ for some prime p and integer n.
   (*ii*) $a^q = a$ for all $a \in F$.
   (*iii*) if $b \in K$ is algebraic over F, then $b^{q^m} = b$ for some $m > 0$.

Roots of Polynomials

Let F be a field and $f(x) \in F[x]$. We ask whether there exists an extension K of F containing a root (Definition on page 336) of $f(x)$? What is the degree of such an extension? How many roots of $f(x)$ can the extension K of F have? The answers to the above queries are provided by the following results.

Theorem 6 : (Remainder theorem). *If $p(x) \in F[x]$ and K is an extension of F, then for any element $a \in K$, $p(x) = (x - a)\, q(x) + p(a)$ where $q(x) \in K[x]$ and $\deg q(x) = \deg p(x) - 1$.*

Proof : Now $p(x) \in F[x] \Rightarrow p(x) \in K[x]$. Also $a \in K \Rightarrow x - a \in K[x]$. By the division algorithm for polynomials in $K[x]$,

$p(x) = (x - a)\, q(x)$ where $q(x) \in K[x]$ and $r(x) \in K[x]$ s.t. $r(x) = 0$ or $\deg r(x) < \deg(x - a) = 1$. Thus $r(x)$ is either 0 or a constant. Let $r(x) = c \in K$.

Now
$$p(x) = (x - a)\, q(x) + c$$
$$\Rightarrow p(a) = c$$
$$\Rightarrow p(x) = (x - a)\, q(x) + p(a) \text{ (where } p(a) \text{ could be zero).}$$

Clearly, $\deg q(x) = \deg p(x) - 1$

Cor. : If $a \in K$ is a root of $p(x) \in F[x]$ where $F \subseteq K$, then $(x-a) \mid p(x)$ in $K[x]$ and conversely.

Proof : By above theorem,

$$p(x) = (x-a)\, q(x) + r, \quad r \in K$$
$$\Rightarrow \; 0 = p(a) = r$$
$$\Rightarrow \; p(x) = (x-a)\, q(x)$$

$(x-a) \mid p(x)$ in $K[x]$ as $q(x) \in K[x]$.

Conversely, if $(x-a) \mid p(x)$ in $K[x]$ then $p(x) = g(x)\,(x-a)$ for some $g(x) \in K[x]$. Thus $p(a) = (a-a)\, g(a) = 0$ and so a is a root of $p(x)$.

Definition : An element $a \in K$ is called a root of $p(x) \in F[x]$ of *multiplicity* m if $(x-a)^m \mid p(x)$ and $(x-a)^{m+1} \nmid p(x)$ in $K[x]$.

If a is a root of $p(x)$ of multiplicity 1 then it is called a *simple root* of $p(x)$. It is called a *multiple root* otherwise (when $m > 1$).

Remark : If a is a root (of multiplicity m) of $p(x)$ then $(x-a)^m \mid p(x)$ $\Rightarrow p(x) = (x-\alpha)^m\, g(x)$, for some $g(x)$.

Now if a is also a root of $g(x)$ then $(x-a) \mid g(x)$

$$\Rightarrow \; g(x) = (x-a)\, h(x)$$
$$\Rightarrow \; f(x) = (x-a)^{m+1}\, h(x) \Rightarrow (x-a)^{m+1} \mid f(x) \text{ a contradiction.}$$

Thus $g(a) \neq 0$.

Indeed, if a is a simple root of $p(x)$, then $p(x) = (x-a)\, g(x)$ where $g(a) \neq 0$.

Theorem 7 : *A polynomial of degree n over a field can have at most n roots in any extension field. A root of multiplicity m to be counted m times.*

Proof : Let $p(x) \in F[x]$, degree $p(x) = n$. We prove the result by induction on n. Let K be an extension of F. Let $n = 1$. Then $p(x)$ is of the form $ax + b$, $a, b \in F$, $a \neq 0$. Then $p(\alpha) = 0 \Rightarrow \alpha = -ba^{-1}$. So, $p(x)$ has unique root $-ba^{-1} \in F$. Therefore K also has only one root of $p(x)$. So, result is true for $n = 1$. Assume it to be true for naturals less than n. Let $\deg p(x) = n$. If $p(x)$ has no root in K, then result is true. Let α be a root of $p(x)$ in K. Let α be of multiplicity m. Then by definition, $(x-\alpha)^m \mid p(x)$.

$\therefore p(x) = (x-\alpha)^m\, q(x)$. Since $(x-\alpha)^{m+1} \nmid p(x)$, $(x-\alpha) \nmid q(x)$. So, α is not a root of $q(x)$. If $\beta \neq \alpha$ is a root of $p(x)$ in K, then $0 = (\beta-\alpha)^m\, q(\beta) \Rightarrow q(\beta) = 0 \Rightarrow \beta$ is a root of $q(x)$. So, any root of $p(x)$ different from α in K is also a root of $q(x)$. But $\deg q(x) = n - m < n$. By induction hypothesis K has at most $n-m$ roots of $q(x)$. So, K has at most $(n-m) + m = n$ roots of $p(x)$. Therefore, result is true for n. By induction result is true for all $n \geq 1$.

Remark : It must be noted that above lemma may not hold if we consider a polynomial over a ring which is not a field.

For example, $f(x) = x^2 + 1$ has at least 6 roots namely $\pm i$, $\pm j$, $\pm k$ in the ring of real quaternions which is not a field.

We now show that a non–constant polynomial over a field has a root in some field extension.

Theorem 8 : *Let $p(x)$ be a non constant irreducible polynomial of degree n in $F[x]$. Then there exists an extension K of F s.t. $[K:F]=n$ and K has a root of $p(x)$.*

Proof : Since $p(x)$ is irreducible polynomial in $f(x)$, it will be an irreducible element (See Remark on page 338) and thus the ideal $M = < p(x) >$ is maximal ideal of $F[x]$ and $\frac{F[x]}{M}$ will be a field. Take $K = \frac{F[x]}{M}$.

Define $\theta : F \to K$, s.t.,

$$\theta(\alpha) = \alpha + M$$

Then θ is easily seen to be a homomorphism.

Again, $\alpha \in \operatorname{Ker}\theta \Rightarrow \theta(\alpha) = 0 + M$

$$\Rightarrow \alpha + M = M \Rightarrow \alpha \in M = < p(x) >$$

and so $\alpha = p(x)\ q(x)$ for some $q(x) \in F[x]$

Since p is irreducible (with deg ≥ 1) and $\alpha \in F$ is either zero or a constant polynomial, we observe that the above relation holds only when $\alpha = 0$

i.e., $\operatorname{Ker}\theta = \{0\}$ or that θ is 1–1.

Hence $F \cong \theta(F)$.

Define now $\psi : F[x] \to K$, s.t.,

$$\psi(f(x)) = f(x) + M \qquad (K = \frac{F[x]}{M})$$

Then ψ is the natural (onto) homomorphism.

Again as $\psi(\alpha) = \alpha + M = \theta(\alpha)\ \ \forall\, \alpha \in F$, we notice θ is restriction of ψ over F.

Now $x = 0 + 1 \,.\, x + 0 \,.\, x^2 + \ldots + \in F[x]$

Let $a = \psi(x) = x + M = x + < p(x) >, \qquad x \in F[x]$ ... (1)

We claim, a is a root of $p(x)$ in K.

Suppose $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n, \qquad \alpha_i \in F$

Then $\psi(p(x)) = \psi(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots \alpha_n x^n)$

$$= \psi(\alpha_0) + \psi(\alpha_1)\,\psi(x) + \psi(\alpha_2)\,\psi(x^2) + \ldots + \psi(\alpha_n)\,\psi(x^n)$$

Also $\psi(p(x)) = p(x) + M = p(x) + < p(x) > = M =$ Zero of K

Thus

Zero of $K = \psi(\alpha_0) + \psi(\alpha_1)\ \ \psi(x) + \ldots + \psi(\alpha_n)\ \ \psi(x^n)$

$$= \theta(\alpha_0) + \theta(\alpha_1)\ \ \psi(x) + \ldots + \theta(\alpha_m)\ \ \psi(x^n)$$

Since $F \cong \theta(F)$, F is isomorphic to a subfield of K and we can think of K as containing F by identifying $\alpha \in F$ with $\theta(\alpha)$ and vice versa.

We thus get

Zero of $K = \alpha_0 + \alpha_1 \psi(x) + \alpha_2 \psi(x^2) + \ldots + \alpha_n\,(\psi(x^n)$

$$= \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n \qquad \text{from (1)}$$

$$= p(a)$$

Hence a is a root of $p(x)$ in K.

We show now $\{1+M,\ x+M,\ x^2+M.....,\ x^{n-1}+M\}$ forms a basis of K over F.

Let $\beta_0(1+M)+\beta_1(x+M)\ +.....+\ \beta_{n-1}(x^{n-1}+M)=M$ (Zero of K)

As above then $\beta_i=\theta(\beta_i)=\beta_i+M$ and thus

$(\beta_0+M)\,(1+M)+(\beta_1+M)\,(x+M)+.....+(\beta_{n-1}+M)\,(x^{n-1}+M)=M$

or $\qquad (\beta_0+\beta_1x+\beta_2x^2+.....+\beta_{n-1}\ x^{n-1})+M=M$

or $\qquad q(x)+M=M$ where $q(x)=\beta_0+\beta_1x+.....+\beta_{n-1}x^{n-1}$

or $\qquad q(x)\in M=<p(x)>$

$\Rightarrow\ q(x)=p(x)\,h(x)$

$\Rightarrow\ \deg q=\deg p+\deg h$

$\Rightarrow\ \deg q\geq\deg p$ or that $n-1\geq n$, which leads us to a contradiction, unless $q(x)=0$

i.e., $\beta_i=0\ \ \forall i$

and hence $1+M,\ x+M,.....,x^{n-1}+M$ are linearly independent.

Let now $f(x)+M\in K$ be any member.

Since $f(x),\ p(x)\in F[x],\ \exists\ t(x), r(x)$ s.t.,

$$f(x)=p(x)\,t(x)+r(x),\ \text{ where either } r(x)=0 \text{ or } \deg r(x)<\deg p(x)$$

$$\Rightarrow\ f+M=(pt+r)+M=\ (p+M)(t+M)+(r+M)$$

$$=\ M(t+M)+(r+M)=M+(r+M)=r+M$$

Suppose $r(x)=r_0+r_1x+r_2x^2+.....+r_{n-1}x^{n-1}$ where, of course, some or all r_i could be zero as either $r(x)=0$ or $\deg r(x)<\deg p(x)$

Thus $\qquad f+M=\ r+M=(r_0+r_1x+.....+r_{n-1}\ x^{n-1})+M$

$$=\ (r_0+M)+(r_1x+M)+.....+(r_{n-1}x^{n-1}+M)$$

$$=(r_0+M)\,(1+M)+(r_1+M)\,(x+M)+.....+(r_{n-1}M_1)\ (x^{n-1}+M)$$

$$=\ r_0(1+M)+r_1\ \ (x+M)+.....+r_{n-1}\ \ (x^{n-1}+M)$$

[because of $F\cong\theta(F)$]

or that $1+M,\ x+M,.....,\ x^{n-1}+M$ span K

Hence $[K:F]=n$.

Cor. : If $f(x)\in F[x]$ is of degree n, then there is a finite extension K of F in which $f(x)$ has a root. Also, $[K:F]\leq\deg\ f(x)$.

Proof : If $f(x)$ is irreducible polynomial then result follows by above theorem. If not then let $f(x)=p(x)\,q(x)$, where $p(x)$ is irreducible. By above thoerem $\exists$ an extension K of F in which $p(x)$ has a root.

$\therefore\ p(\alpha)=0$ for some $\alpha\in K$. So, $f(\alpha)=p(\alpha)\,q(\alpha)=0\ \Rightarrow\ \alpha$ is a root of $f(x)$. Also $[K:F]=\deg p(x)\leq\deg\ f(x)$.

Remark : The construction of an extension of K in which a given polynomial f has a root is not, in general, unique. Let $f=x^4-4$ over $\mathbf{Q}$. Then $f=(x^2-2)\,(x^2+2)$ Then $\exists$ two non-isomorphic extensions $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2}i)$ of containing a root of f.

For if, σ is an isomorphism from $\mathbf{Q}(\sqrt{2})$ to $\mathbf{Q}(\sqrt{2}i)$, then $\sigma(1) = 1 \Rightarrow \sigma(a) = a$ for all $a \in \mathbf{Q}$. So $(\sigma(\sqrt{2}))^2 = \sigma(\sqrt{2})^2 = \sigma(2) = 2$

$$\Rightarrow \sigma(\sqrt{2}) \text{ is a zero of } x^2 - 2$$
$$\Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$$
$$\Rightarrow Im\ \sigma = \mathbf{Q}(\sqrt{2})$$
$$\Rightarrow \mathbf{Q}(\sqrt{2}\ i) = \mathbf{Q}(\sqrt{2})$$
$$\Rightarrow \sqrt{2}\, i \in \mathbf{Q}(\sqrt{2})$$
$$\Rightarrow \sqrt{2}\, i \text{ is a real number, which is not true.}$$

Therefore, $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{2}\, i)$ are non - isomorphic.

In the next result we determine the degree of extension which contains all roots of a given polynomial.

Theorem 9 : *Let $f(x) \in F[x]$ be of degree $n \geq 1$. Then $\exists$ an extension K of F s.t. $[K : F] \leq n!$ and K has n roots of $f(x)$.*

Proof : We prove the result by induction on n. If $n = 1$, then $f(x) = \alpha x + \beta$, $\alpha \neq 0$, $\alpha, \beta \in F$ has only one root $-\beta\alpha^{-1} \in F$. Thus $K = F$ and $[K : F] = 1 = n$. So, result is true for $n = 1$. Assume it to be true for naturals less then n. Let $\deg f(x) = n > 1$. Then by above cor. $\exists$ an extension L of F containing a root α of $f(x)$ and $[L : F] \leq n$. Let $f(x) = (x - \alpha)\ q(x)$, $\deg q(x) = n - 1$, $q(x) \in L[x]$. By induction hypothesis $\exists$ an extension K of L containing all $n - 1$ roots of $q(x)$ and $[K : L] \leq (n - 1)!$.

$$\therefore \qquad [K : F] = [K : L]\ \ [L : F] \leq n\,(n - 1)! = n!$$

Also $\alpha \in L \Rightarrow \alpha \in K \Rightarrow K$ has all n roots of $f(x)$. (The n–1 roots of $q(x)$ are also roots of $f(x)$). So, result is true for n. By induction, result is true for all $n \geq 1$.

In the next section, we shall study the smallest field containing all roots of $f(x)$. This field will be called a splitting field of $f(x)$.

We now give an example of an algebraic extension which is not a finite extension.

Example 1 : Let K be the field of complex numbers and F, the field of rationals.

Let K_a be the set of all elements of K which are algebraic over F.

Then K_a is a subfield of K and $F \subseteq K_a$. By def., K_a is an algebraic extension of F. Suppose $[K_a : F] = n$.

Let $$f(x) = x^{n+1} - 3 \in F[x]$$

By Eisenstein criterion, $f(x)$ *is irreducible* over $\mathbf{Q} = F$. Let α be a root of $f(x)$ in K. Then α is algebraic over $F = \mathbf{Q}$. So, $\alpha \in K_a$.

Since $$[F(\alpha) : F] = \deg\ Irr\,(F, \alpha) = \deg\ f(x) = n + 1,$$
$$[K_a : F] = [K_a : F(\alpha)]\,[F(\alpha) : F] = [K_a : F(\alpha)]\,(n + 1)$$

$\therefore\ n = [K_a : F(\alpha)]\,(n + 1)$, which is absurd.

Hence $[K_a : F]$ is not finite.

Splitting Fields

Let K be an extension of a field F and suppose $f(x) \in F[x]$ can be expressed as product of linear factors in $K[x]$.

i.e., $f(x) = c(x - a_1)(x - a_2) \ldots\ldots (x - a_n)$, $c \in F$ $a_i \in K$ then we say that $f(x)$ splits up in $K[x]$ (or splits over K) and K is called a splitting field of $f(x)$ over F. Further K is called minimal splitting field of $f(x)$ over F if $f(x)$ can be expressed as product of linear factors in $K[x]$ and it can not be so factored over any proper subfield of K. Thus in above case $F(a_1, a_2, \ldots a_n)$ is minimal splitting field of $f(x)$ over F.

We will show that splitting fields always exist and the minimal splitting fields are unique upto isomorphism, i.e. if $\exists$ more than one minimal splitting field then these are isomorphic. Sometimes (when there is no chance of confusion) the word minimal is dropped and we simply talk of splitting fields.

Note : If $f \in k[x]$ splits in $k[x]$, then k is the only minimal splitting field of f over k. For, let $f = c(x - a_1)(x - a_2) \ldots\ldots (x - a_n)$, $a_i \in k$. If f splits in any extension K of k, then the roots of f in K will also be $a_1, a_2, \ldots\ldots, a_n$. So, $k(a_1, a_2, \ldots, a_n) = k$ is the only minimal splitting field of f over k.

Splitting field of a polynomial over a field depends on both the polynomial as well as the field and that is why it is essential to mention splitting field of $f(x)$ *over* F. Take for instance, $f(x) = x^2 + 1 \in \mathbf{Q}[x]$, then as $x^2 + 1 = (x + i)(x - i)$, we find splitting field of $f(x)$ over $\mathbf{Q}$ will be $\mathbf{Q}(i)$. However if $f(x) = x^2 + 1$ is taken as a polynomial over $\mathbf{R}$ then its splitting field over $\mathbf{R}$ is $\mathbf{R}(i) = \mathbf{C}$ the field of complex numbers.

Theorem 10 : *Let k be a field and $f(x)$, a non zero polynomial in $k[x]$. Then there exists a splitting field of f over k. Further if deg $f = n$, then any minimal splitting field E of f over k satisfies $[E : k] \leq n!$*

Proof : We prove the result by induction on deg $f = n$.

Let $n = 1$. Then $f = \alpha x + \beta, \quad \alpha, \beta \in k.$

$$= \alpha(x + \beta\alpha^{-1}).$$

So, f splits in $k[x]$.

Assume that the result is true for all polynomials of degree $< n$. Let deg $f = n$. If $f = gh$, $g, h \in k[x]$, then deg $g, h < n$. By induction hypothesis, $\exists$ an extension K of k s.t. g splits in $K[x]$. Now $h \in k[x] \subseteq K[x]$. Again, by induction hypothesis $\exists$ an extension E of K s.t. h splits, in $E[x]$. So, both g and h split in $E[x]$. Thus f splits is $E[x]$ where $E \supseteq K \supseteq k$. If f is irreducible, then $\exists$ an extension K of k s.t. $f(\alpha) = 0$ for some $\alpha \in K$.

Now $f(x) = (x - \alpha)\, g(x)$, $g(x) \in K[x]$.

Since deg $g < n$, by induction hypothesis $\exists$ an extension E of K s.t. $g(x)$ splits in $E[x]$. So $f(x)$ splits in $E[x]$ as $(x - \alpha) \in K[x] \subseteq E[x]$. By induction, the result follows.

For the second part, note that if α is a zero of f, then

$$[k(\alpha) : k] = \deg Irr(k, \alpha)$$
$$\leq \deg f = n.$$

Let $f = \alpha_0 (x - \alpha_1) \ \ldots\ldots \ (x - \alpha_n), \ \ \alpha_i \in E.$

Then $E = k(\alpha_1, \ldots\ldots, \alpha_n).$

Now, $[k(\alpha_1) : k] \leq n$

$$[k(\alpha_1, \alpha_2) : k(\alpha_1)] = \deg \ Irr(k(\alpha_1), \alpha_2)$$
$$\leq n - 1 \text{ as } f(x) = \alpha_0(x-\alpha_1)(x-\alpha_2)\ldots\ldots(x-\alpha_n)$$

$$\Rightarrow f(x) = (x - \alpha_1) g(x)$$

where $g(x) = \alpha_0(x - \alpha_2)\ldots\ldots\ldots(x - \alpha_n) \in k(\alpha_1)[x]$

In this way, $[k(\alpha_1, \alpha_2 \ldots, \alpha_r) : k(\alpha_1, \alpha_2, \ldots\ldots, \alpha_{r-1})] \leq n - (r - 1)$

Thus
$$[E : k] = [k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k]$$
$$= [k(\alpha_1, \alpha_2, \ldots \alpha_n) : k(\alpha_1, \alpha_2, \ldots \alpha_{n-1}] \ \ldots\ldots [k(\alpha_1) : k]$$
$$\leq (n - (n + 1))\ldots\ldots(n - 1)\, n = n!$$

which proves the second part.

Definition : Let E and L be two extensions of a field k. An isomorphism $f : E \to L$ is called a *k - isomorphism* if $f(a) = a \ \forall \ a \in k$ and in that case we say E and L are k - isomorphic. Similarly we talk of k - homomorphism or k - automorphism.

Theorem 11 : *Let k_1, k_2 be two fields. Suppose $\sigma : k_1 \to k_2$ is an isomorphism and $f_1 \in k_1[x]$ is irreducible over k_1. Then*

$\sigma(f_1(x)) = \sigma(a_0 + a_1 x + \ldots\ldots + a_n x^n) = \sigma(a_0) + \sigma(a_1) x + \ldots\ldots + \sigma(a_n) x^n$ *is irreducible over k_2.*

Proof : Suppose $\sigma(f_1(x)) = g_2 h_2, \qquad g_2, h_2 \in k_2[x].$

Let
$$g_2 = b_o + b_1 x + \ldots\ldots + b_r x^r$$
$$h_2 = c_o + c_1 x + \ldots\ldots\ldots + c_s x^s, \qquad b_i, c_j \in k_2.$$

Since σ is onto, given $b_i \in k_2 \ \exists \ b'_i \in k_1$ s.t. $\sigma(b'_i) = b_i$

Therefore, $g_2 = \sigma(b'_o) + \ldots\ldots + \sigma(b'_r) x^r$

Similarly $h_2 = \sigma(c'_o) + \ldots\ldots + \sigma(c'_s) x^s.$

So,
$$g_2 = \sigma(b'_o + b'_1 x + \ldots\ldots + b'_r x^r) = \sigma(g'_2)$$
$$h_2 = \sigma(c'_o + c'_1 x + \ldots\ldots\ldots + c'_s x^s) = \sigma(h'_2), \text{ where } g'_2 \text{ and } h'_2 \in k_1[x].$$

Thus $\sigma(f_1(x)) = \sigma(g'_2)\, \sigma(h'_2) = \sigma(g'_2 h'_2).$

So, $f_1 = g'_2 h'_2$, contradicting the fact that f_1 is irreducible over k_1.

Hence $\sigma(f_1(x))$ is irreducible over k_2.

Theorem 12 : *Suppose $\sigma : k_1 \to k_2$ is an isomorphism from a field k_1 to a field k_2.*

Let α_1 be a zero of an irreducible polynomial $f_1(x)$ over k_1 and α_2 be a zero of the corresponding polynomial $f_2(x) = \sigma(f_1(x))$ over k_2. Then there exists a unique isomorphism θ from $k_1(\alpha_1)$ to $k_2(\alpha_2)$ s.t. $\theta(\alpha_1) = \alpha_2$ and $\sigma(\alpha) = \alpha \ \ \forall \ \alpha \in k_1$.

Proof : Now $\varphi_1 : k_1[x] \to k_2[\alpha_1]$

with $\varphi_1(g_1(x)) = g_1(\alpha_1)$

is an onto homomorphism s.t., $\text{Ker}\, \varphi_1 = \langle f_1 \rangle$.

So, $\theta_1 : \dfrac{k_1[x]}{<f_1>} \to k_2[\alpha_1]$ is an isomorphism, where

$$\theta_1(<f_1> + g_1(x)) = \varphi(g_1(x)) = g_1(\alpha_1).$$

Here $\theta_1(<f_1> + x) = \alpha_1$.

Similarly $\exists$ an isomorphism

$$\theta_2 : \frac{k_2[x]}{<f_2>} \to k_2[\alpha_2] \text{ s.t.,}$$

$$\theta_2(<f_2> + g_2(x)) = g_2(\alpha_2).$$

Here $\theta_2(<f_2> + x) = \alpha_2$.

Also

$$\theta_3 : \frac{k_1[x]}{<f_1>} \to \frac{k_2[x]}{<f_2>} \text{ s.t.,}$$

$$\theta_3(<f_1> + g_1) = <f_2> + \sigma(g_1),$$

is well defined and is an isomorphism.

If $<f_1> + g_1 = <f_1> + g'_1$,

then $g_1 - g'_1 \in <f_1>$

$\Rightarrow g_1 - g'_1 = 0$ or $\deg(g_1 - g'_1) \geq \deg f_1$,

But $\deg g_1 < \deg f_1$, $\deg g'_1 < \deg f_1$

$\Rightarrow \deg(g_1 - g_1') < \deg f_1$

$\Rightarrow g_1 - g'_1 = 0$

$\Rightarrow \sigma(g_1 - g'_1) = 0 \in <f_2>$

$\Rightarrow \sigma(g_1) - \sigma(g'_1) \in <f_2>$

$\Rightarrow <f_2> + \sigma(g_1) = <f_2> + \sigma(g'_1)$

$\Rightarrow \theta_3$ is well defined.

Here, $\theta_3(<f_1> + x) = <f_2> + x$, as $\sigma(1) = 1$.

Hence, $\theta_1^{-1} : k_1[\alpha_1] \to \dfrac{k_1[x]}{<f_1>}$

$$\theta_3 : \frac{k_1[x]}{<f_1>} \to \frac{k_2[x]}{<f_2>}, \theta_2 : \frac{k_2[x]}{<f_2>} \to k_2[\alpha_2]$$

are isomorphisms.

So, $\theta = \theta_2 \theta_3 \theta_1^{-1}$ is an isomorphism.

In fact, $\theta = k_1[\alpha_1] \to k_2[\alpha_2]$

and $\theta(\alpha_1) = \theta_2\theta_3\theta_1^{-1}(\alpha_1)$

$= \theta_2\theta_3(<f_1> + x)$

$$= \theta_2(<f_2> + x)$$
$$= \alpha_2$$
$$\theta(\alpha) = \theta_2\theta_3\theta_1^{-1}(\alpha)$$
$$= \theta_2\theta_3(<f_1> + \alpha)$$
$$= \theta_2(<f_2>) + \sigma(\alpha)$$
$$= \sigma(\alpha) \qquad \forall\, \alpha \in k_1$$

If $\varphi : k_1[\alpha_1] \to k_2[\alpha_2]$ is another isomorphism s.t. $\varphi(\alpha_1) = \alpha_2, \varphi(\alpha) = \sigma(\alpha)\ \forall\ \alpha \in k_1$,

Then $\varphi(a_o + a_1\alpha_1 + \ldots + a_n\alpha_1^n)$

$$= \varphi(a_o) + \varphi(a_1)\,\varphi(\alpha_1) + \ldots + \varphi(a_n)\,\varphi(\alpha_1^n), \qquad a_i \in k,$$
$$= \sigma(a_o) + \sigma(a_1)\alpha_2 + \ldots + \sigma(a_n)\alpha_2^n.$$
$$= \theta(a_0) + \theta(a_1)\,\theta(\alpha_1) + \ldots + \theta(a_n)\,\theta(\alpha_1^n)$$
$$= \theta(a_o + a_1\alpha_1 + \ldots + \alpha_n\alpha_1^n)$$

i.e. $\theta = \varphi$

and thus φ is uniquley determined.

Theorem 13 : *Let k' be a field isomorphic to k, f' the polynomial over k' corresponding to f over k. If E, E' are minimal splitting fields of f over k and f' over k' respectively, then the given isomorphism between k and k' can be extended to an isomorphism between E and E'.*

Proof Let $\sigma : k \to k'$ be an isomorphism. Let $[E : k] = n$. We prove the result by induction on n.

Let $n = 1$ Then $E = k$.

Let $f = \alpha_0(x - \alpha_1)\ldots\ldots(x - \alpha_m), \quad \alpha_i \in E, \quad \alpha_0 \in k.$

Since $E = k, \quad \alpha_i \in k.$

Therefore, $f' = \sigma(f) = \sigma(\alpha_0)\,(x - \sigma(\alpha_1)\ldots\ldots(x - \sigma(\alpha_m))$ splits in $k'[x]$.

So, $E' = k'$ (See note on page 516)

Then, σ is an extension of σ and the result is true in this case.

Let $n > 1$. Let $f = p_1p_2\ldots p_r$, where each p_i is irreducible over k. Since $[E : k] > 1$, some p_i has degree greater than 1, say p_1.

Now $f' = \sigma(f) = \sigma(p_1)\ldots\ldots\sigma(p_r)$

$$= p'_1\ldots\ldots p'_r, \quad \sigma(p_i) = p'_i \in k'[x].$$

Let α be a zero of p_1 in E and α^1, any zero of p'_1 in E'. Then by previous result, $\exists$ an isomorphism $\theta : k(\alpha) \to k'(\alpha')$ s.t. $\theta(b) = \sigma(b)\ \forall\ b \in k,\ \theta(\alpha) = \alpha'$. Now $p_1 = Irr\,(k, \alpha)$ and $\deg p_1 > 1 \Rightarrow [k(\alpha) : k] = \deg p_1 > 1$.

So, $[E : k] = [E : k(\alpha)]\,[k(\alpha) : k]$

$$> [E : k(\alpha)].$$

Now, a minimal splitting field of f over $k(\alpha)$ is $k(\alpha)$ (Zero of f in E) $= E$.

Also, a minimal splitting field of f' over $k'(\alpha') = k'(\alpha')$ (Zero of f' in E') $= E'$.

By induction hypothesis (Since $\{E : k(\alpha)] < [E : k])$, $\exists$ an isomorphism

$$\psi : E \to E'$$

s.t. $\psi(a) = \theta(a) \quad \forall\, a \in k(\alpha)$.

Also $\psi(b) = \theta(b) \quad \forall\, b \in k$.

$= \sigma(b) \qquad b \in k$.

Therefore, ψ is an extension of σ. So, the result is true in this case. By induction the result is true for all $n \geq 1$.

Cor : If E and E' are minimal splitting fields of f over k, then E and E' are k - isomorphic.

Proof : Take $k' = k$, σ = identity map I in above result. Then $\exists$ an isomorphism $\psi : E \to E'$ s.t. $\psi(a) = \sigma(a) = I(a) = a, \quad a \in k$.

Problem 9 : *Describe the spltting field of $x^3 - 2$ over* **Q**, *the field of rationals.*

Solution : Let $f(x) = x^3 - 2$

If $f(x)$ is reducible over **Q**, then $f(x)$ has a rational root, say $\frac{m}{n}$, $n \neq 0$, $(m, n) = 1$.

$$\therefore \quad m^3 = 2n^3$$

$$\Rightarrow 2 \mid m^3 \Rightarrow 2 \mid m \Rightarrow m = 2k \Rightarrow 8k^3 = 2n^3$$

$$\Rightarrow 4k^3 = n^3$$

$$\Rightarrow 2 \mid n^3 \Rightarrow 2 \mid n$$

$\therefore$ $2 \mid (m, n) = 1$, a contradiction.

$\therefore$ $f(x)$ is irreducible over **Q**.

Let a be a root of $f(x)$ s.t. a is real.

Then $(x^3 - 2) = (x - a)(x^2 + ax + a^2)$

$= (x - a)(x - aw)(x - aw^2)$

where $w = \dfrac{-1 \pm \sqrt{3}i}{2}$

$\therefore$ splitting field of $f(x)$ over **Q**

$K = \mathbf{Q}(a, aw, aw^2)$

$= \mathbf{Q}(a, \sqrt{3}i)$

Now $\mathbf{Q} \subseteq \mathbf{Q}(a) \subseteq K$. Since deg $f(x) = 3$, $[K : \mathbf{Q}] \leq 3! = 6$. Since a is real, $\mathbf{Q}(a)$ is a subfield of real numbers, while K is a subfield of complex numbers as $\sqrt{3}i \in K$.

$\therefore$ $K \neq \mathbf{Q}(a)$ $\qquad \therefore$ $[K : \mathbf{Q}(a)] \geq 2$

But $[\mathbf{Q}(a) : \mathbf{Q}] = \deg\ Irr\,(\mathbf{Q}, a) = \deg\ f(x) = 3$

$\therefore$ $[K : \mathbf{Q}] = [K : \mathbf{Q}(a)]\ [\mathbf{Q}(a) : \mathbf{Q}] \geq 6$

$\therefore$ $[K : \mathbf{Q}] = 6$.

Problem 10 : *Let F be a field of characteristic p. Let b be a root of $f(x) = x^p - x - a \in F[x]$. Show that splitting field of $f(x)$ over F is $F[b]$.*

Solution : Since b is a root of $f(x)$,

$$b^p - b = a \in K$$

Also $$(b+1)^p - (b+1) = b^p + 1 - b - 1 = a$$

$\therefore$ $b+1$ is a root of $f(x)$

Similarly $b+2, \ldots\ldots, b+(p-1)$ are roots of $f(x)$.

$$\therefore \quad f(x) = (x-b)(x-b-1)\ldots\ldots(x-b-p+1)$$

$\therefore$ Splitting field of $f(x)$ over F

$$= F(b, b+1, \ldots, b+(p-1)) = F(b).$$

Problem 11 : *Let* $f(x) = x^4 + x^2 + 1 \in \mathbf{Q}[x]$. *Show that the splitting field of* $f(x)$ *over* $\mathbf{Q}$ *is* $\mathbf{Q}(w)$ and $[\mathbf{Q}(w) : \mathbf{Q}] = 2$.

Solution : Since $w^2 + w + 1 = 0$

$$w^4 + w^3 + w^2 = 0$$

$$\therefore \quad w^4 + w^2 + 1 = 0 \quad \text{as} \quad w^3 = 1$$

$\therefore$ w is a root of $x^4 + x^2 + 1$ and so w is also a root of $x^4 + x^2 + 1$

$$\therefore \quad f(x) = x^4 + x^2 + 1 = (x^2 - w^2)\ (x^2 - w^4) \quad \text{as} \quad w^4 = w$$

$$= (x-w)\ (x+w)\ (x-w^2)\ (x+w^2)$$

$\therefore$ Splitting field of $x^4 + x^2 + 1$ over $\mathbf{Q}$ is

$$\mathbf{Q}(w, -w, w^2, -w^2) = \mathbf{Q}(w)$$

Problem 12 : *Show that the splitting field of* $x^4 + 1$ *over* $\mathbf{Q}$ *is* $\mathbf{Q}(\sqrt{2}, i)$ *whose degree over* $\mathbf{Q}$ *is* 4.

Solution : Roots of $x^4 + 1$ are given by

$$x = (-1)^{1/4}$$

$$= (\cos(2r+1)\pi + i\sin(2r+1)\pi)^{1/4}$$

$$r = 0, 1, 2, 3$$

$$= \cos(2r+1)\frac{\pi}{4} + i\sin(2r+1)\frac{\pi}{4}$$

$$r = 0, 1, 2, 3$$

$$= \frac{1}{\sqrt{2}}(1+i), \quad -\frac{1}{\sqrt{2}}(1-i), \quad -\frac{1}{\sqrt{2}}(1+i), \quad \frac{1}{\sqrt{2}}(1-i)$$

$\therefore$ Splitting field K of $x^4 + 1$ over $\mathbf{Q}$ is

$$K = \mathbf{Q}\left(\pm\frac{1}{\sqrt{2}}(1+i), \pm\frac{1}{\sqrt{2}}(1-i)\right)$$

We show $K = \mathbf{Q}(\sqrt{2}, i)$

$$\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}} \in K \Rightarrow \frac{1+i}{\sqrt{2}} \pm \frac{1-i}{\sqrt{2}} \in K$$

$$\Rightarrow \sqrt{2}, \sqrt{2}\ i \in K$$

$$\Rightarrow \sqrt{2}, i \in K$$

Also $\mathbf{Q} \subseteq K$ and thus $\mathbf{Q}(\sqrt{2}, i) \subseteq K$

Again, $\sqrt{2}, i \in \mathbf{Q}(\sqrt{2}, i) \Rightarrow \pm \frac{1}{\sqrt{2}}(1+i), \pm \frac{1-i}{\sqrt{2}} \in \mathbf{Q}(\sqrt{2}, i)$

$$\Rightarrow K \subseteq \mathbf{Q}(\sqrt{2}, i) \text{ as } \mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}, i)$$

Thus $K = \mathbf{Q}(\sqrt{2}, i)$

Now $x^2 + 1 \in \mathbf{Q}(\sqrt{2})[x]$ is irreducible over $\mathbf{Q}(\sqrt{2})$

$$\Rightarrow [\mathbf{Q}(\sqrt{2}, i) : \mathbf{Q}(\sqrt{2})] = \deg Irr(\mathbf{Q}\sqrt{2}, i)$$
$$= 2 \text{ as } i \text{ satisfies } x^2 + 1$$

But $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = \deg Irr(\mathbf{Q}, \sqrt{2})$
$$= \deg(x^2 - 2) = 2$$

$\therefore$ $[K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{2})]\ [\mathbf{Q}(\sqrt{2}) : \mathbf{Q}]$
$$= 2 . 2 = 4.$$

Aliter : Let θ be a root of $f(x) = x^4 + 1$ in $\mathbf{C}$, the field of complex numbers. Then $-\theta, \theta^{-1}, -\theta^{-1}$ are other distinct roots of $f(x)$ in $\mathbf{C}$. Let E be a minimal splitting field of $f(x)$ over $\mathbf{Q}$.

Then $E = \mathbf{Q}(\theta, -\theta, \theta^{-1}, -\theta^{-1}) = \mathbf{Q}(\theta)$

So, $[E : \mathbf{Q}] = [\mathbf{Q}(\theta) : \mathbf{Q}]$
$$= \deg Irr(\mathbf{Q}, \theta)$$
$$= \deg f(x) = 4.$$

(Note, $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ is irreducible over $\mathbf{Q}$ by Eisentein's Criterion (Take $p = 2$). So, $f(x)$ is irreducible over $\mathbf{Q}$).

Problem 13 : *Find necessary and sufficient conditions on a and b so that the splitting field of irreducible cubic $x^3 + ax + b$ has degree 3 over $\mathbf{Q}$.*

Solution : Let $f(x) = x^3 + ax + b \in \mathbf{Q}[x]$

Let K be the splitting field of $f(x)$ over $\mathbf{Q}$. Let $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$

Then $K = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$

Now $\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = a$

$\alpha_1\alpha_2\alpha_3 = -b$

Let $D = [(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)]^2$

Then $D = -4a^3 - 27b^2$ (Prove it!)

Now $\mathbf{Q}(\sqrt{D}, \alpha_3) \subseteq K$

as $\alpha_1, \alpha_2, \alpha_3 \in K \Rightarrow \alpha_1 - \alpha_2, \alpha_2 - \alpha_3, \alpha_3 - \alpha_1 \in K$
$$\Rightarrow (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in K$$
$$\Rightarrow \sqrt{D} \in K. \text{ Also } \alpha_3 \in K$$
$$\Rightarrow \mathbf{Q}(\sqrt{D}, \alpha_3) \subseteq K$$

Now $\sqrt{D} = (\alpha_1 - \alpha_2)\ [\alpha_3(\alpha_1 + \alpha_2) - \alpha_3^2 - \alpha_1\alpha_2] \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

Since $\alpha_1\alpha_2 = -\dfrac{b}{\alpha_3} \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

and $\alpha_1 + \alpha_2 = -\alpha_3 \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

$\alpha_1 - \alpha_2 \in \mathbf{Q}(\sqrt{D}, \alpha_3) \Rightarrow \alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{D}, \alpha_3)$

$\therefore \quad K \subseteq \mathbf{Q}(\sqrt{D}, \alpha_3)$

$\therefore \quad K = \mathbf{Q}(\sqrt{D}, \alpha_3)$

Suppose $\sqrt{D} \in \mathbf{Q}$. Then $K = \mathbf{Q}(\alpha_3)$

$$\begin{aligned} \therefore \quad [K : \mathbf{Q}] &= [\mathbf{Q}(\alpha_3) : \mathbf{Q}] \\ &= \deg \mathit{Irr}(\mathbf{Q}, \alpha_3) \\ &= \deg f(x) = 3 \end{aligned}$$

Conversely, let $[K : \mathbf{Q}] = 3$

Let $\sqrt{D} \notin \mathbf{Q}$

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{D}) \subseteq \mathbf{Q}(\sqrt{D}, \alpha_3) = K$

But $\sqrt{D}$ satisfies $x^2 - D \in \mathbf{Q}[x]$

$\therefore \quad [\mathbf{Q}(\sqrt{D}) : \mathbf{Q}] = 2$ as $x^2 - D$ is irreducible over $\mathbf{Q}$.

$[K : \mathbf{Q}] = [K : \mathbf{Q}(\sqrt{D})] \; [\mathbf{Q}(\sqrt{D}) : \mathbf{Q}]$

$3 = [K : \mathbf{Q}(\sqrt{D})] \; 2$, a contradiction

$\Rightarrow \sqrt{D} \in \mathbf{Q}$

Hence a necessary and sufficient condition for the splitting field of irreducible cubic $x^3 + ax + b$ over $\mathbf{Q}$ to have degree 3 is $\sqrt{D} \in \mathbf{Q}$.

Problem 14 : *Find the degree of a minimal splitting field of* $x^6 + 1$ *over* $\mathbf{Q}$.

Solution : Let $f(x) = x^6 + 1$

Then the roots of $f(x)$ are

$$\frac{\sqrt{3}}{2} + \frac{i}{2}, \; \frac{-\sqrt{3}}{2} + \frac{i}{2}, \; \frac{-\sqrt{3}}{2} - \frac{i}{2}, \; \frac{\sqrt{3}}{2} - \frac{i}{2}, \; i, \; -i.$$

Let E be a minimal splitting field of $f(x)$ over $\mathbf{Q}$. Then

$E = \mathbf{Q}(\sqrt{3}, i)$

and
$$\begin{aligned} [E : \mathbf{Q}] &= [\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}] \\ &= [\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] \; [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] \\ &= \deg \mathit{Irr}(\mathbf{Q}(\sqrt{3}), i) \times \deg \mathit{Irr}(\mathbf{Q}, \sqrt{3}) \\ &\leq 2 \times 2 \text{ as } \deg \mathit{Irr}(\mathbf{Q}, \sqrt{3}) = \deg x^2 - 3 = 2 \end{aligned}$$

and i satisfies $x^2 + 1$ over $\mathbf{Q}(\sqrt{3})$.

So, $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 1$ or 2.

If $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 1$, then

$\mathbf{Q}(\sqrt{3}) = \mathbf{Q}(\sqrt{3}, i)$ which is not true as i does not belong to $\mathbf{Q}(\sqrt{3})$, the subfield of real numbers.

Therefore, $[\mathbf{Q}(\sqrt{3}, i) : \mathbf{Q}(\sqrt{3})] = 2$

Thus, $[E : \mathbf{Q}] = 4.$

Problem 15 : *Find the degree of a minimal splitting field of $x^4 + 2$ over $\mathbf{Q}$.*

Solution : Let $f(x) = x^4 + 2.$

Then roots of $f(x)$ are

$$2^{1/4}\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{-1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right),\ 2^{1/4}\left(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}\right)$$

If E is a minimal splitting field of $f(x)$ over $\mathbf{Q}$, then

$$E = \mathbf{Q}(2^{1/4}, i), \text{ as } (2^{1/4})^2 = \sqrt{2}.$$

Now
$$\begin{aligned}[E : \mathbf{Q}] &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})]\ [\mathbf{Q}(2^{1/4}) : \mathbf{Q}] \\ &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})]\ \deg\ Irr\,(\mathbf{Q}, 2^{1/4}) \\ &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})]\ \deg\,(x^4 - 2)\end{aligned}$$

$\Rightarrow$ 4 divides $[E : \mathbf{Q}]$

$\Rightarrow$ $[E : \mathbf{Q}] \geq 4.$

Also
$$\begin{aligned}[E : \mathbf{Q}] &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(i)]\ [\mathbf{Q}(i) : \mathbf{Q}] \\ &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(i)]\ \deg\ Irr\,(\mathbf{Q}, i) \\ &= [\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(i)]\ \deg\,(x^2 + 1) \\ &\leq 4 \times 2 = 8 \text{ as } 2^{1/4} \text{ satisfies } x^4 - 2 \text{ over } \mathbf{Q}(i).\end{aligned}$$

So, 4 divides $[E : \mathbf{Q}]$ and $[E : \mathbf{Q}] \leq 8$

$\Rightarrow$ $[E : \mathbf{Q}] = 4$ or 8

If $[E : \mathbf{Q}] = 4$, then

$$[\mathbf{Q}(2^{1/4}, i) : \mathbf{Q}(2^{1/4})] = 1$$

$\Rightarrow$ $\mathbf{Q}(2^{1/4}) = \mathbf{Q}(2^{1/4}, i)$

$\Rightarrow$ $i \in \mathbf{Q}(2^{1/4})$ which is not true as $\mathbf{Q}(2^{1/4})$ is a subfield of real numbers.

Thus, $[E : \mathbf{Q}] = 8.$

Problem 16 : *Show that a minimal splitting field over k for a polynomial of degree n is generated over k by any of $n - 1$ of its zeros.*

Solution : Let $f(x) \in k\,[x]$, $\deg\ f(x) = n.$

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0, \qquad a_i \in k$

Let $E = k(\alpha_1, \ldots\ldots, \alpha_n)$ be a minimal splitting field of f over k.

Now, $$\sum \alpha_i = -\frac{a_{n-1}}{a_n} \in k \subseteq k\,(\alpha_1,\ \alpha_2, \ldots\ldots, \alpha_n) = E.$$

Therefore, $\alpha_1 + \alpha_2 + \ldots\ldots + \alpha_n \in E$ and $\alpha_i \in E.$

Let $E' = k\,(\alpha_1, \ldots\ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots\ldots, \alpha_n)$

Now $$\alpha_i = -\frac{a_{n-1}}{a_n} - (\alpha_1, \ldots\ldots, \alpha_{i-1}, \alpha_{i+1} + \ldots\ldots + \alpha_n)$$
$$\in E'$$
$$\Rightarrow E \subseteq E'. \text{ But } E' \subseteq E.$$

Therefore, $E = E'$, which is generated by $n-1$ zeros of $f(x)$ over k.

Exercises

1. Find the degree of splitting field of $x^5 - 3x^3 + x^2 - 3$ over $\mathbf{Q}$. [4]
2. Find the splitting of $x^p - 1$ over $\mathbf{Q}$, p being a prime number.
3. Find the splitting fields and their degrees of the following polynomials over $\mathbf{Q}$
   (*i*) $x^6 + 1$ (*ii*) $x^4 - 2$ (*iii*) $x^5 - 1$

   (*i*) $\mathbf{Q}(\sqrt{3}, i)$, 4 (*ii*) $\mathbf{Q}(2^{1/4}, i)$, 8 (*iii*) $\mathbf{Q}(e^{2\pi i/5})$, 4
4. If E is an extension of F and $f(x) \in F[x]$ and if φ is an automorphism of E leaving every element of F fixed, prove that φ must take a root of $f(x)$ lying in E into a root of $f(x)$ in E.
5. Prove that $F(3\sqrt{2})$ where F is the field of rationals, has no automorphisms other than the identity automorphism.
6. Using exercise (4), prove that if the complex number α is a root of the polynomial $p(x)$ having real coefficients, then $\bar{\alpha}$, the complex conjugate of α, is also a root of $p(x)$.
7. If F is the field of real numbers, prove that if φ is an automorphism of F then φ leaves every element of F fixed.
8. Find the degree of a minimal splitting field of $x^6 + 1$ over F_2 the field $\{0, 1\}$ mod 2.

   (Hint : $x^6 + 1 = (x+1)^2 (x^2 + x + 1)^2$
   $= (x+1)^2 (x+\alpha)^2 (x+\alpha^2)^2$

   Let E be a minimal splitting field of $x^6 + 1$ over F_2.

   Then $E = F_2(\alpha)$

   and $[E : F_2] = \deg Irr(F_2, \alpha) = \deg\ x^2 + x + 1 = 2$.

Ruler and Compass Constructions

The word "ruler" means straight edge. Greeks used only two instruments, the ruler and the compass. They could perform many geometrical constructions with these. However, some of the constructions which they thought were constructible but could not perform were : Duplication of the cube, Trisection of the angle, Squaring the circle. They found these constructions very difficult. Indeed, we shall prove in this section that these constructions are impossible.

Let P_0 be a subset of $\mathbf{R}^2$ having at least two points with integer co-ordinates. We say a point in $\mathbf{R}^2$ is *constructible at one step from* P_0 if (*i*) it is the intersection of two lines of P_0 (By a line of P_0 we mean the line joining two points of P_0).

or (*ii*) it is the intersection of two circles of P_0 (By a circle of P_0 we mean a circle with centre from P_0 and passing through a point of P_0)

or (*iii*) it is the intersection of a line and a circle of P_0.

A point $r \in \mathbf{R}^2$ is said to be constructible from P_0 if $\exists$ a finite sequence of points $r_1, r_2, \ldots\ldots, r_n = r$ s.t. each r_i is constructible at one step from $P_0 \cup \{r_1, \ldots\ldots, r_{i-1}\}$. Infact, *this is called ruler and compass construction.* For example, let $P_0 = \{p_1, p_2\}$ be a set of two points in $\mathbf{R}^2$. Let l be the line joining two points p_1 and p_2. Let c_1 be the circle with centre p_1 and passing through p_2 and c_2 be the circle with centre p_2 and passing through p_1. Then l is a line of P_0 and c_1, c_2 are circles of P_0. Let r_1 and r_2 be the points of intersection of c_1 and c_2 and c_3 be the intersection of l and line r_1r_2. Then r_3, the middle point of line joining p_1, p_2 is constructible from P_0.

Remark : Since P_0 has at least 2 points with integer co-ordinates, $(0, 0)$ and $(1, 0)$ can be taken as two points in P_0. From now onward instead of writing constructible from P_0 we shall write it as constructible. Similarly line or circle of P_0, we shall write as constructible line or circle.

Problem 17 : *Show that* (a, b) *is constructible for all integers* a *and* b.

Solution : Since (0, 0) and (1, 0) are constructible, line x-axis is also constructible. Also circle with centre (1, 0) and passing through (0, 0) is constructible and meets x-axis at (2, 0). So (2, 0) is constructible. In this way $(a, 0)$ is constructible for all integers a. Circles $(x-1)^2 + y^2 = 4$ and $(x+1)^2 + y^2 = 4$ are constructible as these have centres (1, 0), (–1, 0) and pass through (–1, 0) (1, 0) respectively. $\therefore$ Their intersection $(0, \sqrt{3})$ is also constructible and so line y-axis is constructible. So, circle $x^2 + y^2 = 1$ meets y-axis at (0, 1). Thus (0, 1) is constructible. In this way $(0, b)$ is constructible for all integers b. Line $y = x$ is constructible being the intersection of circles $(x-1)^2 + y^2 = 1$ and $x^2 + (y-1)^2 = 1$. Also (a, a) is constructible being the intersection of line $y = x$ and circle $(x-a)^2 + y^2 = a^2$ for all integers a.

Thus line $x = a$ joining $(a, 0)$ and (a, a) is constructible. Also $y = b$ joining $(0, b)$ and (b, b) is constructible.

$\therefore$ (a, b) = Intersection of lines $x = a$ and $y = b$ is constructible for all integers a and b.

Definition : A real number c is said to be constructible if the point $(c, 0)$ is constructible.

Problem 18 : *If real number* a *is constructible, show that* $(a, 0)$, (a, a) *and* $(0, a)$ *are also constructible.*

Solution : $(a, 0)$ is constructible follows from the definition. Consider the circle $C : (x-a)^2 + y^2 = a^2$. It is constructible as its centre is $(a, 0)$ and passes through (0, 0) which are constructible points. Also line L $y = x$ joining (0, 0) and (1, 1) is constructible.

$\therefore$ $(a, a) = L \cap C$ is constructible.

Line $y = -x$ passing through (0, 0), (1, −1) and circle $x^2 + y^2 = 2a^2$ with centre (0, 0) and passing through (a, a) are constructible.

$\therefore$ $(-a, a)$, their point of intersection is constructible. So, line $y = a$ joining (a, a) and $(-a, a)$ is constructible. $\therefore$ $(a, 0) = (y = a) \cap (x = 0)$ is constructible.

Problem 19 : *If real numbers a and b are constructible, show that* (a, b) *is constructible.*

Solution : By above theorem $(a, 0)$ and (a, a) are constructible $\Rightarrow$ line $x = a$ joining them is constructible. Also $(0, b)$ and (b, b) are constructible. Thus line $y = b$ joining them is constructible. So, $(a, b) = (x = a) \cap (y = b)$ is constructible.

Problem 20 : *If a, b are constructible numbers, show that* $a \pm b, ab, ab^{-1}$ $(b \neq 0)$ *are constructible.*

Solution : Circle $(x - a)^2 + y^2 = b^2$ with centre $(a, 0)$ are passing through (a, b) is constructible. Also $y = 0$ is constructible $\Rightarrow$ $(a \pm b, 0)$, the intersection of above line and circle are constructible.

$\Rightarrow$ $a \pm b$ are constructible numbers.

Since b, 1 are constructible numbers, so is $b - 1$. Thus $(a, b - 1)$ and $(0, b)$ are constructible points (Problem 13). So, the line $ay = -x + ab$ joining them is constructible.

$\therefore$ $(ab, 0) = (y = 0) \cap (ay = -x + ab)$ is constructible.

$\therefore$ ab is constructible number. Also line joining $(0, a)$ and $(a, a(1 - b))$, $bx = a - y$ is constructible.

$\therefore$ $(a/b, 0) = (y = 0) \cap (bx = a - y)$ is constructible.

$\therefore$ a/b is constructible number.

It follows from above problem that the set of rational numbers forms a set of constructible numbers. Also, the set of constructible numbers forms a subfield of real numbers that contains the rationals.

Remark : Since rational numbers are constructible numbers, (a, b) is constructible point for all rationals a and b. So, we can take

$P_0 = \{(a, b) \mid a = \text{rational}, b = \text{rational}\}$.

Problem 21 : *If* $a > 0$ *is constructible, show that* $\sqrt{a}$ *is constructible.*

Solution : Since a is constructible, so is $\dfrac{1+a}{2}$.

$\therefore$ $\left(\dfrac{1+a}{2}, 0\right)$ is a constructible point. Then the circle $(x - \dfrac{1+a}{2})^2 + y^2 = \left(\dfrac{1+a}{2}\right)^2$ passes through (0, 0) and has centre $\left(\dfrac{1+a}{2}, 0\right)$.

$\therefore$ It is constructible circle.

Consider its intersection with the constructible line $x = 1$. The intersection point is $(1, \sqrt{a})$. So $(1, \sqrt{a})$ is constructible. Consider the circle $(x - 1)^2 + (y - \sqrt{a})^2 = a + 1$

with constructible centre $(1, \sqrt{a})$ and passing through (0, 0). So, it is constructible. Its intersecion with $x = 0$, gives $(0, 2\sqrt{a})$ as a constructible point. Then the circle with centre (0, 0) and passing through $(0, 2\sqrt{a})$will meet x-axis at $(2\sqrt{a}, 0)$. So $(2\sqrt{a}, 0)$ is a constructible point. i.e., $2\sqrt{a}$ is a constructible number. Hence $\sqrt{a}$ is a constructible number.

Problem 22 : *If P is a constructible point, not on a constructible line l, then show that line through P perpendicular to l is constructible.*

Solution : Let Q be a constructible point on l. Let C be the constructible circle with centre P and passing through Q. If C meets l at Q only, then l is tangent at Q to C and so $PQ \perp l$, is constructible. If C meets l at Q and R, then circles with centres Q and R and passing through R and Q respectively, are constructible. The line of intersection of these circles is also constructible. But this line passes through P and perpendicular to l.

Theorem 14 : *The real number c is constructible if and only if $\exists$ real numbers $v_1, \ldots\ldots, v_n$ s.t. $\mathbf{Q} = F_0 \subseteq F_1 = \mathbf{Q}(v_1) \subseteq F_2 = F_1(v_2) \subseteq \ldots\ldots\ldots \subseteq F_n = F_{n-1}(v_n) = \mathbf{Q}(v_1, \ldots\ldots, v_n)$, $v_1^2 \in \mathbf{Q}$, $v_1^2 \in \mathbf{Q}(v_1, \ldots\ldots, v_{i-1})$ for all i and $c \in F_n$.*

Proof : Suppose c is constructible number then $(c, 0)$ is a constructible point. Also $\exists$ a finite sequence of points $r_1, \ldots\ldots, r_n = (c, 0)$ s.t. each r_i is constructible at one step from $P_0 \cup \{r_1, \ldots\ldots, r_{i-1}\}$. Consider r_1. Then r_1 is constructible at one step from P_0. r_1 is the intersection of two lines or two circles or a line and a circle constructible from P_0. Suppose r_1 is the intersection of line L given by $dx + ey + f = 0$ where $d, e, f \in \mathbf{Q}$ and circle given by $x^2 + y^2 + ax + by + c = 0$ where $a, b, c \in \mathbf{Q}$. It can be proved that $r_1 = (x_1, y_1)$ where $x_1, y_1 \in \mathbf{Q}(v_1)$ where $v_1 \in \mathbf{Q}$, $u_1 \geq 0$. Let $u_1 = v_1^2$. Then $v_1^2 \in \mathbf{Q}$ and $x_1, y_1 \in \mathbf{Q}(v_1)$. In this way, we shall get

$$\mathbf{Q} \subset \mathbf{Q}(v_1) \subset \mathbf{Q}(v_1, v_2) \subset \ldots\ldots \subset \mathbf{Q}(v_1, \ldots\ldots, v_n)$$

s.t. $\quad v_i^2 \in \mathbf{Q}(v_1, \ldots\ldots, v_{i-1})$ for all i

and $r_n = (c, 0)$ where $c \in \mathbf{Q}(v_1, \ldots\ldots, v_n)$

Conversely, let L be the field of all constructible numbers. We saw just before the theorem that $\mathbf{Q} \subseteq L$. We show that $F_i \subseteq L$ for all i. It is true for $i = 0$ as $F_0 = \mathbf{Q}$. Suppose $F_r \subseteq L$. We show $F_{r+1} \subseteq L$. Now $F_{r+1} = F_r(v_{r+1})$. If $F_{r+1} = F_r$, then $F_{r+1} \subseteq L$.

Let $F_{r+1} \neq F_r$. Since $v_{r+1}^2 \in \mathbf{Q}(v_1, \ldots\ldots, v_r) = F_r \subseteq L$. v_{r+1}^2 is constructible. Thus by above problem $\sqrt{v_{r+1}^2} = v_{r+1}$ is constructible and so $v_{r+1} \in L$.

$\therefore\ F_r(v_{r+1}) = F_{r+1} \subseteq L$.

So our assertion is true for $r + 1$. By induction $F_i \subseteq L$ for all $i \geq 0$. In particular $F_n \subseteq L \Rightarrow c \in L \Rightarrow c$ is constructible.

Cor. 1 : If c is a constructible number, then c lies in some extension of the rationals of degree a power of 2.

Proof : Since $v_i^2 \in \mathbf{Q}(v_1, \ldots\ldots, v_{i-1})$ by above theorem

$$= F_{i-1}$$

v_i satisfies $x^2 - v_i^2 \in F_{i-1}[x]$ for all i

Thus $$[F_i : F_{i-1}] = [F_{i-1}(v_i) : F_{i-1}]$$
$$= \deg Irr(F_{i-1}, v_i) \leq 2$$

$\therefore$ $$[F_n : \mathbf{Q}] = [F_n : F_{n-1}] \ldots\ldots [F_i : F_{i-1}] \ldots\ldots [F_1 : \mathbf{Q}]$$
$$= 2^r, \quad r \leq n.$$

Cor. 2 : If the real number c satisfies an irreducible polynomial over $\mathbf{Q}$ of degree k and k is not a power of 2, then c is not constructible.

Proof : We are given $[\mathbf{Q}(c) : \mathbf{Q}] = k$. Let c be constructible. Now $\mathbf{Q} \subseteq \mathbf{Q}(c) \subseteq F_n$

and $$[F_n : \mathbf{Q}] = [F_n : \mathbf{Q}(c)] \; [\mathbf{Q}(c) : \mathbf{Q}]$$

By Cor. 1, $$[F_n : \mathbf{Q}] = 2^r$$

$\therefore$ $$[\mathbf{Q}(c) : \mathbf{Q}] = \text{power of } 2$$

$\therefore$ $$k = \text{power of } 2, \text{ a contradiction}$$

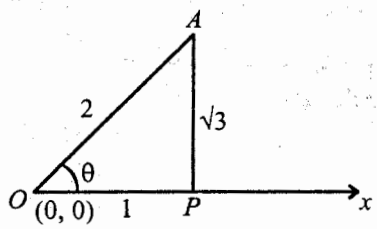
$\therefore$ c is not constructible.

Definition : An angle is said to be constructible if its vertex and arms are constructible.

Problem 23 : *Show that* 60° *is constructible.*

Solution : Take the vertex at $O(0, 0)$ and take one arm as the x-axis..

Since 3 is constructible, $\sqrt{3}$ will be constructible and, therefore, $A(1, \sqrt{3})$ is constructible. Join O and A and we get line OA as constructible line. Then $\theta = \angle XOA = 60°$ as



A is constructible, x axis is constructible, therefore, line AP, (through A and $\perp$ to x - axis) is constructible.

Now $$OP = 1, \; PA = \sqrt{3}, \; OA = \sqrt{3+1} = 2$$

$\therefore$ $\cos\theta = \dfrac{1}{2}$ or that $\theta = 60°$.

Problem 24 : *It is impossible to trisect* 60° *by ruler and compass.*

Solution : Suppose angle 60° can be trisected by ruler and compass. Then (α, β) is constructible as (α, β) is the point of intersection of constructible circle with centre (0, 0) and passing through (1, 0) and arm of angle 20° which is constructible. So $(\alpha, 0)$ the point of intersection of x - axis and perpendicular from (α, β) is also constructible. So, $\alpha = \cos 20°$ is constructible.

Now $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

Put $\theta = 20°$, to get

$$\frac{1}{2} = 4\cos^3 20° - 3\cos 20° = 4\alpha^3 - 3\alpha$$

$\therefore$ α satisfies $f(x) = 8x^3 - 6x - 1 \in Q[x]$.

By Eisenstein criterion $f(x+2)$ is irreducible over **Q**(by taking $p = 3$) and so, $f(x)$ is irreducible over **Q**.

$\therefore$ α satisfies an irreducible polynomial over **Q** of degree 3 which is not a power of 2. By Cor. 2 above, α is not constructible, a contradiction.

Hence, it is impossible to trisect 60° by ruler and compass.

Problem 25 : *It is impossible to duplicate the cube by ruler and compass.*

Solution : Suppose cube is of unit length. Volume of this cube is 1. If we could construct a cube of volume 2, then we could construct a point $(\alpha, 0)$, a vertex of cube s.t. $\alpha^3 = 2$, where one side of the cube is the join of points $(0, 0)$ and $(\alpha, 0)$. But $\alpha^3 = 2 \Rightarrow \alpha$ satisfies $x^3 - 2 \in \mathbf{Q}[x]$.

Let $f(x) = x^3 - 2$. We have seen before that $f(x)$ is irreducible over **Q**. Since degree of $f(x)$ is not a power of 2, α is not constructible. So, it is impossible to duplicate cube by ruler and compass.

Problem 26 : *It is impossible to square the circle by ruler and compass.*

Solution : Suppose given circle has unit radius. So, its area is π. If we could construct a circle of area π^2, then its radius would be $\sqrt{\pi}$. We could take one radius of the circle to be x-axis and centre as $(0, 0)$. $\therefore$ $(\sqrt{\pi}, 0)$ would be constructible, being the intersection of $x^2 + y^2 = \pi$ and x-axis which are constructible. so $(\pi, 0)$ would be constructible.

$\therefore$ $[\mathbf{Q}(\pi) : \mathbf{Q}]$ = power of 2 by Cor. 1

$\Rightarrow$ π is algebraic over **Q**, a contradiction.

Problem 27 : *Show that regular pentagon is constructible.*

Solution : It would be possible to construct a pentagon if we can construct $\alpha = 2\cos\frac{2\pi}{5} = 2\cos 72° = 2\sin 180°$.

Since $\sin 180° = \frac{-1+\sqrt{5}}{4}$ which is constructible, (See Problem 21) we find it is possible to construct a regular pentagon.

Exercises

1. Prove that the regular septagon is not constructible.
2. Prove that the regular hexagon is constructible.
3. Prove that the regular 9-gon is not constructible.
4. Prove that it is possible trisect 72°.
5. Prove that the regular 15-gon is constructible.

Prime Subfields

Definition : Let F be a field. The intersection of all subfields of F is the smallest subfield of F and is called the *prime subfield* of F.

Example 2 : Let $F = Z_p = \{0, 1, 2, \ldots\ldots, p-1\}$ mod p, p being prime. Suppose P is the prime subfield of F. Since $1 \in P$, $2, 3, \ldots\ldots, p-1 \in P$. Therefore, $P = F$.

Example 3 : Let $\mathbf{Q}$ be the field of rationals.

Let $\frac{m}{n} \in \mathbf{Q}$, $m > 0$, $n > 0$, m, $n \in \mathbf{Z}$. Then

$$m = 1 + 1 \ldots\ldots + 1 \quad (m \text{ times})$$
$$n = 1 + 1 + \ldots\ldots + 1 \quad (n \text{ times})$$

$\Rightarrow m, n \in P$, the prime subfield of $\mathbf{Q}$ (as $1 \in P$). So, $\frac{m}{n} \in P \Rightarrow \frac{-m}{n} \in P$. Therefore, $\mathbf{Q} \subseteq P$. Thus, $P = \mathbf{Q}$.

In both the above examples, the prime subfield of the field turns out to be the field itself. But that is not always the case. Consider

Example 4 : Let P_1 and P_2 be the prime subfields of two fields F_1 and F_2 respectively where $F_1 \subseteq F_2$.

Now $P_1 \subseteq F_1 \subseteq F_2 \Rightarrow P_1 \subseteq F_2$.

But P_2 is the smallest subfield of F_2, so, $P_2 \subseteq P_1 \subseteq F_1 \Rightarrow P_2 \subseteq F_1$.

Again, P_1 is the smallest subfield of F_1. So, $P_1 \subseteq P_2$.

Thus, $P_1 = P_2$.

Since, $\mathbf{Q} \subseteq \mathbf{R}$ and $\mathbf{Q}$ is the prime subfield of $\mathbf{Q}$, it follows from above that $\mathbf{Q}$ is the prime subfield of $\mathbf{R}$.

We now tackle the problem in general to determine the prime subfield of any field F. We write char F to denote the characteristic of F.

Theorem 15 : *Let P be the prime subfield of a field F. Then either $P \cong \mathbf{Q}$ or $P \cong \frac{\mathbf{Z}}{(p)}$, for some prime p, $\mathbf{Z}$ being the ring of integers.*

Proof : Define $\theta : \mathbf{Z} \to P \subseteq F$ s.t.,

$$\theta(n) = ne, \text{ where } e \text{ denotes the unity of } F$$

(of course, unity is denoted by 1, but here $\mathbf{Z}$ also has unity 1. So, we denote unity of F by e).

Then θ is a homomorphism. (verify !)

Case 1 : Char $F = 0$

Let $n \in \operatorname{Ker}\theta$. Then $\theta(n) = 0 \Rightarrow ne = 0 \Rightarrow n = 0$ as $e \neq 0$.

So, $\operatorname{Ker}\theta = \{0\} \Rightarrow \theta$ is one-one and so $\mathbf{Z} \cong \theta(\mathbf{Z}) \subseteq P$.

Since $\mathbf{Z}$ is an integral domain, so will be $\theta(\mathbf{Z})$.

Let $\mathbf{Q}'$ be the quotient field of $\theta(\mathbf{Z})$. Since $\mathbf{Q}$ is the quotient field of $\mathbf{Z}$, $\mathbf{Q} \cong \mathbf{Q}'$.

Also $\mathbf{Q}'$ is the smallest field containing $\theta(\mathbf{Z})$. But $\theta(\mathbf{Z}) \subseteq P$. Therefore, $\mathbf{Q}' \subseteq P \subseteq F$.

Again P is the smallest subfield of $F \Rightarrow P \subseteq \mathbf{Q}' \Rightarrow P = \mathbf{Q}'$.

Since $\mathbf{Q}' \cong \mathbf{Q}$, we get $P \cong \mathbf{Q}$.

Case 2 : Char $F \neq 0$. Let char $F = p$, p being prime.

Let $n \in \text{Ker}\,\theta$. Then $\theta(n) = 0 \Rightarrow ne = 0 \Rightarrow p \mid n$ as $e \neq 0$

$\Rightarrow n \in (p) \Rightarrow \text{Ker}\,\theta \subseteq (p)$.

Also, $m \in (p) \Rightarrow m = pr \Rightarrow \theta(m) = \theta(pr) = (pr)\,e = (pe)\,(re) = 0$

$\Rightarrow m \in \text{Ker}\,\theta \Rightarrow (p) \subseteq \text{Ker}\,\theta$.

So, Ker $\theta = (p)$.

But (p) is a maximal ideal of $\mathbf{Z}$

$$\Rightarrow \frac{\mathbf{Z}}{\text{Ker}\,\theta} = \frac{\mathbf{Z}}{(p)} = \text{field}$$

$$\Rightarrow \theta(\mathbf{Z}) \cong \frac{\mathbf{Z}}{\text{Ker}\,\theta} \text{ is a field.}$$

Now, $\theta(\mathbf{Z}) \subseteq P \subseteq F$ and P is the smallest subfield of F, $P \subseteq \theta(\mathbf{Z})$. So $\theta(\mathbf{Z}) = P$

Thus $$P \cong \frac{\mathbf{Z}}{(p)}.$$

Remarks (*i*) : Let F_1, F_2 be fields such that $F_1 \subseteq F_2$. Then F_1, F_2 have the same prime subfield P.

If char $F_2 = 0$, then $P \cong \mathbf{Q}$. So, char $F_1 = 0$.

If char $F_2 = p$, then $P \cong \dfrac{\mathbf{Z}}{(p)}$. So, char $F_1 = p$.

In any case, char F_1 = char F_2.

(*ii*) If F is a finite field, then char $F = p$, for some prime p.

For let, char $F = 0$. Let P denote the prime subfield of F. Then $P \cong \mathbf{Q} \Rightarrow P$ is infinite $\Rightarrow$ F is infinite, a contradiction. Therefore, char $F = p$, for some prime p.

(*iii*) Char $\mathbf{Q} = 0$. For let char $\mathbf{Q} = p$, then the prime subfield $\mathbf{Q}$ of $\mathbf{Q}$ is isomorphic to $\dfrac{\mathbf{Z}}{(p)}$, which is not true as $\mathbf{Q}$ is infinite while $\dfrac{\mathbf{Z}}{(p)}$ is finite. So, char $\mathbf{Q} = 0$.

Example 5 : We now give an example of an infinite field which has finite characteristic p.

Let $F = \{0, 1, 2, \ldots\ldots, p-1\}$ mod p.

Let P be the prime subfield of F.

Then $P = F \cong \dfrac{\mathbf{Z}}{(p)}$. So, char $F = p$.

Now $F[x]$ is an infinite integral domain. Let $F(x)$ denote the quotient field of $F[x]$. Clearly, $F \subseteq F[x] \subseteq F(x)$. So, $\text{char}\, F = \text{char}\, F(x) \Rightarrow \text{char}\, F(x) = p$. Thus, $F(x)$ is an example of an infinite field with finite characteristic p.

Problem 28 : *Let* $\text{char}\, F = p$. *Then*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad \textit{for all } n \geq 1,\ a, b \in F.$$

Solution : Let $n = 1$. Then

$$(a+b)^p = a^p + \sum_{r=1}^{p-1} p_{c_r} a^r b^{p-r} + b^p.$$

Since $p \mid p_{c_r}$, for all r, $1 \leq r \leq p-1$.

We find $p_{c_r} a^r b^{p-r} = 0$

Therefore, $(a+b)^p = a^p + b^p$.

So the result is true for $n = 1$.

Assume that the result is true for $n = m$.

Now
$$\begin{aligned}(a+b)^{p^{m+1}} &= [(a+b)^p]^{p^m} \\ &= (a^p + b^p)^{p^m} \\ &= (a^p)^{p^m} + (b^p)^{p^m} \quad \text{by induction hypothesis} \\ &= a^{p^{m+1}} + b^{p^{m+1}}\end{aligned}$$

Therefore, the result is true for $n = m+1$. By induction, the result is true for all $n \geq 1$.

Problem 29 : *Every automorphism of a field F leaves the prime subfield P of F, elementwise fixed.*

Solution : Let θ be an automorphism of F.

Let $K = \{a \in F \mid \theta(a) = a\}$

Then K is a subfield of F (Prove !)

Since P is the smallest subfield of F, $P \subseteq K$. Let $b \in P$. Then $b \in K \Rightarrow \theta(b) = b \Rightarrow \theta$ fixes each element of P.

Seperable Extensions

This section deals with those polynomials which have simple roots and the fields generated by these simple roots.

Recall, a root α of $f(x) \in K[x]$ is called simple if $x - \alpha$ divides $f(x)$ and $(x-\alpha)^2$ does not divide $f(x)$. Similarly, a root α of $f(x) \in K[x]$ is said to be

a root with multiplicity m, if $(x-\alpha)^m$ divides $f(x)$ but $(x-\alpha)^{m+1}$ does not divide $f(x)$.

Let $\quad f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n \in K[x]$.

Define $\quad f'(x) = a_1 + 2a_2 + \ldots\ldots + na_nx^{n-1} \in K[x]$.

Then $f'(x)$ or f' is called the *derivative* of f.

If $f, g \in K[x]$, then it can be easily proved that

(*i*) $(f \pm g)' = f' \pm g'$

(*ii*) $(fg)' = f'g + fg'$

(*iii*) $(af)' = af', \quad a \in K$

(*iv*) $x' = 1$.

It can be easily checked that α is a simple root of $f(x) \in K[x]$ iff $f'(\alpha) \neq 0$. In other words, α is not a simple root of $f \in K[x]$ iff $f'(\alpha) = 0$.

Theorem 16 : *Suppose all roots of $f(x) \in K[x]$ in a minimal splitting field of f over K are simple. Then the roots of f in* any *minimal splitting field of f over K are simple.*

Proof : Let $f(x) = \alpha_0(x-\alpha_1) \ldots\ldots (x-\alpha_n), \qquad \alpha_i \in E$.

where $E = K(\alpha_1, \ldots\ldots, \alpha_n)$ is a minimal splitting field of f over K.

Suppose each α_i is a simple root of f.

Let E' be another minimal splitting field of f over K.

Then $E' = K(\beta_1, \ldots\ldots, \beta_n)$ where $\beta_i s$ are roots of f.

Then there exists a K-isomorphism $\sigma : E \to E'$.

Since α_i is a root of f, $\sigma(\alpha_i)$ is also a root of f in E'.

Therefore $\{\sigma(\alpha_1), \ldots\ldots, \sigma(\alpha_n)\} = \{\beta_1, \ldots\ldots, \beta_n\}$.

Since σ is 1-1 and $\alpha_i s$ are distinct roots of f, $\sigma(\alpha_i)s$ are all distinct. So $\beta_i s$ are all distinct.

Thus, the roots of f in E' are also simple roots.

Note : By the above arguments, we can also prove that if there is a root of multiplicity m in a minimal splitting field of f over K, then every minimal splitting field of f over K will have a root of f of multiplicity m.

Theorem 17 : *Let F be an extension of K. Let $f, g \in K[x]$. Then the g.c.d. of f and g regarded as polynomials in $K[x]$ is same as that of f and g regarded as polynomials in $F[x]$, upto associates.*

Proof : Let d be the g.c.d. of $f, g \in K[x]$ and d_1 be the g.c.d. of $f, g \in F[x]$.

Now $d \mid f, d \mid g$ in $K[x] \Rightarrow d \mid f, d \mid g$ in $F[x]$

$\Rightarrow d \mid d_1$ in $F[x] \Rightarrow d_1 = du, \qquad u \in F[x]$.

Also, $\qquad d = ff_1 + gg_1, \qquad f, f_1 \in K[x]$.

Since $\qquad d_1 | f, \; d_1 | g, \; d_1 | ff, \; d_1 | gg_1$.

Therefore, $\qquad d_1 \mid ff_1 + gg_1 = d$ in $F[x]$.

$\Rightarrow \qquad d = d_1 v \qquad v \in F[x]$.

So, $d = duv \Rightarrow uv = 1 \Rightarrow u$, v are units in $F \Rightarrow d$, d_1 are associates. Thus d and d_1 are same upto associates.

Theorem 18 : *Let F be an extension of K. Then f and g are relatively prime regarded as elements of $K[x]$ iff f and g are relatively prime regarded as elements of $F[x]$.*

Proof : Suppose f and g are relatively prime regarded as elements of $F[x]$.

Then $(f, g) =$ g.c.d. of $f, g \in F[x]$ is a unit $d \in F$.

Let $(f, g) =$ g.c.d. of $f, g \in K[x]$ be d_1

Then d and d_1 are associates

$\Rightarrow d = ud_1$, $u =$ unit in F

$\Rightarrow d_1 = u^{-1} d =$ unit in F

Since $d_1 \in K$, d_1 is a unit in K.

The converse follows similarly.

Theorem 19 : *Let F be an extension of K. Let $f(x) \in K[x]$, $\alpha \in F$. Then f can be written as $f = (x-\alpha)^2 g + (x-\alpha) f'(\alpha) + f(\alpha)$ for some $g \in F[x]$.*

Proof : Now $(x-\alpha) \in F[x]$.

Let $\quad f = (x-\alpha)^2 g + h, \qquad g, h \in F[x]$

and $\quad h = (x-\alpha) g_1 + h_1, \qquad g, h_1 \in F$

So, $\quad f(\alpha) = h(\alpha) = h_1 \quad (\deg\ h < 2)$

Also, $\quad f' = 2(x-\alpha) g + (x-\alpha)^2 g' + h'$

and $\quad h' = g_1$

$\Rightarrow f'(\alpha) = h'(\alpha) = g_1$.

Therefore, $\quad f = (x-\alpha)^2 g + (x-\alpha) f'(\alpha) + f(\alpha)$.

Theorem 20 : *Let $f \in K[x]$. Then the roots of f are simple iff f and f' are relatively prime.*

Proof : Suppose the roots of f are simple. Let $(f, f') = d$.

If d is a non-constant polynomial in $K[x]$, then d has a root α in some extension F of K.

Now $\quad f = df_1, \ f' = dg_1, \qquad f_1, g \in K[x]$

$\Rightarrow f(\alpha) = d(\alpha) f_1(\alpha), \qquad f'(\alpha) = d(\alpha) g_1(\alpha)$

$\Rightarrow f(\alpha) = 0 = f'(\alpha)$.

Using above result, we get

$$f = (x-\alpha)^2 g + (x-\alpha) f'(\alpha) + f(\alpha)$$
$$= (x-\alpha)^2 g$$

$\Rightarrow \alpha$ is not a simple root of f, a contradiction.

So, $d =$ constant $\in K$.

Since $f \neq 0$, d is a non zero element in K.

Therefore, d is a unit $\Rightarrow f$, f' are relatively prime.

Conversely, let f and f' be relatively prime. Then $(f, f') = d =$ unit in K. Let α be a root of f such that α is not a simple root of f. Let $\alpha \in F \supseteq K$.

Then $\quad f(\alpha) = 0 = f'(\alpha)$

$\Rightarrow \quad x - \alpha$ divides f and f' in $F[x] \supseteq K[x]$

$\Rightarrow \quad x - \alpha$ divides d

But $d \in K \Rightarrow \deg d = 0 \quad (d \neq 0)$.

and $x - \alpha$ divides d

$\Rightarrow \deg (x - \alpha) \leq \deg d = 0$, a contradiction.

So all roots of f are simple.

Definition : A polynomial is said to be *seperable* if all its roots are simple.

In view of the above theorem, the following result follows.

Theorem 21 : *A polynomial $f(x) \in F[x]$ is seperable iff f and f' are relatively prime.*

Cor. 1 : If $f(x) \in F[x]$ is irreducible over F such that $f' \neq 0$, then f is seperable.

Proof : Let g.c.d. $(f, f') = d$ then $\deg d \leq \deg f' < \deg f$.

Since f is irreducible over F and d is a factor of f such that $\deg d < \deg f$, we find d is (non zero) constant and thus a unit. So, f and f' are relatively prime. By above theorem, f is seperable.

Cor. 2 : Let $f(x) \in F[x]$ be irreducible over F. If characteristic of F is zero, then f is seperable. (In other words, an irreducible polynomial over a field of characteristic zero is seperable).

Proof : Let $\quad f = a_0 + a_1 x + \ldots\ldots + a_n x^n \in F[x]$.

Then $\quad f' = a_1 + 2a_2 + \ldots\ldots + na_n x^{n-1}$.

If $f' = 0$, then $ra_r = 0$ for all $r = 1, 2, \ldots\ldots, n$. Since char $F = 0$, $a_r = 0$ for all $r = 1, 2, \ldots\ldots, n \Rightarrow f = a_0$, a contradiction as F is irreducible (deg $f \geq 1$).

Thus, $f' \neq 0$. By Cor. 1, f is seperable.

Theorem 22 : *Let F be a field of characteristic p. Then for any polynomial $f(x) \in F[x]$, $f' = 0$ iff $f(x) = g(x^p)$ for some polynomial $g(x) \in F[x]$.*

Proof : Let $\quad f(x) = a_0 + a_1 x + \ldots\ldots + a_n x^n$ and $f' = 0$.

Then $\quad ra_r = 0 \quad \forall\, r = 1, 2, \ldots\ldots, n$.

$\Rightarrow \quad a_r = 0$ or p divides r as char $F = p$.

Thus, $\quad f = a_0 + a_p x^p + \ldots\ldots + a_{sp} x^{sp}$

$\quad = g(x^p)$, where $g(x) = a_0 + a_p x + \ldots\ldots + a_{sp} x^s \in F[x]$.

Conversely, let $\quad f = g(x^p)$, where

$g(x) = b_0 + b_1 x + \ldots\ldots + b_n x^n \in F[x]$

Then $\quad f = b_0 + b_1 x^p + \ldots\ldots + b_n x^{np}$

$\Rightarrow \quad f' = pb_1 x^{p-1} + \ldots\ldots + npb_n x^{np-1} = 0$ as $pa = 0 \quad \forall\, a \in F$.

Theorem 23 : *Let $f(x) \in F[x]$ be irreducible over F. Then all its roots have the same multiplicity.*

Proof (i) : Let char $F = 0$. Then by cor. 2 to theorem 21 f is seperable. So, all roots of f are simple.

(*ii*) Let char $F = p$. If $f' \neq 0$, then by cor. 1 to theorem 21 f is seperable. So, all roots of f are simple.

If $f' = 0$, then $f(x) = g(x^p)$, for some $g \in F[x]$.

Since f is irreducible over F, so is g over F.

If $g' \neq 0$, then g is seperable over F. Let α be a root of f.

Then $\quad 0 = f(\alpha) = g(\alpha^p) \Rightarrow g(x) = Irr\,(F, \alpha^p)$.

Now, $\quad g(x) = (x - \alpha^p)\ h(x),\ h(\alpha^p) \neq 0$ as α^p is a simple root of $g(x)$.

So,
$$f(x) = g(x^p) = (x^p - \alpha^p)\ \ h(x^p)$$
$$= (x - \alpha)^p\, h_1(x)$$
$$[h_1(x) = h(x^p) \Rightarrow h_1(\alpha) = h(\alpha^p) \neq 0]$$

$\Rightarrow \alpha$ appears exactly p times in $f(x)$.

This is true for all roots of $f(x)$.

If $g' = 0$, then $g(x) = q(x^p)$, $q \in F[x]$

$$\Rightarrow f(x) = q(x^{p^2}).$$

Proceeding in this way, since, deg f is finite, after finite number of steps we get $f(x) = r(x^{p^e})$, $r' \neq 0$. Then r is seperable over F and every root of f appears exactly p^e times.

Hence all roots of f have same multiplicity p^e $(e \geq 0)$.

Cor. : If $f \in F_p[x]$ is irreducible over F_p and f is not seperable, then p divides n, where $n = \deg f$. (F_p denotes the field $\{0, 1, 2, \ldots, p-1\}$ mod $p\}$.

Proof : By above theorem, all roots of f have same multiplicity p^e, $e > 0$ as f is not seperable.

So, deg $f = rp^e$

$\Rightarrow p$ divides $n = \deg f$. (Note, char $F_p = p$).

Theorem 24 : *Let $x^p - a \in F[x]$, where $p = char\, F$. Then either $x^p - a$ is irreducible over F or $x^p - a$ is a p-th power of a linear polynomial in F.*

Proof : Let $f(x) = x^p - a$.

If b is a root of $f(x)$, then $f(b) = 0 \Rightarrow a = b^p$.

$\Rightarrow f(x) = x^p - b^p = (x - b)^p$.

If $b \in F$, then $f(x)$ is p-th power of linear polynomial $x - b \in F[x]$.

Suppose $b \notin F$. Let $p(x)$ be a monic irreducible factor of $f(x)$ in $F[x]$.

Since $p(x)$ divides $f(x)$, $p(x) = (x - b)^m$ for some m, $1 \leq m \leq p$.

So, $p(b) = 0$. Thus, $p(x) = Irr\,(F, b)$.

If $q(x)$ is another monic irreducible factor of $f(x)$ in $F[x]$, then $q(x) = Irr\,(F, b) = p(x)$.

So, $f(x) = (p(x))^2$.

Since deg $f = p$, $p = rm$.

If $r > 1$, then $m = 1 \Rightarrow p(x) = x - b \in F[x] \Rightarrow b \in F$, a contradiction.

So, $r = 1 \Rightarrow f(x) = p(x)$ is irreducible over F.

Example 6 : We saw earlier that any polynomial over a field of characteristic zero is seperable. However, this need not be true over a field of characteristic p. We give an example of an irreducible polynomial which does not have distinct roots.

Let $K = F_2(t)$, $F_2 = \{0, 1\} \bmod 2$ and t is an indeterminate over F_2. Let $f(x) = x^2 - t \in K[x]$.

If f is reducible over K, then there would be an element $a \in K$ s.t., $f(a) = 0$.

$$\Rightarrow t = a^2. \text{ But } a \in K \Rightarrow a = \frac{g(t)}{h(t)}.$$

$$\text{So, } t = \frac{(g(t))^2}{(h(t))^2} \Rightarrow \deg (g(t))^2 = \deg\ t(h(t))^2.$$

$\Rightarrow 2 \deg g(t) = \deg t + 2 \deg h(t) = 1 + 2 \deg h(t)$, which is not true.

So, f is irreducible over K.

If α is a root of f, then $f'(\alpha) = 0$ (as $\operatorname{char} K = 2 = \operatorname{char} F_2$) $\Rightarrow \alpha$ is not a simple root of f.

So, $f = (x - \alpha)^2$.

Thus, f is an irreducible polynomial having no simple roots.

Definition : Let F be an algebraic extension of K. Then $a \in F$ is called seperable over K iff $Irr\,(K, a)$ is seperable.

Thus, $a \in F$ is seperable over K iff a is a simple root of $Irr\,(K, a)$. Further, if each $a \in F$ is seperable over K, then F is called a seperable extension of K. (we write F/K is seperable).

In the example above, $x^2 - t = Irr\,(K, \alpha)$ and α is not a simple root of $x^2 - t$.

If F is a minimal splitting field of $f = x^2 - t$ over K, containing α then F/K is algebraic and $a \in F$ is not seperable over K.

So, $F = K(\alpha)$ is not seperable over F.

However, if $\operatorname{char} K = 0$ then every algebraic extension of K is seperable by cor 2. to theorem 21.

Theorem 25 : *Let char $K = p$. Then every algebraic extension of K is seperable iff $K = K^p$.*

Proof : Suppose every algebraic extension of K is seperable. Let $a \in K$. Let $f(x) = x^p - a$ and b be a zero of $f(x)$. Then $0 = f(b) = b^p - a \Rightarrow a = b^p$ $\Rightarrow f(x) = x^p - b^p = (x - b)^p$. If $b \notin K$ then $f(x)$ is irreducible over K.

So, $x^p - a = Irr(K, b)$.

But $f(x) = x^p - a$

$\Rightarrow$ $f'(x) = p\,x^{p-1}$

$\Rightarrow$ $f'(b) = 0$ as $\text{char}\, K = p$

$\Rightarrow$ b is not a simple root of $f(x)$

$\Rightarrow$ $K(b)/K$ is not seperable, contradicting the given fact that every algebraic extension of K is seperable.

So, $b \in K$ and $a = b^p \in K^p \Rightarrow K \subseteq K^p$.

However, $K^p \subseteq K$. So $K = K^p$ (Note, $K^p = \{a^p \mid a \in K\}$).

Conversely, let $K = K^p$. Let F/K be algebraic.

Let $x \in F$, $f(x) = Irr(K, \alpha)$. If f is not seperable, then $f' = 0$. So, $f = g(x^p)$ for some $g \in K[x]$.

Let $g = a_0 + a_1 x + \ldots\ldots + a_n x^n, \quad a_i \in K.$

Then $f = g(x^p) = a_0 + a_1 x^p + \ldots\ldots + a_n x^{np}$

Since $K = K^p, \quad a_i = b_i^p, \quad b_i \in K.$

So, $f = b_0^p + b_1^p x^p + \ldots\ldots + b_n^p x^{np}$

$= (b_0 + b_1 x + \ldots\ldots + b_n x^n)^p, \quad b_i \in K$

contradicting that f is irreducible over K.

Thus f is seperable $\Rightarrow$ α is seperable.

Since α is an arbitrary element of F, F/K is seperable.

Definition : A field K is called *perfect field* if every algebraic extension of K is seperable.

A field of characteristic zero is perfect by cor. 2 to theorem 21. So, **Q, R, C** are perfect fields.

Theorem 26 : *Let* $\text{char}\, K = p$. *Then the following are equivalent:*

(*i*) *K is perfect.*

(*ii*) $K = K^p$

(*iii*) *Every element in K is a p-th power of some element in K*

(*iv*) $\theta : K \to K$ *such that* $\theta(a) = a^p$ *is an automorphism.*

Proof : (*i*) $\Rightarrow$ (*ii*) follows by theorem 25

(*ii*) $\Rightarrow$ (*iii*) obvious

(*iii*) $\Rightarrow$ (*iv*) : Since $\text{char}\, K = p$, θ is clearly a homomorphism and is 1-1.

Also, $b \in K \Rightarrow b = a^p$, $a \in K$ by (*iii*).

$\Rightarrow b = \theta(a) \Rightarrow \theta$ is onto. So, θ is an automorphism.

(*iv*) $\Rightarrow$ (*i*) : Now $\theta(K) = \{\theta(a) \mid a \in K\}$

$= \{a^p \mid a \in K\}$

$= K^p.$

Since θ is onto, $K = K^p$.

By theorem 25 then K is perfect.

Theorem 27 : *Let $F \subseteq K \subseteq L$ be a tower of fields. Suppose L/F is seperable. Then L/K is seperable.*

Proof : Let $a \in L$, $p(x) = Irr\,(K, a)$

$$q(x) = Irr\,(F, a)$$

Then $q(x) \in K[x]$ and $q(a) = 0$.

So, $p(x)$ divides $q(x)$ in $K[x]$

$$\Rightarrow q(x) = p(x)\, r(x), \qquad r(x) \in K[x]$$

$$\Rightarrow q'(x) = p'(x)\, r(x) + p(x)\, r'(x)$$

$$\Rightarrow q'(a) = p'(a)\, r(a).$$

Since L/F is seperable, a is seperable over F.

So a is a simple root of $q(x) \Rightarrow q'(a) \neq 0$

$\Rightarrow p'(a) \neq 0 \Rightarrow a$ is a simple root of $p(x)$

$\Rightarrow a$ is seperable over K

$\Rightarrow L/K$ is seperable.

Cor. : Every finite extension of a perfect field is perfect

Proof : Let F be a perfect field. Let K/F be finite extension. Then K/F is algebraic. Let L/K be algebraic. Then L/F is algebraic. Since F is perfect, L/F is seperable. From above, L/K is seperable. So, K is perfect.

Problem 30 : *Let F be a perfect field. Show that the set of elements fixed under all automorphisms of F is a perfect subfield.*

Solution : Let char $F = p$, $K = \{a \in F \mid \sigma(a) = a \ \forall\, \sigma \in G\}$, where G is the group of all automorphisms of F. Then K is a subfield of F.

Define $\qquad \theta : F \to F$ s.t.,

$$\theta(\alpha) = \alpha^p$$

Then θ is a homomorphism. Since F is perfect, θ is onto. So, $\theta \in G$.

Let $\alpha \in K$. Then $\sigma(\alpha) = \alpha \ \ \forall\, \sigma \in G$

$$\Rightarrow \theta(\alpha) = \alpha \ \Rightarrow \ \alpha^p = \alpha \Rightarrow \alpha \in K^p \ \Rightarrow \ K \subseteq K^p$$

$\Rightarrow K = K^p \Rightarrow K$ is perfect.

Normal Extensions

As seen earlier if $f(x) \in K[x]$ is irreducible over K, then $\exists$ an extension E of K containing a root of $f(x)$. In this section we consider those extensions of K which contain all roots of $f(x)$ and study properties of such extensions.

Definition : Let E be an extension of K. E is called *normal extension* of K if (*i*) E/K is algebraic (*ii*) $\alpha \in E \Rightarrow p(x) = Irr\,(K, \alpha)$ splits in $E[x]$ or E.

Example 7 : A quadratic extension is a normal extension.

Let E be a quadratic extension of K. Then $[E : K] = 2$.

Since E/K is finite, E/K is algebraic.

Let $\alpha \in E$, $p(x) = Irr\,(K, \alpha)$.

Now $K \subseteq K(\alpha) \subseteq E$. Since $2 = [E : K] = [E : K(\alpha)]\,[K(\alpha) : K]$.

Either $[E : K(\alpha)] = 1$ or $[K(\alpha) : K] = 1$.

If $[K(\alpha) : K] = 1$, then $K(\alpha) = K \Rightarrow \alpha \in K \Rightarrow p(x) = x - \alpha$ splits in $K[x] \subseteq E[x]$.

If $[E : K(\alpha)] = 1$, then $E = K(\alpha)$.

So, $2 = [E : K] = [K(\alpha) : K] = \deg Irr\,(K, \alpha) = \deg p(x)$.

Now α is a root of $p(x) \Rightarrow x - \alpha$ divides $p(x)$ in $E[x]$.

$\Rightarrow p(x) = (x - \alpha)\ q(x)$, $q(x) \in E[x]$.

Since $\deg p(x) = 2$, $\deg q(x) = 1$. So $q(x) = (x - \beta)$, $\beta \in F$.

Therefore, $p(x) = (x - \alpha)\,(x - \beta)$ splits in $E[x]$.

Thus, E/K is normal.

Example 8 : Let $f(x) = x^3 - 2 \in \mathbf{Q}[x]$. Let α be the real root of $f(x)$. Consider $\mathbf{Q}(\alpha)/\mathbf{Q}$. We show that $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Now $f(x)$ is irreducible over $\mathbf{Q}$ by Eisenstein's criterion (take $p = 2$). So, $f(x) = Irr\,(\mathbf{Q}, \alpha)$.

Since α is algebraic over $\mathbf{Q}$(being root of $f(x) \in \mathbf{Q}[x]$), $\mathbf{Q}(\alpha)/\mathbf{Q}$ is algebraic.

If $f(x)$ splits in $\mathbf{Q}(\alpha)$, then $\mathbf{Q}(\alpha)$ contains a minimal splitting field E of $f(x)$ over $\mathbf{Q}$.

So, $\mathbf{Q} \subseteq E \subseteq \mathbf{Q}(\alpha)$.

But $[E : \mathbf{Q}] = 6$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg Irr\,(\mathbf{Q}, \alpha) = \deg f(x) = 3$.

Since $3 = [\mathbf{Q}(\alpha) : \mathbf{Q}] \geq [E : \mathbf{Q}] = 6$, we get a contradiction.

So, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Similarly, $\mathbf{Q}(\alpha w)/\mathbf{Q}$ and $\mathbf{Q}(\alpha w^2)/\mathbf{Q}$ are not normal extensions.

Theorem 28 : *Let $F \subseteq K \subseteq E$ be a tower of fields. If E/F is normal, then so is E/K.*

Proof : Since E/F is normal, E/F is algebraic. So, E/K is algebraic.

Let $\alpha \in E, p(x) = Irr\,(K, \alpha), q(x) = Irr\,(F, \alpha)$. Then $q(x) \in F[x] \subseteq K[x] \Rightarrow q(x) \in K[x]$ and $q(\alpha) = 0$.

So, $p(x)$ divides $q(x)$ in $K[x]$.

Since E/F is normal and $\alpha \in E$, $q(x)$ splits in $E[x]$.

So, $p(x)$ splits in $E[x]$. Thus, E/K is normal.

Theorem 29 : *A minimal splitting field of a non-constant polynomial $f(x) \in K[x]$ over K is normal extension of K.*

Proof : Let E be a minimal splitting field of $f(x)$ over K. Then E/K is algebraic and finite. Let $f(x) = \alpha_0(x - \alpha_1).....(x - \alpha_n)$, $\alpha_i \in E$.

Then $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Let $\alpha \in E$, $p(x) = Irr\,(K, \alpha) \in K[x] \subseteq E[x]$.

Then $p(x)$ splits in some extension of E.

Let β be a root of $p(x)$ in some extension of E. We show that $\beta \in E$.

Now α, β are roots of $p(x) \Rightarrow \exists$ a K-isomorphism $\sigma : K(\alpha) \to K(\beta)$ s.t., $\sigma(\alpha) = \beta$.

Then, a minimal splitting field of f over $K(\alpha)$ is $K(\alpha)\,(\alpha_1, \alpha_2, \ldots, \alpha_n)$

$$= K(\alpha_1, \alpha_2, \ldots, \alpha_n)\,(\alpha_n)$$
$$= E(\alpha)$$
$$= E \quad \text{as } \alpha \in E$$

Also, a minimal splitting field of $\sigma(f) = f$ over $K(\beta)$ is

$$K(\beta)\,(\alpha_1, \alpha_2, \ldots, \alpha_n)$$
$$= K(\alpha_1, \alpha_2, \ldots, \alpha_n)\,(\beta)$$
$$= E(\beta).$$

So, $\exists$ an isomorphism $\theta : E \to E(\beta)$ s.t., $\theta(a) = \sigma(a)\ \forall\ a \in K(\alpha) \Rightarrow \theta(\alpha) = \sigma(\alpha) = \beta$.

Now $K \subseteq K(\alpha) \subseteq E \subseteq E(\beta)$

$$\Rightarrow [E : K(\alpha)] = [\theta(E) : \theta(K(\alpha)]$$
$$= [E(\beta) : \sigma(K(\alpha)]$$
$$= [E(\beta) : K(\beta)]$$

So, $[E(\beta) : K] = [E(\beta) : K(\beta)]\ \{K(\beta) : K]$

$$= [E : K(\alpha)] \deg p(x)$$
$$= [E : K(\alpha)]\ [K(\alpha) : K]$$
$$= [E : K].$$

Since $E \subseteq E(\beta)$ and E, $E(\beta)$ as vector spaces over K have same dimension, $E = E(\beta)$. So, $\beta \in E$. Thus, $p(x)$ splits in E. This proves E/K is normal.

Theorem 30 : *A finite normal extension is a minimal splitting field of some polynomial.*

Proof : Let E/K be a finite normal extension.

E/K is finite $\Rightarrow E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Let $p_i(x) = Irr\,(K, \alpha_i)$. Since $\alpha_i \in E$ and E/K is normal, each $p_i(x)$ splits in E.

Let $f = p_1 p_2 \ldots p_n \in K[x]$.

Then, a minimal splitting field of f over K is

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n, \text{ roots of } p_i s \text{ in } E)$$
$$= E.$$

So, E is a minimal splitting field of f over K.

Cor. : Let $K \subseteq E_1 \subseteq E$, $K \subseteq E_2 \subseteq E$ be towers of fields s.t., E_1/K, E_2/K are finite normal extensions. Then E_1E_2, the smallest subfield of E containing $E_1 \cup E_2$ is finite normal extension of K.

Proof : Since E_1/K is finite, $E_1 = K(\alpha_1, \ldots, \alpha_n)$.

So, $$E_1E_2 = K(\alpha_1, \ldots, \alpha_n)E_2$$
$$= E_2(\alpha_1, \ldots, \alpha_n), \text{ as } K \subseteq E_2 \Rightarrow KE_2 = E_2$$

Thus
$$[E_1E_2 : E_2]$$
$$= [E_2(\alpha_1, \ldots, \alpha_n) : E_2]$$
$$= [E_2(\alpha_1, \ldots, \alpha_n) : E_2(\alpha_1, \ldots, \alpha_{n-1})] \ldots\ldots\ldots\ldots [E_2(\alpha_1) : E_2]$$
$$\leq [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \ldots\ldots\ldots\ldots [K(\alpha_1) : K]$$
$$= [K(\alpha_1, \ldots, \alpha_n) : K]$$
$$= [E_1 : K].$$

Therefore, $$[E_1E_2 : K] = [E_1E_2 : E_2]\,[E_2 : K]$$
$$\leq [E_1 : K]\,[E_2 : K] = \text{finite}$$
$$\Rightarrow [E_1E_2 : K] = \text{finite}.$$

Now E_1/K is finite normal $\Rightarrow E_1$ is a minimal splitting field of f_1 over K

Also, E_2/K is finite normal $\Rightarrow E_2$ is a minimal splitting field of f_2 over K

Let $f = f_1f_2$, $E_1 = K(a_1, \ldots\ldots, a_r)$, $E_2 = K(b_1, \ldots\ldots, b_s)$. Then, a minimal splitting field of f over K is $K(a_1, \ldots\ldots, a_r, b_1, \ldots\ldots, b_s)$
$$= E_1(b_1, \ldots\ldots, b_s)$$
$$= E_1K(b_1, \ldots\ldots, b_s) \text{ as } E_1K = E_1$$
$$= E_1E_2.$$

Thus, E_1E_2/K is finite normal extension.

(Note, we have also shown above that E_1/K, E_2/K are finite $\Rightarrow E_1E_2/K$ is finite).

Example 9 : We now give an example to show that a normal extension of a normal extension need not be a normal extension.

Consider the tower of fields $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(2^{1/4})$.

Now $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = \deg\ Irr\,(\mathbf{Q}, \sqrt{2}) = x^2 - 2 = 2$

and $[\mathbf{Q}(2^{1/4}) : \mathbf{Q}(2^{1/2})] = \deg\ Irr\,(\mathbf{Q}(\sqrt{2}),\ 2^{1/4}) = \deg\,(x^2 - \sqrt{2}) = 2$

So, $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$, $\mathbf{Q}(2^{1/4})/\mathbf{Q}(\sqrt{2})$ are normal.

If $\mathbf{Q}(2^{1/4})/\mathbf{Q}$ is normal, then $f(x) = Irr\,(\mathbf{Q}, 2^{1/4}) = x^4 - 2$ must split in $\mathbf{Q}(2^{1/4})$.

So, $\mathbf{Q}(2^{1/4})$ contains a minimal splitting field E of $f(x)$.

But $[E : \mathbf{Q}] = 8$ and $\mathbf{Q} \subseteq E \subseteq \mathbf{Q}(2^{1/4}) \Rightarrow [\mathbf{Q}(2^{1/4}) : \mathbf{Q}] = 4 \geq [E : \mathbf{Q}] = 8$, a contradiction.

Therefore, $\mathbf{Q}(2^{1/4})/\mathbf{Q}$ is not normal, proving our assertion.

Theorem 31 : *Let $K \subseteq F \subseteq E$ be a tower of fields s.t., E/K is finite normal. Then any K-homomorphism of F into E can be extended to K-automorphism of E.*

Proof : Since E/K is finite, $E = K(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$. Also E/K is finite normal $\Rightarrow E$ is a minimal splitting field of some $f(x) \in K[x]$ over K. Let σ be a K-homomorphism of F into E. Then σ is a K-isomorphism from F onto $\sigma(F) = F'$. $f = p_1p_2 \ldots\ldots p_n$, where $p_i = Irr\,(K, \alpha_i)$ splits in E.

So, a minimal splitting field of f over F is

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n, \text{ roots of } f \text{ in } E)$$
$$= E(\text{roots of } f \text{ in } E) = E$$

$(E = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq E \Rightarrow E = F(\alpha_1, \alpha_2, \ldots, \alpha_n))$

Also, a minimal splitting field of $\sigma(f(x)) = f$ over F' is $F'((\alpha_1, \alpha_2, \ldots, \alpha_n,$ roots of f in $E)$

$$= E(\text{roots of } f(x) \text{ in } E)$$
$$= E$$

$$[E = K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n)$$
$$\cong F'(\alpha_1, \alpha_2, \ldots, \alpha_n)$$
$$\subseteq F(\alpha_1, \alpha_2, \ldots, \alpha_n) = E$$
$$\Rightarrow E = F'(\alpha_1, \alpha_2, \ldots, \alpha_n)]$$

Therefore, $\exists$ an isomorphism $\theta : E \to E$ s.t., $\theta(a) = \sigma(a)\ \forall\ a \in F \Rightarrow \theta(\alpha) = \sigma(\alpha) = \alpha\ \forall\ \alpha \in K \Rightarrow \theta$ is a K-automorphism of E extending σ. This proves the result.

Normal Closure : Let E/K be a finite extension. Then $E = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $p_i = Irr\,(K, \alpha_i)$ and $f = p_1 p_2 \ldots p_n \in K[x]$.

Then E' the minimal splitting field of f over K is

$K(\alpha_1, \ldots, \alpha_n,$ roots of f in some extension of $E)$
$= E(\text{roots of } f \text{ in some extension of } E)$

$\Rightarrow E \subseteq E'$ and E'/K is finite normal

(as a minimal splitting field of f over K is finite normal extension of K)

Suppose $K \subseteq E \subseteq F$ s.t., F/K is finite normal.

We show that E' can be embedded in F.

$\alpha_i \in E \subseteq F \Rightarrow \alpha_i \in F\ \forall\ i$. Also F/K is normal.

So, $p_i(x)$ splits in $F[x]\ \forall\ i \Rightarrow f$ splits in $F[x]$

$\Rightarrow F$ contains a minimal splitting field E_1 of f over K

$\Rightarrow E_1 \subseteq F$. But E' is also a minimal splitting field of f over K.

Therefore, $E' \cong E_1 \subseteq F \Rightarrow E'$ can be embedded in F.

Thus, E' is the least finite normal extension of K s.t., $K \subseteq E \subseteq E'$.

E' is called the normal closure of E/K.

Example 10 : Let $f(x) = x^3 - 2$

$$= (x - \alpha)(x - \alpha w)(x - \alpha w^2)$$

We find the normal closure of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

Now $\quad [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg\ f(x) = 3$

where $\quad f = Irr\,(\mathbf{Q}, \alpha)$.

Then, a minimal splitting field of f over $\mathbf{Q}$ is $\mathbf{Q}(\alpha, \alpha w, \alpha w^2) = \mathbf{Q}(\alpha, w)$.

So, $\mathbf{Q}(\alpha w)/\mathbf{Q}$ is the normal closure of $\mathbf{Q}$.

Algebraically closed fields and algebraic closure

In this section, we give a characterization of normal extensions. Also, we show that given a tower of fields $k \subseteq F \subseteq K$ such that K/k is normal, any k-homomorphism of F into K can be extended to a k-automorphism of K. We have already seen this result when K/k is finite normal. We also show that given a field k, there is an algebraic extension $\bar{k}$ of k such that $\bar{k}$ has no algebraic extension other than $\bar{k}$ itself. $\bar{k}$ is called an *algebraic closure* of k. We define the product of two subfields of a field and show that the product and the intersection of two normal extensions of k is again a normal extension of k.

Let S be a set of polynomials over k. Suppose each $f \in S$ splits in a field E containing k. Then E is called a *splitting field of S over k* and k(zeros of $f \in S$ in E) is called a *minimal splitting field of S over k*. For a finite set S, it is very easy to show the existence of a minimal splitting field of S over k. For, let $S = \{f_1, f_2, \ldots\ldots, f_n \mid f_i \in k[x]\}$.

Let E_1 be a minimal splitting field of f_1 over k, E_2 be a minimal splitting field of f_2 over E_1 and so on, E_n be a minimal splitting field of f_n over E_n. Then $E_1 \subseteq E_2 \subseteq \ldots\ldots \subseteq E_n$ and each f_i splits in $E_i \subseteq E_n \Rightarrow S$ splits in E_n. So, k(zeros of f_i in E_n) is a minimal splitting field of S over k. It is also a minimal splitting field of $f = f_1 f_2 \ldots\ldots f_n$ over k.

Definition : A field k is called *algebraically closed* if every polynomial f over k splits in k.

By fundamental theorem of algebra, every polynomial over **C**, the field of complex numbers splits in **C**. So, **C** is an algebraically closed field. However, **R** the field of reals is not algebraically closed as $x^2 + 1 \in \mathbf{R}[x]$ does not split in **R**. We have the following characterizations of algebraically closed fields.

Theorem 32 : *A field k is algebraically closed iff every irreducible polynomial over k has degree one.*

Proof : Suppose k is algebraically closed.

Let f be an irreducible polynomial over k. Since k is algebraically closed, f splits in k.

So, $f = f_1 f_2 \ldots\ldots f_n$ where each f_i is linear over k.

Since f is irreducible over k, $f = f_1 \Rightarrow f$ is linear over $k \Rightarrow \deg f = 1$.

Conversely, let $g \in k[x]$.

Then $g = g_1 g_2 \ldots\ldots g_m$, where each g_i is irreducible over k.

By hypothesis, $\deg g_i = 1 \Rightarrow g_i$ is linear over k for each i

$\Rightarrow g$ is a product of linear factors over $k \Rightarrow g$ splits in k.

So, k is algebraically closed.

Theorem 33 : *A field k is algebraically closed iff every algebraic extension of k is k itself.*

Proof : Let k be algebraically closed. Let K/k be algebraic.

Let $\alpha \in K$, $p(x) = Irr(k, \alpha)$.

By above theorem deg $p(x) = 1 \Rightarrow p(x) = x - \alpha \in k[x] \Rightarrow \alpha \in k \Rightarrow K = k$.

Conversely, let $f \in k[x]$. Let K be a minimal splitting field of f over k. Then K/k is algebraic. By hypothesis, $K = k$.

So, $f(x)$ splits in $k[x] \Rightarrow k$ is algebraically closed.

Summarising the last two results, we have the following

Theorem 34 : *Let k be a field. Then following are equivalent*

(*i*) *k is algebraically closed.*

(*ii*) *Every irreducible polynomial over k has degree one.*

(*iii*) *Every algebraic extension over k is k itself.*

Theorem 35 : *A finite field is not algebraically closed.*

Proof : Let k be the finite field $\{a_1, a_2, \ldots\ldots, a_n\}$

Let $$f = 1 + (x - a_1)(x - a_2) \ldots\ldots (x - a_n) \in k[x].$$

Since $f(a_i) \neq 0$ for all i, we find f does not split in k.

Hence k is not algebraically closed.

Definition : Let k be a field. An extension E of k is called *algebraic closure* of k if

(*i*) E/k is algebraic.

(*ii*) E is algebraically closed.

The following result is now an immediate consequence of theorem 33.

Theorem 36 : *Let E be an algebraic extension of k. Then E is algebraically closed iff E has no algebraic extension other than E itself.*

Example 11 : Since $[\mathbf{C} : \mathbf{R}] = 2$, $\mathbf{C}/\mathbf{R}$ is algebraic. Also, $\mathbf{C}$ is algebraically closed. So, $\mathbf{C}$ is an algebraic closure of $\mathbf{R}$. However, $\mathbf{C}$ is not an algebraic closure of $\mathbf{Q}$ as $\mathbf{C}/\mathbf{Q}$ is not algebraic ($\pi \in \mathbf{C}$ is not algebraic over $\mathbf{Q}$).

Theorem 37 : *Let K/k be algebraic. Let $\bar{k}$ denote an algebraic closure of K. Then $\bar{k}$ is an algebraic closure of k such that*

$$k \subseteq K \subseteq \bar{k}.$$

Proof : Since $\bar{k}$ is an algebraic closure of K, $\bar{k}/K$ is algebraic. Also, K/k is algebraic. So, $\bar{k}/k$ is algebraic. But $\bar{k}$ is algebraically closed. Thus $\bar{k}$ is also an algebraic closure of k.

Theorem 38 : *Let K be an algebraically closed field such that K is an extension of k. Let $F = \{a \in K \mid a$ is algebraic over $k\}$.*

Then F is an algebraic closure of k.

Proof : We know that

$$k \subseteq F \subseteq K \text{ is a tower of fields.}$$

Also, by definition of F, F/k is algebraic.

Let $f \in F[x]$. Then $f \in K[x]$. Since K is algebraically closed, f splits in K.

Let $f = \alpha(x - \alpha_1) \ldots\ldots\ldots (x - \alpha_n)$, $\alpha_i \in K$.

Since α_i is algebraic over F, $F(\alpha_i)/F$ is algebraic for all i.

Also F/k is algebraic. So, $F(\alpha_i)/k$ is algebraic for all i.

$\Rightarrow$ $\alpha_i \in K$ is algebraic over k

$\Rightarrow$ $\alpha_i \in F$

$\Rightarrow$ f splits in F

$\Rightarrow$ F is algebraically closed

$\Rightarrow$ F is an algebraic closure of k.

From above theorem it follows that $F = \{a \in \mathbf{C} \mid a$ is algebraic over $\mathbf{Q}\}$ is an algebraic closure of $\mathbf{Q}$.

We now show the existence of a minimal splitting field of a set of polynomials over k.

Theorem 39 : *Let S be a set of polynomials over k. Then there is a minimal splitting field of S over k.*

Proof : Suppose $S = \{f_i \mid f_i \in k[x],\ i \in I\}$.

Let $A = \{i_1, i_2, \ldots\ldots, i_n\}$ be a finite subset of I.

Put $$f_A = f_{i_1} f_{i_2} \ldots\ldots\ldots\ldots f_{i_n} \in k[x].$$

Let E_A be a minimal splitting field of f_A over k.

Suppose $B \subseteq A$. Then f_B divides f_A. So, f_B splits in E_A.

Let $F_B = k$(zeros of f_B in E_A).

Then F_B is a minimal splitting field of f_B over k. So, $F_B \cong E_B$. But $F_B \subseteq E_A$. Therefore, we can regard $E_B \subseteq E_A$. So, we have $B \subseteq A \Rightarrow E_B \subseteq E_A$.

Let $E = \bigcup_A E_A$. Let $a, b \in E$. Then $a \in E_A$, $b \in E_B$ for some finite sets $A, B \subseteq I$.

Let $C = A \cap B$. Then $A, B \subseteq C$.

So, $$E_A,\ E_B \subseteq E_C \Rightarrow a, b \in E_C$$

$\Rightarrow$ $a \pm b$, ab, ab^{-1}, (if $b \neq 0$) are in $E_C \subseteq E$

$\Rightarrow$ E is a field.

Therefore, for each $f_i \in S$, f_i splits in E_A, where $A = \{i\}$.

$\Rightarrow$ each $f_i \in S$ splits in E.

$\Rightarrow$ E is a splitting field of S over k.

$\Rightarrow$ k(zeros of f_i in E) is a minimal splitting field of S over k.

Using Zorn's lemma or otherwise one can prove the following result. We, however, omit the proof.

Theorem 40 : *Any two minimal splitting fields of a set of polynomials over k are isomorphic.*

We can now show the existence of an algebraic closure of a field k.

Theorem 41 : *Let S be the set of all polynomials over k. Then a minimal splitting field of S over k is an algebraic closure of k.*

Proof : Let F be a minimal splitting field of S. Since F is generated by zeros of $f \in S$, F is generated by algebraic elements over k. So, F/k is algebraic.

Let $\quad f = a_0 + a_1 x + \ldots\ldots + a_n x^n \in F[x]$.

Let $\quad E = k(a_0, a_1, \ldots\ldots\ldots, a_n) \subseteq F$.

Then $f \in E[x]$. Let E' be a minimal splitting field of f over E.

Let $\quad f = \alpha(x - \alpha_1) \ldots\ldots (x - \alpha_n), \qquad \alpha_i \in E$.

Then $\quad E' = E(\alpha_1, \ldots\ldots\ldots, \alpha_n)$.

Since each α_i is algebraic over E, E'/E is algebraic. Also, each $a_i \in F$ is algebraic over $k \Rightarrow E/K$ is algebraic. So, E'/k is algebraic.

Let $\quad g_i = Irr\,(k, \alpha_i)$

Let $\quad g = g_1 g_2 \ldots\ldots g_n \in k[x]$

Now $\quad g_i = (x - \alpha_i) f_i, \qquad f_i \in E'[x]$.

Therefore,
$$\begin{aligned} g &= (x - \alpha_1) \ldots\ldots (x - \alpha_n) f_1 \ldots\ldots f_n \\ &= \alpha(x - \alpha_1) \ldots\ldots (x - \alpha_n)\alpha^{-1} f_1 \ldots\ldots f_n \\ &= ff', \quad f' = \alpha^{-1} f_1 \ldots\ldots f_n \in E'[x] \end{aligned}$$

Let $\quad g = \Sigma c_i x^i, \; f' = \Sigma b_i x^i, \; f = \Sigma a_i x^i$

where $\quad c_i \in k, \; b_i \in E', \; a_i \in F$.

Now $\quad c_r = \sum_i a_i b_{r-i}$

Let a_j be the first non zero coefficient in $f(x)$.

Therefore, $\quad c_j = a_j b_0 \Rightarrow b_0 = a_j^{-1} c_j \in F$.

Suppose $\quad b_0, b_1, \ldots\ldots, b_r \in F$.

Then
$$c_{j+r+1} = a_{j+r+1} b_0 + a_{j+r} b_1 + \ldots\ldots + a_{j+1} b_r + a_j b_{r+1}$$
$$\Rightarrow \quad b_{r+1} = a_j^{-1} \; (c_{j+r+1} - a_{j+r+1} b_0 \ldots\ldots - a_{j+1} b_r) \in F$$

By induction, each $b_i \in F \Rightarrow f' \in F[x]$.

By hypothesis, $g \in k[x] \Rightarrow g$ splits in F.

Let $\quad g = (x - \beta_1) \ldots\ldots (x - \beta_m), \qquad \beta_i \in F$

Suppose $f \in F[x]$ splits in some extension F' of F.

Let $\quad f = d(x - d_1) \ldots\ldots (x - d_n), \qquad d_i \in F' \supseteq F$.

Now $f' \in F[x] \subseteq F'[x] \Rightarrow f'$ splits in some extension F'' of F'.

Let $\quad f' = e(x - e_1) \ldots\ldots (x - e_r), \qquad e_i \in F'' \supseteq F' \supseteq F$

So, $\quad g = ff' \Rightarrow g(d_i) = 0$ for all i

$\Rightarrow d_i - \beta_j = 0$ for some j depending on i

$\Rightarrow d_i = b_j \in F$

$\Rightarrow d_i \in F$ for all i

$\Rightarrow f$ splits in F.

Thus, F is algebraically closed

Hence F is an algebraic closure of k.

Converse of above theorem is also true.

Theorem 42 : *Let F be an algebraic closure of k. Then F is a minimal splitting field of the set S of all polynomials over k.*

Proof : Now F is an algebraic closure of k

$\Rightarrow$ F is algebraically closed

$\Rightarrow$ each $f \in S$ splits in F.

Let $F' = k(\text{zeros of } f \in S \text{ in } f) \subseteq F$.

Let $\alpha \in F$. Then α is algebraic over k as F/k is algebraic. Let $p(x) = Irr(k, \alpha)$

Then α is a zero of $p(x) \in S$ in F.

So, $\qquad \alpha \in F' \Rightarrow F \subseteq F$.

Therefore, $F' = F \Rightarrow F$ is a minimal splitting field of F' of the set of all polynomials over k. The following is then immediate.

Theorem 43 : *Any two algebraic closures of a field are isomorphic.*

Proof : Let k be a field and F_1, F_2 be algebraic closures of k. Then F_1, F_2 are minimal splitting fields of the set of all polynomials over k. So, F_1, F_2 are isomorphic by theorem 40.

Theorem 44 : *Algebraic closure of a countable field is countable.*

Proof : Let k be a countable field. For each integer $n \geq 1$, there is a countable set of polynomials of degree n over k. Thus, the set S of all polynomials over k is countable. Let $S = \{f_1, f_2, \ldots\ldots, f_n, \ldots\ldots\}$. Let $E_0 = k$, and E_1 be a minimal splitting field of f_1 over $E_0 = k$. In this way, let E_i be a minimal splitting field of f_i over E_{i-1}. Then $E_{n-1} \subseteq E_n$ for all n.

So, $E = \bigcup_n E_n$ is a field $\Rightarrow$ each f_i splits in E

$\Rightarrow$ E is a splitting field of S over k.

Let $F = k(\text{zeros of } f_i \text{ in } E) \subseteq E$.

Then $k \subseteq F \subseteq E$ is a tower of fields and F is a minimal splitting field of S over k. So, F is an algebraic closure of $k \Rightarrow F$ is algebraically closed $\Rightarrow$ F is not finite. Since E is countable, F is also countable. Thus, any algebraic closure F' of k being isomorphic to F is also countable.

Lemma : *Let E be an algebraic extension of k and let $\sigma : E \to E$ be a k-homomorphism. Then σ is a k-automorphism.*

Proof : Let $\alpha \in E$, $p(x) = Irr(k, \alpha)$.

Let $\alpha_1 = \alpha, \alpha_2, \ldots\ldots, \alpha_r$ be zeros of $p(x)$ lying in E.

Let $E' = k(\alpha_1, \alpha_2, \ldots\ldots, \alpha_r) \subseteq E$.

Then E'/k is finite.

Let $p(x) = (x - \alpha_i)\, q_i(x), \qquad q_i(x) \in k(\alpha_i)[x]$.

Since $\sigma(a) = a$ for all $a \in k$, $\sigma(p(x)) = p(x)$.

Therefore, $p(x) = \sigma(p(x)) = (x-\sigma(\alpha_i))\, \sigma(q_i(x))$

$\Rightarrow$ $\sigma(\alpha_i)$ is a zero of $p(x)$ for all i.

But $\sigma : E \to E \Rightarrow \sigma(\alpha_i) \in E$ for all i.

So, $\sigma(\alpha_i)$ is a zero of $p(x)$ in E for all i.

$\Rightarrow$ $\sigma(\alpha_i) \in E'$ for all i.

$\Rightarrow$ $\sigma : E' \to E'$ is a k-homomorphism.

Also E'/k is finite. Since σ is also 1-1, $\sigma : E' \to E'$ must be onto (See below).

Therefore, $E' = \sigma(E') \Rightarrow \alpha = \sigma(\beta)$, for some $\beta \in E' \subseteq E$

$\Rightarrow$ $\sigma : E \to E$ is onto $\Rightarrow$ σ is a k-automorphism of E.

That $\sigma : E \to E'$ is onto follows from the result

"If V is a finite dimensional vector space over F and $T : V \to V$ is a linear transformation, then T is 1-1 iff T is onto". Here $\sigma : E' \to E'$ is a k-homomorphism $\Rightarrow$ σ is a linear transformation as $\sigma(a\beta) = \sigma(a)\, \sigma(\beta) = a\, \sigma(\beta)$ for all $a \in k$, $\beta \in E'$. Also E' as a vector space over k is finite dimensional.

We now give two characterisations of normal extensions. These are very useful in finding whether the given extension is normal or not.

Theorem 45 : *Let K be an algebraic extension of k. Let $\bar{k}$ denote an algebraic closure of k such that $k \subseteq K \subseteq \bar{k}$. Then K/k is normal iff every k-homomorphism of K into $\bar{k}$ is a k-automorphism of K.*

Proof : Let K/k be normal. Let $\sigma : K \to \bar{k}$ be a k-homomorphism. Let $a \in K$. Since K/k is algebraic, a is algebraic over k. Let $p(x) = Irr\,(k, \alpha)$. Let $\sigma(a) = b$. Since $\sigma(p(x)) = p(x)$, b is a zero of $p(x)$ in $\bar{k} \supseteq K$.

Since K/k is normal, $p(x)$ splits in $K[x]$. So, $b \in K$.

Therefore, $\sigma : K \to K$ is a k-homomorphism.

By above lemma, σ is a k-automorphism of K.

Conversely, let $\alpha \in K$ and $p(x) = Irr\,(k, \alpha)$.

Since $\bar{k}$ is an algebraic closure of k, $p(x)$ splits in $\bar{k}[x]$.

Let β be a zero of $p(x)$ in $\bar{k}$.

Then there exists a k-isomorphism $\sigma : k(\alpha) \to k(\beta)$ such that $\sigma(\alpha) = \beta$.

Since $\beta \in k$, $k(\beta) \subseteq \bar{k}$. So, σ is a k-homomorphism from $k(\alpha)$ into $\bar{k}$.

Thus σ can be extended to k-homomorphism $\bar{\sigma} : K \to \bar{k}$.

By hypothesis, $\bar{\sigma}$ is a k-automorphism of K.

So, $\bar{\sigma}(K) = K$. Also $\bar{\sigma}(a) = \sigma(a)$ for all $a \in k(\alpha)$. In particular, $\bar{\sigma}(\alpha) = \sigma(\alpha) = \beta$.

Since $\alpha \in K$, $\bar{\sigma}(\alpha) \in \bar{\sigma}(K) = K \Rightarrow \beta \in K$.

Therefore, $p(x)$ splits in $K[x]$,.

Hence K/k is normal.

Theorem 46 : *Let K be an algebraic extension of k. Then K/k is normal iff K is a minimal splitting field over k of a set of polynomials in $k[x]$.*

Proof : Let K/k be normal. Let $\alpha \in K$. Let $f_\alpha(x) = Irr\ (k, \alpha)$. Then $f_\alpha(x)$ splits in $K[x]$ for all $\alpha \in K$. Let $S = \{f_\alpha \mid \alpha \in K\}$. Let $F = k(\text{zeros of } f_\alpha \text{ in } K,\ \alpha \in K)$.

Then F is a minimal splitting field of S over k.

Clearly, $F \subseteq K$. Also $\alpha \in K \Rightarrow \alpha$ is a zero of $f_\alpha \Rightarrow \alpha \in F$. So, $F = K$. Thus K is a minimal splitting field of S over k.

Conversely, let K be a minimal splitting field of a set S of polynomials over k. Let $\bar{k}$ be an algebraic closure of k such that $k \subseteq K \subseteq \bar{k}$.

Let $\sigma : K \to \bar{k}$ be a k-homomorphism.

Let $a \in K$ be a zero of some $f \in k[x]$ in S.

Then $\sigma(a)$ is also a zero of f as σ is a k-homomorphism.

As f splits in $K[x]$, we can write $f = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$, $\alpha_i \in K$, $\alpha \in k$.

Since $\sigma(\alpha_i)$ is a zero of f for all i, $\sigma(\alpha_i) \in \bar{k}$, $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ as $\bar{k}$ can't have more than n zeros of f. So, $\sigma(\alpha_i) \in K$ for all i.

Let $T = \{\text{zeros of } f \text{ in } K,\ f \in S\}$. Then $\sigma : T \to T$. Also $\sigma : T \to T$ is 1-1 as $\sigma : K \to \bar{k}$ is 1-1.

Let $b \in \sigma(K)$. Then $b = \sigma(c)$, $c \in K$. Now $c \in K \Rightarrow c = \dfrac{f(\beta_1, \ldots, \beta_n)}{g(\beta_1, \ldots, \beta_n)}$, $\beta_i \in T$.

Then $b = \dfrac{f(\sigma(\beta_1), \ldots, \sigma(\beta_n))}{g(\sigma(\beta_1), \ldots, \sigma(\beta_n))} = \dfrac{f(\gamma_1, \ldots, \gamma_n)}{g(\gamma_1, \ldots, \gamma_n)}$, $\gamma_i \in T$

So, $b \in K \Rightarrow \sigma(K) \subseteq K$. Also $d \in K \Rightarrow d = \dfrac{f_1(\delta_1, \ldots, \delta_m)}{g_1(\delta_1, \ldots, \delta_m)}$,

$$\delta_i \in T \Rightarrow d = \frac{f_1(\sigma(u_1), \ldots, \sigma(u_m))}{g_1(\sigma(u_1), \ldots, \sigma(u_m))},\ u_i \in T$$

$$\Rightarrow \qquad d = \frac{\sigma(f_1(u_1, \ldots, u_m))}{\sigma(g_1(u_1, \ldots, u_m))} = \sigma\left(\frac{f_1(u_1, \ldots, u_m)}{g_1(u_1, \ldots, u_m)}\right),\ u_i \in T$$

$$\Rightarrow \qquad d \in \sigma(K) \Rightarrow K \subseteq \sigma(K) \Rightarrow \sigma(K) = K.$$

So, $\sigma : K \subseteq K$ is onto. Thus, σ is a k-automorphism of K. By previous result, K/k is normal.

Summarising, the last two theorems we get

Theorem 47 : *Let K be an algebraic extension of k. Then following are equivalent.*

(*i*) *K/k is normal.*

(*ii*) *Every k-homomorphism of K into* $\bar{k}$ *is a k-automorphism of K where* $\bar{k}$ *is an algebraic closure of k.*

(*iii*) *K is a minimal splitting field of a set of polynomials over k.*

Theorem 48 : *Let F/k be algebraic. If every finite extension of k admits a k-homomorphism into F, then F is an algebraic closure of k.*

Proof : Let $f = a_0 + a_1x + \ldots\ldots + a_nx^n \in k[x]$. Let E be a minimal splitting field of f over k. Then E/k is finite.

By hypothesis, there is a k-homomorphism $\sigma : E \to F$.

Let $\qquad f = \alpha(x - \alpha_1) \ldots\ldots\ldots (x - \alpha_n), \qquad \alpha_i \in E.$

Then $\qquad f = \sigma f = \alpha(x - \sigma(\alpha_1)) \ldots\ldots\ldots (x - \sigma(\alpha_n))$

$\Rightarrow f$ splits in F

$\Rightarrow$ every polynomial over k splits in F.

Let F' be a minimal splitting field of the set of all polynomials over k.

Then $F' = k(\text{zero of } f \in k[x] \text{ in } F) \subseteq F$

Also, $\alpha \in F \Rightarrow \alpha$ is algebraic over k.

Let $p(x) = Irr\,(k, \alpha)$. Then $\alpha \in F$ is a zero of $p(x) \in k[x]$

$\Rightarrow \alpha \in F' \Rightarrow F \subseteq F' \Rightarrow F = F'$.

So, F is an algebraic closure of k.

Theorem 49 : *Let K/k be an algebraic extension. Let* $\bar{k}$ *be an algebraic closure of k such that* $k \subseteq K \subseteq \bar{k}$. *Let F be an algebraically closed field such that* $k \subseteq F$. *Then any k-homomorphism from K into F can be extended to a k-homomorphism from* $\bar{k}$ *into F.*

Proof : Let $\sigma : K \to F$ be a k-homomorphism.

$$\text{Let } S = \left\{ (E, g) \;\middle|\; \begin{array}{l} E \text{ is a subfield of } \bar{k} \text{ and } K \subseteq E \\ g : E \to F \text{ is a homomorphism extending } \sigma \end{array} \right\}.$$

Define a relation $\leq$ on S as follows :

$(E_1, g_1) \leq (E_2, g_2)$ if $E_1 \subseteq E_2$ and g_2 is an extension of g_1 to E_2.

Then $\leq$ is a partial order on S.

Let $\{(E_i, g_i)\}_i$ be a chain in S. Let $E = \bigcup_i E_i$ and define $g : E \to F$ such that $g(\alpha) = g_i(\alpha)$ if $\alpha \in E_i$.

Then $(E, g) \in S$ and is an upper bound of the chain $\{(E_i, g_i)\}$.

By Zorn's lemma S has a maximal element, say (E_0, g_0).

We show that $E_0 = \bar{k}$. Suppose $E_0 \neq \bar{k}$.

Then we can find $a \in \bar{k}$ such that $a \notin E_0$. Since $\bar{k}/k$ is algebraic, a is algebraic over k.

Let $f = Irr(k, a)$. Now $k \subseteq E_0 \Rightarrow f \in E_0[x]$. Since F is algebraically closed, $g_0(f) \in F[x]$ splits in $F[x]$.

Let b be a zero of $g_0(f)$ in F. Then there exists an isomorphism $\theta : E_0(a) \to E_0'(b)$ extending g_0, where $E_0' = g_0(E_0)$.

But $b \in F$, $E_0' \subseteq F \Rightarrow E_0'(b) \subseteq F$. So, $\theta : E_0(a) \to F$ is a homomorphism extending g_0.

Therefore, $(E_0, g_0) \leq (E_0(a), \theta)$ and $E_0 \neq E_0(a) \Rightarrow (E_0, g_0) \neq (E_0(a), \theta)$. This contradicts the maximality of (E_0, g_0).

So, $E_0 = \bar{k}$. Therefore, $g_0 : \bar{k} \to F$ is a k-homomorphism extending σ.

Cor. : Let K/k be algebraic such that $k \subseteq K \subseteq \bar{k}$. Then any k-homomorphism of K into $\bar{k}$ can be extended to a k-homomorphism of $\bar{k}$ into $\bar{k}$.

Proof : Take $F = \bar{k}$ in above theorem.

Cor. : Any two algebraic closures of a field k are k-isomorphic.

Proof : Let K_1, K_2 be algebraic closures of k.

Now $k \subseteq K_1, K_2$. Let $\sigma : k \to K_1$ be the inclusion map *i.e.*, $\sigma(\alpha) = \alpha$ for all $\alpha \in k$.

By taking $K = k$, $\bar{k} = K_2$, $F = k_1$, in above theorem, σ can be extended to a k-homomorphism $\eta : K_2 \to K_1$.

As $K_2 \cong \eta(K_2)$ and K_2 is algebraically closed we find $\eta(K_2)$ is algebraically closed.

Also $k \subseteq K_2 \Rightarrow \eta(K_2)$ can be regarded as an extension of k.

So, we have $k \subseteq \eta(K_2) \subseteq K_1$.

Since K_1/k is algebraic, $K/\eta(K_2)$ is also algebraic.

But $\eta(K_2)$ is algebraically closed $\Rightarrow \eta(K_2)$ has no algebraic extension other than itself $\Rightarrow K_1 = \eta(K_2) \Rightarrow \eta$ is onto $\Rightarrow \eta$ is a k-isomorphism.

Hence, K_1, K_2 are k-isomorphic.

Note : This result was proved earlier also.

We now prove the result on normal extensions stated in the beginning of this section.

Theorem 50 : *Let k, E, K be fields such that $k \subseteq E \subseteq K$ and K/k is normal. Then any k-homomorphism $\sigma : E \to K$ can be extended to a k-automorphism of K.*

Proof : Since K/k is normal, K is a minimal splitting field a set of polynomials over k. Let $\bar{k}$ denote an algebraic closure of k.

Then $\bar{k}$ is a minimal splitting field of the set of all polynomials over k.

So K can be regarded as a subfield of $\bar{k}$.

Now $\sigma : E \to K$ is a k-homomorphism.

Thus $\sigma : E \to \bar{k}$ is a k-homomorphism.

Since K/k is algebraic, so is E/k. Now $k \subseteq E \subseteq \bar{k}$, E/k is algebraic.

By previous theorem, σ can be extended to a k-homomorphism $\tau : \bar{k} \to \bar{k}$. Therefore, $\tau : K \to \bar{k}$ is also a k-homomorphism.

Again, K/k is normal $\Rightarrow$ τ is a k-automorphism of K.

This proves the result.

Let M, N be extensions of a field k such that M, N are contained in a field L. Then MN is defined as the smallest subfield of L containing M and N.

Let $M[N] = \{a_1 b_1 + \ldots\ldots + a_n b_n \mid a_i \in M, b_i \in N\}$.
$n = \text{finite}$

Then $M[N]$ is an integral domain. Let K be field of quotients of $M[N]$. Clearly, $M \subseteq M[N]$, $N \subseteq M[N]$.

So, $\qquad M, N \subseteq M[N] \subseteq K.$

But MN is the smallest field containing M, N, $MN \subseteq K$.

Also, $\displaystyle\sum_{i=1}^{n} a_i b_i \in M[N]$, for all $a_i \in M$, $b_i \in N$

$$\Rightarrow \sum_{i=1}^{n} a_i b_i \in MN, \text{ as } \left.\begin{array}{l} a_i \in M \Rightarrow a_i \in MN \\ b_i \in N \Rightarrow b_i \in MN \end{array}\right\} \Rightarrow \sum_{i=1}^{n} a_i b_i \in MN$$

$\Rightarrow$ $M[N] \subseteq MN$.

But K is the smallest field containing $M[N]$ $\Rightarrow$ $K \subseteq MN$

$\Rightarrow$ $K = MN$

$\Rightarrow$ MN is a quotient field of $M[N]$.

Lemma : *Let K_1, K_2 be extensions of a field k contained in a field K and let σ be a k-homomorphism of K in some field L. Then*

$$\sigma(K_1 K_2) = \sigma(K_1)\,\sigma(K_2).$$

Proof : Let $\qquad \alpha = \dfrac{a_1 b_1 + \ldots\ldots + a_n b_n}{a_1' b_1' + \ldots\ldots + a_n' b_n'} \in K_1 K_2$

where $\qquad a_i,\ a_i' \in K_1,\ b_i,\ b_i' \in K_2$

Then $\qquad \sigma(\alpha) = \dfrac{\sigma(a_1)\sigma(b_1) + \ldots\ldots + \sigma(a_n)\sigma(b_n)}{\sigma(a_1')\sigma(b_1') + \ldots\ldots + \sigma(a_n')\sigma(b_n')} \in \sigma(K_1)\,\sigma(K_2)$

$\Rightarrow \qquad \sigma(K_1 K_2) \subseteq \sigma(K_1)\,\sigma(K_2)$

Let $\qquad \beta \in \sigma(K_1)\,\sigma(K_2)$.

Then $$\beta = \frac{\sigma(c_1)\sigma(d_1)+.....+\sigma(c_r)\sigma(d_r)}{\sigma(c_1')\sigma(d_1')+.....+\sigma(c_r')\sigma(d_r')}$$

$$= \sigma(\alpha), \text{ where } \alpha = \frac{c_1d_1+.....+c_rd_r}{c_1'd_1'+.....+c_r'd_r'} \in K_1K_2$$

$\Rightarrow$ $\beta \in \sigma(K_1K_2)$

$\Rightarrow$ $\sigma(K_1)\sigma(K_2) \subseteq \sigma(K_1K_2)$

$\Rightarrow$ $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2)$.

Theorem 51 : *If E, F are normal extensions of k, then EF and $E \cap F$ are normal over k.*

Proof (*i*) : Let $\bar{k}$ denote an algebraic closure of k. Let σ be a k-homomorphism from EF into $\bar{k}$ such that $k \subseteq EF \subseteq \bar{k}$.

Now $\sigma(EF) = \sigma(E)\sigma(F)$ by above lemma.

Since $E, F \subseteq EF$, σ is also k-homomorphism from E into $\bar{k}$ and F into $\bar{k}$. Also, E, F are normal over $k \Rightarrow \sigma : E \to E$ and $\sigma : F \to F$ are k-automorphisms

$\Rightarrow$ $\sigma(E) = E$, $\sigma(F) = F$

$\Rightarrow$ $\sigma(EF) = EF$

Now $\sigma : EF \to \bar{k}$ is also a k-homomorphism from EF into EF. But $\sigma(EF) = EF$

$\Rightarrow$ $\sigma : EF \to EF$ is onto

So, $\sigma : EF \to EF$ is a k-automorphism

$\Rightarrow$ EF/k is normal.

(*ii*) Let σ be a k-homomorphism from $E \cap F$ into $\bar{k}$ such that $k \subseteq E \cap F \subseteq \bar{k}$. Then σ can be extended to k-homomorphism $\eta : \bar{k} \to \bar{k}$.

Since E/k is normal, E is a minimal splitting field of a set of polynomials over k. However, $\bar{k}$ is a minimal splitting field of the set of all polynomials over k. So, E can be regarded as a subfield of $\bar{k}$. Therefore, $k \subseteq E \subseteq \bar{k}$. Similarly $k \subseteq F \subseteq \bar{k}$.

Let $\eta/E = \eta_1$, $\eta/F = \eta_2$.

Now $\eta_1 : E \to \bar{k}$, $\eta_2 : F \to \bar{k}$ are k-homomorphisms. Since E/k, F/k are normal, η_1 and η_2 are k-automorphisms of E and F respectively. So, $\eta_1(E) = E$, $\eta_2(F) = F$. Now $E \cap F \subseteq E$, $F \subseteq \bar{k}$.

Thus, $$\begin{aligned}\eta(E \cap F) &= \eta(E) \cap \eta(F)\\ &= \eta_1(E) \cap \eta_2(F)\\ &= E \cap F.\end{aligned}$$

But $\eta | E \cap F = \sigma$

$\Rightarrow$ $\sigma(E \cap F) = E \cap F$

$\Rightarrow$ σ is a k-automorphism of $E \cap F$

$\Rightarrow$ $E \cap F/k$ is normal.

Automorphism of field extensions

The purpose of this section is to find conditions under which a finite extension F/K is seperable in terms of k-automorphisms of F. We first show that the number of k-automorphisms of F is at most $n = [F : K]$. We then show that the upper bound n is achieved iff F/K is both normal and seperable.

Definition : Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be homomorphisms from a field E into a field E'. Then, $\sigma_i s$ are called *linearly independent* over E' if $\alpha_1\sigma_1 + \ldots + \alpha_n\sigma_n = 0, \Rightarrow \alpha_i = 0 \ \forall\ i$ where $\alpha_i \in E'$.

Note, $\alpha_i\sigma_i : E \to E'$ s.t., $(\alpha_i\sigma_i)(a) = \alpha_i(\sigma_i(a)) \quad \forall\ a \in E$.

In the following result, we show that any family of homomorphisms from a field into another field is linearly independent.

Theorem 52 : (Dedekind). *Let $\{\sigma_i\}_i$ be a family of distinct homomorphisms from a field E into a field E'. Then $\{\sigma_i\}_i$ is linearly independent over E'.*

Proof : Suppose $\{\sigma_i\}_i$ is not linearly independent over E'. Then $\exists$ finite subset of $\{\sigma_i\}_i$ which is not linearly independent over E'. (i.e., it is linearly dependent over E'). Let $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ be a minimal linearly dependent subset of $\{\sigma_i\}_i$ over E'.

So, $\exists\ \alpha_1, \alpha_2, \ldots, \alpha_r \in E'$ s.t.,

$$\alpha_1\sigma_1 + \ldots + \alpha_r\sigma_r = 0 \qquad \text{and some } \alpha_i \neq 0.$$

$$\Rightarrow \qquad (\alpha_1\sigma_1 + \ldots + \alpha_r\sigma_r)(a) = 0 \qquad \forall\ a \in E$$

$$\Rightarrow \qquad \alpha_1\sigma_1(a) + \ldots + \alpha_r\sigma_r(a) = 0 \qquad \forall\ a \in E$$

Suppose $\alpha_1 \neq 0$.

Now
$$\sigma_1(a) = (-\alpha_1^{-1}\alpha_2)\sigma_2(a) + \ldots + (-\alpha_1^{-1}\alpha_r)\sigma_2(a) \qquad \forall\ a \in E$$

$$\sigma_1(a) = \beta_2\sigma_2(a) + \ldots + \beta_r\sigma_r(a),\ \beta_i = -\alpha_1^{-1}\alpha_i \in E',\ \forall a \in E \qquad (i)$$

So,
$$\sigma_1(ab) = \beta_2\sigma_2(ab) + \ldots + \beta_r\sigma_r(ab) \qquad \forall\ a, b \in E$$

$$\Rightarrow \qquad \sigma_1(a)\ \sigma_1(b) = \beta_2\sigma_2(a)\sigma_2(b) + \ldots + \beta_r\sigma_r(a)\sigma_r(b) \qquad \forall\ a, b \in E \qquad (ii)$$

Consider $(ii) - \sigma_1(b)\ (i)$.

Then
$$0 = \beta_2\sigma_2(a)\,(\sigma_2(b) - \sigma_1(b)) + \ldots + \beta_r\sigma_r(a)\,(\sigma_r(b) - \sigma_1(b))$$

$$= \sum_2^r \beta_i(\sigma_i(b) - \sigma_1(b))\,\sigma_i(a) \qquad \forall\ a \in E$$

$$\Rightarrow \qquad 0 = \sum_2^r \beta_i(\sigma_i(b) - \sigma_1(b))\,\sigma_i$$

$$\Rightarrow \qquad \beta_i(\sigma_i(b) - \sigma_1(b)) = 0 \qquad \forall\ i = 2, 3, \ldots, r,\ \forall\ b \in E$$

as $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ is a minimal linearly dependent subset of $\{\sigma_i\}_i$.

Since $\sigma_i \neq \sigma_1 \ \forall\, i > 1, \ \exists\, c_i \in E$ s.t., $\sigma_i(c_i) \neq \sigma_1(c_i)$.

Now $\beta_i(\sigma_i(c_i) - \sigma_1(c_i) = 0 \qquad \forall\, i = 2, 3, \ldots\ldots, r$

$\Rightarrow \beta_i = 0 \qquad \forall\, i = 2, 3, \ldots\ldots, r.$

So, $\sigma_1(a) = 0 \qquad \forall\, a \in E,$ by (i)

$\Rightarrow \sigma_1(1) = 0$

$\Rightarrow 1 = 0,$ which is not true.

Thus, $\{\sigma_i\}_i$ is a linearly independent set over E'.

Theorem 53 : *Let E, E' be extensions of K. Let $[E : K] = n$. Then, there are at most n K-homomorphisms from E into E'.*

Proof : Let $\{u_1, u_2, \ldots\ldots, u_n\}$ be a basis of E/K. Let $\sigma_0, \sigma_1, \ldots\ldots, \sigma_n$ be $n+1$ distinct K-homomorphisms from E into E'.

Consider the system of equations $\displaystyle\sum_{i=0}^{n} \sigma_i(u_j)x_i = 0, \ j = 1, 2, \ldots\ldots, n.$

Then, we have n equations in $n+1$ unknowns $x_i s \in E'$. Since the number of equations is less than number of unknowns, the above system of equations has a non zero solution, say $c_0, c_1, \ldots\ldots, c_n \in E'$ where some $c_i \neq 0$.

Let $a \in E$. Since $\{u_1, u_2, \ldots\ldots, u_n\}$ spans E/K, $a = \alpha_1 u_1 + \ldots\ldots + \alpha_n u_n, \qquad \alpha_i \in K$

Thus
$$\begin{aligned}
\sum_{i=0}^{n} \sigma_i(a)c_i &= \sum_i \sigma_i\Big(\sum_j \alpha_j u_j\Big)c_i \\
&= \sum_i \sum_j (\sigma_i(\alpha_j)\sigma_i(u_j))c_i \\
&= \sum_i \sum_j (\alpha_j \sigma_i(u_j))c_i \\
&= \sum_j \alpha_j\Big(\sum_i \sigma_i(u_j))c_i\Big) \\
&= 0 \qquad \text{as } \sum_i \sigma_i(u_j)c_i = 0
\end{aligned}$$

$$\Rightarrow \sum_{i=0}^{n} c_i\sigma_i(a) = 0 \qquad \forall\, a \in E$$

$$\Rightarrow \sum_{i=0}^{n} c_i\sigma_i = 0 \Rightarrow c_i = 0 \ \ \forall\, i \text{ by above theorem.}$$

But some $c_i \neq 0$. So, we get a contradiction. Thus, there are at most n K-homomorphisms from E into E'.

Cor. : There are at most n K-automorphisms of E, where $n = [E : K]$.

Proof : Take $E' = E$ in above theorem. By automorphism of E, we mean isomorphism of E into E. Now any K-homomorphism from E into E is a linear

transformation from E into E as vector space over K. Also, any homomorphism from E into E is 1-1 and so onto as $[E : K]$ = finite. By above theorem, there are at most n K-automorphisms of E where $n = [E : K]$.

Example 12 : Define $\theta : \mathbf{C} \to \mathbf{C}$ s.t.,

$$\theta(z) = \bar{z}\ , \text{ where } \bar{z} = \text{conjugate of } z$$

Then θ is $\mathbf{R}$-homomorphism and $\theta \neq I$. So, θ, I are two distinct $\mathbf{R}$-homomorphisms of $\mathbf{C}$ into $\mathbf{C}$. But $[\mathbf{C} : \mathbf{R}] = 2 \Rightarrow$ there are at most two $\mathbf{R}$-automorphisms of $\mathbf{C}$. Also, any $\mathbf{R}$-homomorphism of $\mathbf{C}$ into $\mathbf{C}$ is an $\mathbf{R}$-automorphism of $\mathbf{C}$. So, θ, I are only $\mathbf{R}$-automorphisms of $\mathbf{C}$. Note, $\mathbf{C}/\mathbf{R}$ is normal as $[\mathbf{C} : \mathbf{R}] = 2$ and $\mathbf{C}/\mathbf{R}$ is seperable as $\text{char}\,\mathbf{R} = 0 \Rightarrow \mathbf{R}$ is perfect $\Rightarrow$ every algebraic extension of $\mathbf{R}$ is seperable.

Example 13 : Let α be the real cube root of $f(x) = x^3 - 2$. Let $F = \mathbf{Q}(\alpha) \subseteq \mathbf{R}$. Let θ be a $\mathbf{Q}$-automorphism of F.

Since α is a root of $f(x)$ in $\mathbf{R}$, $\theta(\alpha)$ is a root of $\theta(f(x)) = f(x)$ in $\mathbf{R}$.

So, $\theta(\alpha) = \alpha$. But $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg\, Irr\,(\mathbf{Q}, \alpha) = \deg\, f(x) = 3$ and $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

$\Rightarrow$ $\mathbf{Q}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbf{Q}\}$.

Since $\theta(a_i) = a_i$ and $\theta(\alpha) = \alpha$, θ fixes every element of $\mathbf{Q}(\alpha)$.

So, $\theta = I \Rightarrow$ Identity map is the only $\mathbf{Q}$-automorphism of $F = \mathbf{Q}(\alpha)$.

Note $\mathbf{Q}(\alpha)/\mathbf{Q}$ is seperable as $\text{char}\,\mathbf{Q} = 0 \Rightarrow \mathbf{Q}$ is perfect $\Rightarrow$ every algebraic extension of $\mathbf{Q}$ is seperable.

As seen before $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not normal.

Thus, we notice that if E/K is seperable but not normal, then one may not get the *full quota* (i.e., $[E : K]$) of K-automorphisms of E.

Example 14 : Let $\text{char}\,K = p$ and $F = K(t)$. Then $x^p - t$ is irreducible over F.

Let α be a root of $f(x)$ in some extension of F.

Now $f(x) = x^p - t$ is irreducible over $F \Rightarrow [F(\alpha) : F] = p$

$\Rightarrow$ $\{1, \alpha, \ldots\ldots, \alpha^{p-1}\}$ is a basis of $F(\alpha)/F$.

So, $$F(\alpha) = \{\sum_{i=0}^{p-1} a_i\alpha^i \mid a_i \in F\}.$$

If θ is F-automorphism of $F(\alpha)$, then $\theta(\alpha)$ is a root of $f(x) = \theta(f(x))$ in $F(\alpha)$.

But α is the only root of $f(x)$ in any extension of F

$\Rightarrow$ $\theta(\alpha) = \alpha \Rightarrow \theta$ fixes every element of $F(\alpha)$

$\Rightarrow$ θ is the identity map.

Thus, identity map is the only F-automorphism of $F(\alpha)$.

Since α is not a simple root of $f(x)$, α is not seperable over F.

Therefore, if E/K is not seperable then one may not get $[E : K]$, K-automorphisms of E.

The above two examples clearly demonstrate that in order that an extension E/K has $[E : K]$, K-automorphisms of E, E/K should be both normal and seperable. In the first example, we saw that we do get $[E : K]$, K-automorphisms of E when E/K is both normal and seperable. We would like to prove this in general.

Theorem 54 : *Let $K \subseteq L \subseteq F \subseteq E$ be a tower of fields. Suppose E/K is finite normal. If r is the number of K-homomorphisms from L into E and s the number of L-homomorphisms from F into E, then the number of K-homomorphisms from F into E is rs.*

Proof : Let $\sigma_1, \ldots, \sigma_r$ be the K-homomorphisms of L into E and $\tau_1, \tau_2, \ldots, \tau_s$ be the L-homomorphisms from F into E. Since E/K is finite normal, each σ_i can be extended to K-automorphisms $\overline{\sigma_i}$ of E.

We show that $\{\overline{\sigma_i}\tau_j \mid 1 \le i \le r,\ 1 \le j \le s\}$ is the set of distinct K-homomorphisms from F into E.

Suppose $\overline{\sigma_i}\tau_j = \overline{\sigma_p}\,\tau_q$. Then $\overline{\sigma_i}\tau_j(a) = \overline{\sigma_p}\,\tau_q(a)$, $\forall\, a \in F$

$\Rightarrow\ \overline{\sigma_i}\tau_j(l) = \overline{\sigma_p}\,\tau_q(l) \qquad \forall\, l \in L$

$\Rightarrow\ \overline{\sigma_i}(l) = \overline{\sigma_p}(l) \qquad \forall\, l \in L$

$\Rightarrow\ \sigma_i(l) = \sigma_p(l) \qquad \forall\, l \in L$

$\Rightarrow\ \sigma_i = \sigma_p \Rightarrow i = p \ \Rightarrow\ \tau_j = \tau_q \ \Rightarrow\ j = q.$

Let σ be any K-homomorphism from F into E. Then σ/L is a K-homomorphism from L into E

$\Rightarrow\ \sigma/L = \sigma_i$ for some i.

Then $\overline{\sigma_i}^{-1}\sigma$ is K-homomorphism from F into E.

So, $\sigma_i^{-1}\sigma(l) = \sigma_i^{-1}\sigma_i(l) = \sigma_i^{-1}\overline{\sigma_i}(l) = l \qquad \forall\, l \in L$

$\Rightarrow\ \overline{\sigma_i}^{-1}\sigma$ is L-homomorphism from F into E

$\Rightarrow\ \sigma_i^{-1}\sigma = \tau_j$ for some $j \Rightarrow \sigma = \overline{\sigma_i}\tau_j$.

Thus, $\overline{\sigma_i}\tau_j$ are the only K-homomorphisms from F into E and so, there are exactly rs K-homomorphisms from F into E.

Theorem 55 : *Let $K \subseteq E \subseteq E'$ be a tower of fields. Suppose E'/K is finite normal. Then E/K is seperable if and only if the number of K-homomorphisms from E into E' is $[E : K]$.*

Proof : Suppose E/K is seperable. We prove the result by induction on $n = [E : K]$.

If $n = 1$, then $E = K$ and $I : E \to E'$ s.t., $I(a) = a$ is K-homomorphism from E into E'.

So, the result is true for $n = 1$.

Let $n > 1$. Assume that the result is true for all integers $< n$.

Let $a \in E$, $a \notin K$.

Now $K \subseteq K(a) \subseteq E \subseteq E'$ and E'/K is finite normal $\Rightarrow$ $E'/K(a)$ is finite normal.

Also, $[E : K] = [E : K(a)]\,[K(a) : K]$ and $[K(a) : K] > 1$

$\Rightarrow \quad [E : K(a)] < [E : K] = n.$

Since E/K is seperable $E/K(a)$ is also seperable.

By induction hypothesis (applied to tower of fields $K(a) \subseteq E \subseteq E'$), the number of $K(a)$-homomorphisms from E into E' is $[E : K(a)]$.

Let $p(x) = Irr\,(K, a)$. Since $a \in E$, a is seperable over K. So, all roots of $p(x)$ are simple.

Let $\deg p(x) = r$. Since E'/K is normal, $p(x)$ splits in E' as $a \in E \subseteq E'$.

Let $a = a_1, a_2, \ldots, a_r$ be distinct roots of $p(x)$ in E'. Then $\exists$ K-isomorphisms.

$\sigma_i : K(a) \to K(a_i)$ s.t., $\sigma_i(a) = a_i \quad \forall\, i = 1, 2, \ldots, r$. $\sigma_i s$, $a_i s$ being distinct.

Since $a_i \in E'$, $\sigma_i s$ are r K-homomorphisms from $K(a)$ into E'.

Also as $[K(a) : K] = \deg Irr\,(K, a) = \deg p(x) = r$, these σ_i's are only K-homomorphisms from $K(a)$ into E'.

By previous theorem these are exactly $[E : K(a)]\,[K(a) : K] = [E : K]$, K-homomorphisms from E into E'.

So, the result is true in this case. By induction the result is true for all $n \geq 1$.

Conversely, let there be $n = [E : K]$ K-homomorphisms from E into E'. Let $a \in E$.

Now, the number m of K-homomorphisms from $K(a)$ into E' is at most $r = [K(a) : K]$.

Let $m < r$. Let s be the number of $K(a)$-homomorphisms from E into E'. Then

$$s \leq [E : K(a)] = \frac{[E : K]}{[K(a) : K]} = \frac{n}{r}.$$

By above theorem, the number of K-automorphisms from E into E' is $ms < r\dfrac{n}{r} = n$, a contradiction. So, $m = r$. That is, the number of K-homomorphisms from $K(a)$ into E' is $[K(a) : K] = \deg Irr\,(K, a)$.

Let $p(x) = Irr\,(K, a)$, $\deg p(x) = r$.

Since E'/K is normal, $p(x)$ splits in E' as $a \in E \subseteq E'$.

Let $a = a_1, a_2, \ldots, a_t$ be distinct roots of $p(x)$ in E'.

Then, for each i $\exists$ K-isomorphism $\theta_i : K(a) \to K(a_i)$ s.t., $\theta_i(a) = a_i$.

Since $a_i \in E'$, $K(a_i) \subseteq E'$. So, $\theta_i : K(a) \to E'$ is K-homomorphism.

Again as $a_i s$ are distinct, $\theta_i s$ are also distinct K-homomorphisms from $K(a)$ into E'.

If θ is a K-homomorphism from $K(a)$ into E', then a is a root of $p(x)$ in E

$\Rightarrow$ $\theta(a)$ is a root of $\theta(p(x)) = p(x)$ in E'

$\Rightarrow$ $\theta(a) = a_i$ for some $i \Rightarrow \theta(a) = \theta_i(a)$ for some $i \Rightarrow \theta = \theta_i$ for some i.

So, $\theta_1, \theta_2, \ldots, \theta_t$ are the only K-homomorphisms from $K(a)$ into E

$\Rightarrow$ $t = [K(a) : K] = \deg p(x) = r$.

$\Rightarrow$ all roots of $p(x)$ are distinct and so simple

$\Rightarrow$ a is seperable over K. Thus, E/K is seperable.

Cor. 1 : Let E/K be finite normal. Then E/K is seperable if and only if the number of K-automorphisms of E is $[E : K] = n$.

Proof : Since E/K is finite, a K-homomorphism of E is K-automorphism of E and conversely. The result then follows by above theorem.

Cor. 2 : Let $K \subseteq E \subseteq E'$ be a tower of fields s.t., E/K and E'/E are finite seperable. Then E'/K is also finite seperable.

Proof : Let $[E : K] = r$, $[E' : E] = s$. Since E/K, E'/E are finite so is E'/K.

Thus $\exists$ an extension F of K s.t., F/K is finite normal and $K \subseteq E \subseteq E' \subseteq F$.

By above theorem since E/K is seperable, there are r K-homomorphisms from E into F.

Now F/K is normal $\Rightarrow$ F/E is also normal.

As E'/E is seperable, there are s E-homomorphisms from E' into F.

Therefore, there are rs K-homomorphisms from E' into F. But $rs = [E' : K]$.

By above theorem then E'/K is finite seperable.

Cor. 3 : Let E be an extension of K. Let $a_1, a_2, \ldots, a_n \in E$ be seperable over K. Then $K(a_1, a_2, \ldots, a_n)/K$ is seperable.

Proof : We prove the result by induction on n. Since $a_1, a_2, \ldots, a_n$ are seperable over K, $a_1, a_2, \ldots, a_n$ are algebraic over K. So, $K(a_1, a_2, \ldots, a_n)/K$ is finite. Let E'/K be finite normal extension s.t., $K \subseteq K(a_1, \ldots, a_n) \subseteq E'$. Let $n = 1$. Let $p(x) = Irr\,(K, a_1)$, $\deg\ p(x) = r$. Then $\exists\, r$ K-homomorphisms from $K(a_1)$ into E' as seen in above theorem. But $r = [K(a_1) : K]$. By above theorem, $K(a_1)/K$ is seperable. So, the result is true for $n = 1$. Let $n > 1$. Assume that the result is true for all integers $< n$. By induction hypothesis, $K(a_1, \ldots, a_{n-1})/K$ is finite seperable. Also, a_n is seperable over K and $K \subseteq K(a_1, \ldots, a_{n-1}) \subseteq K(a_1, \ldots, a_n) \Rightarrow a_n$ is seperable over $K(a_1, \ldots, a_{n-1}) \Rightarrow K(a_1, \ldots, a_n)/K(a_1, \ldots, a_n)$ is finite seperable. By above corollary, $K(a_1, \ldots, a_n)/K$ is seperable. By induction the result is true $\forall\, n \geq 1$.

Cor. 4 : Let $F \subseteq K \subseteq E$ be a tower of fields s.t., E/K and K/F are seperable. Then, E/F is also seperable.

Proof : Let $a \in E$.

Let $\quad p(x) = Irr\,(K, a)$

$$= b_0 + b_1 x + \ldots\ldots + b_r x^r, \qquad b_i \in K$$

Let $\quad K' = F(b_0, b_1, \ldots, b_r) \subseteq K$

$b_i \in K \Rightarrow b_i$ is seperable over F

$\Rightarrow K'/F$ is seperable by above Cor.

Since $p(x)$ is irreducible over K, it is also irreducible over K'.

So, $\quad p(x) = Irr\,(K', a)$

Now $K' \subseteq K \subseteq E$ and $a \in E$ is seperable over $K \Rightarrow p'(a) \neq 0 \Rightarrow a$ is seperable over $K' \Rightarrow K'(a)/K'$ is seperable and finite. Also, K'/F is finite seperable.

So, $K'(a)/F$ is finite seperable.

$\Rightarrow a$ is seperable over F.

Thus, E/F is seperable.

Theorem 56 : *Let $K \subseteq E \subseteq E'$ be a tower of fields s.t., E'/K is finite normal. Then following are equivalent:*

(a) There are exactly $n = [E : K]$ K-homomorphisms from E into E'.

(b) E/K is seperable.

(c) E/K is generated by seperable elements.

Proof $(a) \Leftrightarrow (b)$ follows from previous theorem

$(b) \Leftrightarrow (c)$ $[E : K] = n \Rightarrow E = K(a_1, \ldots, a_n)$. Since $a_i \in E$, a_i is seperable over K. So, E is generated by seperable elements over K.

$(c) \Rightarrow (b)$. Let $E = K(S)$, where $S \subseteq E$ is a set of seperable elements over K. Let $a \in E$. then $a = \dfrac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}$, $f, g \in K[x_1, \ldots, x_n]$, $u_i \in S$. So, $a \in K(u_1, u_2, \ldots, u_n)$. Since $u_1, u_2, \ldots, u_n$ are seperable over K, $K(u_1, u_2, \ldots, u_n)/K$ is seperable. Therefore, a is seperable over K. Thus, E/K is seperable. This proves (b).

Theorem 58 (Artin's) : *Let E be a field, G the group of automorphisms of E and suppose K is the set of elements of E fixed by G. Then K is a subfield of E, called the fixed field of G. E/K is finite if and only if G is finite. In that case, $[E : K] = o(G)$.*

Proof : $K = \{a \in E \mid \sigma(a) = a \quad \forall\, \sigma \in G\}$

$0, 1 \in K \Rightarrow K \neq \varphi$.

Let $a, b \in K$. Then $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = a \pm b \Rightarrow a \pm b \in K$. Also $\sigma(ab) = \sigma(a)\,\sigma(b) = ab \Rightarrow ab \in K$. If $b \neq 0$, then $\sigma(ab^{-1}) = \sigma(a)\,\sigma(b)^{-1} = ab^{-1}$ $\Rightarrow ab^{-1} \in K$. So, K is a subfield of E.

Clearly, G is a group of K-automorphism of E. If E/K is finite, then the number of K-automorphisms of E is at most $[E : K]$. So, G is finite. Suppose $o(G) = r$. Let $u_0, u_1, \ldots, u_r \in E$ be linearly independent over K. Consider the r equations (in $r+1$ unknowns $x_j s$ in E)

$$\sum_{j=0}^{r} \sigma(u_j) x_j = 0 \qquad \text{for all } \sigma \in G$$

Since the number of equations is less then the number of unknowns, the system of equations has a non-zero solution.

Let $(a_0, a_1, \ldots, a_s, 0, 0, \ldots, 0)$ be a non zero solution of least length $s + 1 (a_i \neq 0\ \forall\, i = 0, 1, \ldots, s)$.

Then $\sigma(u_0) a_0 = -\sigma(u_1) a_1 + \ldots + -\sigma(u_s) a_s$

$$\Rightarrow \qquad \sigma(u_0) = \sigma(u_1)b_1 + \ldots\ldots + \sigma(u_s)b_s \qquad \text{for all } \sigma \in G \qquad \ldots\ldots (i)$$

Take $\sigma = I$. Then $u_0 = u_1 b_1 + \ldots\ldots + u_s b_s$

If $b_i \in K$ for all i, then

$(-1)u_0 + b_1 u_1 + \ldots\ldots + b_s u_s = 0$, contradicting that $u_0, u_1, \ldots, u_s$ are linearly independent over K.

So, some $b_i \notin K$. Let $b_1 \notin K$.

Then $\exists\, \tau \in G$ s.t., $\tau(b_1) \neq b_1$.

Replace σ by $\tau^{-1}\sigma$ in (i) to get

$$\tau^{-1}\sigma(u_0) = \sum_{j=1}^{r} \tau^{-1}\sigma(u_j)b_j \qquad \text{for all } \sigma \in G$$

$$\Rightarrow \tau(\tau^{-1}\sigma(u_0)) = \sigma(u_0) = \sum_{j=1}^{r} \sigma(u_j)\,\tau(b_j) \qquad \text{for all } \sigma \in G \qquad \ldots\ldots(ii)$$

Then $(ii)\ldots(i)$ gives

$$\sum_{j=1}^{r} \sigma(u_j)\,(\tau(b_j) - b_j) = 0, \qquad \text{for all } \sigma \in G$$

$$\Rightarrow \sum_{j=1}^{r} \sigma(u_j)c_j = 0, \text{ for all } \sigma \in G, \text{ where } c_j = \tau(b_j) - b_j$$

Since $\qquad c_1 = \tau(b_1) - b_1 \neq 0.$

We have a non zero solution $(0, c_1, \ldots\ldots, c_s, 0, \ldots, 0)$ of length less then $s+1$, a contradiction.

Therefore, $r+1$ elements in E are not linearly independent over K

$\Rightarrow [E : K] \leq r \Rightarrow E/K$ is finite.

So, $[E : K] \leq o(G)$. But $o(G) \leq [E : K] \Rightarrow o(G) = [E : K]$.

Problem 31 : *Let E be a field with n distinct automorphisms and suppose K is the fixed field of the set of automorphisms. Show that $[E : K] \geq n$.*

Solution : Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be distinct automorphisms of E. Let G be the group generated by $\sigma_1, \sigma_2, \ldots\ldots, \sigma_n$. Then $o(G) \geq n$. If F is the fixed field of G, then $K \subseteq F \subseteq E$. By Artin's theorem, $[E : F] = o(G) \geq n$.

So, $\qquad [E : K] \geq [E : F] \geq n.$

Problem 32 : *Find the fixed field F of $K(x)$ under the automorphisms $x \to 1-x$, $x \to \frac{1}{x}$. Show that the degree is 6. Verify that $\dfrac{(x^2-x+1)^3}{(x^2-x)^2}$ lies in F and use this to find an equation for x over F.*

Solution : Let $\sigma(x) = 1 - x$, $\eta(x) = \frac{1}{x}$. Then $\sigma, \eta, \sigma\eta, \eta\sigma, \sigma\eta\sigma, I$ are six distinct automorphisms of $E = K(x)$. Let F' be the fixed field of these 6 automorphisms of E. So, $F \subseteq F' \subseteq E$. By previous problem, $[E : F'] \geq 6 \Rightarrow [E : F] \geq 6$.

Let $\quad g(x) = \dfrac{(x^2 - x + 1)^3}{(x^2 - x)^2}$

Then $\quad \eta(g(x)) = g(x), \quad \sigma(g(x)) = g(x)$

$\Rightarrow \quad g(x) \in F$

Let $\quad L = K(g(x)) \subseteq F \subseteq E$

Then $\quad [E : L] = [E : F]\,[F : L] \geq 6.$

Now $\quad L(x) = K(x) = E.$

Also, $\quad (x^2 - x + 1)^3 - g(x)\ x^2(x-1)^2 = 0$

$\Rightarrow x$ is a root of a polynomial of degree 6 with coefficients in L

$\Rightarrow [L(x) : L] \leq 6$

$\Rightarrow [E : L] \leq 6 \Rightarrow [E : L] = 6$

So, $\quad [E : F]\,[F : L] = 6 \leq [E : F]$

$\Rightarrow [F : L] \leq 1$

$\Rightarrow F = L = K(g(x))$

$\Rightarrow (x^2 - x + 1)^3 - g(x)\,x^2(x-1)^2 = 0$ is an equation for x over F.

Problem 33 : *If φ is an automorphism of the field of real numbers* **R**, *show that φ leaves every element of* **R** *fixed.*

Solution : Since $\varphi(1) = 1$, $\varphi(n) = n$ for any positive integer n.

Also, $\varphi(0) = 0$, $\varphi(-n) = -\varphi(n) = -n$ and $\varphi(m^{-1}) = \varphi(m)^{-1} = m^{-1}$ for all non zero integers m.

Thus, $\varphi(nm^{-1}) = \varphi(n)\,\varphi(m)^{-1} = nm^{-1}$.

Let $r \in \mathbf{R}$ and $r > 0$. Then $r = s^2$, $s \in \mathbf{R}$.

So, $\varphi(r) = \varphi(s)^2 > 0$.

Also, $r > t \Rightarrow r - t > 0 \Rightarrow \varphi(r - t) > 0 \Rightarrow \varphi(r) > \varphi(t)$.

Let $r \in \mathbf{R}$ and let $p < r < q$, where $p, q \in \mathbf{Q}$.

Then $\varphi(p) = p < \varphi(r) < \varphi(q) = q$.

Thus, given any rational numbers p, q such that $p < r < q$, both r and $\varphi(r)$ are in the interval between p and q.

So, $\varphi(r) = r$ for all $r \in \mathbf{R}$. Hence, identity is the only automorphism of **R**.

Theorem 58 : *Let K/F be a finite seperable extension. Then $K = F(a)$ for some $a \in K$.*

Proof : Since K/F is finite, $K = F(a_1, \ldots\ldots, a_n)$ for some $a_1, \ldots\ldots, a_n \in K$. It is enough to prove the theorem for $n = 2$.

Let $K = k(\alpha, \beta)$. Then α, β are seperable over F.

Case 1 : Let F be an infinite field.

Let $$p(x) = Irr(F, \alpha)$$
$$q(x) = Irr(F, \beta)$$

Let $\alpha = \alpha_1, \ldots, \alpha_n$, $\beta = \beta_1, \ldots, \beta_m$ be the roots of $p(x)$, $q(x)$ respectively in a splitting field of $p(x)Tq(x)$. Since K is finite, there exists $a \in K$ such that $a \neq 0$ and $a \neq \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$ for $1 \leq i \leq n$, $2 \leq j \leq m$.

Since α, β are seperable over F, $\alpha_i s$ and $\beta_j s$ are distinct roots of $p(x), q(x)$ respectively.

Let $\theta = a\beta + \alpha$. We show that $F(\theta) = F(\alpha, \beta)$. Clearly $F(\theta) \subseteq F(\alpha, \beta)$.

Define $$g(x) = p(\theta - ax).$$

Then $$g(\beta) = p(\theta - a\beta) = p(\alpha) = 0.$$

Also, $g(\beta_j) = p(\theta - a\beta_j) \neq 0$ for all $j = 2, \ldots, m$.
(For, $p(\theta - a\beta j) = 0 \Rightarrow \theta - a\beta_j - \alpha_i = 0$ for some i

$$\Rightarrow a\beta + \alpha - a\beta_j - \alpha_i = 0$$

$$\Rightarrow a = \frac{\alpha_i - \alpha}{\beta - \beta_j}, \text{ a contradiction)}$$

Now β is a root of $g(x)$ and $q(x)$ and no β_j $(j \neq 1)$ is a root of $g(x) \Rightarrow \beta$ is the only common root of $g(x)$ and $q(x)$. Let $f(x) = Irr(F(\theta), \beta)$.

Since $g(x) \in F(\theta)[x]$ and $g(\beta) = 0$, $f(x)$ divides $g(x)$.

Similarly $f(x)$ divides $q(x)$.

So, $f(x)$ divides g.c.d. of $g(x)$ and $q(x)$.

$\Rightarrow f(x)$ divides $x - \beta \Rightarrow f(x) = x - \beta$

Since $$f(x) \in F(\theta)[x], \ \beta \in F(\theta).$$

Also, $$\alpha = \theta - a\beta \in F(\theta)$$
$$\Rightarrow F(\alpha, \beta) \subseteq F(\theta).$$

Thus, $$F(\theta) = F(\alpha, \beta).$$

Case 2 : K is finite. We shall prove later that $K^* = K - \{0\}$ is a cyclic group. If $K^* = \langle a \rangle$, then $K = F(a)$.

Note : An extension K/F is called a *simple extension* if $K = F(a)$ for some $a \in K$. In the above theorem, we have shown that a finite seperable extension is a simple extension. a is called a *primitive element* of K over F if $K = F(a)$.

Problem 34 : *Find a primitive element for* $\mathbf{Q}(i, 2^{1/2})$ *over* $\mathbf{Q}$.

Solution : Since char $\mathbf{Q} = 0$, $\mathbf{Q}$ is perfect. So, $\mathbf{Q}(i, 2^{1/2})/\mathbf{Q}$ is seperable. Therefore, primitive element of $\mathbf{Q}(i, 2^{1/2})$ over $\mathbf{Q}$ exists.

Let $$p(x) = Irr(\mathbf{Q}, 2^{1/2}) = x^2 - 2 = (x - 2^{1/2})(x + 2^{1/2})$$
$$q(x) = Irr(\mathbf{Q}, i) = x^2 + 1 = (x - i)(x + i).$$

Consider $$\frac{-2^{\frac{1}{2}} - 2^{\frac{1}{2}}}{i-(-i)} = \frac{-2^{\frac{1}{2}}}{i} = 2^{\frac{1}{2}} i.$$

Take $a = 1$.

Then $\theta = a\beta + \alpha = i + 2^{1/2}$.

By above theorem $\mathbf{Q}(i, 2^{1/2}) = \mathbf{Q}(\theta) = \mathbf{Q}(i + 2^{1/2})$.

Problem 35 : *Find a primitive element for* $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ *over* $\mathbf{Q}$.

Solution : Here $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$

$$p(x) = Irr\,(\mathbf{Q}, \sqrt{2}) = x^2 - 2 = (x - \sqrt{2})\,(x + \sqrt{2})$$
$$q(x) = Irr\,(\mathbf{Q}, \sqrt{3}) = x^2 - 3 = (x - \sqrt{3})\,(x + \sqrt{3})$$

Consider $$\frac{-\sqrt{2} - \sqrt{2}}{\sqrt{3} - (-\sqrt{3})} = \frac{-\sqrt{2}}{\sqrt{3}}.$$

Take $a = 1$.

Then $\theta = a\beta + \alpha = \sqrt{3} + \sqrt{2}$.

So, $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\theta) = \mathbf{Q}(\sqrt{2} + \sqrt{3})$.

Problem 36 : *Let E/K be normal. Show that an element of E, of degree r over K has at most r conjugates over K with equality iff it is seperable.*

Solution : Let $p(x) = Irr\,(K, \alpha)$. Then $\deg p(x) = r$.

Now $K \subseteq K(\alpha) \subseteq E$. Suppose $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_r$ are distinct conjugates of α, over K.

Then $\exists\, r$ K-automorphisms $\sigma_1, \sigma_2, \ldots, \sigma_r$ of E s.t., $\sigma_i(\alpha) = \alpha_i \;\forall\, i$.

Each σ_i is a K-homomorphism from $K(\alpha)$ into E.

But $[K(\alpha) : K] = \deg\, p(x) = r \Rightarrow$ there are at most r K-homomorphisms from $K(\alpha)$ into E.

But we have $r + 1$ K-homomorphisms, $I, \sigma_1, \ldots, \sigma_r$ from $K(\alpha)$ into E, which is a contradiction.

Thus, there are at most r conjugates of α over K.

Suppose $\alpha \in E$ is seperable over K.

Then α is a simple root of $p(x)$.

$\Rightarrow$ each root of $p(x)$ is simple.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be distinct roots of $p(x)$.

Then $\exists\, K$-isomorphisms $\sigma_i : K(\alpha) \to K(\alpha_i)$ s.t., $\sigma_i(\alpha) = \alpha_i \;\forall\, i = 1, 2, \ldots, r$.

$\sigma_1, \sigma_2, \ldots, \sigma_r$ are distinct maps.

Since $[K(\alpha) : K] = \deg\, p(x) = r$, $\sigma_i s$ are only K-homomorphisms from $K(\alpha)$ into E.

If η is a K-automorphism of E s.t., $\eta(\alpha) = \alpha_i$, then η is also a K-homomorphism of $K(\alpha)$ into E.

$\therefore\ \eta = \sigma_i$ on $K(\alpha)$. So, there are only r K-automorphisms of E transforming α into α_i.

Thus, there are exactly r conjugates of α over K.

Conversely, let $\alpha = \alpha_1, \alpha_2, ..., \alpha_r$ be r conjugates of α over K. Then, there are exactly r K-automorphisms of E transforming α into α_i. These are also K-homomorphisms from $K(\alpha)$ into E. So, there are only r K-homomorphisms of $K(\alpha)$ into E.

Thus, $K(\alpha)/K$ is seperable $\Rightarrow$ α is seperable over K.

Galois Extensions

Definition : An extension E of F is called a *Galois extension* if (*i*) E/F is finite (*ii*) F is the fixed field of a group of automorphisms of E.

We first find a necessary and sufficient condition for a finite extension to be Galois.

Theorem 59 : *Let E/F be a finite extension. Then E/F is a Galois extension if and only if it is both normal and seperable.*

Proof : Let E/F be a Galois extension. Then F is the fixed field of a group G of automorphisms of E. By Artin's theorem, since E/F is finite, G is also finite.

Let $$G = \{\sigma_1 = I,\ \sigma_2, ..., \sigma_n\}.$$

Let $a \in E.$, Let $\sigma_i(a) = a_i,\ i = 1, 2, ..., n.$

Suppose $a_1 = a, a_2, ..., a_r$ are distinct elements of $\{a_1, a_2, ..., a_n\}$. Let $S = \{a_1, a_2, ..., a_r\}$. Then $S \subseteq E$.

Now $$\sigma_j(a_i) = \sigma_j\ \sigma_i\ (a) = \sigma_k(a) = a_k \in S.$$

So, $\sigma_j : S \to S$ for all $j = 1, 2,...., n$. Since $\sigma_j : E \to E$ is 1-1, so is $\sigma_j : S \to S$. Also, S is finite $\Rightarrow \sigma_j : S \to S$ is onto. Therefore, σ_j is a permutation of S for all j.

Let $$f(x) = (x - a_1) ..... (x - a_r)$$
$$= x^r + \alpha_1 x^{r-1} + ... + \alpha_r x^r$$

Now $$\sigma_t\,(f(x)) = (x - \sigma_t(a_1)) ..... (x - \sigma_t(a_r))$$
$$= (x - a_1) ..... (x - a_r) = f(x) \text{ for all } t.$$

So, $$x^r + \sigma_t(\alpha_1)x^{r-1} + ... + \sigma_t(\alpha_r) = x^r + \alpha_1 x^{r-1} + ... + \alpha_r$$
$$\Rightarrow \sigma_t(\alpha_i) = \alpha_i \text{ for all } t \text{ and } i$$
$$\Rightarrow \alpha_i \text{ belongs to the fixed field of } G$$
$$\Rightarrow \alpha_i \in F, \text{ for all } i$$
$$\Rightarrow f(x) \in F[x].$$

Let $g(x)$ be a monic irreducible factor of $f(x)$ in $F[x]$.

Let a_i be a zero of $g(x)$ in E. Now $a_j = \sigma_j(a) = \sigma_j\ \sigma_i^{-1}(a_i) = \sigma_t(a_i)$, So, a_i is a zero of $g(x)$ in E.

$\Rightarrow \sigma_t(a_j)$ is a zero of $\sigma_t(g(x)) = g(x)$ in E

$\Rightarrow a_j$ is a zero of $g(x)$ in E for all j

$\Rightarrow g(x) = f(x)$

$\Rightarrow f(x) = Irr\,(F, a)$.

Since a is a simple zero of $f(x)$, a is seperable over F. So, E/F is seperable. Also, $f(x)$ splits in $E[x]$.

$\Rightarrow E/F$ is normal.

Conversely, let G be the group of all F-automorphisms of E. Let F' be the fixed field of G.

Then $F \subseteq F' \subseteq E$ and $o(G) = [E : F]$.

Since E/F is finite, so is E/F'.

Also, E/F is seperable normal $\Rightarrow E/F'$ is seperable, normal.

Therefore, there are exactly $n = [E : F]$ F-automorphisms of E.

$\Rightarrow o(G) = n \Rightarrow [E : F'] = n \Rightarrow [F' : F] = 1 \Rightarrow F' = F$.

$\Rightarrow F$ is the fixed field of $G \Rightarrow E/F$ is Galois.

Cor. 1 : Let E/F be finite extension. Then E/F is Galois if and only if F is the fixed field of the group of all F-automorphisms of E.

Proof : Let E/F be Galois. Then from above E/F is finite, normal, seperable. Again by converse part of the above result, F is the fixed field of the group of all F-automorphisms of E. Converse, follows by definition.

Cor. 2 : Let char $k = 0$. Then k is contained in some Galois extension of k.

Proof : Let $f(x)$ be a non constant polynomial in $k[x]$. Let E be a minimal splitting field of $f(x)$ over k. Then E/K is finite normal. Since char $k = 0$, k is perfect $\Rightarrow E/K$ is seperable. So, E/k is Galois.

Note : When E/F is Galois, the group of all F-automorphisms of E is denoted by $Gal(E/F)$ or $G(E/F)$ called the *Galois group* of E/F.

Theorem 60 : *Let E/F be a finite extension. Then E/F is contained in a Galois extension if and only if it is seperable.*

Proof : Let E/F be contained in a Galois extension E'/F. Then $F \subseteq E \subseteq E'$.

Now E'/F is Galois $\Rightarrow E'/F$ is seperable $\Rightarrow E/F'$ is seperable.

Conversely, let E/F be seperable. Since E/F is finite, $E = F(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$.

Let $\qquad p_i = Irr\,(F, \alpha_i), \quad \alpha_i \in E$

$\alpha_i \in E \Rightarrow \alpha_i$ is seperable over F

$\Rightarrow \alpha_i$ is a simple zero of p_i, for all i

$\Rightarrow$ each zero of p_i in a splitting field is simple

Let $f = \prod_{i=1}^{n} p_i$. Then $f \in k[x] \subseteq E[x]$, and f splits in some extension of E.

Let L be a minimal splitting field of $f(x)$ over F.

Then $L = F$ (zeros of f in an extension of E)

$= F(\alpha_1, \alpha_2, ..., \alpha_n,$ zeros of f other than $\alpha_i s$ in an extension of E)

$= E$ (zeros of f other than $\alpha_i s$ in an extension of E)

$\Rightarrow F \subseteq E \subseteq L$

Also, L is generated by seperable elements over F (as each zero of f in an extension of E is simple and is a zero of an irreducible polynomial of $p_i \in F[x]$) $\Rightarrow L/F$ is seperable $\Rightarrow E/F$ is contained in a seperable extension L/F.

Theorem 61 : *Let E/k be Galois and F be any extension of k. Then EF/F is Galois and $G(EF/F)$ is isomorphic to a subgroup of $G(E/k)$.*

Proof : Since E/k is Galois, E/k is finite normal. So, E is a minimal splitting field of some polynomial $f(x) \in k[x]$.

Let $f(x) = \alpha(x - \alpha_1)(x - \alpha_2) .... (x - \alpha_n)$, $\alpha_i \in E$, $\alpha \in k$.

Then $E = k(\alpha_1, \alpha_2, ..., \alpha_n)$.

Also, E/k is seperable $\Rightarrow$ each α_i is seperable over k. Now $k \subseteq F \subseteq EF$ and α_i is seperable over $k \Rightarrow \alpha_i$ is seperable over F.

Again, $E = k(\alpha_1, \alpha_2, ..., \alpha_n)$

$\Rightarrow EF = FE = Fk(\alpha_1, \alpha_2, ..., \alpha_n) = F(\alpha_1, \alpha_2, ..., \alpha_n)$ as $k \subseteq F$

$\Rightarrow EF$ is a minimal splitting field of $f(x)$ over F

$\Rightarrow EF/F$ is finite normal

Also, EF is generated by seperable elements over $F \Rightarrow EF/F$ is seperable.

So, EF/F is Galois.

Let $\sigma \in G(EF/F)$.

Let $f = \alpha\, f_1 f_2 ..... f_r$ where each f_i is monic irreducible polynomial in $k[x]$.

So, each α_i is a zero of some $f_j \in k[x]$.

Since α_i is seperable over k, α_i is a simple zero.

Let $S = \{\alpha_1, \alpha_2, ..., \alpha_n\}$. Then α_i is a zero of f in $E \subseteq EF$

$\Rightarrow \sigma(\alpha_i)$ is a zero of $\sigma(f) = f$ in $EF \Rightarrow \sigma(\alpha_i) \in S$.

So, $\{\sigma(\alpha_1), \sigma(\alpha_2), ..., \sigma(\alpha_n)\} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$

$\Rightarrow \sigma(E) = k(\sigma(\alpha_1), \sigma(\alpha_2), ..., \sigma(\alpha_n)) = k(\alpha_1, \alpha_2, ..., \alpha_n) = E$

$\Rightarrow \sigma$ restricted to E belongs to $G(E/k)$

Define $\theta : G(EF/F) \to G(E/k)$ s.t.,

$\theta(\sigma) = \sigma/E$

Then θ is a homomorphism.

Also θ is 1-1 as $\sigma/E = I \Rightarrow \sigma(\alpha_i) = \alpha_i$ for all $i \Rightarrow \sigma(a) = a$ for all $a \in EF$ as $EF = F(\alpha_1, \alpha_2, ..., \alpha_n)$ and σ fixes each element of $F \Rightarrow \sigma = I$ on EF.

So, $G(EF/F) \cong \theta(G(EF/F)) \leq G(E/F)$.

Cor. : If E/k is Galois and F, an extension of k, then $[EF : F]$ divides $[E : k]$.

Proof : By above theorem, EF/F is Galois

$\Rightarrow \qquad [EF : F] = o(G(EF/F))$

Also, $\qquad [E : k] = o(G(E/k))$

But $\qquad \theta(G(EF/F)) \leq G(E/F)$

$\Rightarrow \; o(\theta(G(EF/F)))$ divides $o(G(E/F))$

$\Rightarrow \; o(G(EF/F))$ divides $o(G(E/F))$

$\Rightarrow \; [EF : F]$ divides $[E : k]$.

Remark : The above corollary need not be true if E/k is not Galois. For example, let $k = \mathbf{Q}$, let α be the real cube root of 2. Then $\alpha, \alpha w, \alpha w^2$ are roots of $f(x) = x^3 - 2$ in $\mathbf{C}$.

Let $\qquad E = \mathbf{Q}(\alpha w), \quad F = \mathbf{Q}(\alpha)$.

Then $\qquad EF = \mathbf{Q}(\alpha w)\,\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha, \alpha w) = \mathbf{Q}(\alpha, \sqrt{3}i)$

$$= F(\sqrt{3}i)$$

So, $\qquad [EF : F] = [F(\sqrt{3}i) : F] = 2$

while $\qquad [E : k] = [\mathbf{Q}(\alpha w) : \mathbf{Q}] = \deg \; Irr\,(\mathbf{Q}, \alpha w)$

$$= \deg \; f(x) = 3.$$

Theorem 62 : (The fundamental theorem of Galois Theory).

Let E/k be Galois. Let $G = G(E/k)$ be the group of all k-automorphisms of E. Then

(*i*) *There is one-one correspondence between the sets $\mathscr{A} = \{F \mid F = \text{field}, \; k \subseteq F \subseteq E\}$ and $\mathscr{B} = \{H \mid H \leq G\}$ which is an order inverting bijection.*

(*ii*) *$F \in \mathscr{A}$ is the fixed field of the subgroup $H \in \mathscr{B}$ corresponding to F and $H \in \mathscr{B}$ is the group of H^*-automorphisms of E, where H^* is the fixed field of H.*

(*iii*) *If H is the subgroup of $\mathscr{B}$ corresponding to the field F in $\mathscr{A}$, then $o(H) = [E : F]$ and $[G : H] = [F : k]$.*

(*iv*) *If $H_1, H_2 \in \mathscr{B}$ correspond to $F_1, F_2 \in \mathscr{A}$ respectively, then F_1, F_2 are conjugate under an automorphism $\sigma \in G$ if and only if $\sigma^{-1} H_1 \sigma = H_2$.*

(*v*) *If $H \in \mathscr{B}$ corresponds to $F \in \mathscr{A}$, then F/k is normal if and only if H is normal subgroup of G and in that case, $G(F/k) \cong \dfrac{G}{H}$.*

Proof : Define $\theta : \mathscr{A} \to \mathscr{B}$ s.t.,

$$\theta(F) = F^*$$

where $F^* = \{\sigma \in G \mid \sigma(x) = x \text{ for all } x \in F\}$. Then $F^* \in \mathscr{B}$.

Similarly, define $\theta : \mathscr{B} \to \mathscr{A}$ s.t.,

$$\theta(H) = H^*$$

where $H^* = \{x \in E \mid \sigma(x) = x \text{ for all } \sigma \in H\}$

Then $H^* \in \mathscr{A}$ is the fixed field of H.

Let $F_1, F_2 \in \mathscr{A}$ such that $F_1 \subseteq F_2$.

Let $\sigma \in F_2^*$. Then $\sigma(x) = x$ for all $x \in F_2$

$\Rightarrow \sigma(x) = x$ for all $x \in F_1$ as $F_1 \subseteq F_2$

$\Rightarrow \sigma \in F_1^* \Rightarrow F_2^* \subseteq F_1^* \Rightarrow \theta(F_2) \subseteq \theta(F_1) \Rightarrow \theta$ is an order inverting map.

Similarly, φ is an order inverting map.

Let $H \in \mathscr{B}$. Then $\sigma \in H \Rightarrow \sigma(x) = x$ for all $x \in H^* \Rightarrow \sigma \in H^{**} \Rightarrow H \subseteq H^{**}$.

Also $x \in F (F \in \mathscr{A}) \Rightarrow \sigma(x) = x$ for all $\sigma \in F^*$

$\Rightarrow x$ belongs to the fixed field of F^*

$\Rightarrow x \in F^{**} \Rightarrow F \subseteq F^{**}$ for all $F \in \mathscr{A}$.

Let $F \in \mathscr{A}$ and $F^* = H$. Then $H^{**} = F^{***}$.

Now $H \subseteq H^{**} \Rightarrow F^* \subseteq F^{***}$ for all $F \in \mathscr{A}$.

Also, $F \subseteq F^{**} \Rightarrow \theta(F^{**}) \subseteq \theta(F) \Rightarrow F^{***} \subseteq F^*$ for all $F \in \mathscr{A}$. So, $F^* = F^{***}$. Similarly, $H^* = H^{***}$ for all $H \in \mathscr{B}$.

Now θ is 1-1 onto if and only if $\theta\varphi =$ Identity and $\varphi\theta =$ Identity if and only if $H = H^{**}$ for all $H \in \mathscr{B}$ and $F = F^{**}$ for all $F \in \mathscr{A}$.

Let $H \in \mathscr{B}$. Then $H^* = F$ is the fixed field of H.

By Artin's theorem $o(H) = [E : F]$.

Also, $o(H^{**}) = [E : H^{***}] = [E : H^*] = [E : F]$.

So, $o(H) = o(H^{**})$. But $H \subseteq H^{**}$. Therefore, $H = H^{**}$.

Let $F \in \mathscr{A}$. Then $k \subseteq F \subseteq E$.

Now E/k is Galois $\Rightarrow E/F$ is Galois $\Rightarrow F$ is the fixed field of the group H of all F-automorphisms of E.

$\Rightarrow H \leq G \Rightarrow H \in \mathscr{B}$.

Now $H^* =$ fixed field of $H = F \Rightarrow H^{***} = F^{**} \Rightarrow H^* = F^{**} \Rightarrow F = F^{**}$ for all $F \in \mathscr{A}$.

Thus, θ is 1-1 onto.

This proves (*i*).

(*ii*) Let $F \in \mathscr{A}$. Let $\theta(F) = H$. Then $F^* = H \Rightarrow F^{**} = H^* \Rightarrow F = H^* \Rightarrow F$ is the fixed field of H.

Let $H \in \mathscr{B}$. Then there exists $F \in \mathscr{A}$ such that $\theta(F) = H \Rightarrow H = F^*$.

Let $\sigma \in H$. Then $\sigma \in F^* \Rightarrow \sigma(x) = x$ for all $x \in F \Rightarrow \sigma$ is an F-automorphism of E.

Conversely, let σ be an F-automorphism of E.

Then $\sigma(x) = x$ for all $x \in F \Rightarrow \sigma \in F^* = H$.

So, H is the group of all $F = H^*$-automorphisms of E.

(*iii*) By Artin's theorem

$$o(H) = [E : H^*] = [E : F]$$

$$[G : H] = \frac{o(G)}{o(H)} = \frac{[E : k]}{[E : F]} = [F : k].$$

(*iv*) Suppose $F_1, F_2 \in \mathscr{A}$ are conjugate under $\sigma \in G$. Then $\sigma(F_1) = F_2$.

Let $y \in F_2$. Then $y = \sigma(z)$, $z \in F_1$. Therefore, $\sigma^{-1}(y) = z$.

$$\Rightarrow \tau\sigma^{-1}(y) = \tau(z), \qquad \text{for all } \tau \in H_1$$
$$\Rightarrow \sigma\tau\sigma^{-1}(y) = \sigma\tau(z) = \sigma(z), \qquad \text{for all } \tau \in H_1$$
$$\Rightarrow \sigma\tau\sigma^{-1}(y) = y, \qquad \text{for all } \tau \in H_1,\ y \in F_2$$
$$\Rightarrow \sigma\tau\sigma^{-1} \in H_2, \qquad \text{for all } \tau \in H_1$$
$$\Rightarrow \sigma H_1 \sigma^{-1} \subseteq H_2$$

Let $a \in F_1$. Then $\sigma(a) = b \in F_2$

$$\Rightarrow \eta\sigma(a) = \eta(b), \text{ for all } \eta \in H_2$$
$$\Rightarrow \eta\sigma(a) = b, \text{ for all } \eta \in H_2$$
$$\Rightarrow \sigma^{-1}\eta\sigma(a) = \sigma^{-1}(b) = a, \text{ for all } \eta \in H_2,\ a \in F_1$$
$$\Rightarrow \sigma^{-1}\eta\sigma \in H_1, \text{ for all } \eta \in H_2$$
$$\Rightarrow \sigma^{-1}H_2\ \sigma \subseteq H_1$$
$$\Rightarrow H_2 \subseteq \sigma H_1 \sigma^{-1}$$

So, $$H_2 = \sigma H_1 \sigma^{-1}.$$

Conversely, let $H_2 = \sigma H_1 \sigma^{-1}$ for $\sigma \in G$.

Let $y \in F_2$. Now $\sigma\tau\sigma^{-1} \in H_2$, for all $\tau \in H_2$

$$\Rightarrow \sigma\tau\sigma^{-1}(y) = y$$
$$\Rightarrow \tau\sigma^{-1}(y) = \sigma^{-1}(y) = z$$
$$\Rightarrow \tau(z) = z, \qquad \text{for all } \tau \in H_1$$
$$\Rightarrow z \in F_1$$
$$\Rightarrow y = \sigma(z) \in \sigma(F_1)$$
$$\Rightarrow F_2 \subseteq \sigma(F_1)$$

Let $x \in F_1$. Now $\sigma^{-1}\eta\sigma \in H_1$, for all $\eta \in H_2$

$$\Rightarrow \sigma^{-1}\eta\sigma(x) = x$$
$$\Rightarrow \eta\sigma(x) = \sigma(x) = x'$$
$$\Rightarrow \eta(x') = x', \qquad \text{for all } \eta \in H_2$$
$$\Rightarrow x' \in F_2$$
$$\Rightarrow \sigma(x) \in F_2$$
$$\Rightarrow \sigma(F_1) \subseteq F_2.$$

So, $\sigma(F_1) = F_2 \Rightarrow F_1, F_2$ are conjugate under σ.

(*v*) Suppose F/k is normal. Since E/k is finite, so is F/k. Therefore, F/k is finite normal $\Rightarrow$ F is a minimal splitting field of some $f \in k[x]$.

Let $$f = \alpha(x - \alpha_1) \ldots\ldots (x - \alpha_n), \qquad \alpha_i \in E,\ \alpha \in k.$$

Then $$F = k(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n).$$

Let $\sigma \in G$. Then σ is a k-automorphism of $E \Rightarrow \sigma(f) = f$.

$$\Rightarrow f = \alpha(x - \sigma(\alpha_1)) \ldots\ldots (x - \sigma(\alpha_n))$$

$\Rightarrow$ $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are zeros of f in E

$\Rightarrow$ $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$.

So, $\sigma(F) = k(\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$

$= k(\alpha_1, \ldots, \alpha_n) = F$ for all $\sigma \in G$.

By (*iv*), $\sigma^{-1}H\sigma = H$ for all $\sigma \in G$

$\Rightarrow$ H is a normal subgroup of G.

Conversely, let $H = F^*$ be normal subgroup of G. Then $\sigma^{-1}H\sigma = \sigma$ for all $\sigma \in G$

$\Rightarrow$ $\sigma(F) = F$ by (*iv*) for all $\sigma \in G$

Let $\alpha \in F$, $p(x) = Irr\,(k, \alpha)$.

Since E/k is normal and $\alpha \in E$, we find $p(x)$ splits in E.

Let β be a zero of $p(x)$ in E.

Then α, β are zeros of $p(x)$ in E

$\Rightarrow$ there is an isomorphism $\theta : k(\alpha) \to k(\beta)$ s.t.,

$\theta(\alpha) = \beta$, $\theta(a) = a$ for all $a \in k$.

Since $\beta \in E$, $k(\beta) \subseteq E$. So θ is a k-homomorphism from $k(\alpha)$ to E.

Since E/K is finite normal, θ can be extended to k-automorphism σ of E. So, $\sigma \in G$.

Now $\sigma(\alpha) = \theta(\alpha) = \beta$ and $\sigma(\alpha) \in \sigma(F) = F$ $\Rightarrow$ $\beta \in F$.

Thus, $p(x)$ splits in F $\Rightarrow$ F/K is normal.

Let H be a normal subgroup of G. Then the corresponding field F is normal over k from above. Since E/k is Galois, so is F/k. Let $N = \mathrm{Gal}(F/k)$

Define $\psi : G \to N$ s.t.,

$\psi(\sigma) = \bar{\sigma}$, where $\bar{\sigma}$ is the restriction of σ on F.

(Since $H \leq G$, $\sigma^{-1}H\sigma = H$ $\Rightarrow$ $\sigma(F) = F$)

Let $\sigma, \eta \in G$.

Then
$$\begin{aligned}
\overline{\eta}\,(\alpha) &= (\sigma\eta)\,(\alpha), && \alpha \in F \\
&= \sigma(\eta(\alpha)), && \eta(\alpha) \in F \\
&= \bar{\sigma}\,(\eta(\alpha)) \\
&= \bar{\sigma}\,(\overline{\eta}(\alpha)) \\
&= (\bar{\sigma}\,\overline{\eta})\,(\alpha), && \text{for all } \alpha \in F
\end{aligned}$$

$\Rightarrow$ $\overline{\eta} = \bar{\sigma}\,\overline{\eta}$

$\Rightarrow$ $\psi(\sigma\eta) = \psi(\sigma)\,\psi(\eta)$

$\Rightarrow$ ψ is a homomorphism

Let $\theta \in N$. Then θ can be extended to k-automorphism σ of $E \Rightarrow \sigma \in G$ $\Rightarrow$ $\psi(\sigma) = \bar{\sigma} = \theta$. So, ψ is onto. Now $\sigma \in \mathrm{Ker}\,\psi$ $\Leftrightarrow$ $\psi(\sigma) = \text{Identity of } N$ $\Leftrightarrow$ $\bar{\sigma} = \text{Identity on } F \Leftrightarrow \bar{\sigma}\,(\alpha) = \alpha$, for all $\alpha \in F$.

The result now follows by using fundamental theorem of homomorphism.

Example 15 (i) : Let E be a minimal splitting field of $f(x) = x^3 - 2$ over $\mathbf{Q}$. Let α be the real cube root of 2.

Then $E = \mathbf{Q}(\alpha, \alpha w, \alpha w^2) = \mathbf{Q}(\alpha, \sqrt{3}i)$.

Also, $[E : \mathbf{Q}] = 6$. Since char $\mathbf{Q} = 0$, $E/\mathbf{Q}$ is seperable (as $\mathbf{Q}$ is perfect $\Rightarrow$ every algebraic extension of $\mathbf{Q}$ is seperable).

Also, E is a minimal splitting field of $f(x)$ over $\mathbf{Q} \Rightarrow E/\mathbf{Q}$ is finite normal.

So, $E/\mathbf{Q}$ is Galois.

Let $G = G(E/\mathbf{Q})$ be the group of all $\mathbf{Q}$-automorphisms of $\mathbf{Q}$.

Then $\mathbf{Q}$ is the fixed field of G. By Artin's theorem $o(G) = [E : \mathbf{Q}] = 6$.

Let $\sigma \in G$. Then $\sigma(\sqrt{3}i)^2 = \sigma(-3) = -3$.

$\Rightarrow (\sigma(\sqrt{3}i))^2 + 3 = 0 \Rightarrow \sigma(\sqrt{3}i)$ is a zero of $x^2 + 3$ in $E \subseteq \mathbf{C}$.

$\Rightarrow \sigma(\sqrt{3}i) = \pm\sqrt{3}i$. Also $\sigma(\alpha^3) = \sigma(2) = 2 \Rightarrow (\sigma(\alpha))^3 + 2 = 0 \Rightarrow \sigma(\alpha)$ is a zero of $x^3 + 2$ in $E \subseteq \mathbf{C}$. $\sigma(\alpha) = \alpha$, αw or αw^2.

Therefore, σ has 6 choices.

But $o(G) = 6$. So, these 6 choices give all elements of G. These can be represented as follows :

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\alpha \longmapsto$	α	α	αw	αw	αw^2	αw^2
$\sqrt{3}i \longmapsto$	$\sqrt{3}i$	$-\sqrt{3}i$	$\sqrt{3}i$	$-\sqrt{3}i$	$\sqrt{3}i$	$-\sqrt{3}i$

$G = \{\sigma_1 = I, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

Let 1 denote αw, 2 denote αw^2, 3 denote $\alpha w^3 = \alpha$

Let $S = \{1, 2, 3\}$, Let $\sigma \in G$, $a \in S$.

Then $a \in S \Rightarrow a$ is a zero of $f(x)$ in E.

$\Rightarrow \sigma(a)$ is a zero of $\sigma(f(x)) = f(x)$ in E.

$\Rightarrow \sigma(a) \in S \Rightarrow \sigma : S \to S$ for all $\sigma \in G$.

Since $\sigma : E \to E$ is 1-1, $\sigma : S \to S$ is 1-1 and so $\sigma : S \to S$ is onto as S is finite. Thus σ is a permutation of S.

$\Rightarrow \sigma \in A(S)$, the group of all permutations of S.

This defines a map $\theta : G \to A(S)$ s.t., $\theta(\sigma) = \bar{\sigma} = \sigma|S$ (σ restricted to S).

Then θ is a homomorphism and θ is 1-1 as $\theta(\sigma) = I \Rightarrow \bar{\sigma} = I \Rightarrow \bar{\sigma}(a) = a$ for all $a \in S \Rightarrow \sigma(a) = a$ for all $a \in S \Rightarrow \sigma = I \Rightarrow G \cong \theta(G) \leq A(S)$.

But $o(A(S)) = 6 = o(\theta(G)) = o(G) \Rightarrow \theta(G) = A(S) \Rightarrow G \cong A(S) = S_3$.

We can identify elements of G as follows :

$\sigma_2 = (12)$, $\sigma_3 = (123)$, $\sigma_4 = (13)$, $\sigma_5 = (321)$, $\sigma_6 = (23)$.

Subgroups of G are :

$H_1 = \{I, \sigma_2\}$, $H_2 = \{I, \sigma_4\}$, $H_3 = \{I, \sigma_6\}$, $H_4 = \{I, \sigma_3, \sigma_5\}$, $H_5 = G$, $H_6 = \{I\}$.

Let $F_1 = H_1^*$, the fixed field of H_1.

Now H_1 fixes $\alpha \Rightarrow \mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq F_1 \subseteq E$.

But $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$, $[E : F_1] = [E : H_1^*] = 0(H_1) = 2$ and $[E : \mathbf{Q}] = 6 \Rightarrow F_1 = \mathbf{Q}(\alpha)$.

Let $F_2 = H_2^*$, the fixed field of H_2.

Then $F_2 = \mathbf{Q}(\alpha w^2)$ and F_3, the fixed field of H_3 is $\mathbf{Q}(\alpha w)$.

Let $F_4 = H_4^*$, the fixed field of H_4. Now H_4 fixes $\sqrt{3}i \Rightarrow \mathbf{Q} \subseteq \mathbf{Q}(\sqrt{3}i) \subseteq F_4 \subseteq E$. Since $[E : F_4] = 3$, $[\mathbf{Q}(\sqrt{3}i) : \mathbf{Q}] = 2$, $[E : \mathbf{Q}] = 6$, $F_4 = \mathbf{Q}(\sqrt{3}i)$.

Clearly, $F_5 =$ fixed field of $G = \mathbf{Q}$ and $F_6 =$ fixed field of $H_6 = E$.

So, we have 6 intermediate fields between $\mathbf{Q}$ and E corresponding to 6 subgroups of G.

Since H_1, H_2, H_3 are not normal, $F_1/\mathbf{Q}$, $F_2/\mathbf{Q}$, $F_3/\mathbf{Q}$ are also not normal. Also H_4, H_5, H_6 are normal subgroups of G, and thus $F_4/\mathbf{Q}$, $F_5/\mathbf{Q}$, $F_6/\mathbf{Q}$ are normal subgroups of G.

(ii) Let E be a minimal splitting field of $f(x) = x^4 + 1$ over $\mathbf{Q}$.

Then $E = \mathbf{Q}(\alpha)$, where $\alpha = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$

and $[E : \mathbf{Q}] = [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg Irr(\mathbf{Q}, \alpha) = \deg f(x) = 4$

Char $\mathbf{Q} = 0 \Rightarrow E/\mathbf{Q}$ is seperable.

Also E is a minimal splitting field of $f(x)$ over $\mathbf{Q}$, $E/\mathbf{Q}$ is finite normal.

So, $E/\mathbf{Q}$ is Galois. Let $G = G(E/\mathbf{Q})$ be the Galois group of $E/\mathbf{Q}$.

By Artin's theorem $o(G) = [E : \mathbf{Q}] = 4$.

Let $\sigma \in G$. Then $\sigma(\alpha^4) = \sigma(-1) = -1 \Rightarrow (\sigma(\alpha))^4 + 1 = 0$.

$\Rightarrow \sigma(\alpha)$ is a zero of $f(x)$ in $E \subseteq \mathbf{C} \Rightarrow \sigma(\alpha) = \alpha, \alpha^3, \alpha^5, \alpha^7$.

Since $o(G) = 4$, these 4 choices give all elements of G. So, G can be represented as follows :

	σ_1	σ_3	σ_5	σ_7
$\alpha \longleftrightarrow$	α	α^3	α^5	α^7

$G = \{\sigma_1, = I, \sigma_3, \sigma_5, \sigma_7\}$

Since $\sigma_3^2(\alpha) = \sigma_3(\alpha^3) = \alpha^9 = \alpha$, $\sigma_3^2 = I$.

Similarly, $\sigma_5^2 = \sigma_7^2 = I \Rightarrow G$ is Klein's 4 group.

Subgroups of G are $H_1 = \{I, \sigma_3\}$, $H_2 = \{I, \sigma_5\}$, $H_3 = \{I, \sigma_7\}$, $H_4 = G$, $H_5 = \{I\}$.

Now $\sigma \in G \Rightarrow \sigma(\sqrt{2})^2 = \sigma(2) = 2 \Rightarrow (\sigma(\sqrt{2}))^2 = 2 = 0 \Rightarrow \sigma(\sqrt{2})$ is a zero of $x^2 + 2$ in $E \subseteq \mathbf{C} \Rightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}$. Similarly $\sigma(i) = \pm i$.

So, $$\sigma_3(\alpha) = \alpha^3 \Rightarrow \sigma_3\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{-1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$

$$\Rightarrow \sigma_3(\sqrt{2}) = -\sqrt{2}, \quad \sigma_3(i) = -i$$
$$\Rightarrow \sigma_3(\sqrt{2}i) = \sqrt{2}i$$
$$\Rightarrow H_1 \text{ fixes } \sqrt{2}i$$

Let $F_1 = H_1^*$, the fixed field of H_1

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}i) \subseteq F_1 \subseteq E$

But $[\mathbf{Q}(\sqrt{2}i) : \mathbf{Q}] = 2, \ [E : F_1] = 2, \ [E : \mathbf{Q}]$

So, $F_1 = \mathbf{Q}(\sqrt{2}i)$

Also, $\sigma_5(\alpha) = \sigma_5 \Rightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = -\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$.

$\Rightarrow \sigma_5(\sqrt{2}) = -\sqrt{2}$ and $\sigma_5(i) = i \Rightarrow H_2$ fixes i.

Let $F_2 = H_2^*$, the fixed field of H_2.

Then $\mathbf{Q} \subseteq \mathbf{Q}(i) \subseteq F_2 \subseteq E$ and $[E : F_2] = 2$, $[\mathbf{Q}(i) : \mathbf{Q}] = 2$, $[E : \mathbf{Q}] = 4 \Rightarrow F_2 = \mathbf{Q}(i)$.

Now $\sigma_7(\alpha) = \sigma_7 \Rightarrow \sigma_5\left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}} \Rightarrow \sigma_5(\sqrt{2}) = \sqrt{2} \Rightarrow H_3$ fixes $\sqrt{2}$.

Let $F_3 = H_3^*$, the fixed field of H_3.

Then $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq F_3 \subseteq E$ and $[E : F_3] = 2$, $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$, $[E : \mathbf{Q}] = 4 \Rightarrow F_3 = \mathbf{Q}(\sqrt{2})$.

Clearly $F_4 =$ fixed field of $H_4 (= G)$ is $\mathbf{Q}$ and $F_5 =$ fixed field of $H_5 = E$.

So, F_1, F_2, F_3, F_4, F_5 are intermediate fields lying between $\mathbf{Q}$ and E.

Since F_1, F_2, F_3 are quadratic extensions of $\mathbf{Q}$, $F_1/\mathbf{Q}$, $F_2/\mathbf{Q}$, $F_3/\mathbf{Q}$ are normal. Also $F_4/\mathbf{Q}$, $F_5/\mathbf{Q}$ are normal. But G being abelian, all subgroups of G are normal subgroups of G.

Roots of Unity

Definition : Let E be a minimal splitting field of $f(x) = x^n - 1$ over k. Then the roots of $f(x)$ in E are called *nth roots of unity*. E is called the *associated cyclotomic field*.

Theorem 63 : *The nth roots of unity form a cyclic group under multiplication, whose order is a divisor of n.*

Proof : Let $G = \{\alpha \in E \mid \alpha^n = 1\} \subseteq E^* = E - \{0\}$. Then $1 \in G \Rightarrow G \neq \varphi$.

Let $\alpha, \beta \in G$. Then $\alpha^n = 1 = \beta^n$. Now E^* is abelian group under multiplication. So, $(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = \alpha\beta^{-1} \Rightarrow \alpha\beta^{-1} \in G \Rightarrow G$ is a subgroup of E^*.

So, G is a finite abelian group.

Let $\alpha \in G$ be an element of maximum order m in G.

So, $o(\beta)$ divides m for all $\beta \in G \Rightarrow \beta^m = 1$ for all $\beta \in G$.

Let $n = mq + r$, $0 \leq r < m$. Let $r \neq 0$.

Now $1 = \alpha^n = \alpha^{mq}\alpha^r = \alpha^r \Rightarrow \alpha^r = 1$, $r < m$, $r > 0$, contradicting $0(\alpha) = m$.

So, $r = 0$. Thus, m divides n.

Now $1, \alpha, \alpha^2, \ldots\ldots, \alpha^{m-1}$ are distinct elements of $G \Rightarrow o(G) \geq m$.

Since E has at most n roots of $g(x) = x^m - 1$ over k, $o(G) \leq m$.

So, $o(G) = m$ and $G = \{1, \alpha, \ldots\ldots, \alpha^{m-1}\}$.

$\Rightarrow G$ is a cyclic group generated by α such that $o(G) = o(\alpha) = m$ divides n.

Note : Let k be a field and n, a positive integer. Suppose char $k = 0$ or char $k = p$ such that $(p, n) = 1$. Then all nth roots of unity over k are simple and so distinct.

Proof : Let $\quad f(x) = x^n - 1 \in k[x]$

Then $\quad f'(x) = nx^{n-1}$

Let α be a zero of $f(x)$ in a splitting field of f over k.

If $f'(\alpha) = 0$, then $n\alpha^{n-1} = 0$. If char $k = 0$, then $n = 0$ or $\alpha = 0$, none of which is true. If char $k = p$, $(p, n) = 1$, then $\alpha = 0$ or p divides n, none of which is true. So, $f'(\alpha) \neq 0 \Rightarrow$ roots of f are simple.

Throughout this section, we assume that char $k = 0$ or char $k = p$, $(p, n) = 1$. Then, $o(G) = n$, where $G = \{\alpha \in E \mid \alpha^n = 1\}$, E a minimal splitting field of f over k. Also G is cyclic. A generator of G is called *primitive nth root of unity*. Since the number of generators of G is $\varphi(n)$, the number of primitive nth roots of unity is $\varphi(n)$. Since G is cyclic, let $G = <\alpha>$. Then $\alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}, \alpha^n = 1$ are distinct roots of $f(x)$ in E. So, $E = k(\alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}) = k(\alpha)$, the cyclotomic field over k.

The polynomial $\Phi_n(x) = \prod\limits_{\substack{1 \leq i \leq n \\ 0(\alpha^i) = n}} (x - \alpha^i) = \prod\limits_{\substack{1 \leq i \leq n \\ (i, n) = 1}} (x - \alpha^i)$ is called *nth cyclotomic polynomial*. Then $\Phi_d(x) = \prod\limits_{\substack{0(\alpha^i) = d \\ 1 \leq i \leq n}} (x - \alpha^i) = \prod\limits_{\substack{1 \leq i \leq n \\ (i, d) = 1}} (x - \alpha^i)$ is dth cyclotomic polynomial.

Theorem 64 : $x^n - 1 = \prod\limits_{d \mid n} \Phi_d(x)$

Proof : $x^n - 1 = \prod\limits_{1 \leq i \leq n} (x - \alpha^i)$, where $G = <\alpha>$.

Now $\quad d \mid n \Leftrightarrow n = kd \Leftrightarrow o(\alpha^k) = d$.

So,
$$x^n - 1 = \prod_{d \mid n} \prod_{o(\alpha^k) = d} (x - \alpha^k)$$
$$= \prod_{d \mid n} \Phi_d(x).$$

Now $\Phi_1(x) = x - 1$ by taking $n = 1$.

Let $n =$ prime p. Then $x^p - 1 = \Phi_1(x)\Phi_p(x)$ as $p, 1$ are only divisors of p.

So,
$$\Phi_p(x) = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = 1 + x + \ldots\ldots + x^{p-1}$$

Therefore, $$\Phi_{p^2}(x) = \frac{x^{p^2}-1}{\Phi_1(x)\Phi_p(x)}$$

$$= \frac{x^{p^2}-1}{x^p-1} = 1 + x^p + \ldots\ldots + x^{p(p-1)}$$

Thus, $\Phi_2(x) = 1 + x, \quad \Phi_3(x) = 1 + x + x^2$

$\Phi_4(x) = 1 + x^2$

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}$$

$$= \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)}$$

$$= x^2 - x + 1.$$

Theorem 65 : *For any prime p and a positive integer m,*

$$\Phi_{p^m}(x) = 1 + x^{p^{m-1}} + \ldots\ldots + x^{(p-1)p^{m-1}}$$

Proof : Now $$\Phi_{p^m}(x) = \frac{x^{p^m}-1}{\Phi_1(x)\Phi_p(x)\ldots\ldots\Phi_{p^{m-1}}(x)}$$

$$= \frac{x^{p^m}-1}{x^{p^{m-1}}-1} = 1 + x^{p^{m-1}} + \ldots\ldots + x^{(p-1)p^{m-1}}.$$

Möbius function : The map $\mu : \mathbf{N} \to \{0, 1, -1\}$ such that $\mu(1) = 1$, $\mu(n) = 0$ if p^2 divides n for some prime p and $\mu(p_1 p_2 \ldots\ldots p_r) = (-1)^2$, where $p_1, p_2, \ldots\ldots, p_r$ are distinct primes is called the Möbius function. Clearly, $\mu(12) = 0$, $\mu(15) = 1$, $\mu(3) = -1$.

The following result is known as *Möbius inversion formula.*

If $f, g : \mathbf{N} \to \mathbf{R}$ (where **N** denotes the set of natural numbers and **R**, the set of real numbers), then

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Theorem 66 : $$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

Proof : Now $x^n - 1 = \prod_{d|n} \Phi_d(x)$

$$\Rightarrow \log(x^n - 1) = \sum_{d|n} \log \Phi_d(x)$$

Let $f(x) = \log\ x^n - 1$

$g(d) = \log\ \Phi_d(x)$.

Then $f(n) = \sum_{d|n} g(d)$.

By Möbius inversion formula

$$\log\ \Phi_n(x) = \sum_{d|n} \log(x^d - 1)\, \mu(\tfrac{n}{d})$$

$$= \sum_{d|n} \log(x^d - 1)^{\mu(\frac{n}{d})}$$

$$= \log \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

$$\Rightarrow \quad \Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

Theorem 67 : $\sum_{d|n} \mu(d) = 0$, *for* $n > 1$.

Proof : Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ where $p_i s$ are distinct primes.

Thus, $\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \ldots\ldots + \mu(p_r) + \mu(p_1 p_2) + \ldots\ldots +$

$\mu(p_{r-1} p_r) + \ldots\ldots + \mu(p_1 p_2 \ldots\ldots p_r)$

$= 1 + r_{c_1}(-1) + r_{c_2}(-1)^2 + \ldots\ldots + r_{c_r}(-1)^r$

$= (1 + (-1))^r = 0.$

Problem 37 : *Show that* $\prod_{d|n} (x-1)^{\mu(\frac{n}{d})} = 1$, $n > 1$.

Solution : Let P denote L.H.S.

Then $$\log P = \sum_{d|n} \log (x-1)^{\mu(\frac{n}{d})}$$

$$= \sum_{d|n} (\log (x-1))\mu(\tfrac{n}{d})$$

$$= \log\ (x-1) \sum_{d|n} \mu(\tfrac{n}{d})$$

$$= \log\ (x-1) \sum_{d|n} \mu(d)$$

$$= 0 \Rightarrow P = 1.$$

Problem 38 : *Prove that* $\Phi_n(1) = \prod_{d|n} d^{\mu(\frac{n}{d})}$, $n > 1$. *Deduce that* $\Phi_n(1) = 0$, p *or* 1 *according as* n *is* 1, p^α (p, *a prime*) *or divisible by at least two primes.*

Solution : $$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

$$= \prod_{d|n} (x-1)^{\mu(\frac{n}{d})} \prod_{d|n} (x^{d-1} + \ldots\ldots + x + 1)^{\mu(\frac{n}{d})}$$

$$= \prod_{d|n} (x^{d-1} + \ldots\ldots + x + 1)^{\mu(\frac{n}{d})} \quad \text{by above problem}$$

So, $\Phi_n(1) = \prod_{d|n} d^{\mu(\frac{n}{d})}$, when $n > 1$.

(Note $\Phi_n(1) = \prod_{d|n} (\frac{n}{d})^{\mu(d)}$ as $d \mid n \Rightarrow \frac{n}{d} \mid n$)

when $n = 1$, $\Phi_n(1) = 1$.

when $n = p^\alpha$, $\Phi_n(1) = (p^\alpha)^{\mu(1)} (p^{\alpha-1})^{\mu(p)}$

$$= \frac{p^\alpha}{p^{\alpha-1}} = p$$

when $n = p_1^{\alpha_1} p_2^{\alpha_2}$

Then
$$\Phi_n(1) = (p_1^{\alpha_1-1}p_2^{\alpha_2})^{-1}(p_1^{\alpha_1}p_2^{\alpha_2-2})^{-1}$$
$$\times (p_1^{\alpha_1-1}p_2^{\alpha_2-2})^1 \times (p_1^{\alpha_1}p_2^{\alpha_2})^1$$
$$= 1$$

Let $n = p^k p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ where $p, p_i s$ are distinct primes and $r \geq 2$. Then $n = p^k m$, where $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$.

So,
$$\Phi_{mp^k}(1) = \prod_{d|mp^k} \left(\frac{mp^k}{d}\right)^{\mu(d)}$$
$$= \prod_{d|mp} \left(\frac{mp^k}{d}\right)^{\mu(d)}$$
$$= \prod_{d|m} \left(\frac{mp^k}{d}\right)^{\mu(d)} \prod_{d|m} \left(\frac{mp^{k-1}}{d}\right)^{-\mu(d)} \quad \text{as } \mu(p) = -1$$
$$= \prod_{d|m} p^{\mu(d)} = 1$$

(as $P = \prod_{d|m} p^{\mu(d)} \Rightarrow \log P = \sum_{d|m} (\log p)^{\mu(d)} = \log\ p \sum_{d|m} \mu(d) = 0$

(**Note** : We have used the fact that $\mu(mn) = \mu(m)\,\mu(n)$ whenever $(m, n) = 1$)

Theorem 68 : *$a \in F_p$ is a primitive nth root of unity if and only if $p \equiv 1 (mod\ n)$.*

Proof : Suppose $a \in F_p$ is a primitive nth root of unity. Now $0 \neq a \in F_p$ $\Rightarrow a^{p-1} = 1 \Rightarrow o(a)|p-1 \Rightarrow n|p-1 \Rightarrow p \equiv 1 (\text{mod } n)$

Conversely, let $p \equiv 1$ (mod n). Let $F_p^* = <\alpha>$. Then $o(\alpha) = p - 1 = nm$

$$\Rightarrow o(\alpha^m) = \frac{o(\alpha)}{(o(\alpha), m)} = \frac{nm}{(nm, m)} = \frac{nm}{m} = n$$

$\Rightarrow \alpha^m$ is a primitive nth root in F_p.

Problem 39 : *Let p, q be distinct primes. Show that x^{q-1} splits into linear factors over F_p if and only if $p \equiv 1$ (mod q).*

Solution : Suppose x^{q-1} splits into linear factors over F_p.

Let $1 \neq \alpha$ be a zero of $x^q - 1$ in F_p.

Then $\alpha^q = 1 \Rightarrow o(\alpha)$ divides $q \Rightarrow o(\alpha) = q$ as $\alpha \neq 1 \Rightarrow \alpha$ is a primitive qth root of unity in $F_p \Rightarrow p - 1 \equiv (\text{mod } q)$.

Conversely, let $p \equiv 1 \pmod q$. Then F_p contains a primitive qth root α of unity. $\alpha \in F_p$ and $o(\alpha) = q$. Since q is prime, $\alpha, \alpha^2, \ldots \alpha^{q-1}$ each have order q and are in F_p.

Let $$f(x) = x^q - 1$$

Then $f(x) = (x-1)(x-\alpha) \ldots\ldots (x - \alpha^{q-1})$ splits into linear factors in F_p.

Theorem 69 : *The coefficients of* $\Phi_n(x) \in \mathbf{Q}[x]$ *are integers for all* $n \geq 1$.

Proof : We prove the result by induction on n. Let $n = 1$.

Then $\Phi_n(x) = \Phi_1(x) = x - 1 \in \mathbf{Z}[x]$. Assume that the result is true for all positive integers $m < n$.

Then $\Phi_d(x) \in \mathbf{Z}[x]$, for all $d \mid n$.

Let $$f(x) = \prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) \in \mathbf{Z}[x]$$

Then $$x^n - 1 = \Phi_n(x)\ f(x).$$

Since $f(x)$ is monic, by division algorithm, $x^n - 1 = h(x) f(x) + r(x)$, $h(x), r(x) \in \mathbf{Z}[x]$ and $f(x) = 0$ or $\deg r(x) < \deg f(x)$, $h(x)$, $r(x)$ are uniquely determined.

But $x^n - 1 = \Phi_n(x) f(x)$, $\Phi_n(x) \in \mathbf{Q}[x]$ and $h(x), r(x) \in \mathbf{Z}[x] \subseteq \mathbf{Q}[x]$ are uniquely determined $\Rightarrow \Phi_n(x) = h(x) \in \mathbf{Z}[x]$, $r(x) = 0$.

So, the result is true for n also.

By induction the result is true for all integers $n \geq 1$.

Theorem 70 : *Let* $\Phi_n(x)$ *be nth cyclotomic polynomial over* $\mathbf{Q}$. *Then* $\Phi_n(x)$ *is irreducible over* $\mathbf{Q}$.

Proof : Since $\mathbf{Z}$ is a UFD and $\Phi_n(x) \in \mathbf{Z}[x]$ is monic, $\Phi_n(x)$ is primitive.

$\Phi_n(x)$ is irreducible over $\mathbf{Z}$ if and only if $\Phi_n(x)$ is irreducible over $\mathbf{Q}$, the quotient field of $\mathbf{Z}$.

We show that $\Phi_n(x) \in \mathbf{Z}[x]$ is irreducible over $\mathbf{Z}$.

Let h be an irreducible factor of $\Phi_n(x)$ in $\mathbf{Z}[x]$.

Let $\Phi_n(x) = f(x)\, h(x)$, $f, h \in \mathbf{Z}[x]$, $\deg h \geq 1$.

Since $\Phi_n(x)$ is monic, so are f, h.

Let α be a root of h in $\mathbf{C}$ and let p be a prime such that $(p, n) = 1$.

We show that α^p is also a root of h in $\mathbf{C}$.

Since $h(\alpha) = 0$, $\Phi_n(\alpha) = 0$. So, α is a primitive nth root of unity.

$\Rightarrow o(\alpha) = n \Rightarrow o(\alpha^p) = \dfrac{o(\alpha)}{(p, n)} = n \Rightarrow \alpha^p$ is also a primitive nth root of unity

$\Rightarrow \Phi_n(\alpha^p) = 0 \Rightarrow f(\alpha^p) = 0$ or $h(\alpha^p) = 0$. Suppose $h(\alpha^p) \neq 0$. Then $f(\alpha^p) = 0$ $\Rightarrow \alpha$ is a root of $f(x^p)$.

Now h is irreducible over $\mathbf{Z} \Rightarrow h$ is irreducible over $\mathbf{Q}$ as h is primitive.

Also $h(\alpha) = 0$. So, $h = Irr(\mathbf{Q}, \alpha)$. Since α is also a root of $f(x^p)$ over $\mathbf{Q}$, $h(x)$ divides $f(x^p)$ in $\mathbf{Q}$.

Let $f(x^p) = h(x)\, k(x)$, $k(x) \in \mathbf{Q}[x]$. By division algorithm

$f(x^p) = h(x)\, k_1(x) + r_1(x)$, where $r_1(x) = 0$ or $\deg r_1(x) < \deg h(x)$, $k_1, r_1 \in \mathbf{Z}[x]$. So, $h, r_1 \in \mathbf{Q}[x]$. But in $\mathbf{Q}[x]$, the quotient and remainder obtained by dividing $f(x^p)$ with $h(x)$ are uniquely determined. So, $k(x) = k_1(x) \in \mathbf{Z}[x]$.

Now $\qquad \theta : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$

$$\theta(\Sigma a_i x^i) = \Sigma\, \bar{a}_i\, x^i, \text{ where } a_i = pq_i + \bar{a}_i,\ \bar{a}_i \in \mathbf{Z},\ 0 \le \bar{a}_i < p$$

$$(\text{i.e., } \theta(g(x)) = \bar{g}(x))$$

is a ring homomorphism.

So, $\qquad \theta(f(x^p)) = \theta(h(x))\, \theta(k(x))$

$\Rightarrow \qquad \bar{f}(x^p) = \bar{h}(x^p)\, \bar{k}(x^p)$

Since $\operatorname{char} \mathbf{Z}_p = p$, $\bar{f}(x^p) = (\bar{f}(x))^p$

$\Rightarrow$ $\bar{h}(x)$ divides $(\bar{f}(x))^p$

$\Rightarrow$ some irreducible factor $\overline{h_1}$ of $\bar{h}$ divides $(\bar{f}(x))^p$

$\Rightarrow$ $\overline{h_1}$ divides $\bar{f}(x)$ in $\mathbf{Z}_p[x]$

$\Rightarrow$ $\bar{f}, \bar{h}$ have common factor $\overline{h_1}$ in $\mathbf{Z}_p[x]$

Now $\qquad x^n - 1 = \Phi_n(x)\, r(x)$, $r(x) \in \mathbf{Z}[x]$

$$= f(x)\, h(x)\, r(x)$$

$\Rightarrow \qquad x^n - \bar{1} = \bar{f}(x)\, \bar{h}(x)\, \bar{r}(x)$

$\Rightarrow$ $x^n - \bar{1}$ has a multiple root as $\bar{f}, \bar{h}$ have $\overline{h_1}$ as common factor.

Since $\operatorname{char} \mathbf{Z}_p = p$ and $(p, n) = 1$, $x^n - \bar{1}$ has distinct roots.

So, we get a contradiction.

So, $h(\alpha^p) = 0$. Thus, whenever $h(\alpha) = 0$ and $(p, n) = 1$, p a prime, then $h(\alpha^p) = 0$.

Now $\qquad \Phi_n(x) = \prod_{\substack{(r,n)=1 \\ 1 \le r \le n}} (x - \alpha^r)$, $o(\alpha) = n$.

Let $(r, n) = 1$, $r > 1$, $r = p_1^{k_1} p_2^{k_2} \ldots\ldots p_s^{k_s}$, where $p_i s$ are distinct primes. Since $(r, n) = 1$, $(p_i, n) = 1$ for all i.

Therefore, α^{p_i} is a root of h for all i.

$\Rightarrow$ $\alpha^{p_i^{k_i}}$ is a root of h for all i.

$\Rightarrow$ α^r is a root of h.

Therefore, $\Phi_n(x)$ divides $h(x)$.

But $h(x)$ already divides $\Phi_n(x)$.

Thus, $\Phi_n(x) = h(x)$ is irreducible over $\mathbf{Q}$.

Theorem 71 : *$\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois, where α is a primitive nth root of unity over $\mathbf{Q}$.*

Proof : Now $\mathbf{Q}(\alpha)$ is a minimal splitting field of $f(x) = x^n - 1$ over $\mathbf{Q}$

$\Rightarrow$ $\mathbf{Q}(\alpha)/\mathbf{Q}$ is finite normal.

Also, char $\mathbf{Q} = 0 \Rightarrow \mathbf{Q}$ is perfect $\Rightarrow \mathbf{Q}(\alpha)/\mathbf{Q}$ is seperable.

So, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois.

Theorem 72 : *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be n distinct roots of unity over $\mathbf{Q}$ in $\mathbf{C}$. Then $\Phi_n(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \in \mathbf{Q}[x]$.*

Proof : Let α be a primitive nth root of unity over $\mathbf{Q}$. By above theorem, $\mathbf{Q}(\alpha)/\mathbf{Q}$ is Galois $\Rightarrow \mathbf{Q}$ is the fixed field of G, the group of all $\mathbf{Q}$-automorphisms of $\mathbf{Q}(\alpha)$. Let $\sigma \in G$. Then $0(\sigma(\alpha)) = 0(\alpha) \Rightarrow \sigma(\alpha)$ is also a primitive nth root of unity in $\mathbf{C}$.

So, $\sigma(\Phi_n(x)) = (x - \sigma(\alpha_1)) \ldots (x - \sigma(\alpha_n))$. But $\mathbf{C}$ already has n roots of $f(x) = x^n - 1 \in \mathbf{Q}[x]$

$\Rightarrow$ $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$

$\Rightarrow$ $\sigma(\Phi_n(x)) = (x - \alpha_1) \ldots (x - \alpha_n) = \Phi_n(x)$

Let $\Phi_n(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \quad a_i \in \mathbf{C}$

Then
$$\begin{aligned}\Phi_n(x) &= \sigma(\Phi_n(x)) \\ &= x^n + \sigma(a_1) x^{n-1} + \ldots + \sigma(a_n)\end{aligned}$$

$\Rightarrow$ $\sigma(a_i) = a_i$ for all $i, \sigma \in G$

$\Rightarrow$ a_i belongs to the fixed field of G

$\Rightarrow$ $a_i \in \mathbf{Q}$, for all i

$\Rightarrow$ $\Phi_n(x) \in \mathbf{Q}[x]$.

Theorem 73 : *Let $U_n = \{a \in Z \mid 1 \le a \le n, \ (a, n) = 1\}$. Then U_n is a group under multiplication modulo n. If G is the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}$, then $G \cong U_n$.*

Proof : By Artin's theorem,

$$\begin{aligned}o(G) = [\mathbf{Q}(\alpha) : \mathbf{Q}] &= \deg \ Irr(\mathbf{Q}, \alpha) \\ &= \deg \ \Phi_n(x) \\ &= \varphi(n)\end{aligned}$$

Let $\sigma \in G$. Then $\sigma(\alpha)$ is a primitive nth root of unity in $\mathbf{C} \Rightarrow \sigma(\alpha) = \alpha^i$, for some i, $(i, n) = 1$

Define $\theta : G \to U_n$ s.t.,

$\theta(\sigma) = i$.

Let $\sigma, \eta \in G$. Let $\theta(\sigma) = i$, $\theta(\eta) = j$

Then $(\sigma\eta)(\alpha) = \sigma(\eta(\alpha)) = \sigma(\alpha^j) = (\sigma(\alpha))^j = \alpha^{ioj}$

So, $\theta(\sigma\eta) = ioj = \theta(\sigma) o \, \theta(\eta)$.

Thus, θ is a homomorphism.

Let $\theta(\sigma) = \text{Identity} = 1$.

Then $\sigma(\alpha) = \alpha \Rightarrow \sigma = I \Rightarrow \theta$ is 1-1.

So, $\because \quad G \cong \theta(G) \leq U_n$.

But $o(G) = \varphi(n) \Rightarrow 0(\theta(G)) = \varphi(n) = o(U_n)$.

$\Rightarrow (o(\theta(G)) = o(U_n) \Rightarrow \theta(G) = U_n \Rightarrow G \cong U_n$.

Note : If V_n denotes the units of $\dfrac{\mathbf{Z}}{<n>}$, then V_n forms a group under multiplication and $V_n \cong U_n$.

Proof : $\dfrac{\mathbf{Z}}{<n>} = \{<n>+1, \ <n>+2, \ldots\ldots, <n>+n\}$.

Let $<n>+a$ be a unit in $\dfrac{\mathbf{Z}}{<n>}$.

Then $\quad (<n>+a) \ (<n>+b) = <n>+1, \quad 1 \leq b \leq n$

$\Rightarrow <n>+ab = <n>+1$

$\Rightarrow 1-ab \in <n> \Rightarrow 1-ab = nm$

Let $(a, n) = d > 1$. Let p be a prime dividing d. Then $p \mid d \mid a \Rightarrow p \mid a \Rightarrow p \mid ab$. Also $p \mid n \Rightarrow p \mid nm \Rightarrow p \mid ab + nm = 1$, not true.

$\Rightarrow \quad (a, n) = 1 \Rightarrow a \in U_n$.

Define $\quad f: V_n \to U_n$ s.t.,

$f(<n>+a) = a$

Then f is a 1-1 homomorphism.

Also, $\quad a \in U_n \Rightarrow (a, n) = 1$

$\Rightarrow ar + ns = 1$ for some integers r, s

$\Rightarrow (<n>+a) \ (<n>+r) = <n>+1$

Let $\quad r = nq + t, \quad 0 \leq t < n$

So, $<n>+r = <n>+t$.

If $t = 0$, then $<n>+t = <n>+n$.

So, $<n>+r \in \dfrac{\mathbf{Z}}{<n>}$. Therefore, $<n>+a$ is a unit in $\dfrac{\mathbf{Z}}{<n>}$.

$\Rightarrow <n>+a \in V_n$ and $\theta(<n>+a) = a \Rightarrow \theta$ is onto.

So, $\quad V_n \cong U_n$.

Problem 40 : *If α is a primitive nth root of unity over k, then $k(\alpha)/k$ is Galois.*

Solution : Let $f(x) = x^n - 1 \in k[x]$. Let $g(x) = Irr\,(k, \alpha)$.

Now $f(x)$ splits in $k(\alpha)$ and $f(\alpha) = 0 \Rightarrow g(x) \mid f(x)$ in $k[\alpha]$.

But zeros of $f(x)$ are simple in $k[\alpha]$

$\Rightarrow$ α is a simple zero

$\Rightarrow$ α is seperable over k

$\Rightarrow$ $k(\alpha)/k$ is seperable

Also $k(\alpha)/k$ is a minimal splitting field of $f(x)$ over k, $k(\alpha)/k$ is finite normal $\Rightarrow$ $k(\alpha)/k$ is Galois.

Problem 41 : *Let* $\Phi_n(x) = (x-\alpha_1)(x-\alpha_2) \ldots\ldots (x-\alpha_n)$, where $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ *are nth roots of unity over k. Show that* $\Phi_n(x) \in P[x]$, *where P is the prime subfield of k.*

Solution : We prove the result by induction on n. Let $n = 1$.

Then $\Phi_n(x) = \Phi_1(x) = x - 1 \in P[x]$ as $1 \in P$.

Assume that the result is true for all integers $m < n$.

Then $\Phi_d(x) \in P[x]$ for $d < n$. Let $f(x) = \prod_{d|n} \Phi_d(x) \in P[x]$.

Then $$x^n - 1 = \Phi_n(x) f(x)$$

Since $x^n - 1$, $f(x) \in P[x]$, by division algorithm

$$x^n - 1 = h(x) f(x) + r(x), \qquad h(x),\ r(x) \in P[x]$$

and are uniquely determined such that $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

Now $x^n - 1 = \Phi_n(x)\ f(x)$, where $\Phi_n(x) \in k(\alpha)[x]$ and $x^n - 1 \in P[x] \subseteq k(\alpha)[x]$ (Here α is a primitive nth root of unity over k), $f(x) \in P[x] \subseteq k(\alpha)[x]$.

So, $h(x) = \Phi_n(x) \in P[x] \Rightarrow$ the result is true for n also. By induction the result is true for all integers $n \geq 1$.

Problem 42 : *Determine the Galois group of Cyclotomic extension* $\mathbf{Q}(\alpha)/\mathbf{Q}$, *where* α *is a primitive* 12*th root of unity over* $\mathbf{Q}$. *Also, find the intermediate fields between* $\mathbf{Q}$ *and* $\mathbf{Q}(\alpha)$.

Solution : Let G denote the Galois group of $\mathbf{Q}(\alpha)/\mathbf{Q}$.

Since α is a primitive 12th root of unity, $o(\alpha) = 12$.

Also, $o(G) = \varphi(12) = 4$ and $G = \{\sigma_1 = I,\ \sigma_5, \sigma_6, \sigma_7, \sigma_{11}\}$, where $\sigma_5(\alpha) = \alpha^5$, $\sigma_7(\alpha) = \alpha^7$, $\sigma_{11}(\alpha) = \alpha^{11}$.

Also $\sigma_5^2(\alpha) = \sigma_5\sigma_5(\alpha) = \alpha^{25} = \alpha \Rightarrow \sigma_5^2 = I$.

Similarly, $\sigma_7^2 = I = \sigma_{11}{}^2$.

$\Rightarrow$ G is non cyclic group of order 4 i.e., G is Klein's 4-group.

Let $H_1 = \{I, \sigma_5\}$, $H_2 = \{I, \sigma_7\}$, $H_3 = \{I, \sigma_{11}\}$, $H_4 = \{I\}$, $H_5 = G$.

Then these are the only subgroups of G.

Now $$\sigma_5(\alpha^3) = (\sigma_5(\alpha))^3 = \alpha^{15} = \alpha^3$$

$\Rightarrow$ σ_5 fixes α^3

$\Rightarrow$ H_1 fixes α^3

If F_1 is the fixed field of H_1, then

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha^3) \subseteq F_1 \subseteq \mathbf{Q}(\alpha)$$

But $$[\mathbf{Q}(\alpha^3) : \mathbf{Q}] = [\mathbf{Q}(i) : \mathbf{Q}], \qquad \alpha = e^{\frac{2\pi i}{12}}$$
$$= \deg Irr\,(\mathbf{Q}, i)$$
$$= \deg\,(x^2 + 1) = 2$$

Also, by Artin's theorem

$2 = o(H_1) = [\mathbf{Q}(\alpha) : F_1]$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = o(G) = 4 \Rightarrow F_1 = \mathbf{Q}(\alpha^3)$

If F_2 is the fixed field of H_2, then $\sigma_7(\alpha^4) = \alpha^{28} = \alpha^4 \Rightarrow \alpha^4 \in F_2$. But

$$\alpha^4 = e^{\frac{2\pi i}{3}} = \frac{-1}{2} + \frac{\sqrt{3}\,i}{2}$$

$$\Rightarrow \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i)$$

So, $$\mathbf{Q} \subseteq \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i) \subseteq F_2 \subseteq \mathbf{Q}(\alpha)$$

and $$[\mathbf{Q}(\sqrt{3}i) : \mathbf{Q}] = \deg Irr\,(\mathbf{Q}, \sqrt{3}i)$$
$$= \deg\,(x^2 + 3) = 2$$

Also $[\mathbf{Q}(\alpha) : F_2] = 2$ by Artin's theorem

$$\Rightarrow F_2 = \mathbf{Q}(\alpha^4) = \mathbf{Q}(\sqrt{3}i)$$

Now $$\sigma_{11}(\alpha) = \alpha^{11} \Rightarrow \sigma_{11}(\cos\tfrac{\pi}{6} + i\sin\tfrac{\pi}{6}) = \cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}$$

$$\Rightarrow \sigma_{11}\left(\frac{\sqrt{3}}{2} + \frac{1}{2}i\right) = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

But $$\sigma_{11}(i) = \sigma_{11}(\alpha^3) = \alpha^{33} = \alpha^9 = -i$$

So, $$\tfrac{1}{2}\sigma_{11}(\sqrt{3}) - \tfrac{1}{2}i = \frac{\sqrt{3}}{2} - \frac{1}{2}i$$

$$\Rightarrow \sigma_{11}(\sqrt{3}) = \sqrt{3} \Rightarrow H_3 \text{ fixes } \sqrt{3}$$

Thus, if F_3 is the fixed field of H_3, then $F_3 = \mathbf{Q}(\sqrt{3})$

Also, $F_4 = \mathbf{Q}(\alpha) =$ the fixed field of H_4

$F_5 = \mathbf{Q} =$ the fixed field of H_5.

Finite Fields

A field having finite number of elements is called a finite field or a Galois field.

Theorem 74 : *If F is a finite field, then $o(F) = p^n$ for some prime p and an integer $n \geq 1$.*

Proof : Let P be the prime subfield of F.

Since F is finite, so is P. Therefore, $P \cong \dfrac{\mathbf{Z}}{<p>}$ for some prime p.

But $\dfrac{\mathbf{Z}}{<p>} \cong \{0, 1, 2, \ldots\ldots, p-1\} \bmod p = F_p \Rightarrow P \cong F_p$.

Since $P \subseteq F$, we can regard $F_p \subseteq F$. Now F is a vector space over F_p. Since F is finite, $[F : F_p] = n =$ finite.

Let $\{u_1, \ldots\ldots, u_n\}$ be a basis of F/F_p.

Then $F = \{\alpha_1 u_1 + \ldots\ldots + \alpha_n u_n \mid \alpha_i \in F_p\}$.

Now each α_i can be chosen in p ways and $\Sigma\alpha_i u_i = \Sigma\beta_i u_i \Rightarrow \alpha_i = \beta_i$, therefore $o(F) = p^n$.

Remark : We had proved this result earlier under rings also (see page 237).

Theorem 75 : *Let p be a prime and $n \geq 1$ be an integer. Then there exists a field with p^n elements.*

Proof : Let $f(x) = x^q - x \in F_p[x]$, $q = p^n$. Let F be a minimal splitting field of $f(x)$ over F_p.

Then $\quad F = F_p$ (zeros of f in F).

Let $\quad S = \{$zeros of f in $F\}$.

Now $\quad f' = qx^{q-1} - 1 = -1$ as $\operatorname{char} F = p \Rightarrow q - 1 = p^n - 1 = 0$.

Therefore, $\quad (f, f') = 1$

$\Rightarrow$ all zeros of f in F are simple and so distinct.

So, $\quad o(S) = q$.

Now $0 \in S \Rightarrow S \neq \varphi$.

Also $a, b \in F_q \Rightarrow a^q = a, \quad b^q = b \Rightarrow (a \pm b)^q = a^q \pm b^q = a \pm b$,

$(ab)^q = a^q b^q = ab, \quad (ab^{-1})^q = a^q b^{-q} = ab^{-1}$

$\Rightarrow a \pm b, \ ab, \ ab^{-1}$ (if $b \neq 0) \in S$.

Thus, S is a subfield of F.

Let $a \in F_p$. Then $a^{p-1} = 1 \Rightarrow a^p = a \Rightarrow a^{p^n} = a \Rightarrow a^q = a$.

$\Rightarrow a$ is a zero of f in $F \Rightarrow a \in S \Rightarrow F_p \subseteq S$.

So S is a field containing F_p and S.

But F is the smallest field containing F_p and S.

$\Rightarrow F \subseteq S$. Also $S \subseteq F$. So, $S = F \Rightarrow o(F) = o(S) = q$.

We first prove the following results from group theory.

Lemma 1 : *Let G be an abelian group under multiplication. Let $a, b \in G$ be such that $o(a) = m$, $o(b) = n$ and $(m, n) = 1$. Then there exists $c \in G$ such that $o(c) = mn = l.c.m.$ of m and n.*

Proof : Now $(ab)^{mn} = a^{mn} \ b^{mn} = (a^m)^n (b^n)^m = 1 =$ identity of G

If $(ab)^t = 1$, then $a^t b^t = 1$

$\Rightarrow a^t = b^{-t} \Rightarrow a^{mt} = b^{-mt} \Rightarrow b^{-mt} = 1$

$\Rightarrow b^{mt} = 1 \Rightarrow o(b) \mid mt \Rightarrow n \mid mt \Rightarrow n \mid t$ as $(n, m) = 1$. Similarly, $m \mid t$. So, $mn \mid t \Rightarrow t \geq mn \Rightarrow o(ab) = mn$.

Lemma 2 : *Let G be an abelian group under multiplication. Let $a, b \in G$ be such that $o(a) = m$, $o(b) = n$. Then there exits $c \in G$ such that $o(c) =$ l.c.m. of m and n.*

Proof : Let $(m, n) > 1$.

Let $$m = p_1^{\alpha_1} \ldots\ldots p_r^{\alpha_r}$$

$$n = p_1^{\beta_1} \ldots\ldots p_r^{\beta_r}$$

where $p_1, \ldots\ldots, p_r$ are distinct primes and α_i, β_i are non negative integers.

Let $$l = p_1^{\alpha_1} \ldots\ldots p_s^{\alpha_s}\ p_{s+1}^{\beta_{s+1}} \ldots\ldots p_r^{\beta_r}$$

where $\alpha_i \geq \beta_i$ for $i = 1, \ldots\ldots, s$ and $\beta_j \geq \alpha_j$ for $j = s+1, \ldots\ldots, r$.

Then l is the l.c.m. of m and n.

Let $$x = a^{p_{s+1}^{\alpha_{s+1}} \ldots\ldots p_r^{\alpha_r}}, \quad y = b^{p_1^{\beta_1} \ldots\ldots p_s^{\beta_s}}$$

Then $$o(x) = p_1^{\alpha_1} \ldots\ldots p_s^{\alpha_s}$$

$$o(y) = p_{s+1}^{\beta_{s+1}} \ldots\ldots p_r^{\beta_r}$$

and $$(o(x),\ o(y)) = 1.$$

By lemma 1,

$$o(xy) = \text{l.c.m. of } m \text{ and } n$$

$$= p_1^{\alpha_1} \ldots\ldots p_s^{\alpha_s}\ p_{s+1}^{\beta_{s+1}} \ldots\ldots p_r^{\beta_r}$$

Lemma 3 : *With the hypothesis of lemma 2, if $n \nmid m$, then the l.c.m. l of m and n is greater than m.*

Proof : Now $m \mid l \Rightarrow m \leq l$. If $m = l$, then $n \mid l \Rightarrow n \mid m$, a contradiction. So $l > m$.

Lemma 4 : *Let G be a finite abelian group under multiplication. Let $\alpha \in G$ be of maximum order. Then $o(\beta) \mid o(\alpha)$ for all $\beta \in G$.*

Proof : Let $o(\alpha) = m$, $o(\beta) = n$.

Suppose $n \nmid m$. By lemma 3, $l =$ l.c.m. of $m, n > m$. By lemma 2, there is $\gamma \in G$ such that $o(\gamma) = l > m$ contradicting $\alpha \in G$ is of maximum order. So, $n \mid m$ $\Rightarrow$ $o(\beta) \mid o(\alpha)$ for all $\beta \in G$.

Theorem 76 : *Let F be a finite field. Then F^*, the set of non zero elements of F forms a cyclic group under multiplication in F.*

Proof : Now F^* is an abelian group under multiplication.

Let $\alpha \in F^*$ be an element of maximum order m.

Then by lemma 4, $o(\beta) \mid m$ for all $\beta \in F^*$.

So, $m = o(\beta)r \Rightarrow \beta^m = \beta^{o(\beta)r} = 1$ for all $\beta \in F^*$.

$\Rightarrow \beta$ satisfies $x^m - 1$ over F.

Since F can't have more than m zeros of $x^m - 1$, $o(F^*) \leq m$.

But $\alpha \in F^*$ and $o(\alpha) = m \Rightarrow 1, \alpha, \alpha^2, \ldots\ldots, \alpha^{m-1}$ are distinct elements of F^*

$\Rightarrow o(F^*) \geq m \Rightarrow o(F^*) = m = o(\alpha) \Rightarrow F^* = <\alpha>$.

The generators of F^* are called *primitive elements* of F.

Theorem 77 : *Let F be a finite field of order p^n. Then F is a minimal splitting field of $x^{p^n} - x$ over F_p.*

Proof : We can regard F as an extension of F_p. Let $q = p^n$.

Now $F^* = <\alpha>$, $o(\alpha) = o(F^*) = q - 1$. Also $\alpha^{q-1} = 1$. $\Rightarrow \alpha^q = \alpha$.

$\Rightarrow$ elements of F are zeros of $f(x) = x^q - x$ over F_p.

So, $f(x)$ splits in F.

Therefore, $\qquad f(x) = x(x - \alpha) \ldots\ldots (x - \alpha^{q-1})$

$\Rightarrow$ Minimal splitting field of f over F_p is $F_p(\alpha, \alpha^2, \ldots\ldots, \alpha^{m-1}, 1, 0) = F_p(F) = F$.

Theorem 78 : *Any two finite fields with the same number of elements p^n are F_p-isomorphic.*

Proof : Let F_1, F_2 be finite fields such that $o(F_1) = p^n = o(F_2)$. Then, by above theorem F_1, F_2 are minimal splitting fields of $f(x) = x^{p^n} - x$ over $F_p \Rightarrow F_1, F_2$ are F_p-isomorphic.

The above theorem shows that there is unique field of order $q = p^n$ upto an isomorphism. It is denoted by $GF(p^n)$ or $GF(q)$ or Fq.

Problem 43 : *Show that $x^m - 1$ divides $x^n - 1$ over a field F if and only if m divides n.*

Solution : Let $n = km + r$, $0 \leq r < m$.

Then $x^n - 1 = x^r(\sum_{i=0}^{k-1} x^{im})(x^m - 1) + (x^r - 1)$.

Therefore, $x^m - 1$ divides $x^n - 1$ if and only if $x^r - 1 = 0$.

Also $x^r - 1 = 0$ if and only if $r = 0$.

So $x^m - 1$ divides $x^n - 1$ if and only if m divides n.

Problem 44 : *Show that $x^{p^m} - x$ divides $x^{p^n} - x$ if m divides n.*

Solution : Let $n = mu$.

Then
$$\begin{aligned} p^n - 1 &= p^{mu} - 1 \\ &= (p^m)^u - 1 \\ &= (p^m - 1) \text{ (integer)} \end{aligned}$$

$\Rightarrow p^m - 1$ divides $p^n - 1$

By above problem

$$x^{p^m - 1} - 1 \text{ divides } x^{p^n - 1} - 1$$

$$\Rightarrow \quad x^{p^m}-x \text{ divides } x^{p^n}-x.$$

Theorem 79 : *Let F be a field with p^n elements. Then F has a subfield k with p^m elements if and only if m divides n.*

Proof : Suppose k is a subfield of F. Then k can be regarded as an extension of F_p such that $[k : F_p] = m$. Similarly, F can be regarded as an extension of F_p such that $[F : F_p] = n$. Now $[F : F_p] = [F : k]\,[k : F_p] \Rightarrow m$ divides n.

Conversely, let F be a field such that $o(F) = p^n$. Suppose m divides n. Now F is a minimal splitting field of $x^{p^n}-x$ over F_p.

Let $f(x) = x^{p^n}-x$ and $g(x) = x^{p^m}-x$.

Since m divides n, by above problem $g(x)$ divides $f(x)$.

Consider $F' = \{\text{zeros of } g(x) \text{ in } F\}$.

Then F' is a subfield of F.

Since $g(x)$ has p^m distinct zeros, F' is a subfield of F with p^m elements.

If k is another subfield of F such that $o(k) = p^m$, then $o(k) = o(F') = p^m$.

$\Rightarrow k, F'$ are F_p-isomorphic.

Thus, there is exactly one subfield of F (upto isomorphism) with p^m elements.

Problem 45 : *Determine the algebraic closure of F_p.*

Solution : Now $m!$ divides $n!$ for all positive integers $m < n$. By above theorem $F_{p^{m!}}$ is a subfield of $F_{p^{n!}}$. Thus, there is an ascending chain of subfields

$$F_p \subseteq F_{p^{2!}} \subseteq F_{p^{3!}} \subseteq \cdots\cdots$$

and

$F_{p^\infty} = \bigcup_n F_{p^{n!}}$ is a field such that $F_{p^n} \subseteq F_{p^{n!}} \subseteq F_{p^\infty}$ for any positive integer n.

Let S be the set of all polynomials over F_p. Let $f \in S$.

Then the minimal splitting field of f over F_p is a finite field F_{p^n}.

So, each $f \in S$ splits in F_{p^∞}.

Thus, the minimal splitting field of S over F_p is

$F_p(\text{zeros of } f \in S \text{ in } F_{p^\infty}) \subseteq F_{p^\infty}$.

Also, $a \in F_{p^\infty} \Rightarrow a \in F_{p^n}$ for some $n \Rightarrow a$ is zero of $x^{p^n}-x$ over F_p.

Now $f = x^{p^n}-x \in S \Rightarrow a$ is zero of $f \in S$ in F_{p^∞}

$\Rightarrow$ $F_{p^\infty} \subseteq F_p$ (zeros of $f \in S$ in F_{p^∞})

$\Rightarrow$ Minimal splitting field of S over F_p is F_{p^∞}

$\Rightarrow$ F_{p^∞} is the algebraic closure of F_p.

Theorem 80 : *Every finite extension of a finite field is Galois.*

Proof : Let K be a finite extension of a finite field k. Then K is also a finite field. So, char k = char $K = p$, for some prime p. Let $o(k) = p^m$, $o(K) = p^n$.

Now K is a minimal splitting field of $x^{p^n} - x$ over $F_p \Rightarrow K/F_p$ is finite normal. Also F_p is finite $\Rightarrow F_p$ is perfect $\Rightarrow$ every algebraic extension of F_p is seperable $\Rightarrow K/F_p$ is seperable $\Rightarrow K/F_p$ is Galois. Now, $F_p \subseteq k \subseteq K$ and K/F_p is Galois $\Rightarrow K/k$ is Galois.

Cor. : F_q/F_p is Galois, $q = p^n$.

Theorem 81 : *Let F be a finite field. Then there exists an irreducible polynomial of any given degree n over k.*

Proof : Now $F^{(n)}$ is a field of n-tuples. We can regard F as a subfield of $F^{(n)}$. Let $E = F^{(n)}$. Then $[E : F] = n$. Let $E^* = <\alpha>$. Then $E = F(\alpha)$. So, $n = [E : F] = [F(\alpha) : F] = \deg Irr(F, \alpha) \Rightarrow p(x) = Irr(F, \alpha)$ is an irreducible polynomial of degree n over F.

Theorem 82 : *Let G be the group of F_p-automorphisms of F_q. Then G is a cyclic group generated by Fröbenius map of order n, where $q = p^n$.*

Proof : Let $\theta : F_q \to F_q$ s.t.,

$$\theta(b) = b^p.$$

Then θ is called Fröbenius map.

Since char F_p = char $F_q = p$, θ is a homomorphism.

Also θ is 1-1.

Since F_q is finite, θ is onto.

If $b \in F_p$, then $b^p = b \Rightarrow \theta(b) = b$ for all $b \in F_p$.

So, θ is an F_p-automorphism of $F_q \Rightarrow \theta \in G$.

By Artin's theorem, $o(G) = [F_q : F_p]$ as F_p is the fixed field of G.

$\Rightarrow o(G) = n$. We show that $o(\theta) = n$.

Let $\theta^r = I$, Let $F_q^* = <a>$.

Then $a^{q-1} = 1 \Rightarrow a^q = a \Rightarrow a^{p^n} = a$.

Now $\theta^r = I \Rightarrow \theta^r(a) = a \Rightarrow a^{p^r} = a \Rightarrow a^{p^r - 1} = 1$.

$\Rightarrow o(a) \mid p^r - 1 \Rightarrow q - 1 \mid p - 1 \Rightarrow p^n - 1 \mid p^r - 1 \Rightarrow p^n - 1 \le p^r - 1 \Rightarrow n \le r$.

Also $\theta^n(b) = b^{p^n} = b$ for all $b \in F_q \Rightarrow \theta^n = I$.

So, $o(\theta) = n \Rightarrow G = <\theta>$.

Problem 46 : *Prove that every element in a finite field can be written as the sum of two squares.*

Solution : Let F be a finite field such that $o(F) = p^n$.

Case 1 : $p = 2$. Define $\theta : F \to F$ s.t.,

$$\theta(b) = b^2$$

Then
$$\theta(b_1 + b_2) = (b_1 + b_2)^2 = b_1^2 + b_2^2 = \theta(b_1) + \theta(b_2)$$
$$\theta(b_1 b_2) = (b_1 b_2)^2 = b_1^2 b_2^2 = \theta(b_1)\theta(b_2)$$

$\Rightarrow \theta$ is a homomorphism.

Also, θ is 1-1. Since F is finite, θ is onto.

Let $a \in F$. Then there is $b \in F$ such that $\theta(b) = a \Rightarrow a = b^2 = b^2 + 0^2 =$ sum of two squares in F.

Case 2 : $p \neq 2$. Let $a \in F$. Let $X = \{a - x^2 \mid x \in F\}$.

Then $a - x_1^2 = a - x_2^2$, $x_1, x_2 \in F \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = -x_2$ if $x_1 \neq x_2$

$$\Rightarrow o(X) = \frac{p^n - 1}{2} + 1 = \frac{p^n + 1}{2}.$$

Let $Y = \{y^2 \mid y \in F\}$. Then $o(Y) = \dfrac{p^n + 1}{2}$.

Since $X, Y \subseteq F$ and $o(F) = p^n$, $X \cap Y \neq \varphi$.

So, $a - x^2 = y^2$ for some $x, y \in F \Rightarrow a = x^2 + y^2 =$ sum of two squares in F.

Problem 47 : *Show that for any integer a and prime p, $a^p \equiv a \pmod{p}$.*

Solution : Let $a = pq + r$, $0 \leq r < p$.

Then $a \equiv r \pmod{p}$

Now $0 \leq r < p \Rightarrow r \in F_p$

$$\Rightarrow \underbrace{r o r o \ldots\ldots o r}_{p \text{ times}} = r = r$$

$$\Rightarrow r^p - pu = r$$

$$\Rightarrow r^p \equiv r \pmod{p}$$

$$\Rightarrow r^p \equiv a \pmod{p}$$

So, $a \equiv r \pmod{p}$

$$\Rightarrow a^p \equiv r^p \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

(The above result is known as Fermat's theorem)

Problem 48 : *Show that every irreducible polynomial $f(x) \in F_p[x]$ is a divisor of $x^{p^n} - x$ for some n.*

Solution : Let deg $f(x) = d$ and α be a zero of $f(x)$ in an extension of F_p. Then, $[F_p(\alpha) : F_p] = \deg Irr(F_p, \alpha) = \deg f(x) = d$.

So, $o(F_p(\alpha)) = p^d$. Then $\alpha \in F_p(\alpha) \Rightarrow \alpha^{p^d} = \alpha \Rightarrow \alpha$ is a zero of $x^{p^d} - x \in F_p[x]$

$\Rightarrow f(x)$ divides $x^{p^d} - x$.

Problem 49 : *Show than $x^{p^n} - x$ is the product of monic irreducible polynomials in $F_p[x]$ of degree d, d dividing n.*

Solution : Let $f(x) = x^q - x$, $q = p^n$. Let $p(x)$ be a monic irreducible factor of $f(x)$ over F_p. Let α be a zero of $p(x)$ in F, where F is a minimal splitting field of $f(x)$ over F_p. Then $F = F_q$ and $p(x) = Irr(F_p, \alpha)$

Now $\quad F_p \subseteq F_p(\alpha) \subseteq F_q$

and
$$\begin{aligned} n = [F_q : F_p] &= [F_q : F_p(\alpha)]\ [F_p(\alpha) : F_p] \\ &= [F_q : F_p(\alpha)] \deg Irr(F_p, \alpha) \\ &= [F_q : F_p(\alpha)] \deg p(x) \end{aligned}$$

$\Rightarrow$ deg $p(x)$ divides n.

$\Rightarrow$ any monic irreducible polynomial dividing $x^{p^n} - x$ is of degree dividing n.

Problem 50 : *Show that $x^p - x - a$ $(a \neq 0)$ is irreducible over F_p.*

Solution : Let $f(x) = x^p - x - a$

Let α be a zero of $f(x)$ in some extension of F_p. Then $f(\alpha) = 0$

Consider
$$\begin{aligned} f(\alpha + 1) &= (\alpha + 1)^p - (\alpha + 1) - a \\ &= \alpha^p - \alpha - a = f(\alpha) = 0 \\ f(\alpha + 2) &= (\alpha + 2)^p - (\alpha + 2) - a \\ &= (\alpha + 1)^p - (\alpha + 1) - a \\ &= f(\alpha + 1) = 0 \end{aligned}$$

In this way, $\alpha, \alpha + 1, \alpha + 2, \ldots\ldots, \alpha + (p - 1)$ are all zeros of $f(x)$.

Also $f'(x) = px^{p-1} - 1 = -1 \neq 0 \Rightarrow f'(\beta) = -1 \neq 0$ for $\beta = \alpha, \alpha + 1, \ldots\ldots, \alpha + (p - 1)$

$\Rightarrow \alpha, \alpha + 1, \ldots\ldots, \alpha + (p - 1)$ are distinct zeros of $f(x)$

Now $F_p(\alpha)$ is a minimal splitting field of $f(x)$ over F_p.

Also $[F_p(\alpha) : F_p] = \deg Irr(F_p, \alpha) \leq p$ as α satisfies $f(x)$ of degree p.

Since F_p is finite, so is $F_p(\alpha)$.

Also char $F_p(\alpha) = p \Rightarrow o(F_p(\alpha)) = p^m \Rightarrow [F_p(\alpha) : F_p] = m = \deg Irr(F_p, \alpha)$ $= \deg g(x) \leq p$.

Now $\alpha^{p^m} = \alpha$. But $\alpha^p = \alpha + a \Rightarrow \alpha^{p^2} = (\alpha + a)^p = \alpha^p + a^p = \alpha + 2a$ as $a \in F_p$ $\Rightarrow a^p = a$.

In this way, $\alpha^{p^m} = \alpha + ma \Rightarrow \alpha = \alpha + ma \Rightarrow ma = 0 \Rightarrow p$ divides m as $a \neq 0$ $\Rightarrow p \leq m$.

So, $p = m \Rightarrow \deg g(x) = p$. Also $g(x)$ divides $f(x)$ and $\deg g(x) = \deg f(x)$.

$\Rightarrow g(x) = f(x) \Rightarrow f(x)$ is irreducible over F_p.

Problem 51 : *Construct a field of order* 9.

Solution : Let F_9 be the field of order 9. Let $F_3 = \{0, 1, 2\}$ mod 3. Then $[F_9 : F_3] = 2$. Let $f(x) = x^9 - x$. Then F_9 is a minimal splitting field of $f(x)$ over F_3. Let $p(x)$ be an irreducible factor of $f(x)$ over F_3. Let α be a zero of $p(x)$ in F_9. Then α is a zero of $f(x)$. If $\alpha \in F_3$, then $p(x) = x - \alpha \Rightarrow \deg p(x) = 1$. If $\alpha \notin F_3$, then $F_3 \subseteq F_3(\alpha) \subseteq F_9 \Rightarrow [F_9 : F_3] = 2 = [F_9 : F_3(\alpha)]\ [F_3(\alpha) : F_3]$.

Since $\alpha \notin F_3$, $[F_3(\alpha) : F_3] \neq 1$

$\Rightarrow [F_3(\alpha) : F_3] = 2$

But $[F_3(\alpha) : F_3] = \deg Irr\,(F_3, \alpha)$

$= \deg p(x)$

Thus $\deg p(x) = 2$.

Hence any irreducible factor of $f(x)$ over F_3 has degree 1 or 2.

Now
$$\begin{aligned} x^9 - x &= x(x^8 - 1) \\ &= x(x^4 - 1)(x^4 + 1) \\ &= x(x-1)(x+1)(x^2+1)(x^2-x-1)(x^2+x-1) \end{aligned}$$

Note, $x^2 + 1$, $x^2 - x - 1$, $x^2 + x - 1$ are irreducible over F_3 as none of 0, 1, 2 are zeros of these factors.

Let $p(x) = x^2 + 1$. Let α be a zero of $p(x)$.

Then $\{1, \alpha\}$ is a basis of $F_9 = F_3(\alpha)$ over F_3.

So,
$$\begin{aligned} F_9 &= \{a + b\alpha \mid a, b \in F_3\} \\ &= \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}. \end{aligned}$$

Let $u = \alpha + 1$. Then $u^2 = 2\alpha, u^4 = -1$, $u^8 = 1$. So, $o(u) = 8 \Rightarrow F_9^* = \langle u \rangle$.

Therefore, $F_9 = \{0, 1 = u^8, 2 = u^4, \alpha = u^6, \alpha + 1 = u, \alpha + 2 = u^7, 2\alpha = u^2, 2\alpha + 1 = u^3, 2\alpha + 2 = u^5\}$

Now multiplication is defined by elements u^i in F_9. We wish to define addition in F_9 with the help of u^i.

If $u^n + 1 \neq 0$, let $u^n + 1 = u^{z(n)}$.

Define $u^a + u^b = u^{z(a-b)+b}$ if $u^{a-b} + 1 \neq 0$ where $a \geq b$

$= 0$ if $u^{a-b} + 1 = 0$

Let's find

$$u^7 + u^1$$

Now $u^6 + 1 = \alpha + 1 = u^1 \neq 0$. So, $Z(6) = 1$. Therefore, $u^7 + u^1 = u^{Z(6)+1} = u^2$

Also, $u^6 + u^2 = 0$ as $u^4 + 1 = -1 + 1 = 0$. In this way addition is defined in terms of u^i.

Let $a = u^i$. Then write $\log a = i$. If $b = u^j$, then $ab = u^{i \oplus j}$, where $\oplus$ denotes the addition modulo 9.

So, $\log ab = i \oplus j = \log a \oplus \log b$.

Such a logarithm is known as *Zech logarithm*.

Index

Abelian groups, 40, 209
Addition modulo, 43
Algebraic
    closure, 505, 545
    element, 501, 505
    extension, 501
    integer, 507
    number, 507
Alternating group, 126
Angle, trisection of, 529
Annihilating polynominals, 467
Artin's theorem, 562
Annihilator, 432
Associates, 288
Automorphism, 138
    inner, 140
    outer, 151
    of field extensions, 556

Basis, 371
    dual, 426
    ordered, 371
    orthonormal, 393
    standard, 371
Basis representation theorem, 24
Bessel's inequality, 394
Bijection, 7
Binary composition, 11
    operation, 11
    relation, 11
Boolean ring, 226

Cancellation laws, 46
Canonical homomorphism, 102
Cartesian product, 4
Cauchy Schwarz inequality, 389
Cauchy's theorem, 163
Cayley Hamilton theorem, 469
Cayley's theorem, 123
Centralizer, 59, 65
Centre of
    a group, 59
    a ring, 231
Characteristic
    of a ring, 235
    polynomial, 449
    subgroup, 147
    value, 447
    vector, 447
Chinese Remainder theorem, 206
Class
    conjugate, 152
    equivalence, 6
Class equation, 155
Co-domain, 7
Comaximal ideals, 274
Closure, 12
Commutative
    binary composition, 11
    groups, 40
    ring, 221
Commutator, 135
Complement
    of a set, 2
    of a subspace, 384
Composite number, 34
Composition of maps, 9
Congruences, 34
Conjugate
    classes, 152
    elements, 152
Constructible
    circle, 526
    line, 526
    number, 526
    point, 526

Construction with ruler & compass, 525
Content, 332
Co-prime, 28, 310
Correspondence, 7
Coset, 62
double, 176
left, 64
right, 62
Cycle, 16
Cycles of a permutation, 16
Cyclic groups, 71
generators of, 71
Cyclic permutation, 15
subgroups, 73
Cyclotomic field, 576
polynomial, 577

Dedikind theorem, 556
Degree of
a polynomial, 308
a symmetric group, 13
De-Morgan's laws, 3
Derivative, 534
Derived subgroup, 135
Diagonalisable linear operator, 455
Dihedral group, 118
Dimension, 375
Direct products, 199
external, 200
internal, 200
Direct sum decomposition, 483
Divisibility, 23
Division algorithm, 23
Division ring. 224
Divisor, greatest common
(g.c.d.) 27, 287, 321
Domain
Euclidean, 240
integral, 224
of a map, 7
principal ideal, 292
unique factorization, 324
Double coset, 176
Double dual, 427
Dual basis, 246
Dual space, 425

Duplicating the cube, 530

Eigen
value, 447
vector, 447
space, 448
Eisenstein's criterion, 344
Elements
algebraic, 501, 505
conjugate, 152
order of, 71
irreducible, 301
prime, 301
separable, 538
Empty set, 2
Endomorphism, 101
Epimorphism, 101
Equality of
maps, 8
sets, 1
Equivalence
classes, 6
relation, 4
Euclidean
algorithm, 23, 290
domain, 290
ring, 290
space, 387
valuation, 290
Euler's phi function, 79
theorem, 80
Even permutation, 20
Extension
algebraic, 501
degree of, 498
field, 498
Galois, 567
normal, 540
ring, 264
separable, 533
simple, 498, 565
transcendental, 501
External direct product, 200

Factor group, 95
Factorization domain, 324

Fermat's theorem, 81
Field (s), 224, 498
    extension, 498
    of quotients, 271
    perfect, 539
    splitting. 516
Finite abelian groups, 209
Finite characteristic, 235
Finite dimensional vector space, 367
Finite extension, 498
Functions, 7
    one-one, 7
    onto, 7
Functional, 403
Fundamental theorem of
    finite abelian groups, 213
    Galois theory, 570
    group homomorphism, 105
    ring homomorphism, 258
    vector space homomorphism, 361

Galois extensions, 567
Gauss' lemma, 332
Gaussian integers, 222
Generators of
    groups, 71
    subgroups, 133
Gram-Schmidt orthogonalisation
    process, 393
Greatest common divisor
    (g.c.d.), 27, 287, 321
Group(s), 40
    abelian, 40, 213
    alternating, 126
    automorphism of, 101, 138
    centre of, 58
    centraliser of subset of, 59
    class equation of, 155
    commutative, 40
    cyclic, 71
    dihedral, 118
    factor, 95
    homomorphism of, 100
    isomorphism of, 101
    normaliser of, 59
    of automorphism, 138
    order of, 41
    permutations, 123
    quaternion, 42
    quotient, 95
    residues, 43
    simple, 87
    symmetric, 13

Highest common factor, 27, 287
Homomorphism, 101
    kernel of, 104, 257, 359
Homomorphic image, 101

Ideal(s), 240
    comaximal, 274
    left, 240
    maximal, 277
    prime, 281
    principal, 243
    product of, 246
    right, 240
    semi prime, 285
    sum of 242
Idempotent, 237, 415
Identity
    elements, 40
    mapping, 8
Inner product spaces, 386
Intergral domain, 224
Invariant direct sums, 487
Invariant subgroup, 87
Invariant subspaces, 473
Inverse, 40
Irreducible element, 301
    polynomial, 335
Isomorphism, 101, 517

Kernel of homomorphism, 104, 257, 359
Klein's four group, 131

Lagrange's theorem, 63
Leading coefficient of
    a polynomial, 308
Least common multiple (l.c.m.), 30, 288
Left coset, 64

Length of a cycle, 16
Liner combination, 365
diophantine equation, 31
functional, 403
operator, 403
span, 365
transformations, 358, 399
Linearly dependent, (L.D.), 367
independent (L.I.), 367

Map, see *mapping*
Mapping, 7
bijective, 7
co-domain of, 7
composition of , 9
domain of, 7
identity, 8
injective, 7
invertible, 10
one-one, 7
onto, 7
pre-image of element under, 7
range of, 7
Matrix of L.T., 415
Maximal ideal, 277
Minimal polynomial, 468
Möbius inversion formula, 578
Monic polynomial, 502
Monomorphism, 101
Multiplication modulo, 43

Natural homomorphism, 102, 363
Nilpotent element, 237
Non-abelian groups, 197
Non-Singular linear transformations, 410
Norm of a vector, 389
Normaliser, 59
Normal closure, 544
extension, 540
subgroup, 87
Nullity of a L.T., 401
Null set, 2
Null space, 359

Odd permutation, 20
One-one map, 7
onto map, 7
orbit, 15
order of
element, 71
group, 41
permutation, 124
Ordered basis, 371
Ordered pair, 4
Orthogonality, 392
Orthonormal
basis, 393
set, 392
Outer automorphism, 151
Over-ring, 264

Partial order, 5
Partition of
a set, 7
an integer, 165
Perfect field, 539
Permutations, 12
cyclic, 15
disjoint, 18
even, 20
odd, 20
orbit of, 16
similar, 169
p-groups, 171
Polynomials
content of, 332
degree of, 308
irreducible, 335
minimal, 468
monic, 502
primitive, 332
rings, 308
Primary decomposition theorem, 492
element, 301
ideal, 281
number, 33
subfield, 531
Primitive element, 565
polynomial, 332
Principal ideal domain (PID), 292
Projection, 415, 484
Proper subset, 2

Quaternion group. 42
Quotient
  group, 95
  map, 363
  ring, 253
  space, 356

Rank, 401
Relation, 4
  antisymmetric, 4
  conjugacy, 152
  equivalence, 4
  reflexive, 4
  symmetric, 4
  transitive, 4
Relatively prime elements, 28, 300
Remainder theorem, 511
Right coset, 62
Ring(s), 220
  boolean, 226
  centre of, 231
  characteristic of 235
  imbedding of, 264
  of endomorphisms, 265
  commutative, 221
  imbedding of, 264
  of Gaussain integers, 222
  polynomial, 308
  quotient, 253
  with unity, 221
Root(s), 336
  multiple, 512
  of polynomials, 511
  of unity, 576
  simple, 512
Ruler & Compass construction, 525

Scalars, 350
Self conjugate subgroup, 87
Separable element, 538
  extensions, 533
  polynomials, 536
Sets, 1
  complement of, 2
  difference of, 2
  empty 2
  equal, 1
  finite, 2
  intersection of, 2
  null, 2
  proper subset of, 2
  subset of, 2
  union of, 2
  void, 2
Single extension, 498, 565
  root, 512
Space
  dual, 425
  eigen, 448
  quotient, 356
  vector, 350
Splitting fields, 516
Squaring a circle, 530
Subgroup(s), 57
  costes of, 62
  generated by subset, 133
  index of, 64
  internal direct product, 200
  invariant, 87
  normal, 87
  proper, 57
  self conjugate, 87
  sylow p-subgroups, 179
  trivial, 57
  union of, 61
Subring, 229
Subset, 2
Subspace, 352
Sum direct, 353
  of subspaces, 353
Sylow p-subgroups, 174
Sylow theorems, 175, 176, 177
Sylvester law of nullity, 401
Symmetric
  difference, 12
  group, 13
  relation, 4

Totient function, 79
Transcendental extension, 501
Transpose of L.T., 440
Trisecting an angle, 529

Unique factorisation domain (UFD), 324
Unit, 224

Unitary space, 387
Unity, 221

Vector space, 350
basis of, 371
dimension of, 375
liner transformations of, 358, 399
quotient space of, 356
scalars multiplication, 350
vectors, 350
standard basis of, 371

Well ordering principle, 38

Zero divisor, 223
Zero element, 220
Zero polynomial, 308