MCA •31514

DISCRETE MATHEMATICS

मध्यप्रदेश भोज (मुक्त) विश्वविद्यालय – भोपाल
MADHYA PRADESH BHOJ (OPEN) UNIVERSITY - BHOPAL

COURSE WRITERS

V.K. Khanna, Associate Professor, Department of Mathematics, Kirori Mal College, University of Delhi, Delhi
S.K. Bhambri, Associate Professor, Department of Mathematics, Kirori Mal College, University of Delhi, Delhi
Units (1.0-1.4.4, 1.5, 1.7-1.11, 2.0-2.1, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8-2.12, 3.0-3.2, 3.4, 3.6, 3.7.1, 3.8, 3.9, 3.10-3.17, 4.0-4.2, 4.4-4.4.1, 4.6-4.10, 4.12-4.16)

Ch. S.N. Iyengar, Professor, Dept. of Computer Applications, Vellore Institute of Technology, Vellore
V.M. Chandrasekaran, Assistant Professor, Dept. of Mathematics, Vellore Institute of Technology, Vellore
K.A. Venkatesh, Head, Dept. of Computer Applications, Alliance Business Academy, Bangalore
P.S. Arunachalam, Senior Lecturer, Department of Mathematics, S.R.M. Engineering College, Chennai
Units (3.3, 3.5, 3.7, 5.0-5.2, 5.3, 5.4, 5.9-5.13)

Rohit Khurana, Faculty and Head, I.T.L. Education Solutions Ltd., New Delhi
Units (3.9.1, 4.3, 4.4.2, 4.5-4.5.1)

Shamim Akhtar, Senior Lecturer, Jaypee Institute of Information Technology, Noida
Unit (5.5, 5.6-5.8)

Dr. Pratiksha Saxena, Assistant Professor, School of Applied Sciences, Gautam Buddha University, Greater Noida
Units (1.4.5, 1.5.1, 1.6, 2.2-2.2.2, 2.3.1, 2.6.1, 4.5.2, 4.11, 5.3.1, 5.5.1)

Published by Registrar, MP Bhoj (open) University, Bhopal in 2020

VIKAS® PUBLISHING HOUSE PVT. LTD.
E-28, Sector-8, Noida - 201301 (UP)
Phone: 0120-4078900 • Fax: 0120-4078999
Regd. Office: A-27, 2nd Floor, Mohan Co-operative Industrial Estate, New Delhi 1100 44
• Website: www.vikaspublishing.com • Email: helpline@vikaspublishing.com

SYLLABI-BOOK MAPPING TABLE

Discrete Mathematics

Syllabi	Mapping in Book
Unit - I **Arithmetic Progression,** Sequence, Series, Arithmetic Progression, The General Term or *n*th Term of an AP., The Sum of *n* terms of an AP., Arithmetic Mean, AM. of two Given Numbers, Insertion of N AM. Between Two Given Numbers Properties of A P. **Geometric Progression**, Definition, The *n*th Term of G.P., The Sum of N Terms of a G.P., The Sum of an Infinite G.P., Recurring Decimal an Infinite G.P., Geometric Means, Geometric Mean of Two Given Numbers A and B Insertion of N Geometric Means Between Two Quantities Properties of G.P., To Find the Sum of N Terms of the Series. **Harmonic Progression,** Definition, Harmonic Mean (H.M) of Two Given Numbers Relation between AM., G.M. and H.M.	**Unit 1:** Arithmetic and Harmonic Progression (**Pages: 3-50**)
Unit - II **Miscellaneous Series,** Arithmetic - Geometric Series, The Sum of *n* Terms of the Arithmetic - Geometric Series Sigma (CE) Notation, Sum of first *n* Natural Numbers, The Sum of the Squares of First *n* Natural Numbers, The Sum of the Cubes of First *n* Natural Numbers Method of Difference. **Set Theory,** The Concept of a Set, Notations, Representation of a Set, Types of Sets, Theorem on Subsets, Number of Subsets of a Set, Venn Diagram, Set Operations, Laws of Union of sets, Laws of Intersection of Sets, Law of Complement of a Set, Theorem (on Symmetric Difference) De-Morgan's Laws, Applications of Venn Diagrams.	**Unit 2:** Series and Set Theory (**Pages: 51-86**)
Unit - III **Ordered Pairs, Relations & Functions,** Ordered Pairs, Equality of Ordered Pairs, Cartesian Product of Sets, Theorems on Cartesian Products' Relation, Domain and Range of a Relation, Inverse Relation, The Inverse of an Inverse Relation, *Binary* (or Dyadic) relations , Type of Relations, Equivalence Relations, Equivalence Class, Properties of Equivalence Classes Composition of Two Relations, Partition of a Set, Partial Order, Theorem, Functions (Mapping), Types of Mapping, Other Specific Mappings, Types of Binary Operations, Algebraic Structure, Graph of a Function, Real Valued Map., Product of 'Functions, Method of Construction of Operation Table Countable and-Uncountable Sets. **Group Theory,** Introduction-Algebraic Structures, Groups: Definition, Abelian Group, Order of a Group, Semi-group, Some General Properties of Groups, Some Important Theorems on Groups, Theorem on Subgroups, Homomorphism (Definition), Isomorphism (Definition), Theorems on Homomorphism, Definition (Kernel of *f*), Theorems on Homomorphism, Definition (Cyclic Groups), Fundamental Theorem of Homomorphism,	**Unit 3:** Ordered Pair, Relations and Functions Or Group Theory (**Pages: 87-165**)

Unit - IV

Rings and Fields, Quotient Spaces, Rings in General, Some Special Classes of Rings, Field and its Axioms, Sub-ring and Sub-fields, **Vector Space**, Definition, Linear Combination, Linear Independence and linear Dependence, Basis of Vector Space, Vector Space of linear Transformation, Linear Algebra, Algebra of Quaternions,

Unit 4: Rings and Fields
(**Pages: 167-283**)

Unit - IV

Posets and lattices, Partially Ordered Sets (Posets), Totally Order Set, Diagrammatic Representation of a Poset: (Hasse Diagram) Definitions, Maximal Element, Minimal Element, Duality, Product of Two Posets, lattice, Duality and the Idempotent Law, Semi-lattices, Complete lattices, Sub lattice, Convex Sub lattice, Distributive lattice, Complements, Complemented lattices.

Boolean Algebra & Its Applications, Boolean Expressions and Boolean Functions Identities of Boolean Algebra, Duality, Algebra of Switching Circuits.

Unit 5: Poset, Lattice and Boolean Algebra
(**Pages: 285-326**)

CONTENTS

INTRODUCTION

NOTES

Mathematics includes the study of such topics as quantity (number theory), structure (algebra), space (geometry), and change (mathematical analysis). It has no generally accepted definition.

Discrete mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous. In contrast to real numbers that have the property of varying smoothly, the objects studied in discrete mathematics, such as integers, graphs, and statements in logic, do not vary smoothly but have distinct and separated values. Discrete mathematics, therefore, excludes topics in continuous mathematics, such as calculus or Euclidean geometry. Discrete objects can often be enumerated by integers. More formally, discrete mathematics has been characterized as the branch of mathematics dealing with countable sets, i.e., finite sets or sets with the same cardinality as the natural numbers. However, there is no exact definition of the term 'Discrete Mathematics'. Indeed, discrete mathematics is described less by what is included than by what is excluded: continuously varying quantities and related notions. Principally, the discrete mathematics includes arithmetic, geometric and harmonic progression, miscellaneous, arithmetic and geometric series, the fundamental concepts of sets, relations and functions, mathematical logic, group theory, probability, mathematical induction, and recurrence relations, graph theory, and Boolean algebra. Set theory studies sets, which are collections of objects, such as {blue, white, red} or the (infinite) set of all prime numbers. Graph theory, the study of graphs and networks, is often considered part of combinatorics, but has grown large enough and distinct enough, with its own kind of problems, to be regarded as a subject in its own right. Graphs are one of the prime objects of study in discrete mathematics. They are among the most ubiquitous models of both natural and human-made structures. They can model many types of relations and process dynamics in physical, biological and social systems.

This book, *Discrete Mathematics*, is divided into five units. The topics discussed include definition, theorems and various examples which are related to sequence and series, arithmetic, geometric and harmonic progression, miscellaneous, arithmetic and geometric series, set theory, set operation, Venn diagram, ordered pair, relation and function, theorem on Cartesian product, group theory, algebraic structure, homomorphism, rings and fields, quotient space, subring and subfield, vector space, linear combination, linear dependence and independence, poset and lattice, Boolean algebra.

The book follows the Self-Instructional Mode (SIM) format wherein each unit begins with an 'Introduction' to the topic. The 'Objectives' are then outlined before going on to the presentation of the detailed content in a simple and structured format. 'Check Your Progress' questions are provided at regular intervals to test the student's understanding of the subject. 'Answers to Check Your Progress Questions', a 'Summary', a list of 'Key Terms', and a set of 'Self-Assessment Questions and Exercises' are provided at the end of each unit for effective recapitulation.

UNIT 1 ARITHMETIC AND HARMONIC PROGRESSION

NOTES

Structure

1.0 INTRODUCTION

Sequence and series is one of the basic topics in Arithmetic. In detailed collection of elements in which repetitions of any sort are allowed is known as a sequence, whereas series is the sum of all elements. An arithmetic progression is one of the common examples of sequence and series.

An Arithmetic Progression (AP) is a sequence where the differences between every two consecutive terms are the same. In mathematics, a Harmonic Progression (HP) (or harmonic sequence) is a progression formed by taking the reciprocals of an arithmetic progression. On the other hand, a Geometric Progression (GP), also known as a geometric sequence, is a sequence of non–zero numbers where each term after the first is found by multiplying the previous one by a fixed, non–zero number called the common ratio.

In this unit, you will study about the sequence and series, arithmetic, harmonic and geometric progression.

1.1 OBJECTIVES

After going through this unit, you will be able to:

- Explain the concept of sequence and series

- Elaborate on the Arithmetic Progression (AP)
- Discuss the Harmonic Progression (HP) and harmonic mean
- Analyse the Geometric Progression (GP)

NOTES

1.2 SEQUENCE

A *sequence* is an endless succession of numbers placed in a certain order so that there is a first member, a second and so on. Consider, the example of an array.

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots \frac{1}{n}, \ldots$$

This is a sequence where nth member is obtained by taking the reciprocal of n. We can have many more examples, such as,

$$1, 2, 3, \ldots n, \ldots$$

$$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots, \frac{n}{n+1}, \ldots$$

$$-1, 1, -1, \ldots (-1)^n, \ldots \text{ etc.},$$

So, a sequence is of the form,

$$a_1, a_2, a_3, \ldots, a_n, \ldots$$

Where a_i's are real numbers (we shall be dealing only with sequences of real numbers) and each a_i has a definite position. This sequence in the notational form, is written as $<a_n>$ or $\{a_n\}$ where a_n is the nth (general) term of the sequence.

Note: It is not necessary that all the members of the sequence be distinct (as is otherwise clear from the above examples).

1.2.1 Convergence of a Sequence

Consider the following sequence,

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots$$

In this way we can state that as we go along the members of the sequence, the members come closer and closer to zero. Thus as n becomes larger, the members come nearer to zero. In such cases we say that the sequence converges to the **limit zero**.

Now consider the sequence $a_1, a_2, a_3, \ldots, a_n \ldots$ we say that this sequence converges to a number l, if it is possible to make $|a_n - l|$ as small as we like (by making n sufficiently large) which, in other words, would mean something like saying that the sequence $<a_n>$ converges to l if after a certain stage, all the members of the sequence are very near to l.

Definition: A sequence $<a_n>$ is said to converge to a number l, if given any $\varepsilon > 0$, there exists a +ve integer m, such that,

$$|a_n - l| < \varepsilon, \quad \forall\ r \geq m$$

This number l is called *limit* of the sequence.

Also in this case we write,

$$\lim_{n\to\infty} a_n = l$$

It can be easily shown that a sequence cannot converge to more than one limit.

If we use the definition to find limit of the sequence,

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots$$

We note that here $a_n = \frac{1}{n}$; we claim that l is zero. So if $\varepsilon > 0$, is any given number, then we can see that,

$$\left|\frac{1}{n} - 0\right| < \varepsilon,$$

which will be true if $n > \frac{1}{\varepsilon}$

So if we choose m to be a +ve integer greater than $\frac{1}{\varepsilon}$, we find,

$$\left|\frac{1}{n} - 0\right| < \varepsilon \; \forall \; n \geq m$$

and thus, zero is the limit of the sequence.

As a particular case, suppose that $\varepsilon = \frac{1}{1000}$, then if we choose $m = 1001$

Then $$m > \frac{1}{\varepsilon} = 1000$$

And $$\left|\frac{1}{n} - 0\right| < \frac{1}{1000} \forall\ n \geq m$$

So we find that the value of m depends upon the value of ε, the smaller the value of ε, the larger the value of m.

1.2.2 Divergent Sequence

Let $<a_n>$ be a given sequence and suppose K is any large number. If we find that except for a finite number of elements of the sequence, all members are greater than K, we say that the sequence has $+\infty$ as its limit. In such a case the sequence $<a_n>$ is said to diverge to $+\infty$.

Definition: A sequence $<a_n>$ is said to diverge to $+\infty$, if for each positive number K, (however large), it is possible to find a +ve integer m, such that,

$$a_n > K \quad \forall\ n \geq m$$

Similarly, a sequence $<a_n>$ is said to diverge to $-\infty$, if for each negative number K (however small), it is possible to find a +ve integer m, such that,

$$a_n < K \quad \forall\ n \geq m$$

NOTES

In the notation, the above two are expressed as,

$$\lim_{n\to\infty} a_n = +\infty$$
$$\lim_{n\to\infty} a_n = -\infty$$

As an example the sequence < 1, 2, 3, . . .*n*, . . . > diverges to $+\infty$ and the sequence < –1, –2, –3, . . . –*n*, > diverges to $-\infty$.

A sequence is thus convergent if it has a finite limit and is divergent otherwise (i.e., when the limit is infinite or it does not exist).

Note: Many authors follow the following definition:

Definition: A sequence is convergent if it has finite limit. It is divergent if it tends to $+\infty$ or $-\infty$ and the sequence is called *oscillatory* if the limit does not exist. Thus the sequence, $< -1, 1, -1, 1, \ldots, (-1)^n, \ldots > < -1, 2, -3, 4, \ldots .., (-1)^n n, \ldots >$ are oscillatory.

1.2.3 Bounded Sequence

A sequence $<a_n>$ is said to be *bounded* if there exist numbers *k* and *K* such that,

$$k \le a_n \le K, \forall\ n$$

For example, the sequence $<\frac{1}{n}>$ is bounded as,

$$0 \le \frac{1}{n} \le 1 \quad \forall\ n$$

1.2.4 Monotonic Sequence

A sequence $<a_n>$ is said be *monotonically increasing* if,

$$a_{n+1} \ge a_n \quad \forall\ n$$

and it is called *monotonically decreasing* if,

$$a_{n+1} \le a_n \quad \forall\ n$$

Also if $a_{n+1} \ge a_n \quad \forall\ n$ we say that the sequence $<a_n>$ is strictly monotonically increasing and if $a_{n+1} \le a_n \quad \forall\ n$ it is called strictly monotonically decreasing.

The sequence $<\frac{1}{n}>$ is clearly strictly monotonically decreasing, whereas, the sequence <*n*> is clearly strictly monotonically increasing.

A sequence which is either increasing or decreasing is called a monotonic sequence.

The sequence <1, –1, 1, . . . > is not monotonic as it is neither increasing nor decreasing.

1.3 SERIES

A series can be highly generalised as the sum of all the terms in a *sequence*. However, there has to be a definite relationship between all the terms of the sequence.

An '**Arithmetic Series'** is the sum of an arithmetic sequence. We find the sum by adding the first, a_1 and last term, a_n, divide by 2 in order to get the mean of the two values and then multiply by the number of values, n: $Sn=n^2(a_1+a_n)$.

The basically could be better understood by solving problems based on the formulas. They are very similar to sets but the primary difference is that in a sequence, individual terms can occur repeatedly in various positions. The length of a sequence is equal to the number of terms and it can be either finite or infinite. With the help of definition, formulas and examples we are going to discuss here the concepts of sequence as well as series.

A sequence is an arrangement of any objects or a set of numbers in a particular order followed by some rule. If a_1, a_2, a_3, a_4,…… ,etc. denote the terms of a sequence, then 1,2,3,4,…..denotes the position of the term. The series is finite or infinite depending if the sequence is *finite or infinite*.

A sequence can be defined based on the number of terms, i.e., either finite sequence or infinite sequence.

If a_1, a_2, a_3, a_4, ……. is a sequence, then the corresponding series is given by

$$S_N = a_1+a_2+a_3 + .. + a_N$$

Table 1.1 *Some Basic Formula of Arithmetic Progression and Geometric Progression*

	Arithmetic Progression	Geometric Progression
Sequence	a, a+d, a+2d,…..,a+(n-1)d,….	a, ar, ar^2,…,$ar^{(n-1)}$,..
Common Difference or Ratio	Successive term – Preceding term Common difference = d = $a_2 - a_1$	Successive term/Preceding term Common ratio = r = $ar^{(n-1)}/ar^{(n-2)}$
General Term (nth Term)	$a_n = a + (n-1)d$	$a_n = ar^{(n-1)}$
nth term from the last term	$a_n = l - (n-1)d$	$a_n = 1/r^{(n-1)}$
Sum of first n terms	$s_n = n/2(2a + (n-1)d)$	$s_n = a(1 - r^n)/(1 - r)$ if r < 1 $s_n = a(r^n -1)/(r - 1)$ if r > 1

Whereas, a = first term, d = common difference, r = common ratio, n = position of term, l = last term

Difference between Sequences and Series

Sequences	Series
Set of elements that follow a pattern	Sum of elements of the sequence
Order of elements is important	Order of elements is not so important
Finite sequence: 1,2,3,4,5	Finite series: 1+2+3+4+5
Infinite sequence: 1,2,3,4,….	Infinite Series: 1+2+3+4+….

NOTES

Infinite Series

When an infinite series has infinite number of terms and there may not be any definite rule to determine its terms. Such a series is denoted by an expression of the form,

$$u_1 + u_2 + u_3 + \ldots + u_n \quad \text{or} \quad \sum_{n=1}^{\infty} u_n \text{ or } \Sigma u_n$$

Convergence of an Infinite Series

The word series in this unit would mean an infinite series. Suppose we are given the series,

$$\Sigma u_n = u_1 + \ldots + u_n + \ldots$$

Let us denote it by,

$$S_1 = u_1$$
$$S_2 = u_1 + u_2$$
$$S_3 = u_1 + u_2 + u_3$$
$$\ldots \ldots \ldots \quad \ldots$$
$$S_n = u_1 + u_2 + \ldots + u_n$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

In this manner, we get a sequence $<S_n>$ to which we call the sequence of partial sums of the given series Σu_n.

Definition: A series Σu_n is defined to be *convergent* or *divergent* according to the state of its sequence of partial sums $<S_n>$ being convergent or divergent. If $<S_n>$ converges to S then S is called *sum* of the series Σu_n.

The following two results are direct consequence of the definition:

(a) *Addition or omission of a finite number of terms in a series does not affect its convergence or divergence.*

(b) *Multiplication of all the terms of a series by a non-zero constant does not affect the convergence or divergence of the series.*

Positive Term Series

If all the terms in a series are positive we call it a positive term series. We have already defined convergence of a series in terms of its sequence of partial sums. In general practice it is found that it may not be always easy to write down the sequence of partial sums. To avoid this, we have a few tests which can be applied directly to the series to see whether it converges or diverges. Before giving the list of these tests, we give below a few important limits which will be useful in the application of these tests.

Some Important Limits

(a) $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e$, where $2 < e < 3$

(b) $\lim_{n\to\infty} n^{1/n} = 1$

(c) $\underset{n\to\infty}{\text{Lim}} \log_e n = \infty$

(d) $\underset{n\to 0}{\text{Lim}} \log_e n = -\infty$

NOTES

Tests to Examine the Nature of a Series

Suppose we have a positive term series Σu_n, then the following tests can be applied to determine the nature of the series:

***Test* 1.** $\underset{n\to\infty}{\text{Lim}}\ u_n \neq 0$, then $\Sigma\, u_n$ is divergent.

***Test* 2.** Σu_n is convergent if and only if there exists a number K, such that $u_1 + u_2 + \ldots + u_n < K$, for all n.

***Test* 3.** Σu_n is divergent, if each term after a fixed stage is greater than some fixed positive number.

***Test* 4.** Comparison tests.

Form 1. If $\Sigma\, u_n$ and $\Sigma\, v_n$ are two positive term series such that, $u_n < kv_n\ \forall n$, where k is some fixed positive number, then Σu_n divergent $\Rightarrow \Sigma v_n$ is divergent and Σv_n convergent $\Rightarrow \Sigma u_n$ is convergent.

Form 2. If Σu_n and Σv_n are two positive term series such that, $kv_n < u_n < Kv_n\ \forall n,$,

where k and K are some fixed positive numbers, then Σu_n and Σv_n converge or diverge together.

Form 3. If Σu_n and Σv_n are two series of positive terms, such that $\underset{n\to\infty}{\text{Lim}} \frac{u_n}{v_n} = l$,

where l is non-zero finite real number then Σu_n and Σv_n converge or diverge together.

Example 1.1: Show that the series $1 + 1 + 1 + 1 + \ldots$ is divergent.

Solution: If u_n is the nth term of the series then,

$$\underset{n\to\infty}{\text{Lim}} u_n = 1 \qquad (\because\ u_n = 1)$$

This is non-zero and thus by Test 1, the series is divergent.

Example 1.2: Test for convergence, the geometric series $1 + r + r^2 + r^3 + \ldots$, $(r > 0)$

Solution: *Case I.* $0 < r < 1$

If S_n denotes the sum of the first n terms of the series, then

$$S_n = 1 + r + r^2 + \ldots + r^{n-1}$$

$$= \frac{1 - r^n}{1 - r} < \frac{1}{1 - r} \text{ for all } n.$$

If we write $K = \frac{1}{1 - r}$, we have $S_n < K\ \forall n$ and thus by Test 2, the series is convergent.

Case II. r = 1. The series becomes $1 + 1 + 1 + \ldots$ by Example 1.1, is divergent.

NOTES

Case III. r>1.

Each term of the series is greater than 1 and so by Test 3, the series is divergent.

Thus we conclude that the above series is convergent, if $0 < r < 1$, and is divergent if $r \geq 1$.

Example 1.3: Test for convergence, the series $1 + \frac{1}{2^p} + \frac{1}{3^p} + \frac{1}{4^p} + \ldots + \frac{1}{n^p} + \ldots$

Solution: Let $S = 1 + \frac{1}{2^p} + \frac{1}{3^p} + \frac{1}{4^p} + \ldots$

Case I. Let $p > 1$

Then,

$$S = 1 + \frac{1}{2^p} + \frac{1}{3^p} + \ldots$$

$$= 1 + \left(\frac{1}{2^p} + \frac{1}{3^p}\right) + \left(\frac{1}{4^p} + \frac{1}{5^p} + \frac{1}{6^p} + \frac{1}{7^p}\right) + \ldots$$

We bracket the terms (leaving the first term 1) such that the brackets contain 2, 4, 8, . . . terms. Then,

$$S < 1 + \left(\frac{1}{2^p} + \frac{1}{2^p}\right) + \left(\frac{1}{4^p} + \frac{1}{4^p} + \frac{1}{4^p} + \frac{1}{4^p}\right) + \ldots$$

$$= 1 + \frac{2}{2^p} + \frac{4}{4^p} + \frac{8}{8^p} + \ldots$$

$$= 1 + \frac{1}{2^{p-1}} + \frac{1}{4^{p-1}} + \frac{1}{8^{p-1}} + \ldots$$

i.e.,

$$S < 1 + \frac{1}{2^{p-1}} + \frac{1}{2^{2(p-1)}} + \frac{1}{2^{3(p-1)}} + \ldots$$

Now RHS is a geometric series with common ratio $\frac{1}{2^{p-1}} < 1$ and is, therefore, convergent by Example 1.2.

So by comparison test the given series is also convergent (when $p > 1$)

Case II. When $p = 1$, we have,

$$S = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$$

$$= 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \ldots$$

Where we bracket the terms (leaving the first two terms) such that the brackets contain 2, 4, 8, . . . terms.

Thus, $S > 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \ldots$

Or $$S > 1 + \frac{1}{2} + \frac{2}{4} + \frac{4}{8} + \ldots$$

$$= 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots$$

$\Rightarrow$ $$S > \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots$$

But RHS is a divergent series according to Test 1.

Hence, by comparison test again the given series is divergent.

Case III. When, $p < 1$

Here, $\frac{1}{n^p} > \frac{1}{n} \forall n$

But $\Sigma \frac{1}{n}$ is divergent by *Case II.*

$\Rightarrow \Sigma \frac{1}{n^p}$ (i.e., the given series is divergent by comparison test).

We thus conclude that the series $\Sigma \frac{1}{n^p}$ is convergent when $p > 1$ *and is divergent* when $p \leq 1$.

This series is called *Auxiliary Series* and is used to solve many problems.

Example 1.4: *Test for convergence of the series,*

$$\frac{1}{1.3.5} + \frac{1}{2.4.6} + \frac{1}{3.5.7} + \frac{1}{4.6.8} + \ldots$$

Solution: Here the *n*th term of the series is,

$$u_n = \frac{1}{n(n+2)(n+4)} = \frac{1}{n^3\left(1 + \frac{2}{n}\right)\left(1 + \frac{4}{n}\right)}$$

Take, $$v_n = \frac{1}{n^3}$$

Then, $$\frac{u_n}{v_n} = \frac{1}{\left(1 + \frac{2}{n}\right)\left(1 + \frac{4}{n}\right)}$$

Now $\text{Lim} \frac{u_n}{v_n} = 1$, which is non-zero and finite.

Also since the auxiliary series $\Sigma v_n = \Sigma \frac{1}{n^3}$ is convergent ($p \geq 1$), it follows by comparison test that the given series is also convergent.

Example 1.5: Examine for convergence of the series,

$$\sum_{1}^{\infty}\left\{\sqrt{n^2+1}-n\right\}$$

NOTES

Solution: Let u_n denote the nth term of the series,

Then,
$$u_n = \sqrt{n^2+1}-n$$
$$= n\sqrt{1+\frac{1}{n^2}}-n$$
$$= n\left[\left(1+\frac{1}{n^2}\right)^{1/2}-1\right]$$
$$= n\left[\left(1+\frac{1}{2}\frac{1}{n^2}+\frac{\frac{1}{2}\left(\frac{1}{2}-1\right)}{2}.\frac{1}{n^4}+\ldots\right)-1\right]$$
$$= n\left[\frac{1}{2n^2}-\frac{1}{8n^4}+\ldots\right]$$
$$= \frac{1}{n}\left[\frac{1}{2}-\frac{1}{8n^2}+\ldots\right]$$

Take, $v_n = \frac{1}{n}$

Then, $\frac{u_n}{v_n} = \frac{1}{2}-\frac{1}{8n^2}+$ terms with higher powers of n

$\Rightarrow \lim_{n\to\infty}\frac{u_n}{v_n} = \frac{1}{2} \neq 0,$ finite

$\Rightarrow$ Σu_n and Σv_n converge or diverge together by comparison test.

But Σv_n is divergent according to Example 1.3.

Hence, Σu_n is divergent.

Aliter. We have,

$$u_n = \sqrt{n^2+1}-n$$
$$= \frac{\sqrt{n^2+1}-n}{\sqrt{n^2+1}+n}\times\sqrt{(n^2+1)}+n$$
$$= \frac{n^2+1-n^2}{\sqrt{n^2+1}+n} = \frac{1}{n\left[\sqrt{1+\frac{1}{n^2}}+1\right]}$$

Take, $v_n = \frac{1}{n}$

NOTES

Then, $$\frac{u_n}{v_n} = \frac{1}{\sqrt{1+\frac{1}{n^2}}+1}$$

$\Rightarrow$ $$\lim_{n\to\infty}\frac{u_n}{v_n} = \frac{1}{1+1} = \frac{1}{2}$$

$\Rightarrow$ Σu_n is divergent as above discussed.

Example 1.6: Test for convergence of the series,

$$\sum_{n=1}^{\infty}\frac{1}{(a+n)^p(b+n)^q}$$ p, q being positive.

Solution: We have,

$$u_n = \frac{1}{(a+n)^p(b+n)^q} = \frac{1}{n^p\left(\frac{a}{n}+1\right)^p n^q\left(\frac{b}{n}+1\right)^q}$$

$$= \frac{1}{n^{p+q}\left(\frac{a}{n}+1\right)^p\left(\frac{b}{n}+1\right)^q}$$

Take, $$\Sigma v_n = \Sigma\frac{1}{n^{p+q}}$$

Then, $$\frac{u_n}{v_n} = \frac{1}{\left(\frac{a}{n}+1\right)^p\left(\frac{b}{n}+1\right)^q}$$

$\Rightarrow \lim_{n\to\infty}\frac{u_n}{v_n} = 1$, which is non-zero finite.

$\Rightarrow \Sigma u_n$ and Σv_n converge or diverge together by comparison test.

But Σv_n is convergent if $p+q>1$ and divergent if $p+q\le 1$ (auxiliary series).

Hence, the given series is convergent when $p+q>1$ and divergent when $p+q\le 1$.

Example 1.7: Test for convergence of the series whose nth term is $\sqrt[3]{(n^3+1)-n}$.

Solution. We have,

$$u_n = (n^3+1)^{1/3} - n$$

$$= n\left(1+\frac{1}{n^3}\right)^{1/3} - n$$

$$= n\left[1+\frac{1}{3n^3}+\frac{\frac{1}{3}\left(\frac{1}{3}-1\right)}{2}\cdot\frac{1}{n^6}+\ldots-1\right]$$

$$= n\left[\frac{1}{3n^3}+\frac{\frac{1}{3}\left(\frac{1}{3}-1\right)}{2}\ \frac{1}{n^6}+\ldots\right]$$

NOTES

$$= \frac{1}{3n^2} + \text{Terms with higher powers of } n \text{ in the denominator.}$$

Take, $v_n = \frac{1}{n^2}$

Then $\frac{u_n}{v_n} = \frac{1}{3} + \text{Terms with higher powers of } n \text{ in the denominator.}$

$\Rightarrow \text{Lim} \frac{u_n}{v_n} = \frac{1}{3}$ (non-zero finite)

$\Rightarrow \Sigma u_n$ is convergent as Σv_n is convergent.

Example 1.8: Show that if Σu_n is a convergent positive term series, then $\text{Lim}\, u_n = 0$. Does the converse hold?

Solution: Let Σu_n be a convergent positive term series. Then $<S_n>$ the sequence of partial sums of Σu_n is convergent (by definition).

Let, $\lim_{n\to\infty} S_n = S$

Now, $u_n = (u_1 + u_2 + \ldots + u_n) - (u_1 + u_2 + \ldots + u_{n-1})$

$= S_n - S_{n-1}$

$\Rightarrow \text{Lim}\, u_n = \text{Lim}(S_n - S_{n-1})$

$= \text{Lim}\, S_n - \text{Lim}\, S_{n-1} = S - S = 0$

Hence, proved.

This is called the *necessary condition* for convergence.

The converse of this does not hold. For example, consider the series,

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} + \cdots$$

Which is divergent according to example 3, although,

$$\lim_{t\to\infty} u_n = \lim_{n\to\infty} \frac{1}{n} = 0$$

Some More Tests

Test 5. **Cauchy's Root Test**

If Σu_n is a +ve term series with $\lim_{n\to\infty} (u_n)^{1/n} = l$, then

(*i*) If $l < 1$, Σu_n is is convergent.

(*ii*) If $l > 1$, Σu_n is divergent.

(*iii*) If $l = 1$, the test fails.

Test 6. **D'Alembert's Ratio Test**

If Σu_n is a +ve term series with $\lim_{n\to\infty} \frac{u_n}{u_{n+1}} = l$, then

(*i*) If $l > 1$, Σu_n is convergent.

(*ii*) If $l < 1, \Sigma u_n$ is divergent.

(*iii*) If $l = 1$, the test fails.

Test 7. **Raabe's Test.**

If Σu_n is a +ve term series with $\underset{n\to\infty}{\text{Lim}}\left[n\left(\frac{u_n}{u_{n+1}}-1\right)\right]=l$, then

(*i*) If $l > 1, \Sigma u_n$ is convergent.

(*ii*) If $l < 1, \Sigma u_n$ is divergent.

(*iii*) If $l = 1$, the test fails.

Test 8. **Logarithmic Test.**

If Σu_n is a +ve term series with $\underset{n\to\infty}{\text{Lim}}\left(n\log_e\frac{u_n}{u_{n+1}}\right)=l$, then

(*i*) If $l > 1, \Sigma u_n$ is convergent.

(*ii*) If $l < 1, \Sigma u_n$ is divergent.

(*iii*) If $l = 1$, the test fails.

Example 1.9: Test for convergence of the series $\Sigma\frac{1}{\left(1+\frac{1}{n}\right)^{n^2}}$.

Solution: Here the *n*th term of the series is,

$$u_n = \frac{1}{\left(1+\frac{1}{n}\right)^{n^2}}$$

Then, $$(u_n)^{1/n} = \frac{1}{\left(1+\frac{1}{n}\right)^{n}}$$

$\Rightarrow$ $$\underset{n\to\infty}{\text{Lim}}(u_n)^{1/n} = \underset{n\to\infty}{\text{Lim}}\frac{1}{\left(1+\frac{1}{n}\right)^{n}} = \frac{1}{e} < 1 \quad (\text{as } e > 2)$$

So by Root test, the given series is convergent.

Example 1.10: Test for convergence of the series,

$$x+\frac{x^2}{2}+\frac{x^3}{3}+\frac{x^4}{4}+\ldots \qquad (x > 0)$$

Solution: The *n*th term of the series is $u_n = \frac{x^n}{n}$

Thus, $$\frac{u_n}{u_{n+1}} = \frac{x^n}{n}\times\frac{n+1}{x^{n+1}} = \left(1+\frac{1}{n}\right).\frac{1}{x}$$

NOTES

Then, $\underset{n\to\infty}{\text{Lim}}\frac{u_n}{u_{n+1}} = \text{Lim}\left(1+\frac{1}{n}\right)\frac{1}{x} = \frac{1}{x}$

NOTES

So if $\frac{1}{x} > 1$, i.e., if $x < 1$, the series is convergent.

And if $\frac{1}{x} < 1$, i.e., if $x > 1$, the series is divergent by Ratio test.

If $x = 1$, the Ratio test fails, but in that case, we note that the given series reduces to the auxiliary series, $1+\frac{1}{2}+\frac{1}{3}+....$ which is divergent ($p = 1$).

Hence, the given series is convergent if $x < 1$ and is divergent if $x \geq 1$.

Example 1.11: Test for convergence of the series,

$$\sum_{n=1}^{\infty}\frac{1.3.5.(2n-1)}{2.4.6...2n}.x^n, \ (x > 0)$$

Solution: If u_n is the nth term of the series then,

$$u_n = \frac{1.3.5...(2n-1)}{2.4.6...2n}.x^n$$

$$u_{n+1} = \frac{1.3.5...(2n-1).(2n+1)}{2.4.6...2n.(2n+2)}.x^{n+1}$$

And

$$\frac{u_n}{u_{n+1}} = \frac{2n+2}{2n+1}.\frac{1}{x} = \frac{\left(1+\frac{1}{n}\right)}{\left(1+\frac{1}{2n}\right)}\frac{1}{x}$$

This gives, $\underset{n\to\infty}{\text{Lim}}\frac{u_n}{u_{n+1}} = \frac{1}{x}$

So by Ratio test if $\frac{1}{x} > 1$, i.e., if $x < 1$, the series is convergent and if $\frac{1}{x} < 1$, i.e., if $x > 1$, the series is divergent.

When $x = 1$, Ratio test fails.

We then use Raabe's test.

By putting $x = 1$ in the given series, we get,

$$\frac{u_n}{u_{n+1}} = \frac{2n+2}{2n+1}$$

i.e.,

$$n\left(\frac{u_n}{u_{n+1}}-1\right) = n\left(\frac{2n+2}{2n+1}-1\right) = \frac{1}{\left(2+\frac{1}{n}\right)}$$

So,

$$\underset{n\to\infty}{\text{Lim}}\ n\left(\frac{u_n}{u_{n+1}}-1\right) = \underset{n\to\infty}{\text{Lim}}\frac{1}{\left(2+\frac{1}{n}\right)} = \frac{1}{2} < 1$$

Thus by Raabe's test, the series is divergent.

Hence, the given series is convergent if $x < 1$ and is divergent if $x \geq 1$.

Example 1.12: Test for convergence of the series,

$$x + \frac{2^2 x^2}{2} + \frac{3^3 x^3}{3} + \frac{4^4 x^4}{4} + \ldots$$

Solution: Let u_n be the nth term of the series then,

$$\frac{u_n}{u_{n+1}} = \frac{n^n x^n}{n} \times \frac{n+1}{(n+1)^{n+1} x^{n+1}} = \frac{n^n}{(n+1)^{n+1.}} \frac{(n+1)}{x}$$

$$= \frac{1}{\left(1+\frac{1}{n}\right)^n} \cdot \frac{1}{x}$$

$$\Rightarrow \text{ Lim} \frac{u_n}{u_{n+1}} = \frac{1}{ex} \text{ as } \text{Lim}\left(1+\frac{1}{n}\right)^n = e$$

Hence, by Ratio test the given series is convergent if $\frac{1}{ex} > 1$

i.e., if $x < \frac{1}{e}$ and it is divergent if $x > \frac{1}{e}$

If $x = \frac{1}{e}$, Ratio test fails.

In this case,

$$\frac{u_n}{u_{n+1}} = \frac{e}{\left(1+\frac{1}{n}\right)^n}$$

Now,

$$\log_e \frac{u_n}{u_{n+1}} = \log e - n \log\left(1+\frac{1}{n}\right)$$

$$= 1 - n\left(\frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3} + \ldots.\right)$$

$$= 1 - 1 + \frac{1}{2n} - \frac{1}{3n^3} + \ldots$$

$$= \frac{1}{2n} - \frac{1}{3n^2} + \ldots$$

$$\Rightarrow n \log_e \frac{u_n}{u_{n+1}} = \frac{1}{2} - \frac{1}{3n} + \text{ Other terms with higher powers of } n \text{ in the denominator.}$$

Thus, $\text{Lim}\left(n \log_e \frac{u_n}{u_{n+1}}\right) = \frac{1}{2} < 1$

Hence, by logarithmic test the series is divergent.

Example 1.13: Prove that the series $\sum_{n=0}^{\infty} \frac{n^3 + a}{2^n + a}$ is convergent by using D'Alembert's Ratio test.

NOTES

NOTES

Solution: We have,

$$\frac{u_n}{u_{n+1}} = \frac{n^3+a}{2^n+a} \times \frac{2^{n+1}+a}{(n+1)^3+a}$$

$$= \frac{n+a}{(n+1)^3+a} \times \frac{2^{n+1}+a}{2^n+a}$$

$$= \frac{1+\frac{a}{n^3}}{\left(1+\frac{1}{n}\right)^3+\frac{a}{n^3}} \times \frac{2+\frac{a}{2^n}}{1+\frac{a}{2^n}}$$

$$\Rightarrow \quad \operatorname{Lim}_{n\to\infty} \frac{u_n}{u_{n+1}} = \frac{1+0}{1+0} \times \frac{2+0}{1+0} = 2 > 1$$

$\Rightarrow$ By Ratio test, the series is convergent.

Example 1.14: Test for convergence of the series,

$$\sum_{n=1}^{\infty} \frac{(n+1)}{(n+2)(n+3)} . x^n, (x > 0)$$

Solution: We have,

$$\frac{u_n}{u_{n+1}} = \frac{(n+1)}{(n+2)(n+3)} . x^n . \frac{(n+3)(n+4)}{(n+2)} . \frac{1}{x^{n+1}}$$

$$= \frac{(n+1)(n+4)}{(n+2)^2} . \frac{1}{x} = \frac{\left(1+\frac{1}{n}\right)\left(1+\frac{4}{n}\right)}{\left(1+\frac{2}{n}\right)^2} . \frac{1}{x}$$

$$\Rightarrow \quad \operatorname{Lim}_{n\to\infty} \frac{u_n}{u_{n+1}} = \frac{1}{x}$$

Hence, if $\frac{1}{x} > 1$, i.e., if $x < 1$, the series is convergent.

and if $\frac{1}{x} < 1$, i.e., if $x > 1$, the series is divergent by Ratio test.

If $x = 1$, the Ratio test fails. The series then becomes,

$$\sum \frac{n+1}{(n+2)(n+3)}$$

Here, $$u_n = \frac{n+1}{(n+2)(n+3)} = \frac{1+1/n}{n(1+2/n)(1+3/n)}$$

Take, $$v_n = \frac{1}{n}$$

Thus, $$\operatorname{Lim}_{n\to\infty} \frac{u_n}{v_n} = \operatorname{Lim} \frac{1+1/n}{(1+2/n)(1+3/n)} = 1 \text{ (non-zero finite)}$$

Hence, Σu_n and Σv_n converge or diverge together. But Σv_n is divergent (according to the solution proved in example 1.3)

Therefore, Σu_n is divergent when $x = 1$.

NOTES

Example 1.15: Show that the series $1+\frac{1}{2^2}+\frac{1}{3^3}+\frac{1}{4^4}+...$ is convergent.

Solution: We have $u_n = \frac{1}{n^n}$

$\Rightarrow \quad (u_n)^{\frac{1}{n}} = \frac{1}{n}$

$\Rightarrow \quad \underset{n\to\infty}{\text{Lim}} (u_n)^{\frac{1}{n}} = 0 < 1$

$\Rightarrow \quad \Sigma u_n$ is convergent by Root test.

Example 1.16: Test for convergence of the series $\frac{1}{3}+\frac{2}{9}+\frac{3}{27}+\frac{4}{81}+\cdots$

Solution: We have $u_n = \frac{n}{3^n}$

Thus, $$\frac{u_n}{u_{n+1}} = \frac{n}{3^n}\times\frac{3^{n+1}}{n+1} = \frac{3}{n+1}$$

$\Rightarrow \text{Lim}\frac{u_n}{u_{n+1}} = 0 < 1$

$\Rightarrow \Sigma u_n$ is divergent, by Ratio test.

Example 1.17: Show with the help of examples that the Ratio test fails, when $\underset{n\to\infty}{\text{Lim}}\frac{u_n}{u_{n+1}} = 1.$

Solution: Consider the series, $1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n}...$

Here, $$u_n = \frac{1}{n}$$

$\Rightarrow$ $$\frac{u_n}{u_{n+1}} = \frac{1}{n}\times(n+1)$$

$$= 1+\frac{1}{n}$$

$\Rightarrow$ $$\text{Lim}\frac{u_n}{u_{n+1}} = 1$$

We know that the series is divergent.

Now, consider the series,

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots+\frac{1}{n^2}+\ldots$$

Here, $$\frac{u_n}{u_{n+1}} = \frac{(n+1)^2}{n^2} = \left(1+\frac{1}{n}\right)^2$$

NOTES

$$\Rightarrow \qquad \text{Lim}\frac{u_n}{u_{n+1}} = 1$$

But this series, is convergent (according to the solution of Example 1.3) and thus

$\text{Lim}_{n\to\infty}\frac{u_n}{u_{n+1}}$ can be equal to unity in case of convergent as well as divergent series.

Hence, the Ratio test is not applicable in this case.

Alternating Series

A series of the form,

$$u_1 - u_2 + u_3 - u_4 + \ldots$$

Where $u_n > 0 \ \forall n$, is called an *alternating series.*

Leibnitz's Test. The alternating series $u_1 - u_2 + u_3 - u_4 + \ldots$ is convergent if,

(i) $u_{n+1} \le u_n \ \forall n$

(ii) $\text{Lim}_{n\to\infty} u_n = 0.$

Example 1.18: Show that the series, $1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$ is convergent.

Solution: We know that, $u_{n+1} \le u_n$ for all n. Also $\text{Lim}_{n\to\infty} u_n = 0$. Thus by **Leibnitz**' *test*, the series is convergent.

Example 1.19: Show that the series $1 - \frac{1}{2\sqrt{2}} + \frac{1}{3\sqrt{3}} - \frac{1}{4\sqrt{4}} + \ldots$ is convergent.

Solution: The result is evidently true by Leibnitz' test. Since here the numerical values of the terms are continuously decreasing as,

$$\frac{1}{(n+1)\sqrt{(n+1)}} \le \frac{1}{n\sqrt{n}} \text{ for all } n.$$

and also $\text{Lim}_{n\to\infty} u_n = \text{Lim}\frac{1}{n\sqrt{n}} = 0$

Example 1.20: Test for convergence the series.

$$\sum_{n=1}^{\infty}(-1)^n\left[\sqrt{n+1} - \sqrt{n}\right]$$

Solution: We have,

$$u_n = \sqrt{n+1} - \sqrt{n} = \frac{\sqrt{n+1} - \sqrt{n}}{\sqrt{n+1} + \sqrt{n}} \times (\sqrt{n+1} + \sqrt{n})$$

$$= \frac{n+1-n}{\sqrt{n+1} + \sqrt{n}} = \frac{1}{\sqrt{n+1} + \sqrt{n}}$$

Thus,

$$u_{n+1} - u_n = \frac{1}{\sqrt{n+2}+\sqrt{n+1}} - \frac{1}{\sqrt{n+1}+\sqrt{n}}$$

$$= \frac{\sqrt{n+1}+\sqrt{n}-\sqrt{n+2}-\sqrt{n+1}}{(\sqrt{n+2}+\sqrt{n+1})(\sqrt{n+1}+\sqrt{n})}$$

$$= \frac{\sqrt{n}-\sqrt{n+2}}{(\sqrt{n+2}+\sqrt{n+1})(\sqrt{n+1}+\sqrt{n})} \times \frac{\sqrt{n}+\sqrt{n+2}}{\sqrt{n}+\sqrt{n+2}}$$

$$= \frac{n-(n+2)}{(\sqrt{n+2}+\sqrt{n+1})(\sqrt{n+1}+\sqrt{n})(\sqrt{n}+\sqrt{n+2})}$$

$$= \frac{-2}{(\sqrt{n+2}+\sqrt{n+1})(\sqrt{n+1}+\sqrt{n})(\sqrt{n}+\sqrt{n+2})} < 0, \forall n$$

Because the denominator will always be positive.

Hence, $u_{n+1} < u_n \ \forall n$

Note: When we check the above property we take the terms u_n and u_{n+1} with the positive sign [According to Leibnitz' test.]

Now, $\lim_{n\to\infty} u_n = \lim_{n\to\infty} \frac{1}{\sqrt{n+1}+\sqrt{n}}$

$$= \lim_{n\to\infty} \frac{1}{\sqrt{n}} \left[\frac{1}{\sqrt{1+1/n}+1} \right] = 0$$

Hence, by the Leibnitz's test we observe that the given series is convergent.

Check Your Progress

1. Define the term sequence.
2. What is limit of the sequence?
3. What do you understand by divergent sequence?
4. Define the term series.
5. What do you mean by infinite series?
6. When is K some fixed positive number?
7. What do you understand by Leibnitz test?

1.4 ARITHMETIC PROGRESSION

Quantities $a_1, a_2, a_3, ..., a_n, ...$ are said to be in *Arithmetical Progression* if $a_n - a_{n-1}$ is constant for all integers $n > 1$. The constant quantity $a_n - a_{n-1}$ is called the *common difference* of the arithmetical progression.

NOTES

NOTES

Notation: A.P. stands for an arithmetical progression. Consider the following series.

$1, 3, 5, 7, 9, 11, ...$

$0, \sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, 4\sqrt{2}, ...$

$1, \frac{1}{2}, 0, -\frac{1}{2}, -1, -\frac{3}{2}, ...$

$x + y, x, x - y, x - 2y, ...$

$5.3, 5.55, 5.8, 6.05, 6.3, ...$

Each of the above series is an A.P. Common differences are respectively 2, $\sqrt{2}, -\frac{1}{2}, -y$ and 0.25.

1.4.1 General Term of an Arithmetical Progression

The first term can be denoted by a.

So, $a_n = a + (n - 1)d$

$S_n = \frac{n}{2}[2a + (n - 1)d]$

Let $a_1, a_2, ..., a_n, ...$ be a given A.P. Let d be their common difference. Then $a_n - a_{n-1} = d$ for all n.

$\Rightarrow \quad a_2 - a_1 = d, a_3 - a_2 = d, a_4 - a_3 = d$ and so on,

$\Rightarrow \quad a_2 = a_1 + d, a_3 = a_2 + d = a_1 + d + d = a_1 + 2d$

$a_4 = a_3 + d = a_1 + 2d + d = a_1 + 3d$

... ...

$a_{n-1} = a_1 + (n - 2)d$

$a_n = a_{n-1} + d = a_1 + (n - 2)d + d$

$= a_1 + (n - 1)d$

Thus nth term, a_n, of an arithmetical progression whose first term is a_1 and common difference d, is given by

$$a_n = a_1 + (n - 1)d$$

Example 1.21: Find 16th term of the series 3.75, 3.5, 3.25, ...

Solution.: In this case $a_1 = 3.75, a_2 = 3.5, a_3 = 3.25$

$d = a_2 - a_1 = -0.25$

Hence 16th term $= a_{16}$

$= 3.75 + (16 - 1)(-0.25)$

$= 3.75 - 15 \times 0.25$

$= 3.75 - 3.75 = 0$

Example 1.22: Which term of the A.P. 49, 44, 39, ... is 9?

Solution: Let nth term be 9, i.e., $a_n = 9$.

Here $a_1 = 49, d = 44 - 49 = -5,$

Thus $a_n = 9 = 49 + (n-1)(-5)$

$\Rightarrow$ $9 = 49 - 5n + 5$

or $5n = 54 - 9 = 45$

$n = 9$

Thus 9th term of the given A.P. is 9.

1.4.2 Sum of Finite Number of Quantities in an Arithmetic Progression

Let $a_1, a_2, ..., a_n$ be n quantities in A.P., and let the last term a_n be denoted by l. If d is their common difference then,

$$a_n = a_1 + (n-1)d = l$$

Put $S_n = a_1 + a_2 + ... + a_n$

Thus $S_n = a_1 + (a_1 + d) + (a_2 + 2d) + ... + [a_1 + (n-1)d]$

$= a_1 + (a_1 + d) + (a_1 + 2d) + ... + (l - d) + l$ ...(1.1)

Writing the above series in reverse order, we get

$$S_n = l + (l-d) + (l-2d) + ... + (a_1 + d) + a_1 \quad ...(1.2)$$

Adding Equations (1.1) and (1.2), we get

$2S_n = (a_1 + l) + (a_1 + l) + ... + (a_1 + l)$, ($n$ times)

$= n(a_1 + l)$

Therefore $S_n = \frac{n}{2}(a_1 + l)$

$= \frac{n}{2}\{a_1 + [a_1 + (n-1)d]\}$

Consequently $S_n = \frac{n}{2}[2a_1 + (n-1)d]$

Example 1.23: Find the sum of $\frac{3}{4}, \frac{2}{3}, \frac{7}{12}$,... up to 19 terms.

Solution: Here $a_1 = \frac{3}{4}$, $a_2 = \frac{2}{3}$, $n = 19$

Thus $d = a_2 - a_1 = \frac{2}{3} - \frac{3}{4} = -\frac{1}{12}$

i.e., $S_{19} = \frac{19}{2}\left[2 \times \frac{3}{4} + (19-1)\left(-\frac{1}{12}\right)\right]$

$= \frac{19}{2}\left[\frac{3}{2} - \frac{18}{12}\right]$

$= \frac{19}{2}\left(\frac{18-18}{12}\right) = \frac{19}{2} \times 0 = 0$

NOTES

Example 1.24: How many terms of the following series may be taken so that their sum is 66.

$$-9, -6, -3, \ldots ?$$

Solution: Let $S_n = 66$. Here $a_1 = -9$, $d = -6 + 9 = 3$

Or $$66 = \frac{n}{2}[-18 + (n-1)3]$$

$$132 = -18n + 3n^2 - 3n$$

i.e., $$3n^2 - 21n - 132 = 0$$

Or $$n^2 - 7n - 44 = 0 \Rightarrow (n - 11)(n + 4) = 0$$

$$\Rightarrow n = 11 \text{ or } n = -4$$

As n is a positive integer, the second value of n, i.e., –4 is rejected.

Thus required number of terms is 11.

1.4.3 Arithmetical Mean

If $a_1, a_2, \ldots, a_n$ are in A.P., then the quantities $a_2, a_3, \ldots, a_{n-1}$ are called *Arithmetic Means* (A.M.) between a_1 and a_n.

Thus in the series, 1, 3, 5, 7, 9, 11, 13, 15, ...

3, 5 are arithmetic means between 1 and 7.

9, 11, 13 are arithmetic means between 7 and 15.

1.4.4 To Insert *n* Arithmetic Means Between Two Given Numbers

Let a and b be two given quantities and $A_1, A_2, \ldots, A_n$ be the n arithmetic means between them. Then the quantities,

$$a, A_1, A_2, \ldots, A_n, b \text{ are in A. P.}$$

Let d be their common difference.

Now $$b = (n+2)\text{th term}$$

$$= a + (n+1)d$$

$$\Rightarrow \quad d = \frac{b-a}{n+1}$$

Further, $$A_1 = 2\text{nd term}$$

$$= a + d = a + \left(\frac{b-a}{n+1}\right)$$

$$= \frac{na+b}{n+1}$$

$$A_2 = 3\text{rd term}$$

$$= a + 2d = a + 2\left(\frac{b-a}{n+1}\right)$$

$$= \frac{na+2b-a}{n+1}$$

NOTES

$$A_n = a + nd = a + n\left(\frac{b-a}{n+1}\right)$$

$$= \frac{a+nb}{n+1}$$

Hence $\frac{na+b}{n+1}, \frac{na+2b-a}{n+1}, \ldots, \frac{a+nb}{n+1}$

are n arithmetic means between a and b.

Example 1.25: Insert 6 arithmetic means between 1 and 19.

Solution: Let $A_1, A_2, A_3, A_4, A_5, A_6$, be the required arithmetic means.

Then $1, A_1, A_2, A_3, A_4, A_5, A_6, 19$ are in A.P.

Let d be their common difference.

Then $19 = 8\text{th term}$

$= 1 + (8 - 1)d$

$= 1 + 7d$

Thus $d = \frac{18}{7}$

Hence $A_1 = 2\text{nd term}$

$= 1 + \frac{18}{7} = \frac{25}{7}$

$A_2 = 3\text{rd term} = 1 + 2 \times \frac{18}{7} = 1 + \frac{36}{7} = \frac{43}{7}$

$A_3 = 4\text{th term} = 1 + 3 \times \frac{18}{7} = 1 + \frac{54}{7} = \frac{61}{7}$

$A_4 = 5\text{th term} = 1 + 4 \times \frac{18}{7} = 1 + \frac{72}{7} = \frac{79}{7}$

$A_5 = 6\text{th term} = 1 + 5 \times \frac{18}{7} = 1 + \frac{90}{7} = \frac{97}{7}$

$A_6 = 7\text{th term} = 1 + 6 \times \frac{18}{7} = 1 + \frac{108}{7} = \frac{115}{7}$

So, the required means are

$$\frac{25}{7}, \frac{43}{7}, \frac{61}{7}, \frac{79}{7}, \frac{97}{7}, \frac{115}{7}$$

Example 1.26: How many terms of the series 4, 2, 0, –2, –4, –6, ... should be taken so that their sum is 6?

Solution: Let n be the required number of terms.

Here $a_1 = 4$, $d = 2 - 4 = -2$

So, $6 = S_n = \frac{n}{2}[8 + (n-1)(-2)]$

i.e., $12 = 8n - 2n^2 + 2n$

or $2n^2 - 10n + 12 = 0$

or $n^2 - 5n + 6 = 0$

NOTES

or $(n-3)(n-2)=0$

Hence $n=3$ or $n=2$.

Here, we get two answers. As the third term is zero, therefore, the sum of the first two terms is same as the sum of the first three terms.

Example 1.27: If pth, qth, rth term of an A.P. are a, b, c, respectively, show that

$$(q-r)\,a+(r-p)b+(p-q)c=0$$

Solution: Here pth term $= a = a_1 + (p-1)d$ ...(1)

qth term $= b = a_1 + (q-1)d$ ...(2)

rth term $= c = a_1 + (r-1)d$ ...(3)

where a_1 is the first term and d is the common difference of the A.P.

Multiply (i) by $q-r$, (ii) by $r-p$, (iii) by $p-q$ and add to obtain $(q-r)\,a+(r-p)\,b+(p-q)\,c$

$= a_1(q-r)+a_1(r-p)+a_1(p-q)+d[(p-1)(q-r)+(q-1)(r-p)+(r-1)(p-q)]$

$= a_1[q-r+r-p+p-q]+d[pq+r-pr-q+qr-r+p-pq+rp-rq-p+q]=0$

Example 1.28: The sum of n terms of two A.P.s are in the ratio of $7n+1: 4n+27$. Find the ratio of their 11th terms.

Solution: Let a_1 and b_1 be the first terms of two A.P.s and d_1, d_2 be their common difference respectively.

Then $$S_n = \frac{n}{2}[2a_1+(n-1)\,d_1]$$

$$S'_n = \frac{n}{2}[2b_1+(n-1)\,d_2]$$

So, $$\frac{S_n}{S'_n} = \frac{2a_1+(n-1)d_1}{2b_1+(n-1)d_2} = \frac{7n+1}{4n+27}$$

Putting $n=21$, we get

$$\frac{2a_1+20d_1}{2b_1+20d_2} = \frac{148}{111}$$

Or $$\frac{a_1+10d_1}{b_1+10d_2} = \frac{148}{111}$$

Or $$\frac{a_{11}}{b_{11}} = \frac{148}{111}$$

where a_{11} and b_{11} are the 11th terms of two A.P.s respectively.

The ratio of their 11th term is 4:3

Example 1.29: If a^2, b^2, c^2 are in A.P., show that

$$\frac{1}{b+c}, \frac{1}{c+a}, \frac{1}{a+b} \text{ are also in A.P.}$$

Solution: $\frac{1}{b+c}, \frac{1}{c+a}, \frac{1}{a+b}$ are in an A.P.

$$\Leftrightarrow \quad \frac{1}{c+a} - \frac{1}{b+c} = \frac{1}{a+b} - \frac{1}{c+a}$$

$$\Leftrightarrow \quad \frac{b-a}{(c+a)(b+c)} = \frac{c-b}{(a+b)(c+a)}$$

$$\Leftrightarrow \quad \frac{b-a}{c+b} = \frac{c-b}{b+a}$$

$$\Leftrightarrow \quad b^2 - a^2 = c^2 - b^2$$

$\Leftrightarrow$ a^2, b^2, c^2 are in A.P.

Example 1.30: Sum to n terms of three A.P.s are s_1, s_2 and s_3. The first term of each of them is 1 and the common differences are 1, 2 and 3 respectively. Show that s_1, s_2, s_3 are also in A.P.

Solution: $s_1 = \frac{n}{2}[2 + (n-1)] = \frac{n(n+1)}{2}$

$$s_2 = \frac{n}{2}[2 + (n-1)2] = n^2$$

$$s_3 = \frac{n}{2}[2 + (n-1)3] = \frac{n}{2}(3n-1)$$

Or $s_2 - s_1 = n^2 - \frac{n(n+1)}{2} = \frac{n^2-n}{2} = \frac{n(n-1)}{2}$

$$s_3 - s_2 = \frac{n}{2}(3n-1) - n^2 = \frac{3n^2 - n - 2n^2}{2}$$

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

i.e., $s_2 - s_1 = s_3 - s_2$

Hence s_1, s_2, s_3 are in A.P.

Example 1.31: State giving an example whether the following statement is true or false.

In a given A.P. let a be the first term, d the common difference, n the number of terms and s their sum. Given any three of a, d, n and s, one can always find a unique value of the fourth quantity.

Solution: The statement is false. Given the values of a, d and s, there might be two values of n. Consider the series 12, 9, 6, 3, 0, –3, –6. Find the number of terms from the beginning whose sum is 30.

In this case, $a = 12, d = 9 - 12 = -3, s = 30$

Since $s = \frac{n}{2}[2a + (n-1)d]$

We have $30 = \frac{n}{2}[24 + (n-1)(-3)]$

or $60 = 24n - 3n^2 + 3n$

NOTES

NOTES

or $3n^2 - 27n + 60 = 0$

$\Rightarrow$ $n^2 - 9n + 20 = 0$

$\Rightarrow$ $(n - 4)(n - 5) = 0$

$\Rightarrow$ $n = 4$ or $n = 5$.

Example 1.32: Find the sum of all the numbers between 200 and 400 which are divisible by 7.

Solution: Since 4 is left as remainder on division of 200 by 7, the least number greater than 200 divisible by 7 is 203. Again if we divide 400 by 7, 1 is left as remainder. This implies that the greatest number less than 400 which is divisible by 7 is 399.

So we have to find the sum of the series

$203 + 210 + 217 + ... + 399$

Here $a_1 = 203, d = 7, l = 399$

Let n be the total number of terms in this series.

Then $399 = 203 + (n - 1)7$

$\Rightarrow$ $7n = 399 - 203 + 7$

$= 406 - 203 = 203$

$\Rightarrow$ $n = 29$

Hence required sum $= \frac{n}{2}(a + l) = \frac{29}{2}(203 + 399)$

$= \frac{29}{2}(602)$

$= 29 \times 301$

$= 8729$

Example 1.33: Mr X arranges to pay off a debt of ₹ 9,600 in 48 annual instalments which form an arithmetical series. When 40 of these instalments are paid, Mr X becomes insolvent and his creditor finds that ₹ 2,400 still remains unpaid. Find the value of each of the first three instalments of Mr X. Ignore the interest.

Solution: Let $a, a + d, a + 2d, a + 3d$ be the annual instalments.

The sum of this series up to $n = 48$ terms is 9600.

i.e., $9600 = \frac{48}{2}[2a + (48 - 1)d]$

$\Rightarrow$ $9600 = 24(2a + 47d)$

$\Rightarrow$ $2a + 47d = 400$ ...(1)

After 40 instalments are paid, the balance is ₹ 2,400. In other words, in 40 instalments Mr *X* has paid ₹ (9600 – 2400), i.e., ₹ 7,200.

So the sum of the first 40 terms of the above series is 7200.

Thus $7200 = \frac{40}{2}[2a + (40 - 1)d]$

$\Rightarrow$ $7200 = 20(2a + 39d)$

$\Rightarrow \quad 2a + 39d = 360 \quad ...(2)$

Subtracting equation (2) from (1), we get

$8d = 40 \quad \Rightarrow \quad d = 5$

Then equation (2) $\Rightarrow 2a + 195 = 360$

$\Rightarrow \quad 2a = 165 \quad \Rightarrow \quad a = 82.50$

Hence, the first instalment of Mr X is ₹ 82.50, second instalment is ₹ (82.50 + 5.00), i.e., ₹ 87.50 and the third instalment is ₹ (87.50 + 5.00), i.e., ₹ 92.50.

NOTES

Example 1.34: If $\frac{1}{b+c}, \frac{1}{c+a}, \frac{1}{a+b}$ are in an A.P., prove that a^2, b^2, c^2 are also in A.P.

Solution: Since $\frac{1}{b+c}, \frac{1}{c+a}, \frac{1}{a+b}$ are in an A.P.,

We have $\frac{1}{c+a} - \frac{1}{b+c} = \frac{1}{a+b} - \frac{1}{c+a}$

$\Rightarrow \quad \frac{(b+c)-(c+a)}{(b+c)(c+a)} = \frac{(c+a)-(a+b)}{(a+b)(c+a)}$

$\Rightarrow \quad \frac{b-a}{b+c} = \frac{c-b}{b+a}$

$\Rightarrow \quad b^2 - a^2 = c^2 - b^2$

$\Rightarrow \quad a^2, b^2, c^2$ are in A.P.

Example 1.35: The monthly salary of a person was ₹ 320 for each of the first three years. He then got annual increments of ₹ 40 per month for each of the following successive 12 years. His salary remained stationary till retirement when he found that his average monthly salary during the service period was ₹ 698. Find the period of his service.

Solution: Let n be the total number of years of the person's service.

His total salary = ₹ $12n \times 698$

(As his monthly average is ₹ 698)

Total salary in first three years of service

$= 320 \times 3 \times 12 =$ ₹ 960×12

In the 4th year, his monthly salary was ₹ (320 + 40) = ₹ 360

In the 5th year his monthly salary was ₹ 400, and so on.

Then for the next 12 years, his total salary

$=$ ₹ $12 \times [360 + 400 + ...$ up to 12 terms$]$

$=$ ₹ $12 \times \frac{12}{2}[2 \times 360 + (12 - 1) \times 40]$

$=$ ₹ $12 \times 6\ (720 + 440)$

$=$ ₹ $12 \times 6 \times 1160$

$=$ ₹ 12×6960

NOTES

At the end of following the 12 years, his monthly salary was

$$₹\,[360 + (12 - 1) \times 40] = ₹\,800$$

He got ₹ 800 as salary for the remaining $(n - 15)$ years. So his total salary for the remaining $(n - 15)$ years was $(n - 15)\,800 \times 12$

Hence his total salary throughout his service period

$$= 12[960 + 6960 + 800(n - 15)]$$
$$= 12(7920 + 800n - 12000)$$
$$= 12\,(800n - 4080)$$

This must be same as $12n \times 698$

i.e., $12n \times 698 = 12(800n - 4080)$

$\Rightarrow$ $102n = 4080 \quad \Rightarrow \quad n = 40$ years.

Example 1.36: The sequence of natural numbers is written as

		1		
	2	*3*	*4*	
5	*6*	*7*	*8*	*9*
...	...	...	...	...
...	...	...	...	...

Find the sum of the numbers in the *r*th row.

Solution: Let S_1 denotes the sum of *r*th row.

$$S_1 = 1,\ S_2 = 2 + 3 + 4,\ S_3 = 5 + 6 + 7 + 8 + 9$$

Let initial term of S_k be t_k

and suppose that $M = 1 + 2 + 5 + ... + t_k$

be the sum of the first terms of S_1, S_2, and S_k

Now $M = 1 + 2 + 5 + 10 + ... + t_k$

Also $M = 1 + 2 + 5 + ... + t_{k-1} + t_k$

Subtracting, we get

$$0 = (1 + 1 + 3 + 5 + \text{up to } k \text{ term}) - t_k$$
$$t_k = 1 + [1 + 3 + 5 + ... \text{ up to } (k - 1) \text{ terms}]$$
$$= 1 + \left(\frac{k-1}{2}\right)[2 + (k - 2) \times 2]$$
$$= 1 + (k - 1)^2 = k^2 - 2k + 2$$

In S_1 there is one term, in the S_2 there are three terms and so on. In S_k there will be $(2k - 1)$ term.

Hence, we have to find the sum of the series

$r^2 - 2r + 2,\ r^2 - 2r + 3,\ r^2 - 2r + 4$, up to $(2r - 1)$ terms

So $$S_r = \frac{(2r-1)}{2}\,[2(r^2 - 2r + 2) + (2r - 2) \times 1]$$
$$= (2r - 1)\,(r^2 - 2r + 2 + r - 1)$$

$$= (2r - 1)(r^2 - r + 1)$$
$$= 2r^3 - 3r^2 + 3r - 1$$

Example 1.37: A lamplighter has to light 100 gas lamps. He takes 1½ minutes to go from one lamp post to the next. Each lamp post burns 10 c.c. of gas per hour. How many c.c of gas has been burnt by 8.30 p.m. if he lights the first lamp at 6 p.m.

Solution: Total time from 6 p.m. to 8.30 p.m. is 2.30 hours, i.e., 150 minutes.

$$g_1 = \text{Gas burnt in the 1st lamp} = \frac{150 \times 10}{60}$$

$$= \frac{1}{6}(150) \text{ c.c.}$$

Second lamp burns for (150 – 1.5) minutes

So the gas burnt in the 2nd lamp = $g_2 = \frac{1}{6}(150 - 1.5)$

Similarly $g_3 = \frac{1}{6}(150 - 2 \times 1.5)$ and so on.

We are to calculate

$$S = g_1 + g_2 + ... + g_{100}$$

$$S = \frac{1}{6}[150 + (150 - 1.5) + (150 - 2 \times 1.5) + ...]$$

The series inside the bracket is an A.P. with first term = 150, common difference = –1.5 and number of terms = 100

Hence, $S = \frac{1}{6} \times \frac{100}{2}[300 + 99(-1.5)]$

$$= \frac{25}{3}(300 - 1.5 \times 99)$$
$$= 25(100 - 1.5 \times 33)$$
$$= 25(100 - 49.5)$$
$$= 25(50.5)$$
$$= 1262.5 \text{ c.c.}$$

Example 1.38: Two posts were offered to a man. In one, the starting salary was ₹ 120 per month and the annual increment was ₹ 8; in the other post the salary commenced at ₹ 85 per month but the annual increment was ₹ 12. The man decided to accept the post which would give him more earnings in the first twenty years of service. Which post was acceptable to him? Justify your answer.

Solution: The total earnings of the man in the first job

$$= \frac{20}{2}[2 \times 120 + (20 - 1)8] \times 12$$
$$= 10(240 + 152) \times 12$$
$$= 120(392)$$
$$= 47040 \text{ rupees}$$

NOTES

His total earnings in the second job

$$= \frac{20}{2}[2 \times 85 + (20 - 1)12] \times 12$$

$$= 120\ (170 + 228)$$

$$= 120\ (398)$$

$$= 47760 \text{ rupees}$$

which is greater than ₹ 47040. Hence the second job was accepted by the man.

Example 1.39: Find the sum of all the natural numbers between 500 and 1000 which are divisible by 13.

Solution: 500 on division by 13 leaves 6 as remainder, so 507 is the least number greater than 500 which is divisible by 13.

When 1000 is divided by 13, the remainder is 12. So the greatest number less than 1000, divisible by 13, is 988.

We are to find the sum of $507 + 520 + ... + 988$

Let n be the number of terms in the series

Then $988 = 507 + (n - 1)\ 13$

$\Rightarrow$ $76 = 39 + n - 1 = n + 38$

$\Rightarrow$ $n = 76 - 38 = 38$

Required sum, $S = \frac{n}{2}[2a + (n - 1)d]$

Here $n = 38,\ a = 507,\ d = 13$

Hence $S = \frac{38}{2}\ [2 \times 507 + (38 - 1)13]$

$$= \frac{38}{2}\ (1014 + 37 \times 13)$$

$$= 19\ (1014 + 481)$$

$$= 19\ (1495)$$

$$= 28405$$

Example 1.40: A firm produced 1000 sets of TV during its first year. The total sum of the firm's production at the end of 10 years of operation is 14,500 sets.

(*i*) Estimate, by how many units production increased each year, if the increase in each year is uniform, and

(*ii*) Forecast, based on the estimate of the annual increment in production, the level of output for the 15th year.

Solution: Here $a = 1000$, $S = 14{,}500$, $n = 10$ and d is to be evaluated.

$$14{,}500 = \frac{10}{2}[2 \times 1000 + (10 - 1)d]$$

$$14500 = 5\ (2000 + 9d)$$

$\Rightarrow \quad 2000 + 9d = 2900$

$\Rightarrow \quad 9d = 900 \Rightarrow d = 100$

Hence 1000 units is the increase per annum

$$a + 14d = 1000 + 14 \times 100$$
$$= 1000 + 1400 = 2400$$

NOTES

1.4.5 Properties of Arithmetic Progression (AP)

- If the same number is added or subtracted from each term of an A.P, then the resulting terms in the sequence are also in A.P with the same common difference.
- If each term in an A.P is divided or multiply with the same non–zero number, then the resulting sequence is also in an A.P
- Three number x, y and z are in an A.P if $2y = x + z$
- A sequence is an A.P if its n^{th} term is a linear expression.
- If we select terms in the regular interval from an A.P, these selected terms will also be in AP.

Let will discuss about some of the properties of Arithmetic Progression which we will frequently use in solving different types of problems on arithmetical progress.

Property I: If a constant quantity is added to or subtracted from each term of an Arithmetic Progression (A. P.), then the resulting terms of the sequence are also in A. P. with same Common Difference (C.D.).

Proof: Let $\{a_1, a_2, a_3, a_4, ...\}$ ..... (i) be an Arithmetic Progression with common difference d.

Again, let k be a fixed constant quantity. Now k is added to each term of the above A.P. (i) Then the resulting sequence is $a_1 + k, a_2 + k, a_3 + k, a_4 + k$.....
.

Let $b_n = a_n + k, n = 1, 2, 3, 4, ...$ Then the new sequence is b_1, b_2, b_3, b_4,.....

We have $\boldsymbol{b_{n+1} - b_n = (a_{n+1} + k) - (a_n + k) = a_n + 1 - a_n = d}$ for all $\boldsymbol{n \in N}$, [Since, $\boldsymbol{<a_n>}$ is a sequence with common difference d].

Therefore, the new sequence we get after adding a constant quantity $\boldsymbol{k}$ to each term of the A.P. is also an Arithmetic Progression with common difference $\boldsymbol{d}$.

To get the clear concept of property I let us follow the below explanation.

Let us assume 'a' be the first term and 'd' be the common difference of an Arithmetic Progression. Then, the Arithmetic Progression is $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$

1. By adding a Constant Quantity: If a constant quantity k is added to each term of the Arithmetic Progression (AP) $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$ we get

$\{a + k, a + d + k, a + 2d + k, a + 3d + k, a + 4d + k, ...\}$ ..... (1)

First term of the above sequence (1) is $(a + k)$.

NOTES

Common difference of the above sequence (i) is $(a + d + k) - (a + k) = d$. Therefore, the terms of the above sequence (i) form an Arithmetic Progression. Hence, if a constant quantity be added to each term of an Arithmetic Progression, the resulting terms are also in Arithmetic Progression with the same common difference.

By Subtracting a Constant Quantity: If a constant quantity k is subtracted from each term of the Arithmetic Progression $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$ we get,

$$\{a - k, a + d - k, a + 2d - k, a + 3d - k, a + 4d - k, ...\} \quad ...(2)$$

First term of the above sequence (2) we get $(a - k)$. Common difference of the above sequence (ii) is $(a + d - k) - (a - k) = d$.

Therefore, the terms of the above sequence (2) form an Arithmetic Progression.

Hence, if a constant quantity be subtracted from each term of an Arithmetic Progression, the resulting terms are also in Arithmetic Progression with the same common difference.

Property II: If each term of an Arithmetic Progression is multiplied or divided by a non–zero constant quantity, then the resulting sequence form an Arithmetic Progression.

Proof: Let us assume $\{a_1, a_2, a_3, a_4, ...\}$ ...(i)

be an Arithmetic Progression with common difference d.

Again, let k be a fixed non–zero constant quantity.

Let us obtain, $b_1, b_2, b_3, b_4, ...$ be the sequence, after multiplying each term of the given A.P. (i) by k.

$b_1 = a_1k,\ b_2 = a_2k,\ b_3 = a_3k,\ b_4 = a_4k$..... $b_n = a_nk$.

Now, $b_n+1 - b_n = a_n+1k - a_nk = (a_n+1 - a_n)k = dk$ for all $n \in N$, [Since, $<a_n>$ is a sequence with common difference d]

Therefore, the new sequence we get after multiplying a non–zero constant quantity k to each term of the A. P. is also an Arithmetic Progression with common difference dk.

To get the clear concept of Property II let us follow the below explanation.

Let us assume 'a' be the first term and 'd' be the common difference of an Arithmetic Progression. Then, the Arithmetic Progression is $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$

1. On multiplying a Constant Quantity: If a non–zero constant quantity $(k \neq 0)$ is multiplied by each term of the Arithmetic Progression $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$ we get,

$$\{ak, ak + dk, ak + 2dk, ak + 3dk, ...\} \quad ...(iii)$$

First term of the above sequence (iii) is ak. Common difference of the above sequence (iii) is $(ak + dk) - ak = dk$. Therefore, the terms of the above sequence (iii) form an Arithmetic Progression.

Hence, if a non–zero constant quantity be multiplied by each term of an Arithmetic Progression, the resulting terms are also in Arithmetic Progression.

2. On Dividing a Constant Quantity: If a non–zero constant quantity ($k \neq 0$) is divided by each term of the Arithmetic Progression $\{a, a + d, a + 2d, a + 3d, a + 4d, ...\}$ we get,

$\{ak, \ ak + dk, ak + 2dk, ak + 3dk, ...\}$ ...(iv)

First term of the above sequence (iv) is a/k.

Common difference of the above sequence (iv) is $(a/k + d/k) - a/k = d/k$

Therefore, the terms of the above sequence (iv) form an Arithmetic Progression.

Hence, if a non–zero constant quantity be divided by each term of an Arithmetic Progression, the resulting terms are also in Arithmetic Progression.

Property III: In an Arithmetic Progression of finite number of terms the sum of any two terms equidistant from the beginning and the end is equal to the sum of the first and last terms.

Proof: Let us assume 'a' be the first term, 'd' be the common difference, 'l' be the last term and 'n' be the number of terms of an A.P. (n is finite).

The second term from the end = $l - d$

The third term from the end = $l - 2d$

The fourth term from the end = $l - 3d$

The rth term from the end = $l - (r - 1)d$

Again, the rth term from the beginning = $a + (r - 1)d$

Therefore, the sum of the rth terms from the beginning the end

$$= a + (r - 1)d + l - (r - 1)d$$
$$= a + rd - d + l - rd + d$$
$$= a + l$$

Hence, the sum of two terms equidistant from the beginning and the end is always same or equal to the sum of the first and last terms.

Property IV: Three numbers x, y, and z are in Arithmetic Progression if and only if $2y = x + z$.

Proof: Let us assume that, x, y, z be in Arithmetic Progression.

Now, common difference = $y - x$ and again, common difference = $z - y$

$\Rightarrow \quad y - x = z - y$

$\Rightarrow \quad 2y = x + z$

Conversely, let x, y, z be three numbers such that $2y = x + z$. Then we prove that x, y, z are in Arithmetic Progression.

We have, $2y = x + z$

$\Rightarrow \quad y - x = z - y$

$\Rightarrow \quad x, y, z$ are in Arithmetic Progression.

NOTES

Property V: A sequence is an Arithmetic Progression if and only if its nth term is a linear expression in n, i.e., $a_n = A_n + B$, where A, B are two constant quantities.

In this case the coefficient of n in the Common Difference (C.D.) of the Arithmetic Progression.

Property VI: A sequence is an Arithmetic Progression if and only if the sum of its first n terms is of the form $A_n^2 + B_n$, where A, B are two constant quantities that are independent of n.

In this case the common difference is $2A$ that is 2 times the coefficient of n^2.

Property VII: A sequence is an Arithmetic Progression if the terms are selected at a regular interval from an Arithmetic Progression.

Property VIII: If x, y, and z are three consecutive terms of an Arithmetic Progression then $2y = x + z$.

1.5 GEOMETRICAL PROGRESSION

In mathematics, a '***Geometric Progression'***, also known as a ***'Geometric Sequence'***, is a sequence of non–zero numbers where each term after the first is found by multiplying the previous one by a fixed, non–zero number called the *common ratio*. For example, the sequence 2, 6, 18, 54, ... is a geometric progression with common ratio 3. Similarly 10, 5, 2.5, 1.25, ... is a geometric sequence with common ratio 1/2.

Examples of a geometric sequence are powers r^k of a fixed non–zero number r, such as 2^k and 3^k. The general form of a geometric sequence is,

$$a, ar, ar^2, ar^3, ar^4 \ldots\ldots\ldots$$

Where $r \neq 0$ is the common ratio and $a \neq 0$ is a scale factor, equal to the sequence's start value. The distinction between a progression and a series is that a progression is a sequence, whereas a series is a sum.

Definition: A geometric progression or a geometric sequence is the sequence, in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant (which is, non–zero) to the preceding term. It is represented by following term:

$$a, ar, ar^2, ar^3, ar^4,$$ and so on.

Where a is the first term and r is the common ratio.

Note: It is to be noted that when we divide any succeeding term from its preceding term, then we get the value equal to the common ratio.

Suppose we divide 3rd term by 2nd term we get

$$ar^2/ar = r$$

In the same way:

$$ar^3/ar^2 = r$$

$$ar^4/ar^3 = r$$

NOTES

Non-zero quantities $a_1, a_2, a_3, ..., a_n, ...$, each term of which is equal to the product of preceding term and a constant number, form a *Geometrical Progression* (written as G.P.).

Thus, all the following quantities are in G.P.

(*i*) 1, 2, 4, 8, 16,...

(*ii*) $3, -1, \frac{1}{3}, \frac{-1}{9}, \frac{1}{27}, ...$

(*iii*) $1, \sqrt{2}, 2, 2\sqrt{2}, ...$

(*iv*) $a, \frac{a}{b}, \frac{a}{b^2}, \frac{a}{b^3}, ...,$ where $a \neq 0, b \neq 0.$

(*v*) $1, \frac{1}{5}, \frac{1}{25}, \frac{1}{125}, ...$

The constant number is termed as the *common ratio* of the G.P.

The *n*th Term of a G.P.

Let first term be a and r, the common ratio, By definition the G.P. is $a, ar, ar^2, ...$

$$1\text{st term} = a = ar^0 = ar^{1-1}$$

$$2\text{nd term} = ar = ar^1 = ar^{2-1}$$

... ...

In general, nth term $= ar^{n-1}$.

In examples of the preceding section, we compute 5th, 7th, 3rd, 11th and 8th term of (*i*), (*ii*), (*iii*), (*iv*) and (*v*), respectively.

In (*i*) Ist term is 1 and common ratio = 2.

Hence, 5th term $= ar^4 = 1.2^4 = 16.$

In (*ii*) $a = 3, r = \frac{-1}{3}$, hence, 7th term $= ar^6 = 3\left(\frac{-1}{3}\right)^6 = \frac{1}{243}.$

In (*iii*) $a = 1, r = \sqrt{2}$, hence, 3rd term $= ar^2 = 2.$

In (*iv*) Ist term $= a, r = \frac{1}{b}$, hence, 11th term $= ar^{10} = \frac{a}{b^{10}}.$

In (*v*) $a = 1, r = \frac{1}{5}$, hence, 8th term $= ar^2 = \frac{1}{5^7} = \frac{1}{78125}.$

Sum of First *n* Terms of a G.P.

Let $a, ar, ar^2, ...$ be a given G.P. and let S_n be the sum of its first n terms.

Then, $S_n = a + ar + ar^2 + ... + ar^{n-1}.$

This gives that, $rS_n = ar + ar^2 + ... + ar^{n-1} + ar^n$

Subtracting, we get, $S_n - r S_n = a - ar^n = a(1 - r^n)$

In case $r \neq 1$, $S_n = \frac{a(1-r^n)}{(1-r)}$

In case $r = 1$, $S_n = a + a + a + ... + a$ (n times)

$= na$

Thus, sum of n terms of a G.P. is $\frac{a(1-r^n)}{1-r}$ provided $r \neq 1$.

In case $r = 1$, sum of G.P. is na.

NOTES

Sum of Infinite Geometric Progression

The sum of an infinite Geometric Progression whose first term 'a' and common ratio 'r' ($-1 < r < 1$, i.e., $|r| < 1$) is,

$$s = \frac{a}{1-r}$$

Proof: A series of the form $a + ar + ar^2 + ... + ar^n + ... \infty$ is called an infinite geometric series.

Let us consider an infinite Geometric Progression with first term a and common ratio r, where $-1 < r < 1$, i.e., $|r| < 1$. Therefore, the sum of n terms of this Geometric Progression in given by,

$$S_n = a\left(\frac{1-r^n}{1-r}\right) = \frac{a}{1-r} - \frac{ar^n}{1-r} \quad \ldots\ldots\ldots\ldots\ldots\ldots \text{(i)}$$

Since $-1 < r < 1$, therefore r^n decreases as n increases and r^n tends to zero an n tends to infinity, i.e., $r^n \to 0$ as $n \to \infty$.

Therefore,

$$\frac{ar^n}{1-r} \to 0 \text{ as } n \to \infty.$$

Hence, from Equation (i), the sum of an infinite Geometric Progression given by,

$$S = \lim_{x \to 0} S_n = \lim_{x \to \infty}\left(\frac{a}{1-r} - \frac{ar^2}{1-r}\right) = \frac{a}{1-r} \text{ if } |r| < 1$$

Note: (i) If an infinite series has a sum, the series is said to be convergent. On the contrary, an infinite series is said to be divergent it has no sum. The infinite geometric series $a + ar + ar^2 + ... + ar^n + ... \infty$ has a sum when $-1 < r < 1$; so it is convergent when $-1 < r < 1$. But it is divergent when $r > 1$ or, $r < -1$.

(ii) If $r - 1$, then the sum of an infinite Geometric Progression (G.P.) tens to infinity.

Example 1.41: Find the sum to infinity of the geometric progression.

$$-\frac{5}{4}, \frac{5}{16}, -\frac{5}{64}, \frac{5}{256}, \ldots\ldots\ldots$$

Solution: The given geometric progression is,

$$-\frac{5}{4}, \frac{5}{16}, -\frac{5}{64}, \frac{5}{256}, \ldots\ldots\ldots$$

It has first term $a = -\frac{5}{4}$ and the common ratio $r = -\frac{1}{4}$. Also, $|r| < 1$.

Therefore, the sum to infinity is given by,

$$S = \frac{a}{1-r} = \frac{\frac{5}{4}}{1-\left(-\frac{1}{4}\right)} = -1$$

NOTES

Recurring Decimal an Infinite Geometric Progression

An interesting application of a geometric progression with infinitely many terms is the evaluation of recurring or periodic decimals.

When we attempt to express a common fraction, such as 3/8 or 4/11 as a decimal fraction, the decimal always either terminates or ultimately repeats in blocks. Thus,

$$\frac{3}{8} = 0.375 \text{ (Decimal Terminates)}$$

$$\frac{4}{11} = 0.363636.....\text{(Decimal Repeats)}$$

In the division process which express the fraction p/q as a decimal fraction the remainders can only be the numbers 0, 1, 2, 3, 4,…, q–1. If at any stage in the division we obtain a remainder of 0, the process terminates. Otherwise, after not more than q divisors, one of the remainders 0,1,2,3,4,…, q–1 must recur and the decimal begins to repeat.

Example 1.42: Express the recurring decimal fraction 0.5378378378… as a common fraction.

Solution: Hence our number consists of the decimal 0.5 plus the sum of an infinite geometric progression with the first term a_1=0.0378 and common ratio r = 0.001. The sum of the infinite progression is expressible as the fraction,

Example 1.43: Find the sum of the first 14 terms of a G.P.

3, 9, 27, 81, 243, 729,...

Solution: In this case $a = 3$, $r = 3$, $n = 14$.

$$\text{So,} \quad S_n = \frac{a\left(1-r^n\right)}{1-r} = \frac{3\left(1-3^{14}\right)}{1-3}$$

$$= \frac{3}{2}\left(3^{14}-1\right).$$

Example 1.44: Find the sum of first 11 terms of a G.P. given by:

$$1, \ -\frac{1}{2}, \ \frac{1}{4}, \ -\frac{1}{8} \ \ldots, \ldots$$

Solution: Here, $a = 1$, $r = -\frac{1}{2}$, $n = 11$.

$$\text{So,} \quad S_n = \frac{a\left(1-r^n\right)}{1-r} = \frac{1\left[1-\left(-\frac{1}{2}\right)^{11}\right]}{1+\frac{1}{2}}$$

$$= \frac{2^{11}+1}{3\times 2^{10}} = \frac{683}{1024}.$$

1.5.1 Geometric Mean (G.M.)

In mathematics, the 'Geometric Mean' is a mean or average, which indicates the central tendency or typical value of a set of numbers by using the product of their values (as opposed to the arithmetic mean which uses their sum). The geometric

NOTES

mean is defined as the nth root of the product of n numbers, i.e., for a set of numbers $x_1, x_2, ..., x_n$, the geometric mean is defined as,

$$\left(\prod_{i=1}^{n} x_i\right)^{\frac{1}{n}} = \sqrt[n]{x_1 x_2 \cdots x_n}$$

or, equivalently, as the arithmetic mean in logspace:

$$e^{\frac{\sum_{i-1}^{n} \ln a_i}{n}}$$

For instance, the geometric mean of two numbers, say 2 and 8, is just the square root of their product, that is, $\sqrt{2 \cdot 8} = 4$. As another example, the geometric mean of the three numbers 4, 1, and 1/32 is the cube root of their product (1/8), which is 1/2, that is, $\sqrt[3]{4 \cdot 1 \cdot 1/32} = 1/2$. The geometric mean applies only to positive numbers.

The geometric mean is often used for a set of numbers whose values are meant to be multiplied together or are exponential in nature. The values of the human population or interest rates of a financial investment over time. It also applies to benchmarking, where it is particularly useful for computing means of speedup ratios: since the mean of 0.5x (half as fast) and 2x (twice as fast) will be 1 (i.e., no speedup overall).

The geometric mean can be understood in terms of geometry. The geometric mean of two numbers, *a* and *b*, is the length of one side of a square whose area is equal to the area of a rectangle with sides of lengths *a* and *b*. Similarly, the geometric mean of three numbers, *a*, *b*, and *c*, is the length of one edge of a cube whose volume is the same as that of a cuboid with sides whose lengths are equal to the three given numbers.

The geometric mean is one of the three classical Pythagorean means, together with the arithmetic mean and the harmonic mean. For all positive data sets containing at least one pair of unequal values, the harmonic mean is always the least of the three means, while the arithmetic mean is always the greatest of the three and the geometric mean is always in between.

The geometric mean (G) is the nth root of the product of n values.

$$G = \sqrt[n]{x_1 \times x_2 \times ... \times x_n}$$

The G.M. of 2, 4, 8 is the cube root of their product.

$$G = \sqrt[3]{2 \cdot 4 \cdot 8} = \sqrt[3]{64} = 4$$

If the frequencies of $x_1, x_2, ..., x_k$ are respectively $f_1, f_2, ..., f_k (\Sigma f = n)$

$$G = \sqrt[n]{x_1^{f_1} \cdot x_z^{f_2} ..... x_k^{f_k}}$$

Logarithms may be used in the calculation of G.M.

$$\text{Log } G = \frac{1}{n}\left[f_1 \log x_1 + f_2 \log x_2 + ... + f_k \log x_k\right] = \frac{\Sigma f \log x}{n}$$

$$G = \text{Antilog } \frac{1}{n}\Sigma f \log x$$

If there are no frequencies, $G = (x_1 x_2 ... x_n)^{\frac{1}{n}}$ and $\log G = \frac{1}{n}\Sigma \log x$

Geometric Mean of Two given Number A and B Insertion of N between two quantities geometric means

Definition:–If three terms are in G.P, then the middle term is called the Geometric Mean (G.M) between the two. So if A, B, C are in G.P, then $B = \sqrt{AC}$ is the geometric mean of A and C.

If

$$\mathbf{g_1, g_2, \ldots\ldots\ldots g_n}$$

Are **N** geometric means between and **A** and **B** then,

$$\mathbf{A, g_1, g_2, \ldots\ldots\ldots g_n}$$

B will be a G.P.

Formula: Let $\mathbf{A, g_1, g_2, \ldots\ldots\ldots g_n}$ be N geometric means between two given numbers A and B. Then A, $g_1, g_2, \ldots\ldots\ldots g_n$. B will be also include in geometric progression.

So,

$$B = (N + 2)^{th}$$

term of the geometric progression.

Then here r is the common ratio:

$$B = A^* r^{N+1}$$

$$r^{N+1} = B/A$$

$$r = B/A^{1/(N+1)}$$

Now we have the value of r and also we have the value of the first term A:

$$g_1 = A\, r^1 = A^* B/A^{1/(N+1)}$$

$$g_2 = Ar^2 = A^* B/A^{21/(N+1)}$$

$$g_3 = Ar^3 = A^* B/A^{31/(N+1)}$$

$$g_N = Ar^N = A^* B/A^{N/(N+1)}$$

Example 1.45: Insert 4 geometric means between 3 and 96.

Solution: – Let G_1, G_2, G_3, G_4 be the required geometric means,

Then 3, G_1, G_2, G_3, G_4 are in G.P.

Let r be the common ratio

Here 96 is the 6^{th} terms

NOTES

$$96 = A\, r^{6-1} = 3r^5 \Rightarrow r^5 = 32 = (2)^5 \Rightarrow r = 2$$

$$G_1 = Ar = 3 \times 2 = 6$$

$$G_2 = Ar^2 = 3 \times 2^2 = 12$$

$$G_3 = Ar^3 = 3 \times 2^3 = 24$$

$$G_4 = Ar^4 = 3 \times 2^4 = 48$$

Merits and Uses of Geometric Mean

Most of the properties and merits of G.M. resemble those of A.M.

(i) The GM takes into account all the items in the data and condenses them into one respectative value.

(ii) It has a downward bias. It gives more weight to smaller values than to larger values.

(iii) It is determinate. For the same data there cannot be two geometric means.

(iv) GM balances the ratios of the values on either side of the data. It is ideally suited to average rates of change such as index numbers and ratios between measures and percentages.

(v) It is amenable to algebraic manipulations like the A.M.

Demerits of Geometric Mean

(i) It is difficult to use and to compute.

(ii) It is determined for positive values and cannot be used for negative values of zero. A zero will convert the whole product into zero.

Properties of Geometric Progression

We will discuss about some of the properties of Geometric Progressions and geometric series which we will frequently use in solving different types of problems on Geometric Progressions.

Property I: When each term of a Geometric Progression is multiplied or divided by a same non–zero quantity, then the new series forms a Geometric Progression having the same common ratio.

Proof: Let, $a_1, a_2, a_3, a_4, \ldots\ldots\ldots\ldots, a_n, \ldots\ldots\ldots$ be a Geometric Progression with common r. Then,

$$\frac{a_{n+1}}{a_n} = r, \text{ for all } n \in N \ldots\ldots\ldots\ldots\ldots\ldots (i)$$

Let k be a non–zero constant. Multiplying all the terms of the given Geometric Progression by k, we obtain the sequence,

$$ka_1, ka_2, ka_3, ka_4, \ldots\ldots\ldots\ldots, ka_n, \ldots\ldots\ldots\ldots$$

$$\text{Clearly, } \frac{ka_{(n+1)}}{ka_n} = \frac{a_{(n+1)}}{a_n} = r \text{ for all } n \in N \text{ [Using (i)]}$$

Hence, the new sequence also forms a Geometric Progression with common ratio r.

Property II: In a Geometric Progression the reciprocals of the terms also form a Geometric Progression.

Proof: Let, $a_1, a_2, a_3, a_4, \ldots\ldots\ldots\ldots, a_n, \ldots\ldots\ldots$ be a Geometric Progression with common r. Then,

$$\frac{a_{n+1}}{a_n} = r, \text{ for all } n \in N \qquad \ldots\ldots(i)$$

The series formed by the reciprocals of the terms of the given Geometric Progression is,

$$\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}, \ldots\ldots\ldots\ldots, \frac{1}{a_n}, \ldots\ldots\ldots\ldots$$

We have, $\dfrac{\dfrac{1}{a(n+1)}}{\dfrac{1}{a_n}} = \dfrac{a_n}{a_{n+1}} = \dfrac{1}{r}$ [Using (i)]

So, the new series is a Geometric Progression with common ratio 1/r.

Property III: When all the terms of a geometric progression be raised to the same power, then the new series also forms a geometric progression.

Proof: Let, $a_1, a_2, a_3, a_4, \ldots\ldots\ldots\ldots, a_n, \ldots\ldots\ldots$ be a Geometric Progression with common r. Then,

$$a–(n + 1)/a–n = r, \text{ for all } n \in N \ldots\ldots\ldots\ldots\ldots \text{(i)}$$

Let k be a non–zero real number. Consider the sequence

$a_1^k, a_2^k, a_3^k, \ldots\ldots\ldots, a_n^k, \ldots\ldots\ldots$

We have, $a–(n+1)^{k/a}–n^k = (a–(n+1)/a–n)^k = r^k$ for all $n \in N$, [Using (i)]

Hence, $a_1^k, a_2^k, a_3^k, \ldots\ldots\ldots, a_n^k, \ldots\ldots\ldots$ is a geometric progression with common ratio r^k.

Property IV: The product of the first and the last term is always equal to the product of the terms equidistant from the beginning and the end of finite geometric progression.

Property V: Three non–zero quantity a, b, c are in geometric progression if and only if $b^2 = ac$.

Proof: a, b, c are in geometric progression $\Leftrightarrow$ b/a = c/b = common ratio $\Leftrightarrow b^2 = ac$

Note: When a, b, c are in geometric progression, then b is known as the geometric mean of a and c.

Property VI: When the terms of a geometric progression are selected at intervals then the new series obtained also a geometric progression.

Property VII: In a geometric progression of non–zero non–negative terms, then logarithm of each term is form an arithmetic progression and vice–versa.

i.e., If $a_1, a_2, a_3, a_4, \ldots\ldots\ldots\ldots, a_n, \ldots\ldots\ldots\ldots$ are non–zero non–negative terms of a geometric progression then $\log a_1, \log a_2, \log a_3, \log a_4, \ldots\ldots\ldots\ldots, \log a_n, \ldots\ldots\ldots\ldots$ forms and arithmetic progression.

NOTES

1.6 HARMONIC PROGRESSION

In Mathematics, a progression is defined as a series of numbers arranged in a predictable pattern. It is a type of number set which follows specific, definite rules. There is a difference between the progression and a sequence. A progression has a particular formula to compute its *n*th term, whereas a sequence is based on the specific logical rules. A progression can be generally classified into three different types, such as arithmetic progression, geometric progression and harmonic progression. In mathematics, a harmonic progression (or harmonic sequence) is a progression formed by taking the reciprocals of an arithmetic progression. Equivalently, a sequence is a harmonic progression when each term is the harmonic mean of the neighbouring terms.

As a third equivalent characterization, it is an infinite sequence of the form,

$$\frac{1}{a}, \frac{1}{a+d}, \frac{1}{a+2d}, \frac{1}{a+3d}, \cdots,$$

Where *a* is not zero and "*a*/*d* is not a natural number, or a finite sequence of the form,

$$\frac{1}{a}, \frac{1}{a+d}, \frac{1}{a+2d}, \frac{1}{a+3d}, \cdots, \frac{1}{a+kd},$$

Where *a* is not zero, *k* is a natural number and "*a*/*d* is not a natural number or is greater than *k*.

Definition: A Harmonic Progression (HP) is defined as a sequence of real numbers which is determined by taking the reciprocals of the arithmetic progression that does not contain 0. In harmonic progression, any term in the sequence is considered as the harmonic means of its two neighbours. For example, the sequence *a*, *b*, *c*, *d*, … is considered as an arithmetic progression; the harmonic progression can be written as 1/*a*, 1/*b*, 1/*c*, 1/*d*, …

Harmonic Mean: Harmonic mean is calculated as the reciprocal of the arithmetic mean of the reciprocals. The formula to calculate the harmonic mean is given by:

Harmonic Mean = n /[(1/*a*) + (1/*b*)+ (1/*c*)+(1/*d*)+….]

Where, *a*, *b*, *c*, *d* are the values and *n* is the number of values present.

Harmonic Progression Formula: To solve the harmonic progression problems, we should find the corresponding arithmetic progression sum. It means that the *n*th term of the harmonic progression is equal to the reciprocal of the *n*th term of the corresponding A.P. Thus, the formula to find the *n*th term of the harmonic progression series is given as:

The *n*th term of the Harmonic Progression (H.P) = 1/ [*a*+(*n*–1)*d*]

Where

'*a*' is the first term of A.P

'*d*' is the common difference

'*n*' is the number of terms in A.P

The above formula can also be written as:

The *n*th term of H.P = 1/ (*n*th term of the corresponding A.P)

NOTES

Harmonic Progression Sum

If $1/a, 1/a+d, 1/a+2d, \ldots, 1/a+(n-1)d$ is given harmonic progression, the formula to find the sum of n terms in the harmonic progression is given by the formula:

Sum of *n* terms given by following formula,

$$S_n = \frac{1}{d} ln \left\{ \frac{2a+(2n-1)d}{2a-d} \right\}$$

Where,

'*a*' is the first term of A.P

'*d*' is the common difference of A.P

'ln' is the natural logarithm

Relation Between AM, GM and HM

For any two numbers, if A.M, G.M, H.M are the arithmetic, geometric and harmonic mean respectively, then the relationship between these three is given by:

$G.M^2 = A.M \times H.M$, where A.M, G.M, H.M are in G.P

$A.M \geq G.M \geq H.M$

Example 1.46: Determine the 4th and 8th term of the harmonic progression 6, 4, 3,…

Solution: Given H.P = 6, 4, 3

Now, let us take the arithmetic progression from the given H.P

A.P = $\frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \ldots$.

Here, $T_2 - T_1 = T_3 - T_2 = 1/12 = d$

So, in order to find the 4th term of an A. P, use the formula,

The *n*th term of an A.P = $a+(n-1)d$

Here, $a = \frac{1}{6}$, $d = 1/12$

Now, we have to find the 4th term.

So, take $n = 4$

Now put the values in the formula.

4th term of an A.P = $(\frac{1}{6}) + (4-1)(1/12)$

$= (1/6)+(3/12)$

$= (1/6)+ (1/4)$

$= 5/12$

NOTES

Similarly,

8th term of an A.P = $(\frac{1}{6})$ +(8–1)(1/12)

= $(\frac{1}{6})$ + (7/12)

= 9/12

Since H.P is the reciprocal of an A.P, we can write the values as:

4th term of an H.P = 1/4th term of an A.P = 12/5

8th term of an H.P = 1/8th term of an A.P = 12/9 = 4/3

Harmonic Series

Non-zero quantities whose reciprocals are in A.P. are said to be in Harmonical Progression (H.P.)

Consider the following examples:

1. $1, \frac{1}{3}, \frac{1}{5}, \frac{1}{7}, \ldots\ldots$
2. $\frac{1}{2}, \frac{1}{5}, \frac{1}{8}, \frac{1}{11}, \ldots\ldots$
3. $2, \frac{5}{2}, \frac{10}{3}, \ldots$
4. $\frac{1}{a}, \frac{1}{a+b}, \frac{1}{a+2b}, \ldots\ldots \; a, b > 0$
5. $5, \frac{55}{9}, \frac{55}{7}, 11, \ldots\ldots$

It can be easily checked, that in each case the series obtained by taking the reciprocal of each of the term is an A.P.

Check Your Progress

8. Define the arithmetic progression.
9. What do you understand by arithmetic mean?
10. What is common ratio?
11. Define the term geometric progression.
12. What is geometric mean?
13. Give the definition of harmonic progression.

1.7 ANSWERS TO 'CHECK YOUR PROGRESS'

1. A sequence is an endless succession of numbers placed in a certain order so that there is a first member, a second and so on.
2. A sequence $<a_n>$ is said to converge to a number l, if given any $\varepsilon > 0$, there exists a +ve integer m, such that,

$$|a_n - l| < \varepsilon, \quad \forall\ r \geq m$$

This number l is called limit of the sequence.

3. A sequence $<a_n>$ is said to diverge to $+\infty$, if for each positive number K, (however large), it is possible to find a +ve integer m, such that,

$$a_n > K \quad \forall\ n \geq m\ .$$

4. A series can be highly generalised as the sum of all the terms in a sequence. However, there has to be a definite relationship between all the terms of the sequence.
5. When an infinite series has infinite number of terms and there may not be any definite rule to determine its terms. Such a series is denoted by an expression of the form,

$$u_1 + u_2 + u_3 + \ldots + u_n \quad \text{or} \quad \sum_{n=1}^{\infty} u_n \text{ or } \Sigma u_n\ .$$

6. If $\Sigma\, u_n$ and $\Sigma\, v_n$ are two positive term series such that, $u_n < kv_n\ \forall\, n$, where k is some fixed positive number, then Σu_n divergent $\Rightarrow \Sigma v_n$ is divergent and Σv_n convergent $\Rightarrow \Sigma u_n$ is convergent.
7. Leibnitz's Test. The alternating series $u_1 - u_2 + u_3 - u_4 + \ldots$ is convergent if,

   (*i*) $u_{n+1} \leq u_n\ \forall\, n$

   (*ii*) $\lim_{n \to \infty} u_n = 0.$

8. Quantities $a_1, a_2, a_3, \ldots, a_n, \ldots$ are said to be in Arithmetical Progression if $a_n - a_{n-1}$ is constant for all integers $n > 1$. The constant quantity $a_n - a_{n-1}$ is called the common difference of the arithmetical progression.
9. If $a_1, a_2, \ldots, a_n$ are in A.P., then the quantities $a_2, a_3, \ldots, a_{n-1}$ are called Arithmetic Means (A.M.) between a_1 and a_n.

   Thus in the series, 1, 3, 5, 7, 9, 11, 13, 15, ...

   3, 5 are arithmetic means between 1 and 7.

   9, 11, 13 are arithmetic means between 7 and 15.
10. In mathematics, a 'Geometric Progression', also known as a 'Geometric Sequence', is a sequence of non–zero numbers where each term after the first is found by multiplying the previous one by a fixed, non–zero number called the common ratio.
11. A geometric progression or a geometric sequence is the sequence, in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant (which is, non–zero) to the preceding term.
12. In mathematics, the 'Geometric Mean' is a mean or average, which indicates the central tendency or typical value of a set of numbers by using the product of their values (as opposed to the arithmetic mean which uses their sum). The geometric mean is defined as the nth root of the product of n numbers, i.e., for a set of numbers $x_1, x_2, \ldots, x_n$, the geometric mean is defined as,

NOTES

NOTES

13. A Harmonic Progression (HP) is defined as a sequence of real numbers which is determined by taking the reciprocals of the arithmetic progression that does not contain 0. In harmonic progression, any term in the sequence is considered as the harmonic means of its two neighbours.

1.8 SUMMARY

- A sequence is an endless succession of numbers placed in a certain order so that there is a first member, a second and so on.
- Let $<a_n>$ be a given sequence and suppose K is any large number. If we find that except for a finite number of elements of the sequence, all members are greater than K, we say that the sequence has $+\infty$ as its limit. In such a case the sequence $<a_n>$ is said to diverge to $+\infty$.
- A sequence is thus convergent if it has a finite limit and is divergent otherwise (i.e., when the limit is infinite or it does not exist).
- A series Σu_n is defined to be convergent or divergent according to the state of its sequence of partial sums $<S_n>$ being convergent or divergent. If $<S_n>$ converges to S then S is called *sum* of the series Σu_n.
- Addition or omission of a finite number of terms in a series does not affect its convergence or divergence.
- Multiplication of all the terms of a series by a non-zero constant does not affect the convergence or divergence of the series.
- If all the terms in a series are positive we call it a positive term series.
- Quantities $a_1, a_2, a_3, ..., a_n, ...$ are said to be in Arithmetical Progression if $a_n - a_{n-1}$ is constant for all integers $n > 1$. The constant quantity $a_n - a_{n-1}$ is called the common difference of the arithmetical progression.
- Non-zero quantities $a_1, a_2, a_3, ..., a_n, ...$, each term of which is equal to the product of preceding term and a constant number, form a *Geometrical Progression* (written as G.P.).
- The GM takes into account all the items in the data and condenses them into one respectative value.
- GM balances the ratios of the values on either side of the data. It is ideally suited to average rates of change such as index numbers and ratios between measures and percentages.
- In Mathematics, a progression is defined as a series of numbers arranged in a predictable pattern. It is a type of number set which follows specific, definite rules.
- In mathematics, a harmonic progression (or harmonic sequence) is a progression formed by taking the reciprocals of an arithmetic progression. Equivalently, a sequence is a harmonic progression when each term is the harmonic mean of the neighbouring terms.

- Harmonic mean is calculated as the reciprocal of the arithmetic mean of the reciprocals.
- To solve the harmonic progression problems, we should find the corresponding arithmetic progression sum. It means that the nth term of the harmonic progression is equal to the reciprocal of the *n*th term of the corresponding A.P.

1.9 KEY TERMS

- **Series:** A series can be highly generalised as the sum of all the terms in a sequence. However, there has to be a definite relationship between all the terms of the sequence.
- **Arithmetical progression:** Quantities $a_1, a_2, a_3, ..., a_n, ...$ are said to be in Arithmetical Progression if $a_n - a_{n-1}$ is constant for all integers $n > 1$. The constant quantity $a_n - a_{n-1}$ is called the common difference of the arithmetical progression.
- **Geometric progression:** A geometric progression or a geometric sequence is the sequence, in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant (which is, non–zero) to the preceding term.
- **Harmonic Progression (HP):** A Harmonic Progression (HP) is defined as a sequence of real numbers which is determined by taking the reciprocals of the arithmetic progression that does not contain 0.

1.10 SELF-ASSESSMENT QUESTIONS AND EXERCISES

Short–Answer Questions

1. What do you understand by arithmetic progression?
2. Define sequence.
3. What is series?
4. Give the general terms of A.P.
5. State the concept of geometric progression.
6. Define the geometric mean.
7. Determine the harmonic series.
8. What is harmonic mean?

Long–Answer Questions

1. Discuss the sequence and series with the help of examples.
2. Explain the arithmetic progression with appropriate examples and properties.

NOTES

3. Elaborate on the geometric progression with the help of examples and properties.
4. Analyse the geometric mean of two numbers A and B insertion of N.
5. Describe the harmonic progression with definition and harmonic means between two given numbers relation between A.M, G.M or H.M.

1.11 FURTHER READING

Hazarika, Padmalochan. 2003. *A Class Textbook of Business Mathematics*. New Delhi: S. Chand & Company Ltd.

Tremblay, Jean Paul and R. Manohar. 2004. *Discrete Mathematical Structures With Applications To Computer Science*. New York: McGraw–Hill Higher Education.

Ramaswamy, V. 2006. Discrete *Mathematical Structures with Applications to Combinatorics*. Hyderabad: Universities Press.

Kolman, Bernand, Roberty C. Busby and Sharn Cutter Ross. 2006. *Discrete Mathematical Structures*. London (UK): Pearson Education.

Liu, C. L. 1985. *Elements of Discrete Mathematics*, 2nd Edition. New York: McGraw–Hill Higher Education.

Arumugam, S. and Thangapandi Isaac. 2008. *Modern Algebra*. Chennai: Scitech Publications (India) Pvt. Ltd.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. New Delhi: Cambridge University Press.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

UNIT 2 SERIES AND SET THEORY

NOTES

Structure

2.0 INTRODUCTION

Miscellaneous series is not dependent on the other patterns and it has general nature but they are important and fairly common. An arithmetic series is the sum of the terms of an arithmetic sequence. A geometric series is the sum of the terms of a geometric sequence. In mathematics, a 'Geometric Series' is the sum of an infinite number of terms that have a constant ratio between successive terms.

Set theory is the branch of mathematical logic that studies sets, which can be informally described as collections of an objects. A Venn diagram is an illustration that uses circles to show the relationships among things or finite groups of things. On the other hand according to De-Morgan's Law, the complement of the union of two sets will be equal to the intersection of their individual complements.

In this unit, you will study about the miscellaneous series, arithmetic and geometric series, set theory, Venn diagram, De–Morgan law.

2.1 OBJECTIVES

After going through this unit, you will be able to:

- Interpret the miscellaneous series
- Explain the arithmetic and geometric series
- Describe the set theory
- Illustrate the Venn diagram
- State the De–Morgan law

NOTES

2.2 MISCELLANEOUS SERIES

There are series that do not come under the other patterns and are of general nature but they are important and properly in a common series. Even here, sometimes, there can be a specific pattern in some cases. Take the series 3, 5, 7, 11, 13, this is a series of consecutive prime numbers.

Examples of Miscellaneous Series

Example 2.1: Test the convergence of the series,

(*i*) $1+\frac{1}{2^2}+\frac{2^2}{3^3}+\frac{3^3}{4^4}+\frac{4^4}{5^5}+\ldots$

(*ii*) $\frac{1}{1.3}+\frac{2}{3.5}+\frac{3}{5.7}+\ldots$

(*iii*) $1+\frac{x}{2}+\frac{x^2}{5}+\frac{x^3}{10}+\ldots+\frac{x^n}{n^2+1}+\ldots$

(*iv*) $\sum_{n=1}^{\infty}u_n$ where $u_n=\sqrt{n^3+1}-\sqrt{n^3}$

(*v*) $\sum_{n=1}^{\infty}u_n$ where $u_n=\frac{n^{n^2}}{(1+n)^{n^2}}$

(*vi*) $\sum_{n=1}^{\infty}u_n$ where $u_n=(n^3+1)^{\frac{1}{3}}-n$

Solution: (*i*) The given series Σu_n is a series of positive terms,

$$u_n=\frac{n^n}{(n+1)^{n+1}} \quad \text{for } n\geq 2$$

Now we take $v_n=\frac{1}{n+1}$

$$\therefore \quad \frac{u_n}{v_n}=\frac{n^n}{(n+1)^{n+1}}.(n+1)=\frac{n^n}{(n+1)^n}$$

$$=\frac{1}{\left(1+\frac{1}{n}\right)^n}\to\frac{1}{e} \text{ as } n\to\infty \qquad \left[\because \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n=e\right]$$

$\therefore$ As $\frac{1}{e}$ is non-zero finite and $\sum_{n=0}^{\infty}v_n=1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}-\ldots$ is known divergent series, by the comparison test, the given series is divergent.

(*ii*) The given series Σu_n is a series of positive terms.

Here $u_n=\frac{n}{(2n-1)(2n+1)}$ and we take $v_n=\frac{1}{n}$.

$$\therefore \quad \frac{u_n}{v_n}=\frac{n}{(2n-1)(2n+1)}\times n=\frac{n^2}{4n^2\left(1-\frac{1}{2n}\right)\left(1+\frac{1}{2n}\right)}$$

NOTES

$$= \frac{1}{4\left(1-\frac{1}{2n}\right)\left(1+\frac{1}{2n}\right)}$$

$$\to \frac{1}{4} \text{ as } n \to \infty \text{ which is finite.}$$

Since $\Sigma v_n = \sum \frac{1}{n}$ is a p-series with $p = 1$, which is divergent, by the comparison test, the given series is divergent.

(*iii*) Each term of the given series (Σu_n) is not positive for all values of x. Neglecting the first term, we have

$$u_n = \frac{x^n}{n^2+1},\ u_{n+1} = \frac{x^{n+1}}{(n+1)^2+1}$$

$$\therefore \quad \left|\frac{u_{n+1}}{u_n}\right| = \left|\frac{x^{n+1}}{(n+1)^2+1} \times \frac{n^2+1}{x^n}\right| = \left|\frac{1+\frac{1}{n^2}}{\left(1+\frac{1}{n}\right)^2+\frac{1}{n^2}}\, x\right| \to |x| \text{ as } n \to \infty$$

Hence by the tests for absolute convergence, Σu_n is convergent if $|x| < 1$, *i.e.,* if $-1 < x < 1$ and divergent if $|x| > 1$. When $x = 1$, then Σu_n becomes a series of positive terms with,

$$u_n = \frac{1}{n^2+1},\ u_{n+1} = \frac{1}{(n+1)^2+1} \text{ for } n \geq 2 \text{ and } u_1 = 1$$

$$\therefore \quad \lim_{n\to\infty} \left\{n\left(\frac{u_n}{u_{n+1}}-1\right)\right\} = \lim_{n\to\infty} \left[n\left\{\frac{(n+1)^2+1}{n^2+1}-1\right\}\right]$$

$$= \lim_{n\to\infty} n \cdot \frac{2n+1}{n^2+1} = \lim_{n\to\infty} \frac{2+\frac{1}{n}}{1+\frac{1}{n^2}} = 2 > 1$$

Hence by **Raabe's test**, Σu_n is convergent when $x = 1$.

When $x = -1$, then Σu_n reduces to the series $1-\frac{1}{2}+\frac{1}{5}-\frac{1}{10}+\ldots$

This is an alternating series with negative and positive terms alternately.

Here $u_n = (-1)^{n+1} \frac{1}{n^2+1}$ for $n \geq 2$ and $u_1 = 1$

$$\therefore \quad \frac{|u_n|}{|u_{n+1}|} = \frac{(n+1)^2+1}{n^2+1} = \frac{n^2+2n+2}{n^2+1} = 1+\frac{2n+1}{n^2+1} > 1 \text{ for all } n \geq 2$$

$\therefore\ |u_n| > |u_{n+1}|$ and also $\lim_{n\to\infty} u_n = \lim_{n\to\infty} (-1)^{n+1} \frac{1}{n^2+1} = 0$

Hence Σu_n is convergent.

Thus Σu_n is convergent if $-1 \leq x \leq 1$ and divergent if $x > 1$ and $x < -1$.

(*iv*) Here $u_n = \sqrt{n^3+1} - \sqrt{n^3}$

NOTES

$$= \frac{\left(\sqrt{n^3+1}-\sqrt{n^3}\right)\left(\sqrt{n^3+1}+\sqrt{n^3}\right)}{\sqrt{n^3+1}+\sqrt{n^3}}$$

$$= \frac{1}{\sqrt{n^3+1}+\sqrt{n^3}} > 0 \text{ for all } n$$

So Σu_n is a series of positive terms and we take $v_n = \frac{1}{\sqrt{n^3}} = \frac{1}{n^{3/2}}$ then $\Sigma v_n = \sum \frac{1}{n^{3/2}}$ which is p-series with $p = \frac{3}{2} > 1$ and hence it is convergent.

Now $\frac{u_n}{v_n} = \frac{\sqrt{n^3}}{\sqrt{n^3+1}+\sqrt{n^3}} = \frac{1}{\sqrt{1+\frac{1}{n^3}}+1} \to \frac{1}{2}$ as $n \to \infty$, which is non-zero finite.

Hence by the comparison test, the given series is convergent.

(*v*) Here $u_n = \frac{n^{n^2}}{(1+n)^{n^2}} > 0$ for all $n \geq 1$, so Σu_n is a series of positive terms

And

$$(u_n)^{\frac{1}{n}} = \frac{n^{n^2 \cdot \frac{1}{n}}}{(1+n)^{n^2 \cdot \frac{1}{n}}} = \frac{n^n}{(1+n)^n} = \frac{1}{\left(1+\frac{1}{n}\right)^n}$$

$$= \lim_{n\to\infty} (u_n)^{\frac{1}{n}} = \lim_{n\to\infty} \frac{1}{\left(1+\frac{1}{n}\right)^n} = \frac{1}{e} < 1 \quad (\because\ 2 < e < 3)$$

Hence by the Cauchy's root test, the given series is convergent.

(*vi*) Here $u_n = \sqrt[3]{n^3+1} - n = n\left(1+\frac{1}{n^3}\right)^{\frac{1}{3}} - n = n\left\{\left(1+\frac{1}{n^3}\right)^{\frac{1}{3}} - 1\right\}$

$$= n\left[\left\{1+\frac{1}{3}\cdot\frac{1}{n^3}+\frac{\frac{1}{3}\left(\frac{1}{3}-1\right)}{\lfloor 2}\cdot\frac{1}{n^6}+\frac{\frac{1}{3}\left(\frac{1}{3}-1\right)\left(\frac{1}{3}-2\right)}{\lfloor 3}\cdot\frac{1}{n^9}+\ldots\right\}-1\right]$$

[by binomial expansion]

$$= n\left[\left(1+\frac{1}{3n^3}-\frac{1}{9}\frac{1}{n^6}+\frac{5}{81}\frac{1}{n^9}-\ldots\right)-1\right]$$

$$= n\left[\frac{1}{3n^3}-\frac{1}{9}\cdot\frac{1}{n^6}+\frac{5}{81}\frac{1}{n^9}-\ldots\right] = \left[\frac{1}{3n^2}-\frac{1}{9}\frac{1}{n^5}-\frac{5}{81}\frac{1}{n^8}-\ldots\right]$$

Now taking $v_n = \frac{1}{n^2}$, we see that Σv_n is a p-series with $p = 2 > 1$, which is convergent.

$$\therefore \lim_{n\to\infty} \frac{u_n}{v_n} = \lim_{n\to\infty} \left(\frac{1}{3} - \frac{1}{9}\frac{1}{n^3} + \frac{5}{81}\frac{1}{n^6} - \ldots\right)$$

$$= \frac{1}{3} \text{ which is finite.}$$

Hence by the comparison test, the given series is convergent.

NOTES

Example 2.2: Give the following test of the convergence of the series

(*i*) $\sum_{n=1}^{\infty} \frac{2n^3+5}{4n^5+1}$ (*ii*) $\frac{1.2}{3^2.4^2} + \frac{3.4}{5^2.6^2} + \frac{5.6}{7^2.8^2} + \ldots\infty$

(*iii*) $1 + \frac{1}{2}x + \frac{1.3}{2.4}x^2 + \frac{1.3.5}{2.4.6}x^3 + \ldots\infty$

(*iv*) $\sum_{n=1}^{\infty} \frac{\sqrt{n+1}-\sqrt{n}}{n}$

(*v*) $\frac{x}{1+x} - \frac{x^2}{1+x^2} + \frac{x^3}{1+x^3} - \frac{x^4}{1+x^4} + \ldots\infty \ (0 < x < 1)$

Solution: (*i*) Here $u_n = \frac{2n^3+5}{(4n^5+1)} = \frac{2n^3\left(1+\frac{5}{2n^3}\right)}{4n^5\left(1+\frac{1}{4n^5}\right)} = \frac{1}{2}\frac{\left(1+\frac{5}{2n^3}\right)}{n^2\left(1+\frac{1}{4n^5}\right)}$

Now we taking $v_n = \frac{1}{n^2}$, then Σv_n is a *p*-series with $p = 2 > 1$, which is convergent.

$$\therefore \lim_{n\to\infty} \frac{u_n}{v_n} = \lim_{n\to\infty} \frac{1}{2n^2} \frac{\left(1+\frac{5}{2n^3}\right)}{\left(1+\frac{1}{4n^5}\right)} \times n^2 = \lim_{n\to\infty} \frac{1}{2} \frac{\left(1+\frac{5}{2n^3}\right)}{\left(1+\frac{1}{4n^3}\right)}$$

$$= \frac{1}{2} \text{ which is finite.}$$

Hence by the comparison test, the given series is convergent.

(*ii*) Here $u_n = \frac{(2n-1)\,2n}{(2n+1)^2\,(2n+2)^2} = \frac{4n^2\left(1-\frac{1}{2n}\right)}{4n^2\left(1+\frac{1}{2n}\right)^2 4n^2\left(1+\frac{1}{n}\right)^2}$

$$= \frac{1}{4n^2} \frac{\left(1-\frac{1}{2n}\right)}{\left(1+\frac{1}{2n}\right)^2\left(1+\frac{1}{n}\right)^2}$$

Now we consider $v_n = \frac{1}{n^2}$. Then Σv_n is a *p*-series with $p = 2 > 1$, which is convergent.

$$\therefore \lim_{n\to\infty} \frac{u_n}{v_n} = \lim_{n\to\infty} \frac{1}{4n^2} \frac{\left(1-\frac{1}{2n}\right)}{\left(1+\frac{1}{2n}\right)^2\left(1+\frac{1}{n}\right)^2} \times n^2$$

NOTES

$$= \lim_{n\to\infty} \frac{1}{4} \frac{\left(1-\frac{1}{2n}\right)}{\left(1+\frac{1}{2n}\right)^2\left(1+\frac{1}{n}\right)^2}$$

$= \frac{1}{4}$ which in finite,

Hence by the comparison test, the given series is convergent.

(*iii*) Here $u_n = \frac{1.3.5 \ldots (2n-1)}{2.4.6 \ldots 2n} x^n$

Each term of the series Σu_n is not positive for all values of x and neglecting the first term.

$$\therefore \qquad u_{n+1} = \frac{1.3.5 \ldots (2n-1)(2n+1)}{2.4.6 \ldots 2n(2n+2)} x^{n+1}$$

$$\therefore \lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \lim_{n\to\infty} \frac{2n+1}{2n+2} x = \lim_{n\to\infty} \frac{1+\frac{1}{2n}}{\left(1+\frac{1}{n}\right)} x = x$$

Hence by the D'Alembert's ratio test, the given series is convergent if $x < 1$ and it is divergent if $x > 1$.

The test fails when $x = 1$.

So we apply the Raabe's test for $x = 1$,

Here $R_n = n\left(\frac{u_n}{u_{n+1}} - 1\right) = n\left(\frac{2n+2}{2n+1} - 1\right) = \frac{n(2n+2-2n-1)}{2n+1}$

$$= \frac{n}{2n+1} = \frac{1}{2+\frac{1}{n}}$$

$$\therefore \lim_{n\to\infty} R_n = \lim_{n\to\infty} \frac{1}{2+\frac{1}{n}} = \frac{1}{2} < 1.$$

Hence by the Raabe's test, the given series is divergent for $x = 1$.

Thus the given series is convergent for $x < 1$ and divergent for $x \geq 1$.

(*iv*) Here $v_n = \frac{\sqrt{n+1}-\sqrt{n}}{n} = \frac{\left(\sqrt{n+1}-\sqrt{n}\right)\left(\sqrt{n+1}+\sqrt{n}\right)}{n\left(\sqrt{n+1}+\sqrt{n}\right)}$

$$= \frac{n+1-n}{n\left(\sqrt{n+1}+\sqrt{n}\right)} = \frac{1}{n\left(\sqrt{n+1}+\sqrt{n}\right)} = \frac{1}{n\sqrt{n}\left(\sqrt{1+\frac{1}{n}}+1\right)}$$

Now we take $v_n = \frac{1}{n^{3/2}}$, then Σv_n is a p-series with $p = \frac{3}{2} > 1$ which is convergent.

$$\therefore \lim_{n\to\infty} \frac{u_n}{v_n} = \lim_{n\to\infty} \frac{1}{n^{3/2}\left(\sqrt{1+\frac{1}{n}}+1\right)} n^{3/2} = \lim_{n\to\infty} \frac{1}{\left(\sqrt{1+\frac{1}{n}}+1\right)} = \frac{1}{2}$$ which is finite.

Hence by the comparison test, the given series is convergent.

(*v*) The terms of the given series are alternately positive and negative, so the given series is an alternating series.

NOTES

Here $u_n = \frac{x^n}{1+x^n}$ and $u_{n+1} = \frac{x^{n+1}}{1+x^{n+1}}$

$$\therefore\ u_{n+1} - u_n = \frac{x^{n+1}}{1+x^{n+1}} - \frac{x^n}{1+x^n} = x^n\left[\frac{x}{1+x^{n+1}} - \frac{1}{1+x^n}\right]$$

$$= x^n\left[\frac{x + x^{n+1} - x^{n+1} - 1}{(1+x^{n+1})(1+x^n)}\right] = \frac{x^n(x-1)}{(1+x^{n+1})(1+x^n)} < 0$$

$(\because\ 0 < x < 1)$

$\therefore\ u_{n+1} < u_n$

Hence the sequence $\{u_n\}$ is monotone decreasing

and $\lim_{n\to\infty} u_n = \lim_{n\to\infty} \frac{x^n}{1+x^n} = \lim_{n\to\infty} \frac{1}{1+\frac{1}{x^n}}$ $[\because\ 0 < x < 1$, then $\frac{1}{x} > 1]$

$$= \frac{1}{1+\infty} = \frac{1}{\infty} = 0$$

Hence by the Leibnitz's test, the given series is convergent for $0 < x < 1$.

2.2.1 Arithmetic Series

An arithmetic series is the sum of an arithmetic sequence. We can find the sum by adding the first, a_1 and last term, a_n, divide by 2 in order to get the mean of the two values and then multiply by the number of values, n as per following equation:

$$\boldsymbol{S_n = n/2(a_1 + a_n)}$$

An arithmetic series is the sum of a sequence $\{a_k\}$, k=1, 2, ..., in which each term is calculated from the previous one by adding (or subtracting) a constant d. Therefore, *for k>1,*

$$a_k = a_{k-1} + d = a_{k-2} + 2d = \ldots = a_1 + d(k-1).$$

The sum of the sequence of the first n terms is then given by,

$$S_n = \sum_{k=1}^{n} a_k$$

$$= \sum_{k=1}^{n} [a_1 + (k-1)d]$$

$$= n a_1 + d \sum_{k=1}^{n} (k-1)$$

$$= n a_1 + d \sum_{k=2}^{n} (k-1)$$

$$= n a_1 + d \sum_{k=1}^{n-1} k.$$

NOTES

Using the sum identity,

$$\sum_{k=1}^{n} k = \tfrac{1}{2} n (n+1)$$

Then we get,

$$S_n = n a_1 + \tfrac{1}{2} d n (n-1) = \tfrac{1}{2} n [2 a_1 + d (n-1)].$$

Note, however, that

$$a_1 + a_n = a_1 + [a_1 + d (n-1)] = 2 a_1 + d (n-1),$$

So,

$$S_n = \tfrac{1}{2} n (a_1 + a_n).$$

2.2.2 Geometric Series

In mathematics, a **geometric series** is the sum of an infinite number of terms that have a constant ratio between successive terms. For example, the series is explained by following formula:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$$

is geometric, because each successive term can be obtained by multiplying the previous term by 1/2. In general, a geometric series is written as $a + ar + ar^2 + ar^3 + \ldots$, where a is the coefficient of each term and r is the common ratio between adjacent terms. Geometric series are among the simplest examples of infinite series and can serve as an introduction to **Taylor series** and **Fourier series**. Geometric series play an important role in the early development of calculus, are used throughout mathematics, and have important applications in physics, engineering, biology, economics, computer science, queueing theory, and finance.

The name geometric series indicates each term is the geometric mean of its two neighbouring terms, similar to how the name arithmetic series indicates each term is the arithmetic mean of its two neighbouring terms. The sequence of geometric series terms (without any of the additions) is called a geometric sequence or, equivalently, a geometric progression.

Sum of *n* Terms of the Arithmetic Series and Geometric Series

An arithmetic series is the sum of the terms of an arithmetic sequence. A geometric series is the sum of the terms of a geometric sequence. There are other types of series.

For reasons that will be explained in calculus, we take the 'Partial' sum of an arithmetic sequence. The partial sum is the sum of a limited (i.e., to say, a finite) number of terms, like the first ten terms, or the fifth through the hundredth terms.

The formula for the first n terms of an arithmetic sequence, starting with $i = 1$, is:

$$\sum_{i=1}^{n} a_i = \left(\frac{n}{2}\right)(a_1 + a_n)$$

The 'Equals' sign from under the *n* and convert it to being a one–half multiplied on the parentheses, we can explain that the formula for the sum is, in effect, *n* times the 'Average' of the first and last terms.

$$\left(\frac{n}{2}\right)(a_1 + a_n) = n\left(\frac{a_1 + a_n}{2}\right)$$

The sum of the first *n* terms of a series is called "The *n*th partial sum, and it is denoted by $''S_n''$.

Example 2.3: Find the 35th partial sum, S_{35}, of the arithmetic sequence with terms $a_n = \left(\frac{1}{2}\right)n + 1$.

Solution: The 35th partial sum of this sequence is the sum of the first thirty–five terms. The first few terms of the sequence are:

$$a_1 = \left(\frac{1}{2}\right)(1) + 1 = \frac{3}{2}$$

$$a_2 = \left(\frac{1}{2}\right)(2) + 1 = 2$$

$$a_3 = \left(\frac{1}{2}\right)(3) + 1 = \frac{5}{2}$$

The terms have a common difference *d*= ½, so this is indeed an arithmetic sequence. The last term in the partial sum will be:

$$a_{35} = a_1 + (35-1)\ (d)$$

$$= \frac{3}{2} + (35)\left(\frac{1}{2}\right) = \frac{37}{2}$$

Then, plugging into the formula, the 35th partial sum is:

$$\left(\frac{35}{2}\right)(a_1 + a_{35})$$

$$= \left(\frac{35}{2}\right)\left(\frac{3}{2} + \frac{37}{2}\right)$$

$$= \left(\frac{35}{2}\right)\left(\frac{40}{2}\right)$$

$$= 350$$

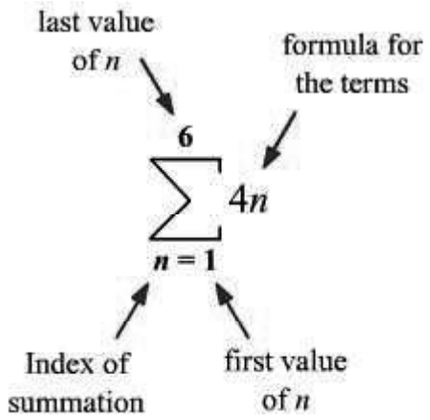
Sigma Notation of a Series

A series can be characterised in a compact form, which are called '**Summation or Sigma Notation'**. The Greek capital letter, $\sum$, is used to represent the sum.

The series 4+8+12+16+20+24 can be expressed as $\sum_{n=1}^{6} 4n$. The expression is read as the sum of 4*n* as *n* goes from 1 to 6. The variable *n* is called the index of

NOTES

summation.



To generate the terms of a series given in sigma notation, successively replace the index of summation with consecutive integers from the first value to the last value of the index.

To create the terms of the series given in sigma notation above, replace *n* by 1,2,3,4,5, and 6 .

$$\sum_{n=1}^{6} 4n = 4(1)+4(2)+4(3)+4(4)+4(5)+4(6)$$

$$= 4+8+12+16+20+24$$

$$= 84$$

The sum of the series is 84.

To learn more about S_n notation, view this lesson: Sum of the First *n* Terms of a Series.

Sum of *n* Natural Numbers

The sum of natural numbers formula is obtained by using the 'Arithmetic Progression' formula where the common difference between the preceding and succeeding numbers is 1. Natural numbers are also called 'Counting Numbers' start from the number 1 until infinity, such as 1,2,3,4,5,6,7, and so on. Let be consider about the sum of *n* natural numbers, how its formula is derived.

The sum of *n* natural numbers formula is used to find 1 + 2 + 3 + 4 +..... up to *n* terms. This is arranged in an arithmetic sequence. Hence we use the formula of the sum of *n* terms in the 'Arithmetic Progression' for deriving the formula for the sum of natural numbers.

Sum of Natural Numbers Formula are following:

$$\sum_{1}^{n} = [n(n+1)]/2,$$

Where *n* is the **natural number**.

Definition: Sum of *n* natural numbers we can defined the form of 'Arithmetic Progression' where the sum of *n* terms are arranged in a sequence with the first term being 1, *n* being the number of terms along with the *n*th term. The sum of *n*

natural numbers is represented as $[n(n+1)]/2$. Natural numbers are the numbers that start from 1 and end at infinity. Natural numbers include whole numbers in them excluding the number 0.

Derivation: Let us derive the sum of natural numbers using the sum of n terms in an AP. In an AP, 'a' is the first term and 'd' is a common difference, 'l' is the last term, i.e., nth term, $l = a+(n-1)d$

In the **arithmetic sequence** of natural numbers, the common difference between the numbers is 1.

The sum of n terms of arithmetic progression will be:

$$\text{Sum} = a + (a+d) + (a+2d) \ldots\ldots + (l-2d) + (l-d) + l \quad (2.1)$$

When the order is reversed, the sum remains the same, hence,

$$\text{Sum} = l+(l-d)+(l-2d)\ldots\ldots+(a+2d)+(a+d)+a \quad (2.2)$$

Adding Equations (2.1) and (2.2), we get

$$2 \times \text{Sum} = (a+l)+[(a+d)+(l-d)]\ldots\ldots\ldots+[(l-d)+(a+d)]+(l+a)]$$

$$2\times \text{Sum} = (a+l)+(a+l)\ldots\ldots\ldots+(a+l)+(a+l)$$

$$2 \times \text{Sum} = n\times(a+l)$$

$$\Rightarrow \text{Sum} = n/2(a+l)$$

Substituting the value of l from the previous equation, we get

$$\text{Sum of } n \text{ terms of arithmetic progression} = n/2[2a + (n-1)d]$$

For natural numbers, $a = 1$ and $d = 1$, therefore,

$$S = n/2[2\times1+(n-1)1]$$

$$S = [n(n+1)]/2$$

From now, Sum of natural numbers formula = $[n(n+1)]/2$.

Example 2.4: Find the sum of the natural numbers from 1 to 100.

Solution: We can use the arithmetic progression formula to find the sum of the natural numbers from 1 to 100. Where $a = 1$, $n = 100$, and $d = 1$

$$\text{Sum of } n \text{ terms of arithmetic progression} = n/2[2a + (n-1)d]$$

$$S = 100/2[2\times1 + (100-1)1]$$

$$S = 5050$$

Therefore, the sum of the natural numbers from 1 to 100 is 5050

Sum of the Squares of first Natural Number

Let n be a natural number. Squaring the number is denoted by n^2. The sum of squares means the sum of the squares of the given numbers. We can finding the sum of squares of 2 numbers or 3 numbers or sum of squares of consecutive n numbers or n even numbers or n odd numbers. We evaluate the sum of the squares in statistics to find the variation in the data. We do these basic arithmetic operations which are required in statistics and algebra. There are different techniques to find the sum of squares of given numbers.

Sum of Squares of Natural Numbers: The natural numbers are the counting numbers from 1 to infinity. If we consider n consecutive natural numbers, then

NOTES

finding the sum of the squares of their numbers is represented as Σn^2, where n ranges from 1 to infinity. Here are the formulas for finding the sum of squares of n natural numbers, the sum of squares of first n even numbers, and the sum of squares of first n odd numbers.

Sum of Squares of n Natural Number $\quad \dfrac{n \times (n+1) \times (2n+1)}{6}$

Sum of Squares of First n Even Number $\quad \dfrac{2n \times (n+1) \times (2n+1)}{3}$

Sum of Squares of First n Odd Number $\quad \dfrac{n \times (2n+1) \times (2n-1)}{3}$

Sum of Squares of *n* Natural Numbers Formula

Sum of n natural numbers can be defined as a form of arithmetic progression where the sum of n terms are arranged in a sequence with the first term being 1, n being the number of terms along with the nth term. The sum of n natural numbers is represented as $[n(n+1)]/2$. Natural numbers are the numbers that start from 1 and end at infinity. Natural numbers include whole numbers in them except the number 0. If we need to calculate the sum of squares of n consecutive natural numbers, the formula is $\Sigma n^2 = \dfrac{n \times (n+1) \times (2n+1)}{6}$ It is easy to apply the formula when the value of n is known. Let us prove this true using the known algebraic identity.

The sum of squares of n natural numbers is $1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + ...n^2$ given by Σn^2, where $n = 1$ to ∞. Using the algebraic identity, $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$, by replacing a with n and b with $(n-1)$, we get

$$n^3 - (n-1)^3 = (n - n+1)(n^2 + n(n-1) + (n-1)^2)$$

$$n^3 - (n-1)^3 = 1(n^2 + n^2 - n + (n-1)^2)$$

$$= 1\ (2n^2 - n + n^2 + 1 - 2n)$$

$$= 3n^2 - 3n + 1$$

$$n^3 - (n-1)^3 = 3n^2 - 3n + 1 \qquad (2.3)$$

$$(n-1)^3 - (n-2)^3 = 3\ (n-1)^2 - 3(n-1) + 1 \qquad (2.4)$$

$$(n-2)^3 - (n-3)^3 = 3\ (n-2)^2 - 3(n-2) + 1 \qquad (2.5)$$

$$2^3 - 1^3 = 3\ (2)^2 - 3(2) + 1$$

$$1^3 - 0^3 = 3\ (1)^2 - 3(1) + 1 \text{——————>(last step)}$$

Add Equations (2.3) + (2.4) + (2.5) +.....+ (the last step)$\Rightarrow$ By adding all the above steps, we get, $n^3 - 0^3 = 3\ \Sigma\ n^2 - 3\Sigma\ n + n$

$$n^3 = 3\Sigma n^2 - \frac{3n(n+1)}{2} + n \text{ [since } \Sigma n = n(n+1)/2 \text{ (sum of n natural numbers)]}$$

$$3\Sigma n^2 = n^3 + \frac{3n(n+1)}{2} - n$$

$$3\Sigma n^2 = n[n^2 + \frac{3(n+1)}{2} - 1] \text{(Taking n as common from RHS)}$$

$$\Sigma n^2 = \frac{n}{3}(n^2 + \frac{3n+3}{2} - 1)$$

$$= \frac{n}{6}(2n^2 + 3n + 1)$$

(Factorizing the quadratic equation)

$$\Sigma n^2 = \frac{n}{6}(2n+1)(n+1)$$

Sum of Squares of the First *n* Even Numbers

The even numbers are denoted by $2n$, where n is the natural number. The summation of the first n even numbers is given as $2^2 + 4^2 + 6^2 + 8^2 + 10^2 + 12^2 + \ldots\ldots(2n)^2$. We are required to identify n and apply in the known formula $\frac{2n \times (n+1) \times (2n+1)}{3}$. When n takes the value from 1 to ∞, we evaluate $\Sigma(2n)^2$ as, $\Sigma(2^2 . n^2)$ as follows.

$\Sigma(2n)^2$ as, $\Sigma(2^2 . n^2)$ as follows.

$$\Sigma(2n)^2 = 2^2.1^2 + 2^2.2^2 + 2^2.3^2 + 2^2.4^2 + \ldots + 2^2.n^2$$

$$\Sigma(2n)^2 = 2^2(1^2 + 2^2 + 3^2 + 4^2 \ldots + n^2)$$

$$\Sigma(2n)^2 = \frac{4n(n+1)(2n+1)}{6} \text{ (Formula for sum of squares of n natural numbers)}$$

$$\textbf{Thus } \Sigma(2n)^2 = \frac{2n(n+1)(2n+1)}{3}$$

Sum of Squares of the First *n* Odd Numbers

The odd numbers are denoted by $(2n–1)$, where n is the natural number. The sum of the squares of the first n odd **natural numbers** is given by $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2$. Identify n and apply in the known formula is,

$$\frac{n \times (2n+1) \times (2n-1)}{3}$$

Let us get the proof as follows:

$\Sigma(2n–1)^2 = 1^2 + 2^2 + 3^2 + \ldots + (2n-1)^2 + (2n)^2 – [2^2 + 4^2 + 6^2 + \ldots + (2n)^2]$

NOTES

$\Sigma(2n–1)^2$ = (the sum of all the consecutive integers from 1 to 100) – (the sum of the squares of the even numbers)

$<\Sigma(2n–1)^2 = [1^2 + 2^2 + 3^2 + \ldots + (2n-1)^2 + (2n)^2] – [2^2 + 4^2 + 6^2 + \ldots + (2n)^2]$

On applying the formula for the addition of squares of $2n$ natural numbers and of n even natural numbers, we get;

$$\Sigma(2n-1)^2 = \frac{2n}{6}(2n+1)(4n+1) - \frac{2n}{3}(n+1)(2n+1)$$

$$- \frac{n}{3}[(2n+1)(4n+1)] - \frac{2n}{3}[(n+1)(2n+1)]$$

Thus,

$$\Sigma(2n-1)^2 = [\frac{n}{3}(2n+1)](4n+1) - 2(n+1)$$

$$= [\frac{n}{3}(2n+1)](4n+1-2n-2)]$$

$$\mathbf{\Sigma(2n-1)^2 = \frac{n}{3}[(2n+1)(2n-1)]}$$

The Sum of Cubes of First *n* Natural Number by Method of Difference

We know that sum of cubes of first n natural numbers is $= (n(n+1)/2)^2$. Here we will discuss about the how to find the sum of the cubes of first n natural numbers.

Let us assume the required sum = S

Therefore, $S = 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + \ldots\ldots\ldots\ldots + n^3$

Now, we will use the below identity to find the value of S as following:

$n^4 – (n-1)^4 = 4n^3 – 6n^2 + 4n – 1$

Substituting, $n = 1, 2, 3, 4, 5, \ldots\ldots\ldots\ldots, n$ in the above identity, we get

$$1^4 – 0^4 = 4 \times 1^3 – 6 \times 1^2 + 4 \times 1 – 1$$

$$2^4 – 1^4 = 4 \times 2^3 – 6 \times 2^2 + 4 \times 2 – 1$$

$$3^4 – 2^4 = 4 \times 3^3 – 6 \times 3^2 + 4 \times 3 – 1$$

$$4^4 – 3^4 = 4 \times 4^3 – 6 \times 4^2 + 4 \times 4 – 1$$

$$n^4 – (n-1)^4 = 4 \,.\, n^3 – 6 \times n^2 + 4 \times n – 1$$

Adding we get, $n^4 – 0^4 = 4(1^3 + 2^3 + 3^3 + 4^3 + \ldots\ldots\ldots + n^3) – 6(1^2 + 2^2 + 3^2 + 4^2 + \ldots\ldots\ldots + n^2) + 4(1 + 2 + 3 + 4 + \ldots\ldots\ldots + n) – (1 + 1 + 1 + 1 + \ldots\ldots\ldots n$ times)

$\sum n^4 = 4S – 6 \times (\{n(n+1)(2n+1)\}\{6\}) + 4 \times n(n+1)/2 – n$

$\sum 4S = n^4 + n(n+1)(2n+1) – 2n(n+1) + n$

$\sum 4S = n^4 + n(2n^2 + 3n + 1) – 2n^2 – 2n + n$

$\sum 4S = n^4 + 2n^3 + 3n^2 + n – 2n^2 – 2n + n$

$\sum 4S = n^4 + 2n^3 + n^2$

$\sum 4S = n^2(n^2 + 2n + 1)$

$\sum 4S = n^2(n + 1)^2$

Therefore, $S = \frac{n^2(n+1)^2}{4} = \{\frac{n(n+1)}{2}\}^2$ = (Sum of the first n natural numbers)^2

i.e., $1^3 + 2^3 + 3^3 + 4^3 + 5^3 + \ldots\ldots\ldots\ldots + n^3 = \{\frac{n(n+1)}{2}\}^2$

Thus, the sum of the cubes of first n natural numbers = $\{\frac{n(n+1)}{2}\}^2$

Example 2.5: Find the sum of the cubes of first 12 natural numbers.

Solution: Sum of the cubes of first 12 natural numbers

i.e., $1^3 + 2^3 + 3^3 + 4^3 + 5^3 + \ldots\ldots\ldots\ldots + 12^3$

We know the sum of the cubes of first n natural numbers (S) = $\{\frac{n(n+1)}{2}\}^2$

Here $n = 12$

Therefore, the sum of the cubes of first 12 natural numbers = $\{\frac{12(12+1)}{2}\}^2$.

$= \{\frac{12 \times 13}{2}\}^2$

$= \{6 \times 13\}^2$

$= (78)^2$

$= 6084$

Check Your Progress

1. Give the definition of arithmetic series?
2. What is geometric series?
3. Define the sum of n natural numbers.
4. What do you understand by sum of cubes first n natural numbers?

2.3 SET THEORY

Set theory is the branch of mathematical logic that studies sets, which can be informally described as collections of objects. Although objects of any kind can be collected into a set, set theory, as a branch of mathematics, is mostly concerned with those that are relevant to mathematics as a whole.

The modern study of set theory was initiated by the German mathematicians Richard Dedekind and Georg Cantor in the 1870s.

NOTES

NOTES

Set theory is commonly employed as a foundational system for the whole of mathematics, particularly in the form of Zermelo–Fraenkel set theory with the axiom of choice. Besides its foundational role, set theory also provides the framework to develop a mathematical theory of infinity, and has various applications in computer science (such as, in the theory of relational algebra), philosophy and formal semantics. Its foundational appeal, together with its paradoxes, its implications for the concept of infinity and its multiple applications, have made set theory an area of major interest for logicians and philosophers of mathematics.

Sets

'A set is any collection of objects such that given an object, it is possible to determine whether that object belongs to the given collection or not.' The members of a set are called elements. We shall use capital letters to denote sets and small letters to denote elements.

2.3.1 Notation and Representation of Set

Notation

Set notation also helps us to explain different relationship between two or more sets using different types of symbol. By the help of it we can easily perform operation on sets, such as union and intersection.

Let A and B be sets.

- $|A|$, called cardinality of A, denotes the number of elements of A. For example, if A= {(1,2),(3,4)}, then $|A|$=2.
- A=B iff they have precisely the same elements. For example, if A={4,9} and B={n^2:n=2 or n=3}, then A=B.
- $A \subseteq B$ if and only if every element of A is also an element of B. We can say that A is a subset of B. For example, $\{1,8,1107\} \subseteq \mathbb{N}$.
- $a \in A$ means a is a member of A. For example, $5 \in \mathbb{Q}$.
- $a \notin A$ means a is not a member of A. For example, $27 \notin \mathbb{Z}$.
- $A \cap B$ denotes the set containing elements that are in both A and B. $A \cap B$ is called the intersection of A and B. For example, if A={1,2} and B={2,3}, then $A \cap B$={2}.
- $A \cup B$ denotes the set containing elements that are in either A or B or both. $A \cup B$ is called the union of A and B. For example, if A={1,2} and B={2,3}, then $A \cup B$={1,2,3}.
- $A \backslash B$ denotes the set having elements that are in A but not in B. $A \backslash B$ is read as "A drop B". For example, if A={1,2} and B={2,3}, then $A \backslash B$={1}.

Representation

Sets are represented as a collection of well-defined objects or elements and which is does not change from person to person. A set is represented by a capital letter. The number of elements in the finite set is known as the 'Cardinal Number' of a set.

The sets are represented in **curly braces**, **{}**. For example, {2,3,4} or {*a,b,c*} or {Bat, Ball, Wickets}. The elements in the sets are depicted in either the Statement form, Roster Form or Set Builder Form.

Statement Form: In statement form, the well-defined explanations of a member of a set are written and enclosed in the curly brackets.

For example, the set of even numbers less than 15.

In statement form, it can be written as {even numbers less than 15}.

Roster Form: In Roster form, all the elements of a set are listed.

For example, the set of natural numbers less than 5.

Natural Number = 1, 2, 3, 4, 5, 6, 7, 8,……

Natural Number less than 5 = 1, 2, 3, 4

Therefore, the set is $N = \{ 1, 2, 3, 4 \}$

Set Builder Form: The general form is, $A = \{ x : \text{property} \}$

For example, Write the following sets in set builder form: $A=\{2, 4, 6, 8\}$

Solution:

$2 = 2 \times 1$

$4 = 2 \times 2$

$6 = 2 \times 3$

$8 = 2 \times 4$

So, the set builder form is $A = \{x: x=2n, n \in N \text{ and } 1 \leq n \leq 4\}$

Also, Venn Diagrams are the simple and best way for visualized representation of sets we will discuss ahead.

Example 2.6: (*i*) The set of all integers.

(*ii*) The set of all students of Delhi University.

(*iii*) The set of all letters of the alphabets.

(*iv*) The set of even integers 2, 4, 6, 8.

Example 2.7: Let M be the collection of all those men (and only those men) in a village who do not shave themselves. Given that (*i*) All men in the village must be clean shaven. (*ii*) The village barber shaves all those men who do not shave themselves.

Suppose *b* denotes the village barber. If $b \in M$, then *b* does not shave himself. Then by (*ii*) *b* shaves himself, a contradiction.

If $b \notin M$, then *b* shaves himself. Then by (*ii*) *b* does not shave himself, again a contradiction.

Solution: Since we cannot answer 'Yes' or 'No' to the question, 'Is barber himself a member of M?' we conclude that M is not a set.

Universal Set

Throughout this book, whenever we talk of a set, we shall assume it to be a subset of a fixed set *U*. This fixed set *U* will be called the universal set.

NOTES

Elements

The members of a set are called elements. We shall use capital letters to denote sets and small letters to denote elements. If a is an element of the set A, we write $a \in A$ (read as 'a belongs to A') and if a is not an element of the set A, we write $a \notin A$ (read as 'a does not belong to A'). There are different ways of describing a set. For example, the set consisting of elements 1, 2, 3, 4, 5 could be written as $\{1, 2, 3, 4, 5\}$ or $\{1, 2, \ldots, 5\}$ or $\{x \mid x \in N, x \leq 5\}$, where N = the set of natural numbers. In fact, we always use { } brackets to denote a set. A set which has finite number of elements is called a finite set. Otherwise, it is called an infinite set. For example, if A is the set of all integers, then A is an infinite set denoted by $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ or $\{x \mid x$ is an integer$\}$.

Singleton

A set having only one element is called singleton. If a is the element of the singleton A, then A is denoted by $A = \{a\}$. Note that $\{a\}$ and a do not mean the same; $\{a\}$ stands for the set consisting of a single element a while a is just the element of $\{a\}$.

Equality of Sets

Two sets A and B are said to be equal if and only every member of A is a member of B and every member of B is a member of A. We express this by writing $A = B$, logically speaking $A = B$ means $(x \in A) \equiv (x \in B)$ or the biconditional statement $(x \in A) \Leftrightarrow (x \in B)$ is true for all x.

Notes:

1. The order of appearance of the elements of a set is of no consequence. For example, the set $\{1, 2, 3\}$ is same as $\{2, 3, 1\}$ or $\{3, 2, 1\}$, etc.
2. We always write each element of a set only once. For example, $\{2, 2, 3\}$ is not a proper way of writing a set and it should be written as $\{2, 3\}$.

2.4 OPERATIONS ON SETS

You are familiar with the operations of addition and multiplication in Arithmetic. Given any two numbers, you know that the operations of addition and multiplication associate the numbers to form the sum or product of the two numbers respectively. Logic, the connectives $\wedge, \vee, \sim, \Rightarrow, \Leftrightarrow$ are used to associate a new statement with any two given statements to form a compound statement. In this section, you will learn three operations for associating any two given sets, to form a third set. These three operations namely, union, intersection and complementation will be, loosely speaking, analogous to the operations of addition, multiplication and subtraction of numbers respectively.

Union

The union of any two sets A and B is the set of all those elements x such that x belongs to at least one of the two sets A and B. It is denoted by $A \cup B$. Logically speaking, if the biconditional statement $(x \in C) \Leftrightarrow (x \in A) \wedge (x \in B)$ is true for all x, then $C = A \cup B$. In other words, $(x \in A \cup B) \equiv (x \in A) \vee (x \in B)$.

Prove that if $A = \{1, 2, 3\}$ and $B = \{3, 4\}$ then $A \cup B = \{1, 2, 3, 4\}$.

Example 2.8: Prove that for any sets A and B (i) $A \subseteq A \cup B$, (ii) $B \subseteq A \cup B$.

Solution: (i) $x \in A$ means $x \in A \cup B$ by definition. So $A \subseteq A \cup B$

(ii) $x \in B \subseteq B$ means $x \in A \cup B$ by definition. So $B \subseteq A \cup B$.

Aliter. (i) We want to prove that the conditional statement

$$(x \in A) \Rightarrow (x \in A \cup B) \text{ is true.}$$

But, this statement is false only if $(x \in A)$ is true and $(x \in A \cup B)$ is false. Such a situation cannot occur, for $(x \in A)$ is true means $(x \in A) \vee (x \in B)$ is true. Therefore, $(x \in A) \vee (x \in B)$ is true and $(x \in A \cup B)$ is false. It means $(x \in A) \vee (x \in B) \Rightarrow (x \in A \cup B)$ is false. This is impossible by definition of $A \cup B$. Similarly, we can prove (ii).

Example 2.9: If $A \subseteq B$, then $A \cup B = B$ and conversely, if $A \cup B = B$, then $A \subseteq B$.

Solution: Suppose $A \subseteq B$. Let $x \in A \cup B$. Then $x \in A$, or $x \in B$ or $x \in$ both A and B. If $x \in A$, then $x \in B$ (as $A \subseteq B$). In any case, $x \in A \cup B$ means $x \in B$. So, $A \cup B \subseteq B$. We have already proved $A \subseteq A \cup B$. Therefore, $A \cup B = B$; conversely, let $A \cup B = B$. Let $x \in A$. Then $x \in A \cup B$, which means $x \in B$. So $A \subseteq B$.

Aliter. Suppose $A \subseteq B$. We want to show that the biconditional statement $(x \in B) \Leftrightarrow (x \in A) \vee (x \in B)$ is true for every x. But, this statement is false if and only if $(x \in B)$ is false and $(x \in A)$ is true. Such a situation cannot occur, as $A \subseteq B$.

This proves $A \cup B = B$.

Conversely, if $A \cup B = B$, then we want to show that the conditional statement $(x \in A) \Rightarrow (x \in B)$ is true for every x. This is false if and only if $(x \in A)$ is true and $(x \in B)$ is false. Now, $(x \in A)$ is true means $(x \in A) \vee (x \in B)$ is also true. Therefore, $(x \in A) \vee (x \in B) \Rightarrow (x \in B)$ is false. This is impossible as $B = A \cup B$. This proves $A \in B$.

Example 2.10: If $A \subseteq C$ and $B \subseteq C$, then $(A \cup B) \subseteq C$.

Solution: We want to show that $(x \in A \cup B) \Rightarrow (x \in C)$ is true for every x. This is equivalent to saying that $(x \in A \cup B)$ is true and $(x \in C)$ is false cannot occur together. Suppose $(x \in A \cup B)$ is true. Then $(x \in A) \vee (x \in B)$ is true. This means $(x \in A)$ is true or $(x \in B)$ is true. If $(x \in A)$ is true then $(x \in C)$ is true as $A \subseteq C$. If $(x \in B)$ is true then $(x \in C)$ is true as $B \subseteq C$. In any case, $(x \in C)$ is true. So, when $(x \in \mathrm{A} \cup B)$ is true, $(x \in C)$ should also be true. This proves our assertion.

Aliter. Let $x \in A \cup B$. This means $x \in A$ or $x \in B$ or x belongs to both A and B. If $x \in A$, then $x \in C$ (as $A \subseteq C$). If $x \in B$, then $x \in C$ (as $B \subseteq C$). In any case, $x \in C$. So, $x \in A \cup B$ means $x \in C$.

This proves $A \cup B \subseteq C$.

Intersection

The intersection of two sets A and B is the set of all those elements x such that x belongs to both A and B and is denoted by $A \cap B$. If $A \cap B = \phi$, then A and B are said to be disjoint.

NOTES

Logically speaking, if the biconditional statement $(x \in C) \Leftrightarrow (x \in A) \wedge (x \in B)$ is true for all x, then $C = A \cap B$. In other words,

$$(x \in A \cap B) \equiv (x \in A) \cap (x \in B)$$

NOTES

Example 2.11: (*i*) If $A = \{1, 2, 3, 4\}$, $B = \{1, 2\}$ then $A \cap B = \{1, 2\}$.

(*ii*) *If* $A = \{1, 2, 3\}$, $B = \{4, 5\}$, then $A \cap B = \phi$.

Example 2.12: (*i*) $A \cap B \subseteq A$ (*ii*) $A \cap B \subseteq B$ for any sets A and B.

Solution: Let $x \in A \cap B$. Then, by definition $x \in A$ and $x \in B$. So, $A \cap B \subseteq A$ and $A \cap B \subseteq B$.

Aliter. (*i*) You want to show that

$$(x \in A \cap B) \Rightarrow (x \in A) \text{ is true for all } x.$$

You have to only consider the case when $(x \in A \cap B)$ is true and $(x \in A)$ is false. Now, $(x \in A)$ is false shall mean $(x \in A) \cap (x \in B)$ is false and so $(x \in A \cap B) \Rightarrow (x \in A) \cap (x \in B)$ is also false which is impossible by definition of $(A \cap B)$. This proves the result.

(*ii*) You want to show that

$$(x \in A \cap B) \Rightarrow (x \in B) \text{ is true for all } x.$$

The only doubtful case is when $(x \in A \cap B)$ is true and $(x \in B)$ is false. Such a case is not possible by definition of $A \cap B$. This proves (*ii*).

Example 2.13: If $A \subseteq B$ *and* $A \subseteq C$, then

$$A \subseteq (B \cap C).$$

Solution: Let $x \in A$. Then $x \in B$ and $x \in C$ (as $A \subseteq B$ and $A \subseteq C$). So, $x \in B \cap C$.

This proves $A \subseteq B \cap C$.

Aliter. You want to show that

$(x \in A) \Rightarrow (x \in B \cap C)$ is true for all x.

The only doubtful case is when $(x \in A)$ is true and $(x \in B \cap C)$ is false.

Now, $(x \in A)$ is true means $(x \in B)$ is also true (as $A \subseteq B$). Also, $(x \in C)$ is true (as $A \subseteq C$). This means $(x \in B) \cap (x \in C)$ is true and so $(x \in B \cap C)$ is also true. This proves the result.

Example 2.14: $A \cup B = A \cap B$ if and only if $A = B$.

Solution: Suppose $A \cup B = A \cap B$. Let $x \in A$. Then, $x \in A \cup B$ and so $x \in A \cap B$. Therefore, $x \in B$. This proves $A \subseteq B$. Similarly, $B \subseteq A$ and so $A = B$.

Aliter. Suppose $A \cup B = A \cap B$.

Adsorption law

$$\begin{aligned}
\text{Then, } (x \in A) &\equiv (x \in A) \cap [(x \in A) \vee (x \in B] \\
&\equiv (x \in A) \wedge [(x \in A \cup B)] \\
&\equiv (x \in A) \wedge [x \in A \cap B)] \\
&\equiv [(x \in A) \wedge (x \in A)] \wedge (x \in B) \\
&\equiv (x \in A) \wedge (x \wedge B)
\end{aligned}$$

$$\equiv (x \in A \cap B)$$
$$\equiv (x \in A \cup B)$$
$$\equiv (x \in B) \vee (x \in A)$$
$$\equiv (x \in B) \vee [(x \in A) \cup (x \in A)]$$
$$\equiv (x \in B) \vee [(x \in B \cup A]$$
$$\equiv (x \in B) \vee [x \in A \wedge B]$$
$$\equiv (x \in B) \vee [x \in A) \wedge (x \in B)]$$
$$\equiv [(x \in B) \vee (x \in A)] \wedge (x \in B]$$
$$\equiv (x \in B) \text{ Adsorption law}$$

This proves $A = B$.

Conversely, if $A = B$, then

$$(x \in A \cup B) \equiv (x \in A) \cup (x \in B)$$
$$\equiv (x \in B) \cup (x \in B)$$
$$\equiv (x \in B)$$
$$\equiv (x \in B) \cap (x \in B)$$
$$\equiv (x \in A) \cap (x \in B)$$
$$\equiv (x \in A \cap B)$$

Note: Adsorption laws in logic mean the following:

(*i*) $p \cap (p \cup r) \equiv p$ (*ii*) $p \cup (p \cap r) \equiv p$

Complements

If A and B are two sets then complement of B relative to A is the set of all those element $x \in A$ such that $x \notin B$ and is denoted by $A - B$. Logically speaking, if for a set C the biconditional statement $(x \in C) \Leftrightarrow (x \in A) \cap (x \notin B)$ is true for all x, then $C = A - B$. In other words, if $(x \in C) \equiv (x \in A) \wedge (x \notin B)$, then C is called the complement of B relative to A.

Notes:

1. It is very clear from the preceding definition that $A - B$ is a subset of A.
2. Whenever we say complement of B we mean, complement of B relative to the universal set U. In such case, we denote complement of B by B'.

   So, $B' = U - B$.

Prove that if $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5\}$ then $A - B = \{1, 2\}$.

Example 2.15: Show that $A - B = A \cap B'$.

Solution: Let $x \in A - B$. This means $x \in A$ and $x \notin B$. By definition of the universal set, $A - B \subseteq U$. So, $x \in U$. Therefore, $x \in U, x \notin B$, implies $x \in B'$. This proves $A - B \subseteq A \cap B'$. Again, if $x \in A \cap B'$, then $x \in A$ and $x \in B'$. Now, $x \in B'$ implies $x \notin B$. So, $x \in A - B$. This proves $A \cap B' \subseteq A - B$.

Therefore, $A - B = A \cap B'$.

NOTES

Aliter. $(x \in A - B) \equiv (x \in A) \wedge (x \notin B)$

$\equiv (x \in A \wedge U) \wedge (x \in B)$ as $A \wedge U = A$

$\equiv [(x \in A) \wedge (x \in U)] \wedge (x \notin B)$

$\equiv [(x \in A) \wedge [(x \in U) \wedge (x \notin B)]$

$\equiv [(x \in A) \wedge (x \in B')]$

This proves $A - B = A \cap B'$.

Example 2.16: $A \subseteq B$ if and only if $B' \subseteq A'$.

Solution: Suppose $A \subseteq B$. Let $x \subseteq B'$. Then, $x \in U$ and $x \notin B$. Now, $x \notin B$ implies $x \notin A$ (as $A \subseteq B$). Therefore, $x \in U$ and $x \notin A$ implies $x \in A'$. This proves $B' \subseteq A'$. Conversely, let $B' \subseteq A'$. Let $B \in A$. Then, $x \notin A$. Now, $x \notin A'$ implies $x \notin B'$ (as $B' \subseteq A'$). This means $x \in B$. So, $A \subseteq B$.

Aliter. Now, $(x \in A) \Rightarrow (x \in B)$

$\equiv \sim (x \in B) \Rightarrow \sim (x \in A)$ (by Contrapositive law in logic)

$\equiv (x \notin B) \Rightarrow (x \notin A)$

$\equiv (x \in B') \Rightarrow (x \in A')$

Suppose $A \subseteq B$. Then, $(x \in A) \Rightarrow (x \in B)$ is true for all x. You know that $(x \in B') \Rightarrow (x \in A')$ is true for all x. This means $B' \subseteq A'$. Conversely, suppose $B' \subseteq A'$. Then, $(x \in B') \Rightarrow (x \in A')$ is true for all x. Moreover, $(x \in A) \Rightarrow (x \in B)$ is true for all x. This implies $A \subseteq B$. Hence, the result follows.

2.5 SUBSETS

Let A and B be two sets. If every element of A is an element of B then A is called a subset of B and we write $A \subseteq B$ or $B \supseteq A$ (read as 'A is contained in B' or 'B contains A').

Logically speaking, $A \subseteq B$ means $(x \in A) \Rightarrow (x \in B)$ is true for every x.

Notes:

1. If $A \subseteq B$ and $A \neq B$, we write $A \subset B$ or $B \supset A$ (read as: A is a proper subset of B or B is a proper superset of A).
2. Every set is a subset and a superset of itself.
3. If A is not a subset of B, we write $A \subseteq B$.

Definition: (Subset). Let A, B be sets. Then A is a subset of B, written $A \subseteq B$ iff $(\forall x)$ if $x \in A$ then $x \in B$.

Theorem 2.1: If $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Proof: Let x be arbitrary.

Because $A \subseteq B$ if $x \in A$ then $x \in B$

Because $B \subseteq A$ if $x \in B$ then $x \in A$

Hence, $x \in A$ iff $x \in B$, thus $A = B$.

Empty Set or Null Set

A set which has no element is called the null set or empty set. It is denoted by the symbol ϕ.

Each of the following is a null set:

(*a*) *The set of all real numbers whose square is –1.*

(*b*) *The set of all those integers that are both even and odd.*

(*c*) *The set of all rational numbers whose square is 2.*

(*d*) *The set of all those integers x that satisfy the equation 2x = 5.*

Example 2.17: The empty set ϕ is a subset of every set.

Solution: Suppose ϕ is not a subset of the set A. This means there exists $a \in \phi$ such that $a \notin A$. This is impossible as ϕ has no element. So, ϕ is a subset of every set.

Aliter. Logically speaking, we want to prove that the conditional statement $(x \in \phi) \Rightarrow (x \in A)$ is true for every x. Since ϕ has no element, the statement '$x \in \phi$' is false. So, the conditional statement $(x \in \phi) \Rightarrow (x \in A)$ is true, which proves the result.

Example 2.18: List the following sets (here N denotes the set of natural numbers and Z, the set of integers).

(*i*) $\{x \mid x \in N \text{ and } x < 10\}$

(*ii*) $\{x \mid x \in Z \text{ and } x < 6\}$

(*iii*) $\{x \mid x \in Z \text{ and } 2 < x < 10\}$.

Solution:

(*i*) We have to find the natural numbers which are less than 10. They are 1, 2, 3, 4, 5, 6, 7, 8, 9. So (*i*) can be described as {1, 2, 3, 4, 5, 6, 7, 8, 9}.

(*ii*) We have to find integers which are less than 6. They are all negative integers and the integers 0, 1, 2, 3, 4, 5. So (*ii*) may be described as {. . . , –3, –2, –1, 0, 1, 2, 3, 4, 5}.

(*iii*) We have to find integers lying between 2 and 10. They are 3, 4, 5, 6, 7, 8, 9. So (*iii*) may be described as {3, 4, 5, 6, 7, 8, 9}.

Example 2.19: Give the verbal translation of the following sets:

(*i*) {2, 4, 6, 8}

(*ii*) {1, 3, 5, 7, 9, . . .}

(*iii*) {–1, 1}.

Solution: (*i*) It consists of all positive even integers less than 10.

(*ii*) It consists of all positive odd integers.

(*iii*) It consists of those integers x which satisfy $x^2 - 1 = 0$.

Example 2.20: If $a_1 \neq b_1$ and $\{a_1, b_1\} = \{a_2, b_2\}$ then show that $a_2 \neq b_2$.

Solution: Let $a_2 = b_2$. Then $a_1 \in \{a_1, b_1\}$ means $a_1 \in \{a_2, b_2\} = \{a_2\}$. So, $a_1 = a_2$. Also, $b_2 \in \{a_1 \in b_1\}$ means $b_1 \in (a_2, b_2) = \{a_2\}$. So, $b_1 = a_2$. Therefore, $a_1 = b_1$ which is wrong. Thus, $a_2 \neq b_2$.

NOTES

NOTES

Example 2.21: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Solution: Let $a \in A$ be any element of A. Then as $A \subseteq B$, $a \in B$.

Also, $B \subseteq C \Rightarrow a \in C$.

Thus, every element of A belongs to $C \Rightarrow A \subseteq C$.

Aliter. Logically speaking, we want to prove that

$[(x \in A) \Rightarrow (x \in B)] \wedge [(x \in B) \Rightarrow (x \in C)] \Rightarrow [(x \in A) \Rightarrow (x \in C)]$

is true for every x. This follows from transitive law (in Logic).

Example 2.22: If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Solution: Since $A \subseteq B$, every element of A is an element of B. Also, $B \subseteq A$, means every element of B is also an element of A. This proves $A = B$.

Aliter. Logically speaking, we want to prove

$$[(x \in A) \Rightarrow (x \in B)] \wedge [(x \in B) \Rightarrow (x \in A)] \Rightarrow [(x \in A) \Leftrightarrow (x \in B)]$$

is true for every x. In other words, $[(p \Rightarrow q) \wedge (q \Rightarrow p)] \Rightarrow (p \Leftrightarrow q)$ is true. Since $p \Rightarrow q$ is true and $q \Rightarrow p$ is true, $(p \Rightarrow q) \wedge (q \Rightarrow p)$ is also true. This also means $p \Leftrightarrow q$ is true. So, $[(q \Rightarrow q) \wedge (q \Rightarrow p)] \Rightarrow (p \Leftrightarrow q)$ is true. This proves the result.

Example 2.23: If $A \subset B$ and $B \subseteq C$, then $A \subset C$.

Solution: If $A = C$, then every element of B is also an element of A (as $B \subseteq A$). But, $A \subset B$ means every element of A is also an element of B. Combining these facts, we get $A = B$ which is a contradiction (as A is a proper subset of B). So, $A \neq C$. Clearly, every element of A is also an element of C. Therefore, A is a proper subset of C.

Aliter. If $A = C$, then $B \subseteq A$. This means $(x \in B) \Rightarrow (x \in A)$ is true for all x.

Also, $A \subset B$ means $(x \in A) \Rightarrow (x \in B)$ is true for all x. Therefore, $(x \in A) \Leftrightarrow (x \in B)$ is true for every x. So, $A = B$, which is not possible as A is proper subset of B. Thus, $A \neq C$. A is subset of C.

Example 2.24: Find all possible solutions for x and y in each of the following cases:

$$(i)\ \{2x, y\} = \{4, 6\} \quad (ii)\ \{x, 2y\} = \{1, 2\} \quad (iii)\ \{2x\} = \{0\}.$$

Solution: (i) Let $A = \{2x, y\}$ and $B = \{4, 6\}$.

Now, $2x \in A$ means $2x \in B$. So, $2x = 4$ or $2x = 6$. If $2x = 4$ then $x = 2$. Also, $y \in A$ means $y \in B$. So, $y = 4$ or $y = 6$. y cannot be equal to 4. For, then A will have only element 4 while B has 4 and 6. Therefore, one solution is $x = 2$ and $y = 6$. If $2x = 6$, then $x = 3$. y cannot be 6. For then, A will have only the element 6. So y must be 4. Therefore, another solution is $x = 3$ and $y = 4$.

(ii) Let $A = \{x, 2y\}$ and $B = \{1, 2\}$

$x \in A$ means $x \in B$.

So, $x = 1$ or $x = 2$

If $x = 1$, then $2y = 2$. So, one solution is $x = 1$ and $y = 1$.

If $x = 2$, then $2y = 1$. So, another solution is $x = 2$ and $y = \frac{1}{2}$.

(iii) Let $A = \{2x\}$, $B = \{0\}$

$2x \in A$ means $2x \in B$

So, $2x = 0$ which means $x = 0$.

Therefore, there is only one solution $x = 0$.

Example 2.25: Find at least one set A such that

(*i*) $\{1, 2\} \subseteq A \subset \{1, 2, 3, 4\}$

(*ii*) $\{0, 1, 2\} \subset A \subset \{2, 3, 0, 1, 4\}$

NOTES

Solution: (*i*) Since $\{1, 2\} \subset A$, it means A must have 1, 2 as its elements and some extra member. Again, $A \subset \{1, 2, 3, 4\}$ means that the extra member should be 3 or 4. So, $A = \{1, 2, 3\}$ or $A = \{1, 2, 4\}$.

(ii) Proceeding as in *(i)*, there are two possibilities. Either $A = \{0, 1, 2, 3\}$ or $A = \{0, 1, 2, 4\}$

If a set contains 'n' elements, then the number of subsets of the set is 2^2.

Number of Proper Subsets of the Set: If a set contains 'n' elements, then the number of proper subsets of the set is $2^n - 1$.

If $A = \{p, q\}$ the proper subsets of A are [{ }, {p}, {q}] (Whereas { } is show that the subset of A containing no elements)

$\Rightarrow$ Number of proper subsets of A are $3 = 2^2 - 1 = 4 - 1$

In general, number of proper subsets of a given set $= 2^m - 1$, where m is the number of elements.

Example 2.26: If A {1, 3, 5}, then write all the possible subsets of A. Find their numbers.

Solution: The subset of A containing no elements – { }

The subset of A containing one element each – {1} {3} {5}

The subset of A containing two elements each – {1, 3} {1, 5} {3, 5}

The subset of A containing three elements – {1, 3, 5)

Therefore, all possible subsets of A are { }, {1}, {3}, {5}, {1, 3}, {3, 5}, {1, 3, 5}

Therefore, number of all possible subsets of A is 8 which are equal 23.

Proper subsets are = { }, {1}, {3}, {5}, {1, 3}, {3, 5}

Number of proper subsets are $7 = 8 - 1 = 23 - 1$

Check Your Progress

5. State the set theory.
6. What is the concept of set?
7. Define the singleton.
8. Give the statement of union set.
9. What do you understand by intersection of two sets?
10. Define subset.
11. What is null set?

NOTES

2.6 VENN DIAGRAMS

To illustrate the various set operations, you learn about diagrams called *Venn diagrams* after John Venn (1834 – 1883). The universal set is represented by the points in and on a rectangle and the subsets $A, B, C, \ldots$ by points in and on the circles or ellipses drawn inside the rectangle. In Figure. 2.1, the shaded portion represents $A \cap B$.

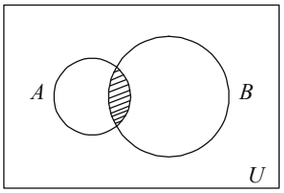


Fig. 2.1

In Figure. 2.2, the shaded portion represents $A \cup B$.

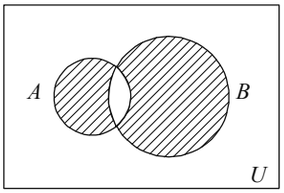


Fig. 2.2

In Figure. 2.3, the shaded portion represents A'.

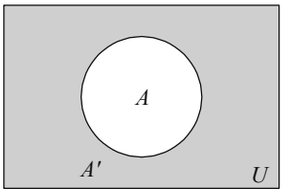


Fig. 2.3

In Figure. 2.4, the shaded portion represents $A - B$.

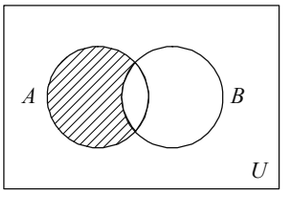


Fig. 2.4

In Figure. 2.5, three sets A, B, C divide the universal set U into 8 parts, 8th part not numbered in the diagram.

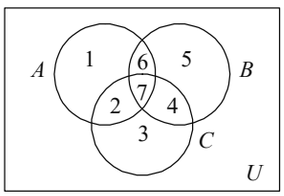


Fig. 2.5

Example 2.27: Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ using Venn diagrams.

Solution: Here, $B \cap C$ is represented by areas 4 and 7, and A is represented by areas 1, 2, 6 and 7. So, $A \cup (B \cap C)$ is represented by areas 1, 2, 4, 6 and 7. Again, areas 1, 2, 4, 5, 6, 7 represent $A \cup B$ and areas 1, 2, 3, 4, 6, 7 represent $A \cup C$. So, areas 1, 2, 4, 6, 7 represents $(A \cup B) \cap (A \cup C)$. This proves our assertion (Refer Figure 2.5).

Example 2.28: Using Venn diagrams show that $A - (B \cup C) = (A - B) \cup (A - C)$.

Solution: In Figure 2.5, areas 2, 3, 4, 5, 6, 7 represent $B \cup C$. Therefore, area 1 represents $A - (B \cup C)$. Now, areas, 1, 2 represent $A - B$ and areas 1, 6 represent $A - C$. So, area 1 represents $(A - B) \cap (A - C)$. This proves the result.

Example 2.29: Using Venn diagrams show that for any two sets A and B

$(A \cup B)' = A' \cup B'$

Solution: In Figure. 2.6, area 1 represents $A \cap B$, while areas 2, 3, 4 represent $(A \cap B')$. Again, areas 3, 4 represent A' and areas 2, 4 represent B'. Therefore, areas 2, 3, 4 represent $A' \cup B'$.

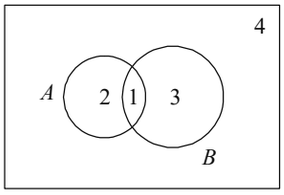


Fig. 2.6

Example 2.30: Use Venn diagrams to show that for any sets A and B

$$A \cup B = A \cup (B - A)$$

Solution: In Figure. 2.6, areas 1, 2, 3 represent $A \cup B$. Also, areas 1, 2 represent A and areas 3 represents $B - A$. So, areas 1, 2, 3 represent $A \cup (B - A)$. This proves the result.

2.6.1 Applications of Venn Diagram

- Venn diagrams are used to depict how items relate to each other against an overall backdrop, universe, data set, or environment.
- A Venn diagram could be used, for example, to compare two companies within the same industry by illustrating the products both companies offer (where circles overlap) and the products that are exclusive to each company (outer circles).

NOTES

- Venn diagrams are, at a basic level, simple pictorial representations of the relationship that exists between two sets of things. However, they can be much more complex. Still, the streamlined purpose of the Venn diagram to illustrate concepts and groups has led to their popularized use in many fields, including statistics, linguistics, logic, education, computer science, and business.
- In math, a Venn diagram is used to visualize the logical relationship between sets and their elements and helps us solve examples based on these sets.
- Venn diagrams are commonly associated with education. They are frequently used in mathematics to understand set theory and also used to do various comparisons in the classroom. However, there are many other uses of Venn diagrams that you can take advantage of during your daily routines.
- The power of Venn diagram lies in its simplicity. They are great for comparing things in a visual manner and to quickly identify overlaps. We have listed down some Venn diagram templates found in our diagramming community so you can get an idea about the power of Venn diagrams and their usages.
- Venn diagrams also have uses in computer science, linguistics, logic, statistics and teaching, including the visualising computer languages and their hierarchies.
- Venn diagrams are commonly used in school to teach basic math concepts such as sets, unions and intersections. They are also used in advanced mathematics to solve complex problems and have been written about extensively in scholarly journals.
- Venn Diagrams are used in Mathematics to divide all possible number types into groups. They are also used in Mathematics to see what groups of numbers have things in common. Venn Diagrams can even be used to analyse music. We can analyse the characters in TV shows like the 'Muppets' with a Venn Diagram.
- In 'Logic' Venn diagrams are used to determine the validity of particular arguments and conclusions. In deductive reasoning, if the premises are true and the argument form is correct, then the conclusion must be true. For example, if all dogs are animals, and our pet Mojo is a dog, then Mojo has to be an animal. If we assign variables, then let's say dogs are C, animals are A, and Mojo is B. In argument form, we say: All C are A. B is C. Therefore B is A. A related diagram in logic is called a Truth Table, which places the variables into columns to determine what is logically valid. Another related diagram is called the **Randolph diagram**, or **R–Diagram**, after mathematician John F. Randolph. It uses lines to define sets.
- In the field of statistics and probability experts use Venn diagrams to predict the likelihood of certain occurrences. These ties in with the field of predictive analytics. Different data sets can be compared to find degrees of commonality and differences.
- Talk about 'Linguistics' Venn diagrams have been used to study the commonalities and differences among languages.

- Teachers can use Venn diagrams to improve their students' reading comprehension. Students can draw diagrams to compare and contrast ideas they are reading about.
- Programmers can use Venn diagrams to visualize computer languages and hierarchies.
- Venn diagrams can be used to compare and contrast products, services, processes or pretty much anything that can depicted in sets. And they are effective communication tool to illustrate that comparison.

2.7 LAWS OF SET THEORY

The following is a list of some of the important laws of sets.

1. ***Laws of Idempotence.*** For any set A

   $A \cup A + A$ and $A \cap A = A$

   Proof. Obvious.

2. ***Commutative Laws.*** For any sets A and B

   $A \cup B = B \cup A, A \cap B = B \cap A$

   Proof. Obvious.

3. ***Associative Laws.*** For any three sets A, B, C

   (*i*) $A \cup (B \cup C) = (A \cup B) \cup C.$

   (*ii*) $A \cap (A \cap C) = (A \cap B) \cap C.$

   Proof. (*i*) We want to show that

   $[x \in A \cup (B \cup C)] \Leftrightarrow [x \in (x \cup B) \subset C]$ is true for all x

   Now by definition,

   $[x \in A \cup (B \cup C)] \equiv [x \in A) \cup \{x \in B) \cup (x \in C\}]$

   And $[x \in (A \cup B) \cup C] \equiv [\{ x \in A) \cup (x \in B)\} \cup (x \in C)]$

   So, by associative law in logic, the result (*i*) follows.

   Similarly, we can prove (*ii*).

4. ***Distributive Laws.*** For any three sets A, B, C

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

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

   Proof: (*i*) Let $x \in A \cap (B \cup C)$. This implies $x \in A$ and $x \in B \cup C$. Now, $x \in B \cup C$ implies $x \in B$ or $x \in C$ or $x \in$ both B and C. If $x \in B$, then $x \in A \cap B$. If $x \in C$, then $x \in A \cap C$. In any case, $x \in (A \cap B) \cup (A \cap C)$.

   So $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

   Similarly, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. This proves (*i*).

   Similarly, we can prove (*ii*)

Aliter. $x \in [A \cap (B \cup C)] \equiv [(x \in A) \wedge (x \in B \cup C)]$

$\equiv [(x \in A) \wedge \{(x \in B) \vee (x \in C)\}]$

$\equiv [(x \in A) \wedge (x \in B)] \vee [(x \in A) \subset (x \in C)]$

NOTES

by distributive law of logic

$$\equiv \quad [x \in (A \cap B)] \cup [x \in (A \cap C)]$$

$$\equiv \quad [\, x \in (A \cap B) \cup (A \cap C)]$$

So, $A \wedge (B \cup C) = (A \cap B) \cup (A \cap \mathrm{C})$

Similarly, we can prove (*ii*) by logic.

5. ***De-Morgan's Laws.*** For any two sets A and B,

   (*i*) $(A \cup B)' = A' \cap B'$.

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

   Proof: (*i*) Let $x \in (A \cup B)'$. This implies $x \notin A \cup B$ and $x \in U$. Now, $x \notin A \cup B$ implies $x \notin A$ and $x \notin B$. But, $x \notin A$ and $x \in U$ implies $x \in A'$ and $x \notin B$ and $x \in U$ implies $x \in B'$. Therefore, $x \in A' \cap B'$ and so $(A \cup B') \subseteq A' \cap B'$. Similarly, $(A' \cap B') \subseteq (A \cup B)'$.

   This proves $(A \cup B)' = A' \cap B'$.

   Alternative proof of (*i*) using logic:

   Now, $x \in (A \cup B)' \equiv \sim[(x \in (A \cup B)]$

   $\equiv \sim [(x \in A) \vee (x \in B)]$

   $\equiv \sim (x \in A) \wedge \sim (x \in B)$

   $\equiv (x \notin A\ ) \wedge (x \notin B)$

   $\equiv (x \in A') \wedge (x \in B')$

   $\equiv (x \in A' \cap B')$

   Therefore, $(A \cup B)' = A' \cap B'$.

Example 2.31: Let A, B, C be any three sets. Prove that

$$A \cap (B - C) = (A \cap B) - (A \cap C).$$

Solution: $(A \cap B) - (A \cap C) = (A \cap B) \cap (A \cap C')$

$= (A \cap B) \cap (A' \cap C')$

[by De-Morgan's law]

$= [(A \cap B) \cap A'] \cup [(A \cap B) \cap C']$

[Distributive law]

$\equiv [(A \cap A') \cap B] \cup [(A \cap B) \cap C']$

[Associative law]

$\equiv [\phi \cap B] \cup [A \cap (B \cap C')]$

$\phi \cup [A \cap (B \cap C')]$

$\equiv A \cap (B \cap C')$

$\equiv A \cap (B - C).$

Example 2.32: For any sets A and B, show that

$(A - B)\,(B - A) = (A \cup B) - (A \cap B)$.

Solution: $(A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B')$

$= (A \cup B) \cap (A' \cup B')$ De-Morgan's law

NOTES

$$= [(A \cup B) \cap A'] \cup [(A \cup B) \cap B']$$

Distributive law

$$= [(A \cap A') \cup (B \cap A')] \cup [(A \cap B') \cup (B \cap B')]$$

$$= [\phi \cup (B \cap A')] \cup [(A \cap B') \cup \phi]$$

$$= (B \cap A') \cup (A \cap B')$$

$$= (B - A) \cup (A - B)$$

$$= (A - B) \cup (B - A).$$ Commutative law

Representation of Symmetric Difference

When representing the symmetric difference between any two sets, let us assume set A and B are denoted by the symbol Δ.

Mathematically it is represented using:

$$A \Delta B = (A \cup B) - (A \cap B)$$

This representation has been repeatedly explained above. It implies that $A \Delta B$ represents a set that contains the elements from the union of two sets, A and B, minus the intersection between them. Symmetric Difference, in other words, is also called 'Disjunctive Union'.

The symbol Δ is also a binary operator. Like other binary operators, it takes two operands, two different or identical sets as we know for other operations and their applications for calculating probability between events.

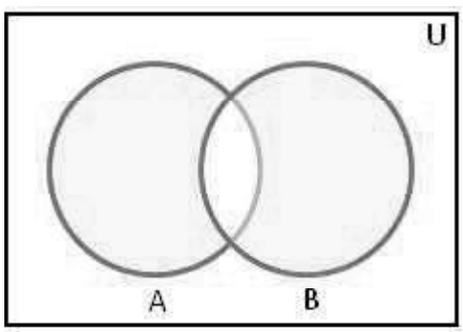
The symmetric difference is not only restricted to set operations. We can also use it to calculate the probability of certain multiple events. We can convert the equation written above to an equation with probability.

Definition: Like any other operation, a symmetric difference also happens between two sets. Suppose we have two sets, A and B. Their symmetric difference would consist of all the elements present in either A or B but not in the intersection of A and B.

The set $(A - B) \cup (B - A)$ and is denoted by $A \Delta B$.

Thus, $A \Delta B = (A - B) \cup (B - A) = \{x : x \notin A \cap B\}$

Or, $A \Delta B = \{x : [x \in A \text{ and } x \notin B] \text{ or } [x \in B \text{ and } x \notin A]\}$



A Δ B

NOTES

The shaded part of the given Venn diagram represents $A \Delta B$.

$A \Delta B$ is the set of all those elements which belongs either to A or to B but not to both.

$A \Delta B$ is also expressed by $(A \cup B) - (B \cap A)$.

It follows that $A \Delta \varnothing = A$ for all subset A,

$A \Delta A = \varnothing$ for all subset A

Properties of Symmetric Difference:

(i) $A \Delta B = B \Delta A$; [Commutative property]

(ii) $A \Delta (B \Delta C) = (A \Delta B) \Delta C$ [Associative property]

Theorem 2.2: Symmetric difference is commutative $S \Delta T = T \Delta S$.

Proof: $S \Delta T = (S \backslash T) \cup (T \backslash S)$ (By the Definition of Symmetric Difference)

$= (T \backslash S) \cup (S \backslash T)$ (Union is Commutative)

$= T \Delta S$ (Definition of Symmetric Difference)

Check Your Progress

12. What do you understand by Venn diagram?
13. How can use Venn diagram in math?
14. Give the proof of De–Morgan law.

2.8 ANSWERS TO 'CHECK YOUR PROGRESS'

1. An arithmetic series is the sum of an arithmetic sequence. We can find the sum by adding the first, a_1 and last term, a_n, divide by 2 in order to get the mean of the two values and then multiply by the number of values, n as per following equation:

$$S_n = n/2(a_1 + a_n)$$

2. In mathematics, a geometric series is the sum of an infinite number of terms that have a constant ratio between successive terms. For example, the series is explained by following formula:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$$

is geometric, because each successive term can be obtained by multiplying the previous term by 1/2.

3. Sum of n natural numbers we can defined the form of 'Arithmetic Progression' where the sum of n terms are arranged in a sequence with the first term being 1, n being the number of terms along with the nth term. The sum of n natural numbers is represented as $[n(n+1)]/2$. Natural numbers are the numbers that start from 1 and end at infinity. Natural numbers include whole numbers in them excluding the number 0.
4. Sum of cubes of first n natural numbers is $= (n(n+1)/2)^2$.

5. Set theory is the branch of mathematical logic that studies sets, which can be informally described as collections of objects. Although objects of any kind can be collected into a set, set theory, as a branch of mathematics, is mostly concerned with those that are relevant to mathematics as a whole.
6. 'A set is any collection of objects such that given an object, it is possible to determine whether that object belongs to the given collection or not.' The members of a set are called elements.
7. A set having only one element is called singleton. If a is the element of the singleton A, then A is denoted by $A = \{a\}$. Note that $\{a\}$ and a do not mean the same; $\{a\}$ stands for the set consisting of a single element a while a is just the element of $\{a\}$.
8. The union of any two sets A and B is the set of all those elements x such that x belongs to at least one of the two sets A and B. It is denoted by $A \cup B$. Logically speaking, if the biconditional statement $(x \in C) \Leftrightarrow (x \in A) \wedge (x \in B)$ is true for all x, then $C = A \cup B$. In other words, $(x \in A \cup B) \equiv (x \in A) \vee (x \in B)$.
9. The intersection of two sets A and B is the set of all those elements x such that x belongs to both A and B and is denoted by $A \cap B$. If $A \cap B = \phi$, then A and B are said to be disjoint.
10. Let A and B be two sets. If every element of A is an element of B then A is called a subset of B and we write $A \subseteq B$ or $B \supseteq A$ (read as 'A is contained in B' or 'B contains A').
11. A set which has no element is called the null set or empty set. It is denoted by the symbol ϕ.
12. To illustrate the various set operations, you learn about diagrams called Venn diagrams after John Venn (1834 – 1883). The universal set is represented by the points in and on a rectangle and the subsets $A, B, C, \ldots$ by points in and on the circles or ellipses drawn inside the rectangle.
13. In math, a Venn diagram is used to visualize the logical relationship between sets and their elements and helps us solve examples based on these sets.
14. Let $x \in (A \cup B)'$. This implies $x \notin A \cup B$ and $x \in U$. Now, $x \notin A \cup B$ implies $x \notin A$ and $x \notin B$. But, $x \notin A$ and $x \in U$ implies $x \in A'$ and $x \notin B$ and $x \in U$ implies $x \in B'$. Therefore, $x \in A' \cap B'$ and so $(A \cup B') \subseteq A' \cap B'$. Similarly, $(A' \cap B') \subseteq (A \cup B)'$.

2.9 SUMMARY

- In mathematics, a geometric series is the sum of an infinite number of terms that have a constant ratio between successive terms.
- In general, a geometric series is written as $a + ar + ar^2 + ar^3 + \ldots$, where a is the coefficient of each term and r is the common ratio between adjacent terms.

NOTES

- The name geometric series indicates each term is the geometric mean of its two neighbouring terms, similar to how the name arithmetic series indicates each term is the arithmetic mean of its two neighbouring terms.
- The sequence of geometric series terms (without any of the additions) is called a geometric sequence or, equivalently, a geometric progression.
- Set theory is commonly employed as a foundational system for the whole of mathematics, particularly in the form of Zermelo–Fraenkel set theory with the axiom of choice.
- 'A set is any collection of objects such that given an object, it is possible to determine whether that object belongs to the given collection or not.' The members of a set are called elements.
- Throughout this book, whenever we talk of a set, we shall assume it to be a subset of a fixed set U. This fixed set U will be called the universal set.
- The members of a set are called elements. We shall use capital letters to denote sets and small letters to denote elements. If a is an element of the set A, we write $a \in A$ (read as 'a belongs to A') and if a is not an element of the set A, we write $a \notin A$ (read as 'a does not belong to A'). There are different ways of describing a set.
- Two sets A and B are said to be equal if and only every member of A is a member of B and every member of B is a member of A. We express this by writing $A = B$, logically speaking $A = B$ means $(x \in A) \equiv (x \in B)$ or the biconditional statement $(x \in A) \Leftrightarrow (x \in B)$ is true for all x.
- We always write each element of a set only once. For example, $\{2, 2, 3\}$ is not a proper way of writing a set and it should be written as $\{2, 3\}$.
- The intersection of two sets A and B is the set of all those elements x such that x belongs to both A and B and is denoted by $A \cap B$. If $A \cap B = \phi$, then A and B are said to be disjoint.
- If A and B are two sets then complement of B relative to A is the set of all those element $x \in A$ such that $x \notin B$ and is denoted by $A - B$. Logically speaking, if for a set C the biconditional statement $(x \in C) \Leftrightarrow (x \in A) \cap (x \notin B)$ is true for all x, then $C = A - B$. In other words, if $(x \in C) \equiv (x \in A) \wedge (x \notin B)$, then C is called the complement of B relative to A.
- Whenever we say complement of B we mean, complement of B relative to the universal set U. In such case, we denote complement of B by B'.

  So, $B' = U - B$.
- Let A and B be two sets. If every element of A is an element of B then A is called a subset of B and we write $A \subseteq B$ or $B \supseteq A$ (read as 'A is contained in B' or 'B contains A').
- If $A \subseteq B$ and $A \neq B$, we write $A \subset B$ or $B \supset A$ (read as: A is a proper subset of B or B is a proper superset of A).
- Every set is a subset and a superset of itself.

- A set which has no element is called the null set or empty set. It is denoted by the symbol ϕ.
- To illustrate the various set operations, you learn about diagrams called Venn diagrams after John Venn (1834 – 1883). The universal set is represented by the points in and on a rectangle and the subsets $A, B, C, \ldots$ by points in and on the circles or ellipses drawn inside the rectangle.
- Let $x \in A \cap (B \cup C)$. This implies $x \in A$ and $x \in B \cup C$. Now, $x \in B \cup C$ implies $x \in B$ or $x \in C$ or $x \in$ both B and C. If $x \in B$, then $x \in A \cap B$. If $x \in C$, then $x \in A \cap C$. In any case, $x \in (A \cap B) \cup (A \cap C)$.
- Let $x \in (A \cup B)'$. This implies $x \notin A \cup B$ and $x \in U$. Now, $x \notin A \cup B$ implies $x \notin A$ and $x \notin B$. But, $x \notin A$ and $x \in U$ implies $x \in A'$ and $x \notin B$ and $x \in U$ implies $x \in B'$. Therefore, $x \in A' \cap B'$ and so $(A \cup B') \subseteq A' \cap B'$. Similarly, $(A' \cap B') \subseteq (A \cup B)'$.

2.10 KEY TERMS

- **Geometric series:** Geometric series play an important role in the early development of calculus, are used throughout mathematics, and have important applications in physics, engineering, biology, economics, computer science, queueing theory, and finance.
- **Set theory:** Set theory is the branch of mathematical logic that studies sets, which can be informally described as collections of objects.
- **Universal set:** Whenever we talk of a set, we shall assume it to be a subset of a fixed set U. This fixed set U will be called the universal set.
- **Elements:** The member of a set are called elements. We shall use capital letters to denote sets and small letters to denote elements.
- **Equality of sets:** Two sets A and B are said to be equal if and only every member of A is a member of B and every member of B is a member of A.
- **Venn diagrams:** Venn diagrams are used to depict how items relate to each other against an overall backdrop, universe, data set, or environment.

2.11 SELF-ASSESSMENT QUESTIONS AND EXERCISES

Short–Answer Questions

1. What is miscellaneous series?
2. Define the arithmetic series.
3. Give the derivation of sum of first n natural number.
4. State the set theory.
5. Define set.
6. What are elements?

NOTES

7. What do you understand by operation on sets?
8. How will you define the intersection?
9. Give the definition of subset.
10. What is Venn diagram?
11. State and proof the theorem of symmetric difference.

Long–Answer Questions

1. Explain in detail about the miscellaneous, arithmetic and geometric series with the help of examples.
2. Describe the sum of square and cubes of first natural number with relevant examples.
3. Discuss in detail the set theory with appropriate examples.
4. Elaborate on the subset with the help of examples.
5. Illustrate the Venn diagram by giving applications.
6. Analyse the different types of laws based on set theory.

2.12 FURTHER READING

Hazarika, Padmalochan. 2003. *A Class Textbook of Business Mathematics*. New Delhi: S. Chand & Company Ltd.

Tremblay, Jean Paul and R. Manohar. 2004. *Discrete Mathematical Structures With Applications To Computer Science*. New York: McGraw–Hill Higher Education.

Ramaswamy, V. 2006. *Discrete Mathematical Structures with Applications to Combinatorics*. Hyderabad: Universities Press.

Kolman, Bernand, Roberty C. Busby and Sharn Cutter Ross. 2006. *Discrete Mathematical Structures*. London (UK): Pearson Education.

Liu, C. L. 1985. *Elements of Discrete Mathematics*, 2nd Edition. New York: McGraw–Hill Higher Education.

Arumugam, S. and Thangapandi Isaac. 2008. *Modern Algebra*. Chennai: Scitech Publications (India) Pvt. Ltd.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. New Delhi: Cambridge University Press.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

UNIT 3 ORDERED PAIR, RELATIONS AND FUNCTIONS OR GROUP THEORY

Structure

3.0 INTRODUCTION

In math, the relation is between the *x*-values and *y*-values of ordered pairs. The set of all *x*-values is called the domain, and the set of all *y*-values is called the range. In mathematics, an ordered pair is a pair of objects. The order in which the objects appear in the pair is significant: the ordered pair is different from the ordered pair unless $a = b$. An inverse relation of a relation is a set of ordered pairs which are obtained by interchanging the first and second elements of the ordered pairs of the given relation. In mathematics, especially order theory, a partially ordered set formalizes and generalizes the intuitive concept of an ordering, sequencing, or

arrangement of the elements of a set. A set, i.e., constructed from two given sets and comprises all pairs of elements such that the first element of the pair is from the first set and the second is from the second set. In mathematics, an equivalence relation is a binary relation that is reflexive, symmetric and transitive. The relation is equal to is the canonical example of an equivalence relation.

In mathematics, a partition of a set is a grouping of its elements into non-empty subsets, in such a way that every element is included in exactly one subset. Whereas the algebraic structure is a type of non-empty set G, which is equipped with one or more than one binary operation.

A function is a rule that assigns each element of a set, called the domain, to exactly one element of a second set, called the codomain. In mathematics, a set is countable if it has the same cardinality (the number of elements of the set) as some subset of the set of natural numbers $N = \{0, 1, 2, 3, ...\}$. In mathematics, an uncountable set (or uncountably infinite set) is an infinite set that contains too many elements to be countable. Group is a monoid with an inverse element. The order of a group G is the number of elements in G and the order of an element in a group is the least positive integer n such that is the identity element of that group G. In group theory, a branch of mathematics, given a group G under a binary operation $*$, a subset H of G is called a subgroup of G if H also forms a group under the operation $*$. A cyclic group is a group that can be generated by a single element. In algebra, a homomorphism is a structure-preserving map between two algebraic structures of the same type.

In this unit, you will study about the relations and ordering, domain and the range of a relation, inverse relation, partially ordered, Cartesian product of sets, equivalence relation, partition, algebraic structures, functions, graph of the function, countable and uncountable sets, groups, subgroups, cyclic groups, homomorphism's.

3.1 OBJECTIVES

After going through this unit, you will be able to:

- Explain the relations and ordering
- Discuss the domain and the range of a relation
- Analyse the inverse relation
- Elaborate on the partially ordered and Cartesian product of sets
- Explain the equivalence relation and partition of sets
- Illustrate the algebraic structures
- Discuss the functions and graph of the function
- Describe the countable and uncountable sets
- Interpret the groups, subgroups and cyclic groups
- State the homomorphisms

3.2 RELATIONS AND ORDERING

NOTES

Let A and B be two sets. A relation R from A to B is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, then it is also denoted by aRb and conversely aRb means $(a, b) \in R$. The symbol aRb is read as 'a is related to b'. If $A = B$, we shall say R is a relation in A instead of 'from A to A'.

Let $A = \{1, 2\}$, $B = \{3\}$,

then $R_1 = \{(1, 3), (2, 3)\}$, $R_2 = \{(1, 3)\}$, $R_3 = \{(2, 3)\}$, are different relations from A to B.

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

Example 3.1: 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 3.2: Let A be the set of all lines in a plane. Let $R \subseteq A \times A$, where $R = \{(l, m) \mid l, m \in A, l \mid\mid m\}$ then R is

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

as $l \mid\mid l$ 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 $l \parallel m$, $m \parallel n \Rightarrow l \mid\mid n \Rightarrow (l, n) \in R$

Thus, the relation of parallelism is an equivalence relation.

Example 3.3: Let **Z** = set of integers then the usual $\leq$ is a partial order relation on **Z** as it is

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

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

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

NOTES

Example 3.4: Let $R = \{(m, n) \mid m, n \in \mathbf{Z}, m \mid n\}$

then R is a partial order relation. Verify.

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

Representation of a Relation by a Matrix

Sometimes, a relation is represented by a matrix, where, first we draw a table. Suppose R is a relation from a finite set A to a finite set B. We first construct a table by writing all the elements of A as a column on left and all the elements of B as the top row. Now, if $(a_i, b_j) \in R$, *i.e.*, $a_i R\, b_j$, then we write 1 in the ith row and jth column. If $(a_i, b_j) \notin R$ we write 0. We illustrate this by the following example

Suppose $A = \{a_1, a_2, a_3, a_4\}$, $B = \{b_1, b_2, b_3\}$. Then

$A \times B = \{(a_1, b_1),(a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_2), (a_3, b_3), (a_4, b_1), (a_4, b_2), (a_4, b_3)\}$

Suppose

$R = \{(a_1, b_1),(a_1, b_2), (a_2, b_2), (a_3, b_3), (a_4, b_1)\}$

The table and the corresponding relation matrix of R is given by

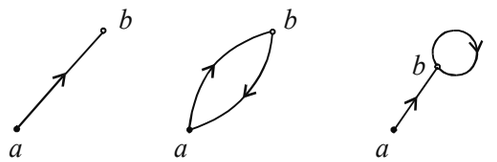
	b_1	b_2	b_3
a_1	1	1	0
a_2	0	1	0
a_3	0	0	1
a_4	1	0	0

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

The above representation of a relation by the relation matrix has an advantage in as far as a look at it gives us some information regarding the relation. For instance, if the diagonal entries in the matrix are all 1 then the corresponding relation is reflexive. Again, if the relation matrix is symmetric then the corresponding relation is also symmetric. Similarly, if the relation happens to be anti-symmetric then in the relation matrix if $a_{ij} = 1$, then $a_{ji} = 0$ $(i \neq j)$.

Diagrammatical Representation of a Relation

Sometimes, a relation is represented with the help of a diagram called the graph of the relation. All we do in this representation is that we represent the elements by small circles (or dots) called nodes and if aRb we join a and b by a line (or an arc) and put an arrow from a to b. In case bRa also holds we draw another arc from b to a and put an arrow from b to a. If aRa, we draw a circular arc showing a being joined to a (which will look like a loop). Thus, if a relation is reflexive, there will be loops at all the nodes.



aRb *aRb, bRa* *aRb, bRb*

3.2.1 Mapping or Function

Let A and B be two sets. A mapping or function f from A *to* B is a relation from A to B such that to each $a \in A$ there exists a unique $b \in B$. In other words, f is a subset of $A \times B$ such that $(a, b_1) \in f$ and $(a, b_2) \in f \Rightarrow b_1 = b_2$ and for each $a \in A$, there is some $b \in B$ such that $(a, b) \in f$. A mapping f from A to B is denoted by $f : A \to B$.

A is called Domain of f.

B is called Co-Domain of f.

Image of f is the set of those elements $b \in B$ such that $(a, b) \in f$ for some $a \in A$. It is denoted by $Im\,(f)$.

Notes:

1. If $f : A \to f$ and $(a, b) \in f$, then we write $b = f(a)$ and b is called the image of a under f. Also, a is called preimage of b under f.
2. Image of every element in A is unique.

Example 3.5: Let $A = \{1, 2, 3\}$, $B = \{4, 5\}$. Define $f = \{1,4), (2, 5), (3, 4)\}$. Then, f is a mapping from A *to* B.

But, $g = \{1, 4), (2, 5), (3, 5), (1, 5)\}$ is not a mapping from A to B as two elements 4 and 5 in B are assigned to the element $1 \in A$.

Again, $h = \{(1,4), (2, 5)\}$ is not a mapping as Dom $(h) = \{1, 2\} \neq A$.

One-One Mapping

A mapping $f : A \to B$ is said to be one-one if $f(a_1) = f(a_2)$ implies $a_1 = a_2$, where $a_1 \in A$ and $a_2 \in A$. This is also sometimes called injective mapping. In other words, a mapping $f : A \to B$ is one-one if and only if whenever $a_1 \neq a_2$ $(a_1 \in A, a_2 \in A)$ then $f(a_1) \neq f(a_2)$, *i.e.*, images of distinct elements in A are distinct.

Onto Mapping

A mapping $f : A \to B$ is said to be onto if given $b \in B$ there exists $a \in A$ such that $f(a) = b$. It is also sometimes called surjective mapping.

Example 3.6: Let $A = \{1, 2, 3\}, B = \{4, 5\}$. Define $f = \{(1,4), (2,4), (3,5)\}$. Then, $f : A \to B$ such that f is not one-one as $f(1) = 4$ and $f(2) = 4$. But, $1 \neq 2$. f is onto as both 4 and 5 have pre-images in A, namely 1 and 3.

Example 3.7: Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$. Define $f = \{(1, 4), (2, 5), (3, 6)\}$. Then, $f : A \to B$ such that f is one-one as distinct elements in A have distinct images in B. f is not onto as 7 has no pre-image in A.

Example 3.8: Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$. Define $f = (1, 6), (2, 4), (3, 5)$.

Then, $f : A \to B$ such that f is neither one-one nor onto.

Example 3.9: Let $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$. Define $f = \{(1, 4), (2, 4), (3, 5)\}$.

Then, $f : A \to B$ such that f is neither one-one nor onto.

NOTES

Example 3.10: If $f: A \to B$ such that f is onto, then Im $(f) = B$.

Solution: By definition, Im $f \subseteq B$. Let $b \in B$.Then there exist $a \in A$ such that $f(a) = b$ (as f is onto). This implies $b \in$ Im (f). So, B $\subseteq$ Im f.

Hence, Im$(f) = B$.

Binary Composition

A binary composition on a set S, is a rule which assigns to each pair of elements a, b of S a unique element c of S.

3.2.2 Domain and the Range of a Relation

Binary Relation

A binary relation R from a set A to a set B is a subset R of the Cartesian product $A \times B$.

For example,

1. Let $A = B = N$, the set of natural numbers.
   (*i*) Define the relation R as '='

   Now, $R = \{(1, 1), (2, 2), (3, 3), ...\} \subseteq N \times N$

   $\therefore$ R is a binary relation.

   (*ii*) Define R as '<'

   Then, $R = \{(1, 2), (2, 3), (3, 4), ... (1, 3), (2, 4), (3, 5), ...\} \subseteq N \times N$

   $\therefore$ R is a binary relation.
2. Let A be the set of all people on earth and $a, b \in A$, and $a\,R\,b$ iff a and b were born on the same day of the same year.

Let R be a binary relation. The set $D(R)$ of all elements x such that for all y, $(x, y) \in R$ is called the domain of R.

i.e., $D(R) = \{x : (x, y) \in R$, for all $y\}$

Similarly, $Rg(R)$ of all elements y such that for all x, $(x, y) \in R$ is called the range of R.

i.e., $Rg(R) = \{y : (x, y) \in R$, for all $x\}$

Operations on Relations

Let R and S be relations from a set A to a set B. Now the union and intersection of R and S is defined as,

(*i*) $R \cup S = \{(a, b) : (a, b) \in R$ or $(a, b) \in S\}$

(*ii*) $R \cap S = \{(a,b) : (a, b) \in R$ and $(a, b) \in S\}$

Example 3.11: Let $X = \{1, 2, 3, 4, 5, 6\}$

Let R and S be relations from X to X as,

$R = \{(x, y) : (x + y)$ is a multiple of $2\}$

$S = \{ (x, y) : (x + y)$ is a multiple of $3\}$

Find $R \cup S$ and $R \cap S$.

Solution: $R = \{(1, 3), (1, 5)\}$ and $S = \{(2, 4), (1, 5)\}$

$R \cup S = \{(1, 3), (2, 4), (1, 5)\}$

$R \cap S = \{(1, 5)\}$

Inverse of R: Let R be a relation from a set A to set B. The inverse of R is relation from B to A and is given by $R^{-1} = \{(y, x): (x, y) \in R\}$.

Representation of a Solution

(*i*) A binary relation R from a set A with n elements to a set B with m elements is represented as an $n \times m$ array M_R by marking the positions in M_R. The positions which correspond to the pairs belong to R with 1 and 0 elsewhere.

i.e., $M_R = [a_{ij}]\begin{cases} 1 \text{ if } i\text{th element of } A \text{ is related to } j\text{th element of } B \\ 0, \text{ otherwise.} \end{cases}$

Example 3.12: Let $A = B = X = \{1, 2, 3, 4, 5, 6\}$. Define R as '<' on X.

Solution: $R = \{(1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 3), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$.

$$M_R = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

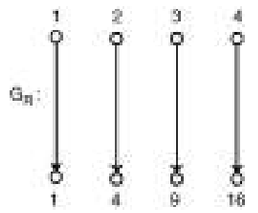
(*ii*) The relation array can be viewed graphically as elements of sets represented by models and an ordered pair is represented by an edge between the vertices that correspond to the paired elements, with an arrow pointing to the second element of the pair.

Example 3.13: Let $A = \{1, 2, 3, 4\}$, $B = \{1, 4, 9, 16\}$ and the relation $R = \{(1, 1), (2, 4), (3, 9), (4, 16)\}$. Draw the relation graph.

Solution: First we shall write the relation matrix M_R.

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Now we shall draw the relation graph G_R.



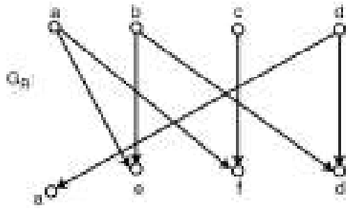
NOTES

Example 3.14: Let $A = \{a, b, c, d\}$, $B = \{a, e, f, d\}$ and let $R = \{(a, e), (a, f), (b, e), (c, f), (b, d), (d, d), (d, a)\}$. Draw the relation graph.

Solution: First we shall write the relation matrix M_R:

$$M_R = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

The relation graph G_R is given as

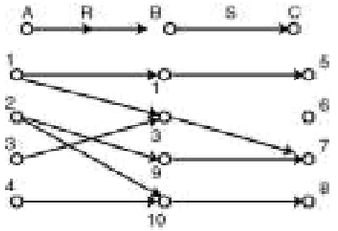


Composition of Two Relations

Let R be a binary relation from the set A to the set B and S be a binary relation from the set B to the set C, then the ordered pair (R, S) is said to be composable. If (R, S) is a composable pair of binary relations, the composite $R \circ S$ and R and S, is a binary relation from the set A to the set C, such that , for $a \in A$ and $c \in C$, $a (R \circ S)c$ if for some $b \in B$, both aRb and bSc are binary relations.

Example 3.15: $A = \{1, 2, 3, 4\}$, $B = \{1, 3, 9, 10\}$ $C = \{5, 6, 7, 8\}$, $R = \{(1, 1), (1, 3), (2, 9), (2, 10), (3, 3), (4, 10)\}$ $S = \{(1, 5), (3, 7), (9, 7), (10, 8)\}$. Find $R \circ S$ and its relation graph.

Solution:

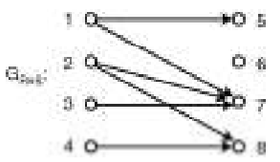


$R \circ S = \{(1, 5), (1, 7), (2, 7), (2, 8), (3, 7), (4, 8)\}$

The corresponding matrix is,

$$M_{R \circ S} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

And the corresponding relation graph $G_{R \circ S}$ is,



We know that a relation is a subset of *Cartesian product of two sets*. A relation shows relationship of a member of one set to that of another set. Thus, a relationship is shown as an ordered pair and is also called binary relation. If we recall the basic concept of a coordinate plane, also called Cartesian plane, we know that it is constituted by choosing two number lines, intersecting at right angles to each other. One line is horizontal, usually called x-axis and another as y-axis. The intersecting point of these two lines is the origin. When only one number line is used, every point on this number line represents a real number. But when we take two lines at right angles to each other it represents a point in the plain containing an ordered pair. Thus, every point on this plane shows a relation. Thus, relationship can be shown as graphs. A domain with a binary relation can be viewed as *vertices* with *edges* connecting them. Thus, any binary relation can be shown as graph, by taking domain elements as vertices and showing them as dots, with arrows as edges between related elements. Vertices can also represent tasks and edges connecting those showing dependencies.

We can make a graph of any relation. For example, we draw the graph of the relation,
R = {(2, 5), (4, 3), (6, 1), (2, 7)}. The graph is shown below:

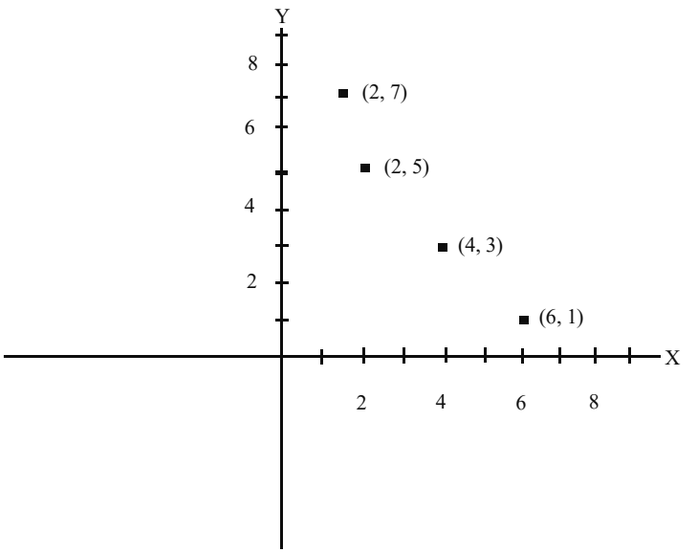


Fig. 3.1 *Graph Showing Relation*

R = {(2, 5), (4, 3), (6, 1), (2, 7)}

A function is also a relation although, all relations are not functions. So, we can call any function a relation too. We now draw the graph of the relation $2x + 3y = 6$. We must have at least two points. If $x = 0$, $y = 2$ and if $y = 0$, $x = 3$. Thus, graph can be sketched by taking points (0, 2) and (3, 0) and connecting these points to find a straight line. The graph has been plotted below.

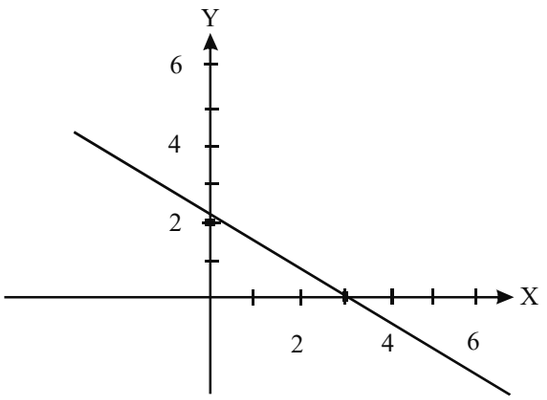
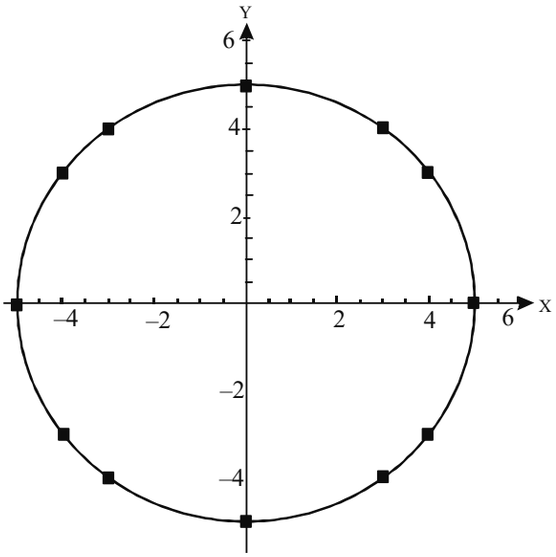


***Fig. 3.2** Graph of Relation 2x + 3y = 6*

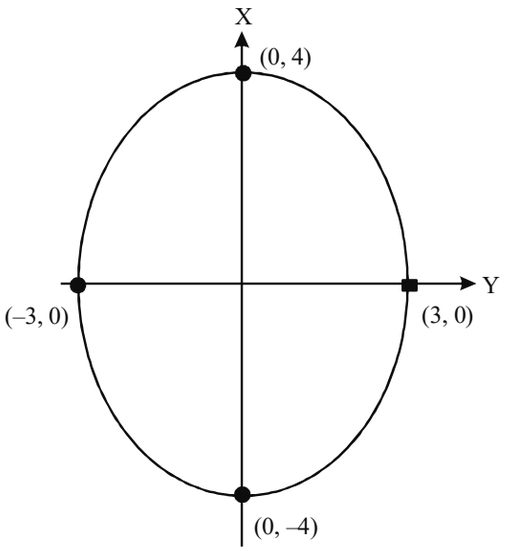
Example 3.16: Draw the graph of the relation $x^2 + y^2 = 25$.

Solution: To sketch the graph we find different points by arbitrarily taking values of x and finding corresponding values of y. Points are: (5, 0), (4, 3), (3, 4), (0, 5), (–3, 4), (–4, 3), (–5, 0), (–4, –3), (–3,–4), (0,–5), (3,–4), (4,–3). We plot this line on the plane and join these.



Example 3.17: Draw the graph of relation $16x^2+9y^2 = 144$ and find the intercepts on axes.

Solution: By equating $y = 0$, we get x-intercepts and by putting $y = 0$, we get y-intercepts. We note different values of y corresponding to some values of x and draw a curve. This shows an ellipse. The x-intercepts are (3, 0) and (–3, 0). The y-intercepts are (4, 0) and (–4, 0). The curve is shown below.



3.2.3 Inverse Relation

In mathematics, the inverse relation of a binary relation is the relation written 'Backwards'. In formal terms, if $L: X \rightarrow Y$ is a binary relation, then the inverse relation is $L^{-1}: Y \rightarrow X$.

The inverse relation is also called the converse relation and may be written as L^C, L^T (in view of its similarity with the transpose of a matrix).

3.3 PARTIALLY ORDERED SET

In mathematics, especially order theory, a partially ordered set (also termed as poset) formalizes and generalizes the intuitive concept of an ordering, sequencing, or arrangement of the elements of a set. A poset consists of a set together with a binary relation indicating that, for certain pairs of elements in the set, one of the elements precedes the other in the ordering. The relation itself is called a 'Partial Order'. The word partial in the names 'Partial Order' and 'Partially Ordered Set' is used as an indication that not every pair of elements needs to be comparable. That is, there may be pairs of elements for which neither element precedes the other in the poset. Partial orders thus generalize total orders, in which every pair is comparable.

Formally, a partial order is any binary relation that is reflexive (each element is comparable to itself), antisymmetric (no two different elements precede each other), and transitive (the start of a chain of precedence relations must precede the end of the chain). One universal example of a partially ordered set is a collection of people ordered by genealogical descendancy. Some pairs of people bear the descendant-ancestor relationship, but other pairs of people are incomparable, with neither being a descendant of the other.

A poset can be visualized through its Hasse diagram, which depicts the ordering relation.

NOTES

Partial Ordering

A relation R on a set A is said to be a partial order relation if R is (*i*) Reflexive, (*ii*) Antisymmetric and (*iii*) Transitive.

For example, Let S be non-empty set. Define R as $\subseteq$ (contained in or equal to) $P(S)$. Clearly $(P(S), \subseteq)$, is a partial order set. If,

(*i*) $A \in P(S), A \subseteq A$

(*ii*) $A, B \in P(S), A \subseteq B$ and $B \subseteq A \Rightarrow A = B$

(*iii*) $A, B, C, \in P(S)$,

Whenever $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$. $\therefore \subseteq$ is a partial order relation on $P(S)$.

Let $\leq$ be a partial order on the set of integers and *a, b, c* be integers. Clearly,

(*i*) $a \leq a$; where $a \in Z$

(*ii*) If $a \leq b$ and $b \leq a$ then $a = b$,where $a, b \in Z$.

(*iii*) If $a \leq b$ and $b \leq c$ then $a \leq c$, where $a, b, c \in Z$.

$\therefore$ $(Z, \leq)$ is a partial order set (poset).

Comparable Integers: Two elements of a poset $(S, \leq)$ are said to be comparable if $a \leq b$ or $b \leq a$. Otherwise a and b are said to be incomparable.

For example, In the poset $(Z^+,1)$, the integers 2 and 8 are comparable whereas 3 and 5 are incomparable.

[a / b is read as a divides b and $a/b \Rightarrow b = k\,a$ for some $k \in Z$]

Chain: A poset $(S, \leq)$ is called a chain if $\leq$ is total order relation.

(If every two elements of S are comparable then S is called a totally released set.)

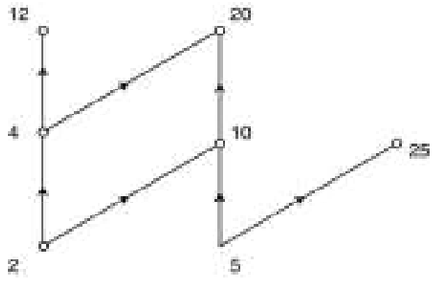
For example, The poset $(Z, \leq)$ is a chain, whereas the poset $(Z^+,1)$ is not a chain.

Representation of Poset

We can represent the poset as a directed graph. Every poset consisting of a set and a relation can be represented as a graph. We have to do minor modification in this relational graph. Since partial ordering relation is reflexive and transitive the relational graph will consist of self loops and edges corresponding to the transitive relations.

In the relational graph, the self loops and edges corresponding to the pairs (*a, c*) are removed whenever (*a, b*) and (*b, c*) are present. Finally, each edge is arranged so that its initial vertex is below its terminal vertex. All the arrows on the directed edges, are removed since all the edges point upward towards their terminal vertex.

Example 3.18: Draw the Hasse diagram representing the partial ordering {(*a, b*) / *a /b*} on {2, 4, 5, 10, 12, 20, 25}.



Solution: Here the relation set = {(2, 4), (2, 12), (4, 12), (5, 10), (5, 20), (5, 25), (10, 20)}

3.3.1 Ordered Pair

In mathematics, an ordered pair (a, b) is a pair of an objects. The order in which the objects appear in the pair is important: the ordered pair (a, b) is different from the ordered pair (b, a) unless $a = b$. (In contrast, the unordered pair $\{a, b\}$ equals the unordered pair $\{b, a\}$.)

Ordered pairs are also called 2-tuples, or sequences of length 2. Ordered pairs of scalars are sometimes called 2-dimensional vectors. (Technically, i.e., an abuse of terminology since an ordered pair need not be an element of a vector space.) The entries of an ordered pair can be other ordered pairs, enabling the recursive definition of ordered *n*-tuples (ordered lists of *n* objects). For example, the ordered triple (a,b,c) can be defined as $(a, (b,c))$, i.e., as one pair nested in another. In the ordered pair (a, b), the object a is called the first entry, and the object b the second entry of the pair. Otherwise, the objects are called the first and second components, the first and second coordinates, or the left and right projections of the ordered pair. Cartesian products and binary relations (and hence functions) are defined in terms of ordered pairs.

Simplifications: Let (a_1, b_1) and (a_2, b_2) be ordered pairs. Then the characteristic (or defining) property of the ordered pair is:

$$\mathbf{(a_1, b_1) = (a_2, b_2) \text{ iff } a_1 = a_2 \text{ and } b_1 = b_2.}$$

The set of all ordered pairs whose first entry is in some set A and whose second entry is in some set B is called the **Cartesian product** of A and B, and , which is written as $A \times B$. A binary relation between sets A and B is a subset of $A \times B$.

The (a, b) notation may be used for other purposes, most notably as denoting *open intervals* on the real number line.

The left and right projection of a pair p is usually denoted by $\pi_1(p)$ and $\pi_2(p)$, or by $\pi_\ell(p)$ and $\pi_r(p)$, respectively. In contexts where arbitrary *n*-tuples are considered, $\pi^n_i(t)$ is a common notation for the *i*-th component of an *n*-tuple t.

Informal and Formal Definitions

For any two objects a and b, the ordered pair (a, b) is a notation specifying the two objects a and b, in that order, i.e., usually followed by a comparison to a set

of two elements; pointing out that in a set a and b must be different, but in an ordered pair they may be equal and that while the order of listing the elements of a set does not matter, in an ordered pair changing the order of distinct entries changes the ordered pair. This 'Definition' is unsatisfactory because it is only descriptive and is based on an intuitive understanding of order. A more satisfactory approach is to observe that the characteristic property of ordered pairs given above is all that is required to understand the role of ordered pairs in mathematics. Hence the ordered pair can be taken as a primitive notion, whose associated axiom is the characteristic property.

Another way to rigorously deal with ordered pairs is to define them formally in the context of set theory. This can be done in several ways and has the advantage that existence and the characteristic property can be proven from the axioms that define the set theory.

Equality of Ordered Pairs

Two Ordered Pairs are said to be equal if the analogous first components are equal alongside the corresponding second components are equal. Consider two ordered pairs (u, v) and (x,y). The two ordered pairs are equal iif $u = x$, $v = y$, i.e., $(u, v) = (x, y)$.

Check Your Progress

1. Define the onto mapping.
2. When A is called partial order relation?
3. What do you understand by binary relation?
4. State the composition of two relation.
5. Define the inverse relation.
6. What is partially ordered set?

3.4 CARTESIAN PRODUCT OF SETS

Definition: Let A and B be two sets. The set of all ordered pairs (a, b) such that $a \in A$, $b \in B$ is called the Cartesian product of A and B and is denoted by $A \times B$.

Notes: 1. The ordered pair (a, b) is not the same as the set $\{a, b\}$.

2. Two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.
3. For the ordered pair (a, b), a is called the first coordinate and b is second coordinate.

Example 3.19: Let A be any set. Then show that $A \times \phi$ and $\phi \times A$ are empty sets.

Solution: Suppose that $A \times \phi$ is not empty.

Then, there is some $x \in A \times \phi$

By definition, $x = (a, b)$, where $a \in A$, $b \in \phi$.

This is absurd as ϕ is empty.

Hence, $A \times \phi = \phi$.

Similarly, $\phi \times A = \phi$.

Example 3.20: Let A, B, C be three sets. Show that,

$A \times (B \cup C) = (A \times B) \cup (A \times C)$

Solution: Let $x \in A \times (B \cup C)$

Then, $x = (a, d)$, where $a \in A$, $d \in B \cup C$

Now, if $d \in B$, then $x \in A \times B$ or if $d \in C$, then $x \in A \times C$

In any case, $x \in (A \times B) \cup (A \times C)$

Therefore, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ ...(1)

Similarly, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$ ...(2)

By Equations (1) and (2):

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

This proves the result.

Example 3.21: Let A, B, C be three sets. Show that,

$A \times (B - C) = (A \times B) - (A \times C)$

Solution: Let $(a, d) \in A \times (B - C)$

Then, $a \in A$, $d \in B$ and $d \notin C$

So, $(a, d) \in A \times B$ and $(a, d) \notin A \times C$

Therefore, $(a, d) \in (A \times B) - (A \times C)$

This proves that $A \times (B - C) \subseteq (A \times B) - (A \times C)$ ...(1)

To prove the other side let us proceed as under,

Let $x \in (A \times B) - (A \times C)$

Then, x is an element of $A \times B$ but it does not belong to $A \times C$. This means that $x = (a, b)$ where $a \in A$, $b \in B$ but $b \notin C$,

or, $x = (a, b) \in A \times C$

This implies that, $b \in B - C$

Therefore, $x \in A \times (B - C)$

Hence, $(A \times B) - (A \times C) \subseteq A \times (B - C)$ ...(2)

By Equation(1) and (2):

$A \times (B - C) = (A \times B) - (A \times C)$

This proves the result.

Example 3.22: If the set A has m elements and the set B has n elements, how many elements does $A \times B$ have?

Solution: Let $a \in A$. Then, number of elements of $A \times B$ with first coordinate as a is n. But a can be chosen in m ways. So, the number of distinct elements of $A \times B$ is mn.

Example 3.23: If $A = \{1, 4\}$, $B = \{4, 5\}$, $C = \{5, 7\}$

Find (*i*) $(A \times B) \cup (A \times C)$ (*ii*) $(A \times B) \cap (A \times C)$

Solution: (*i*) As proved in Example 3.20, $(A \times B) \cup (A \times C) = A \times (B \cup C)$

Now, $B \cup C = \{4, 5, 7\}$

So, $A \times (B \cup C) = \{(1, 4), (4, 4), (1, 5), (4, 5), (1, 7), (4, 7)\}$

$= (A \times B) \cup (A \times C)$

(*ii*) Now, $A \times B = \{(1, 4), (4, 4), (1, 5), (4, 5)\}$

$A \times C = \{(1, 5), (1, 7), (4, 5), (4, 7)\}$

So, $(A \times B) \cap (A \times C) = \{(1, 5), (4, 5)\}$

Relation

Let A and B be two sets. A relation R from A to B is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, then it is also denoted by aRb and conversely, aRb means $(a, b) \in R$. The symbol aRb is read as 'a is related to b'. If $A = B$, we shall say that R is a relation in A instead of 'from A to A'.

Let $A = \{1, 2\}, B = \{3\}$

Then, $R_1 = \{(1, 3), (2, 3)\}, R_2 = \{(1, 3)\}, R_3 = \{(2, 3)\}$, are different relations from A to B.

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: Whenever $(a, b) \in R$ then $(b, a) \in R$

Antisymmetric: If $(a, b) \in R, (b, a) \in R \Rightarrow a = b$

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

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

The following example will make the concept clear. 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

Let A be the set of all lines in a plane. Let $R \subseteq A \times A$,

Where, $R = \{(l, m): l, m \in A, l \mid\mid m\}$

Then R is,

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

As $l \mid\mid l$ for all $l \in A$

***Symmetric*:** As $(l, m) \in R$ then $l \mid\mid m \Rightarrow m \mid\mid l$

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

***Transitive*:** As $(l, m) \in R, (m, n) \in R$, then $l \parallel m, m \parallel n \Rightarrow l \mid\mid n \Rightarrow (l, n) \in R$

Thus, relation of parallelism is an equivalence relation.

You can also prove that if $\mathbf{Z}$ = Set of integers, then the relation $\leq$ is a partial order relation on $\mathbf{Z}$ as it is,

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

***Antisymmetric*:** As $a \leq b, b \leq a \Rightarrow a = b$

***Transitive*:** As $a \leq b, b \leq c \Rightarrow a \leq c$

3.5 EQUIVALENCE RELATION

NOTES

In mathematics, an equivalence relation is a binary relation that is reflexive, symmetric and transitive. The relation "Is Equal To" is the canonical example of an equivalence relation. Each equivalence relation provides a partition of the underlying set into disjoint equivalence classes. Two elements of the given set are equivalent to each other, if and only if they belong to the same equivalence class.

A partial order is a relation that is reflexive, antisymmetric, and transitive. Equality is both an equivalence relation and a partial order. Equality is also the only relation on a set that is reflexive, symmetric and antisymmetric. In algebraic expressions, equal variables may be substituted for one another, a facility that is not available for equivalence related variables. The equivalence classes of an equivalence relation can substitute for one another, but not individuals within a class.

Definition of Equivalence Relation

A relation R on a set A is called an equivalence relation if R is reflexive, symmetric and transitive.

For example,

Let N be the set of natural numbers. Define R on N as,

$$R = \{(x,y) : x + y \text{ is even}, x, y \in N\}$$

Proof: Let $x \in N$. Now $x + x = 2x$.

Clearly $2x$ is even. Therefore R is reflexive. Let $x, y \in N$ and $x + y$ is even. Clearly $y + x$ is also even and hence R is symmetric.

Now, if $x + y$ is even and $y + z$ is even then we have to prove that $x + z$ is even.

Since, $x + y$ and $y + z$ are even, both $(x + y)$ and $(y + z)$ are divisible by 2.

$\therefore (x + y) + (y + z)$ is also divisible by 2, i.e., $x + (y + y) + z$ is divisible by 2.

$\therefore (x + z)$ is divisible by 2.

Hence, R is transitive. So, R is an equivalence relation.

Note: From the relation graph or relation matrix, the kind of relation can be identified.

Example 3.24: The relation R on a set is represented by,

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Is R reflexive, symmetric or antisymmetric?

Solution: In the matrix M_R, the diagonal elements are 1. Therefore, R is reflexive. Since the matrix M_R is symmetric, the relation R is also symmetric.

Example 3.25: The relation R and R_1 on a set is represented by,

$$(i)\ M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (ii)\ M_{R_1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Are the relations R and R_1 reflexive, symmetric, antisymmetric, and/or transitive?

Solution:

(*i*) Since, the matrix M_R is symmetric and its diagonal entries are 1. The relation R is symmetric and reflexive. Since R is not antisymmetric, R is transitive.

(*ii*) The relation R_1 is not reflexive.

R_1 is symmetric [$\because M_{R_1}$ is symmetric] and R_1 is transitive.

Example 3.26: Draw the relation graph for the following relations.

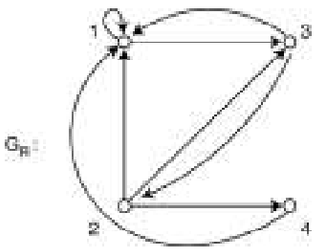
(*i*) $R = \{(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)\}$ on the set $X = \{1, 2, 3, 4\}$.

(*ii*) $R_1 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ on the set $Y = \{1, 2, 3\}$.

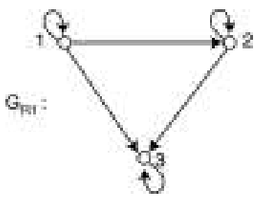
Solution:

(*i*) The relation graph G_R of R is drawn as:

The vertices of G_R are 1, 2, 3, 4.



(*ii*) The relation graph G_{R_1} of R_1 is drawn as:



Example 3.27: Let R be the relation represented by:

$$M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Find the relation matrices representing (*i*) R^{-1} (*ii*) R^c (*iii*) R^2.

Solution:

(*i*) To get the inverse relation matrix $(M_{R^{-1}})$ of a relation matrix (M_R) just write the transpose of M_R.

$$\therefore \quad M_{R^{-1}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

(*ii*) To find the complement relation matrix, replace 0 by 1 and 1 by 0 in the given relation matrix.

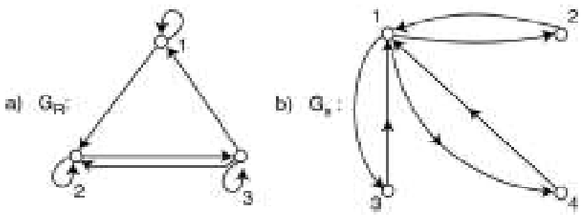
$$\therefore \quad M_{R^c} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

(*iii*) To find the relation matrix of R^2 when $R^2 = R \circ R$.

If the relation matrix M_R is known, then $M_{R^2} = M_R . M_R$ (the matrix multiplication)

$$\therefore \quad M_{R^2} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

Example 3.28: Find whether the relations for the directed graphs shown in the following figures are reflexive, symmetric, antisymmetric and/or transitive.



Solution:

(*i*) In G_R, there are loops at every vertex of the relation graph and hence it is reflexive.

It is neither symmetric nor antisymmetric since there is an edge between 1 and 2 but not from 2 to 1, but there are edges connecting 2 and 3 in both directions.

Moreover, the relation is not transitive, since there is an edge from 1 to 2 and 2 to 3, but no edge from 1 to 3.

(*ii*) Since loops are not present in G_S, this relation is not reflexive. Further, it is symmetric and not antisymmetric.

Moreover, the relation is not transitive.

3.5.1 Equivalence Class

Let R be an equivalence relation on a set A. Let $x \in A$. The equivalence class a is given by,

$$[a]_R = \{x \in A : (a, x) \in R\}$$

Note: $[a]_R \neq \phi$, because $a \in [a]$.

NOTES

Example 3.29: Prove that any two equivalence classes are identical or disjoint.

Solution: First we shall prove that $(a,b) \in R$. This implies that $[a]_R = [b]_R$

Suppose $(a, b) \in R$

Case I: $[a] = [b]$

Let $x \in [a] \Rightarrow (x, a) \in R$

$\Rightarrow (x,b) \in R$ [$\because$ $(x,a) \in R$ and $(a,b) \in R$ and R is Transitive]

$\Rightarrow x \in [b]$

$\Rightarrow [a] = [b]$

$\therefore \quad [a] = [b]$

Now suppose $[a]$, $[b]$ are two equivalence classes.

Case II: $[a] = [b]$ or $[a] \cap [b] = \phi$

If $[a] \cap [b] = \phi$ then nothing to prove.

Suppose $[a] \cap [b] \neq \phi$, then $x \in [a] \cap [b]$

$\Rightarrow x \in [a]$ and $x \in [b]$

$\Rightarrow (x, a) \in R$ and $(x, b) \in R$

$\Rightarrow [x] = [a]$ and $[x] = [b]$

$\Rightarrow [a] = [b]$

$\therefore \quad [a] \cap [b] = \phi$ or $[a] = [b]$

i.e., any two equivalence classes are identical or disjoint.

3.5.2 Partition of Set

Given an equivalence relation on set A, the collection of equivalence classes forms a partition of set A. The converse is also true, given a partition on set A, the relation "Induced by the Partition" is an equivalence relation.

Example 3.30: Prove that an equivalence relation induces a partition and a partition induces an equivalence relation.

Solution: Let $\{A_i : i \in Z\}$ is a partition of a set A. Define a relation R on A by $(a,b) \in R$ if $a, b \in A_i$ for some i.

Case I: R is an equivalence relation on A.

Let, $a \in A$

$\Rightarrow a \in A_i$ for some i

$\Rightarrow a, a \in A_i$ for some i

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

$\therefore R$ is a reflexive relation on A.

Suppose $(a, b) \in R$, then by the definition of R,

$a, b \in A_i$ for some i

$\therefore\ b, a \in A_i$ for some i

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

$\therefore$ R is a symmetric relation on A.

Suppose $(a, b) \in R$ and $(b, c) \in R$, then $a, b \in A_i$ and $b, c \in A_j$ for some i and j.

Here, $b \in A_i$ and $b \in A_j$

$\therefore A_i \cap A_j \neq \phi \Rightarrow A_i = A_j$, otherwise $\{A_i\}_{i \in I}$ is not a partition and hence $a, b, c \in A_i$

$\therefore (a, c) \in R$

$\therefore R$ is a transitive relation on A.

R is also an equivalence relation on A.

Further, we can also show that $A_i = [a]_{a \in A}$

Conversely, we can assume that R is an equivalence relation on set A.

Case II: R induces a partition for A.

Let, $x \in A$, $[x] = \{y \in A / (y, x) \in R\}$ and for any $x, y \in A$, we have

$$[x] \cap [y] = \phi \text{ or } [x] = [y]$$

$\therefore\ A = \cup_{x \in A} [x]$

i.e., $\{[x] : x \in A\}$ is a partition for A.

Let S be a non-empty set. The family of a sets $\{A_1, A_2, ..., A_n\}$ is a partition of the set S if

(i) $S = \bigcup_{i=1}^{n} A_i$ (ii) $A_i \cap A_j = \varnothing$ of $i \neq j$

For example, $S = \{1, 2, 3, 4, 5, 6, 7\}$, $A_1 = \{1, 3, 5, 7\}$, $A_2 = \{2, 4, 6\}$

Clearly, $\{A_1, A_2\}$ is a partition of S.

Note:

Every singleton subset constitutes a partition.

3.6 ALGEBRAIC STRUCTURES

In mathematics, an **algebraic structure** consists of a non-empty set A, termed as the underlying set, carrier set or domain. It is a collection of operations on A of finite arity, typically binary operations, and a finite set of identities, known as axioms that these operations must satisfy.

An algebraic structure may be based on other algebraic structures with operations and axioms involving several structures. For example, a vector space

NOTES

involves a second structure termed as a field, and an operation termed as the scalar multiplication between elements of the field called scalars, and elements of the vector space called vectors.

In the context of universal algebra, the set A with this structure is called an algebra, while in other contexts it is called an algebraic structure, because the term algebra being reserved for specific algebraic structures that are vector spaces over a field or modules over a commutative ring.

The properties of specific algebraic structures are studied in abstract algebra. The general theory of algebraic structures has been formalized in universal algebra. The language of category theory is used to express and study relationships between different classes of algebraic and non-algebraic objects. This is because it is sometimes possible to find strong connections between some classes of objects, sometimes of different kinds. For example, Galois Theory establishes a connection between certain fields and groups - two algebraic structures of different kinds.

Addition and multiplication of real numbers are the ideal and typical examples of operations that combine two elements of a set to produce a third element of the set. These operations follow several algebraic laws.

For example, $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$ as the 'Associative Laws'.

Also $a + b = b + a$ and $ab = ba$ as the 'Commutative Laws'.

Many systems studied by mathematicians have operations that observe some but not necessarily all of the laws of ordinary arithmetic. For example, rotations of an object in three-dimensional space can be combined by performing the first rotation on the object and then applying the second rotation on it in its new orientation made by the previous rotation. Rotation as an operation follows the associative law, but it may not satisfy the commutative law.

Mathematicians give names to sets with one or more operations that obey a particular collection of laws, and study them in the abstract as algebraic structures. In complete generalisation, the algebraic structures may involve an arbitrary collection of operations, including operations that combine more than two elements (higher arity operations) and operations that take only one argument (unary operations).

3.6.1 Algebraic Systems

An algebraic system is a mathematical system consisting of a set called the domain and one or more operations on the domain. Following are the examples and rules defining the algebraic systems with no binary operation, and with one and two binary operations.

One Set with Operations

1. Simple Structures: No Binary Operation

The simple structures with no binary operations can be defined as follows.

Set: A degenerate algebraic structure S having no operations.

Pointed Set: S has one or more distinguished elements, often 0, 1, or both.

Unary System: *S* and a single unary operation over *S*.

Pointed Unary System: A unary system with *S* a pointed set.

2. Group-Like Structures: One Binary Operation

The group-like structures with one binary operation can be indicated by any symbol, or with no symbol (juxtaposition) as is done for ordinary multiplication of real numbers.

- **Magma or Groupoid:** *S* and a single binary operation over *S*.
- **Semigroup:** An associative magma.
- **Monoid:** A semigroup with identity element.
- **Group:** A monoid with a unary operation (inverse), giving rise to inverse elements.
- **Abelian Group:** A group whose binary operation is commutative.
- **Semilattice:** A semigroup whose operation is idempotent and commutative. The binary operation can be called either meet or join.
- **Quasigroup:** A magma obeying the Latin square property. A quasigroup may also be represented using three binary operations.
- **Loop:** A quasigroup with identity.

3. Ring-Like Structures or Ringoids

Ring-like structures can be defined on the basis of two binary operations, often called addition and multiplication, with multiplication distributing over addition.

- **Semiring:** A ringoid such that *S* is a monoid under each operation. Addition is typically assumed to be commutative and associative, and the monoid product is assumed to distribute over the addition on both sides, and the additive identity 0 is an absorbing element in the sense that $0/x = 0$ for all x.
- **Near-Ring:** A semiring whose additive monoid is a (not necessarily Abelian) group.
- **Ring:** A semiring whose additive monoid is an abelian group.
- **Lie Ring:** A ringoid whose additive monoid is an abelian group, but whose multiplicative operation satisfies the Jacobi identity rather than associativity.
- **Commutative Ring:** A ring in which the multiplication operation is commutative.
- **Boolean Ring:** A commutative ring with idempotent multiplication operation.
- **Field:** A commutative ring which contains a multiplicative inverse for every nonzero element.
- **Kleene Algebras:** A semiring with idempotent addition and a unary operation, the Kleene star, satisfying additional properties.
- ***-Algebra:** A ring with an additional unary operation (*) satisfying additional properties.

4. Lattice Structures

Lattice structures can be defined on the basis of two or more binary operations, which typically include operations termed as meet and join, connected by the absorption law.

- **Complete Lattice:** A lattice in which arbitrary meet and joins exist.
- **Bounded Lattice:** A lattice with a greatest element and least element.
- **Complemented Lattice:** A bounded lattice with a unary operation, complementation, denoted by postfix notation '$\perp$'. The join of an element with its complement is the greatest element, and the meet of the two elements is the least element.
- **Modular Lattice:** A lattice whose elements satisfy the additional modular identity.
- **Distributive Lattice:** A lattice in which each of meet and join distributes over the other. Distributive lattices are modular, but the converse does not hold.
- **Boolean Algebra:** A complemented distributive lattice. Either of meet or join can be defined in terms of the other and complementation. This can be shown to be equivalent with the ring-like structure of the same name above.
- **Heyting Algebra:** A bounded distributive lattice with an added binary operation, relative pseudo-complement, denoted by infix '$\rightarrow$', and governed by the axioms, $x \rightarrow x = 1$, $x\ (x \rightarrow y) = x\ y$, $y\ (x \rightarrow y) = y$, $x \rightarrow (y\ z) = (x \rightarrow y)\ (x \rightarrow z)$.

5. Arithmetic

Arithmetic is precisely defined using the two binary operations, addition and multiplication. Consider that S is an infinite set. Arithmetic points unary systems, whose unary operation is injective successor, and with distinguished element '0'.

- **Robinson Arithmetic:** Addition and multiplication are recursively defined by means of successor. '0' is the identity element for addition, and annihilates multiplication. Robinson arithmetic has closeness to Peano arithmetic.
- **Peano Arithmetic:** Robinson arithmetic with an axiom schema of induction. Most ring and field axioms bearing on the properties of addition and multiplication are theorems of Peano arithmetic or of proper extensions thereof.

Two Sets with Operations

Algebraic operations on two sets can be defined as follows.

1. Module-Like Structures

Operations with two sets can be defined on the basis of module-like structures, i.e., composite systems comprising of two sets and using at least two binary operations.

- **Group with Operators:** A group G with a set Ω and a binary operation $\Omega \times G \rightarrow G$ satisfying certain axioms.

- **Module:** An Abelian group M and a ring R acting as operators on M. The members of R are occasionally termed as scalars, and the binary operation of scalar multiplication is a function $R \times M \rightarrow M$, which satisfies several axioms. Counting the ring operations these systems have at least three operations.
- **Vector Space:** A module where the ring R is a division ring or field.
- **Graded Vector Space:** A vector space with a direct sum decomposition separating or dividing the space into 'Grades'.
- **Quadratic Space:** A vector space V over a field F with a quadratic form on V which takes values in F.

2. Algebra-Like Structures

Algebra-like structures can be explained as composite system which are typically defined over two sets, a ring R and an R-module M equipped with an operation termed as multiplication. This can be observed as a system with five binary operations - two operations on R, two operations on M and one operation involving both R and M.

- **Algebra over a Ring (also R-Algebra):** A module over a commutative ring R, which also carries a multiplication operation that is compatible with the module structure. This includes distributivity over addition and linearity with respect to multiplication by elements of R. The theory of an algebra over a field is especially well developed.
- **Associative Algebra:** An algebra over a ring such that the multiplication is associative.
- **Nonassociative Algebra:** A module over a commutative ring, equipped with a ring multiplication operation that is not necessarily associative. Often associativity is replaced with a different identity, such as alternation, the Jacobi identity, or the Jordan identity.
- **Coalgebra:** A vector space with a 'Comultiplication' defined dually to that of associative algebras.
- **Lie Algebra:** A special type of nonassociative algebra whose product satisfies the Jacobi identity.
- **Lie Coalgebra:** A vector space with a 'Comultiplication' defined dually to that of Lie algebras.
- **Graded Algebra:** A graded vector space with an algebra structure which is typically compatible with the grading. Typically, if the grades of two elements a and b are known, then the grade of ab is also known, and consequently the location of the product ab is determined in the decomposition.
- **Inner Product Space:** The inner product space can be defined on the basis of an F vector space V with a definite bilinear form $V \times V \rightarrow F$.

3. Four or More Binary Operations

Four or more binary operations can be explained using the following notations.

NOTES

- **Bialgebra:** An associative algebra with a compatible coalgebra structure.
- **Lie Bialgebra:** A Lie algebra with a compatible bialgebra structure.
- **Hopf Algebra:** A bialgebra with a connection axiom (antipode).
- **Clifford Algebra:** A graded associative algebra equipped with an exterior product from which may be derived several possible inner products. Exterior algebras and geometric algebras are special cases of this construction.

In mathematics, a **Hopf algebra**, named after Heinz Hopf, is a structure that is simultaneously a (unital associative) algebra and a (counital coassociative) coalgebra, with these structures' compatibility making it a bialgebra, and that moreover is equipped with an antiautomorphism satisfying a certain property. The representation theory of a Hopf algebra is principally commendable, since the existence of compatible comultiplication, counit, and antipode allows for the construction of tensor products of representations, trivial representations, and dual representations. This theory is accepted universally.

In mathematics, a **Clifford algebra** is an algebra generated by a vector space with a quadratic form, and is a unital associative algebra. The Clifford algebra is typically named after the English mathematician William Kingdon Clifford. As *K*-algebras, they generalize the real numbers, complex numbers, quaternions and several other hypercomplex number systems. The theory of Clifford algebras is intimately connected with the theory of quadratic forms and orthogonal transformations. Clifford algebras have significant applications in a variety of fields including geometry, theoretical physics and digital image processing.

3.6.2 Universal Algebra

Algebraic structures are defined through different configurations of axioms. Universal algebra abstractly studies such objects. One major dichotomy is between structures that are axiomatized entirely by identities and structures that are not. If all axioms defining a class of algebras are identities, then this class is a variety and it must not to be confused with algebraic varieties of algebraic geometry.

Identities are equations formulated using only the operations the structure allows, and variables that are tacitly universally quantified over the relevant universe. Identities contain no connectives, existentially quantified variables, or relations of any kind other than the allowed operations. The study of varieties is the significant portion of universal algebra. An algebraic structure in a variety may be understood as the quotient algebra of term algebra, also termed as 'Absolutely Free Algebra' divided by the equivalence relations generated by a set of identities. Consequently, a collection of functions with given signatures generate a free algebra, the term algebra *T*. Given a set of equational identities (the axioms), one may consider their symmetric, transitive closure *E*. The quotient algebra *T*/*E* is then the algebraic structure or variety. Thus, for example, groups have a signature containing two operators: the multiplication operator *m*, taking two arguments, and the inverse operator *i*, taking one argument, and the identity element *e*, a constant, which may be considered an operator that takes zero arguments. Given a (countable) set of variables *x*, *y*, *z*, etc., the term algebra is the collection of all possible terms involving *m*, *i*, *e* and the variables; therefore for example, *m* (*i* (*x*), *m* (*x*, *m* (*y*, *e*))) would be

an element of the term algebra. One of the axioms defining a group is the identity $m(x, i(x)) = e$; another is $m(x, e) = x$. The axioms can be represented as trees. These equations induce equivalence classes on the free algebra; the quotient algebra then has the algebraic structure of a group.

Some structures do not form varieties, because either:

1. It is essential that $0 \neq 1$, where '0' being the additive identity element and '1' being a multiplicative identity element, but this is a non-identity.
2. Structures, such as fields have some axioms that hold only for nonzero members of *S*. For an algebraic structure to be a variety, its operations must be defined for all members of *S*; there can be no partial operations.

Structures whose axioms unavoidably include non-identities are among the most significant ones in mathematics, for example fields and division rings. Structures with non-identities have problems while varieties do not. For example, the direct product of two fields is not a field, because $(1, 0) \cdot (0, 1) = (0, 0)$, but fields do not have zero divisors.

3.6.3 Properties of an Algebraic Structure

A non-empty set ***G*** with one or more binary operations is said to be an **algebraic structure**. Assume that '$*$' is a binary operation on ***G***. Then **(*G*, $*$)** is an algebraic structure.

The property of an algebraic structure can be defined on the property possessed by any of its operations. Following are some significant key properties of an algebraic system.

1. Associative and Commutative Laws

An operation '$*$' on a set is said to be associative or to satisfy the associative law if, for any elements ***a, b, c*** in ***S*** we have ***(a * b) * c = a * (b * c)***.

An operation '$*$' on a set ***S*** is said to be commutative or satisfy the commutative law if, ***a * b = b * a*** for any element ***a, b*** in ***S***.

Commutative Property of Addition: Remember that changing or altering the order of addends will not change the sum. The addends may be numbers or expressions, for example,

$(a + b) = (b + a)$ where a and b are any scalar.

Example 3.31: Given are the real numbers 5 and 2. Solve using the commutative law of addition.

Solution: Appling the commutative law of addition, we have,

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

We first obtain the value of Left Hand Side (LHS) of the rule.

$(a + b) = 5 + 2$

$= 7$

Then we obtain the value of Right Hand Side (RHS) of the rule.

$(b + a) = 2 + 5$

$= 7$

Because the sum is same, therefore the commutative property holds for addition.

Example 3.32: Given is the algebraic expression $x^2 + 2x$ where $x \in \mathbb{R}$. Solve using the commutative law of addition.

Solution: As per the commutative law of addition, we have,

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

Appling and putting the given expression, we have,

$(x^2 + x) = (x + x^2)$

Substitute the value $x = -1$ on both sides, i.e., Left Hand Side (LHS) and Right Hand Side (RHS), we obtain,

$(-1)^2 + (-1) = (-1) + (-1)^2$

$1 + (-1) = (-1) + 1$

$0 = 0$

Because the sum is same, therefore the commutative property holds for addition.

2. Commutative Property/Law of Multiplication

As per the commutative property or law of multiplication, changing or altering the order of factors will not change the product. The factors may be numbers or expressions. That is, $(a \times b) = (b \times a)$.

Example 3.33: Given are the real numbers 15, –2. Solve using the commutative law of multiplication.

Solution: As per the commutative law of multiplication, we have,

$(a \times b) = (b \times a)$

We first obtain the value of Left Hand Side (LHS) of the rule.

$(a \times b) = 15 \times (-2)$

$= -30$

Then we obtain the value of Right Hand Side (RHS) of the rule.

$(b \times a) = (-2) \times 15$

$= -30$

Because the product is same, therefore the commutative property holds for multiplication.

3. Identity Element and Inverse

Consider an operation '$*$' on a set $\boldsymbol{S}$. An element $\boldsymbol{e}$ in $\boldsymbol{S}$ is called an identity elements for $*$ if for any elements $\boldsymbol{a}$ in $\boldsymbol{S}$ - $\boldsymbol{a * e = e * a = a}$.

Generally, an element $\boldsymbol{e}$ is called a left identity or a right identity according to as $\boldsymbol{e * a}$ or $\boldsymbol{a * e = a}$ where $\boldsymbol{a}$ is any elements in $\boldsymbol{S}$.

Suppose an operation '$*$' on a set $\boldsymbol{S}$ does have an identity element $\boldsymbol{e}$. The inverse of an element in $\boldsymbol{S}$ is an element $\boldsymbol{b}$ such that: $\boldsymbol{a * b = b * a = e}$.

4. Cancellation Laws

An operation '$*$' on a set S is a said to satisfy the left cancellation law if, $a * b = a * c$ **implies** $b = c$ and is said to satisfy the right cancellation law if, $b * a = c * a$ **implies** $b = c$.

Check Your Progress

7. State the Cartesian product.
8. Define the equivalence relation.
9. What do you understand by partition of an equivalence relation?
10. What is algebraic structure?
11. State the Hopf algebra.

3.7 FUNCTIONS

In mathematics, a function is a binary relation between two sets that associates every element of the first set to exactly one element of the second set. Typical examples are functions from integers to integers, or from the real numbers to real numbers.

Functions were originally the idealization of how a varying quantity depends on another quantity. For example, the position of a planet is a *function of time*. Historically, the concept was elaborated with the infinitesimal calculus at the end of the 17th century, and, until the 19th century, the functions that were considered were differentiable, i.e., they had a high degree of regularity. The concept of a function was formalized at the end of the 19th century in terms of set theory, and this greatly enlarged the domains of application of the concept.

Typically, a function is a process or a relation that associates each element x of a set X, the domain of the function, to a single element y of another set Y (possibly the same set), the codomain of the function. It is customarily denoted by letters, such as f, g and h.

If the function is called f, this relation is denoted by $y = f(x)$ and which reads "f of x", where the element x is the *argument* or *input* of the function, and y is the *value of the function*, the *output*, or the *image* of x by f. The symbol that is used for representing the input is the variable of the function, for example f is a function of the variable x. Functions are also called *maps* or *mappings*, though some authors specify some distinction between 'Maps' and 'Functions'. A *function* is a rule that assigns each input exactly one output. We call the output the *image* of the input. The set of all inputs for a function is called the *domain*. The set of all allowable outputs is called the *codomain*. Functions are widely used in science, and in most fields of mathematics. It has been said that functions are, "The central objects of investigation" in most fields of mathematics.

Characteristically, a function is a relation from a set of inputs to a set of possible outputs where each input is related to exactly one output. This means that if the object x is in the set of inputs (called the *domain*) then a function f will map the object x to exactly one object $f(x)$ in the set of possible outputs (called the *codomain*).

As per Encyclopaedia Britannica, "Function, in mathematics, can be referred as an expression, rule, or law that defines a relationship between one variable (the independent variable) and another variable (the dependent variable)". Functions are ubiquitous in mathematics and are essential for formulating physical relationships in the sciences.

The modern definition of function was first given in 1837 by the German mathematician **Peter Dirichlet**, "If a variable y is so related to a variable x that whenever a numerical value is assigned to x, there is a rule according to which a unique value of y is determined, then y is said to be a **function** of the independent variable x".

This relationship is commonly symbolized as $y = f(x)$. In addition to $f(x)$, other abbreviated symbols, such as $g(x)$ and $P(x)$ are often used to represent functions of the independent variable x, especially when the nature of the function is unknown or unspecified.

Definition of Functions

A function or mapping from set A to set B is a 'Method' that pairs elements of set A with unique elements of set B and you denote $f : A \to B$ to indicate that f is a function from set A to set B.

B is called the *codomain* of the function f and A is called its *domain*. Also, for each element a of A, f defines an element b of B. Write it as $a \xrightarrow{f} f(a)$ or $a \xrightarrow{f} b$, $a \in A$, $b \in B$.

For example,

(*i*) The relation $f = \{(1, d), (2, c), (3, a)\}$ from $A = \{1, 2, 3\}$ to $B = \{a, c, d\}$ is a function from A to B. The domain of f is A and the codomain of f is B.

(*ii*) The relation $f = \{(a, b), (a, c), (b, d)\}$ from $A = \{a, b\}$ to $B = \{b, c, d\}$ is not a function.

Range of Function: Let $f : A \to B$ be a function. The range of the function $R(f) = \{f(a : a \in A\}$. (Note that $R(f) \subseteq B$).

In mathematics, a **real-valued function** is a function whose values are real numbers. On the other hand, it is a function that assigns a real number to each member of its *domain*. Real-valued functions of a real variable (commonly called real functions) and real-valued functions of several real variables are the main object of study of *calculus* and, more commonly, *real analysis*. In particular, many function spaces consist of *real-valued functions*.

Algebraic Structure of Real-Valued Function

Let $\mathcal{F}(X, \mathbb{R})$ be the set of all functions from a set X to real numbers $\mathbb{R}$. Because $\mathbb{R}$ is a field, $\mathcal{F}(X, \mathbb{R})$ may be turned into a *vector space* and a *commutative algebra* over the reals with the following operations:

- $f + g : x \mapsto f(x) + g(x)$ (Vector Addition)
- $\mathbf{0} : x \mapsto 0$ (Additive Identity)

- $cf : x \mapsto cf(x),\ c \in \mathbb{R}$ (Scalar Multiplication)
- $fg : x \mapsto f(x)g(x)$ (Pointwise Multiplication)

These operations extend to partial functions from X to $\mathbb{R}$ with the restriction that the partial functions $f + g$ and f, g are defined iff the domains of f and g have a non-empty intersection; in this case, their domain is the intersection of the domains of f and g.

Also, since $\mathbb{R}$ is an ordered set, there is a partial order

$$f \leq g \iff \forall x : f(x) \leq g(x),$$

on $\mathcal{F}(X, \mathbb{R})$, which makes $\mathcal{F}(X, \mathbb{R})$, a partially ordered ring.

Notes:

1. From above example: $R(f)$ is $\{d, c, a\}$,
2. Let $f : R \to R^+$ be $f(x) = x^2$ (R^+, the set of positive real numbers). Clearly, f is a function whose domain is the set of real numbers and the codomain is the set of positive real numbers.

$$R(f) = \{x^2 : x \in R\} = \{1, 4, 9, ...\}$$

Let $f : A \to B$ be a function f is said to be:

- ***One-to-One* (1–1) *Function:*** If $x_1 \neq x_2$ then, $f(x_1) \neq f(x_2)$, $\forall\ x_1, x_2 \in A$.

  or

  Whenever $f(x_1) = f(x_2)$ then, $x_1 = x_2$. This function is also known as injective function.
- ***Onto Surjective Function:*** If for every element y in the codomain B, atleast one element x in the domain A such that $f(x) = Y$.

  or

  If $R(f)$ = Codomain B.
- ***Bijective Function:*** If f is both 1–1 and onto function.
- ***Constant Function:*** If every element of the domain is mapped to a unique element of the codomain or the codomain consists of only one element.
- ***Into Function:*** If atleast one element of the codomain is not mapped by any element of the domain.
- ***Identify Function:*** If $f(x) = x$, $\forall\ x \in B$, in this case $A \leq B$.

  Sometimes, it is defined as $f : A \to A$ and $f(x) = x$, $\forall\ x \in A$.

For example,

1. Let $f : R \to R$ be a function defined as $f(x) = 2(x + 2)$: Clearly, f is 1 – 1 because if $2(x + 2) = 2(y + 2)$

$$\Rightarrow \quad 2x + 4 = 2y + 4$$
$$\Rightarrow \quad 2x = 2y \Rightarrow x = y$$
$$\therefore \quad f \text{ is } 1 - 1.$$

2. Define $f: R \to R^+$ by $f(x) = e^x$, $\forall\ x \in R$. Clearly, f is 1 – 1 because if $f(x_1) = f(x_2)$

$$\begin{aligned} \Rightarrow \quad e^{x_1} &= e^{x_2} \\ \Rightarrow e^{x_1 - x_2} &= 1 \\ \Rightarrow x_1 - x_2 &= 0 \\ \Rightarrow \quad x_1 &= x_2 \\ \therefore \quad f &\text{ is } 1-1. \end{aligned}$$

3. Let $A = \{5, 6, 7\}$ and $B = \{a, b\}$. Then the mapping $f: A \to B$ is defined as $f(5) = a$; $f(6) = b$; $f(7) = a$. Clearly, f is not 1 – 1. But f is onto.
4. Consider the Example (2). If $f: R \to R^+$, defined by $f(x) = e^x$ is onto. Let x be any element IR^+, then $\log y \in IR$ such that $f(\log y) = e^{\log y} = y$.
5. Define $f: Z^+ \to Z^+$ as $f(n) = n^2$, $\forall\ n \in Z^+$. Clearly, f is an into mapping (not mapped by any element of Z^+) and 1 – 1 mapping but f is not onto.
6. Define $f: Z \to Z$ by $f(n) = n + 1\ \ \forall\ n \in Z$. Clearly, f is 1 – 1 and onto. For if, (i) $f(n) = f(m) \Rightarrow n + 1, = m + 1 \Rightarrow n = m\ \therefore f$ is 1 – 1.
7. If n is any element of Z, then $n - 1 \in Z$ such that $f(n - 1) = n - 1 + 1 = n$. Hence f is onto.

Note: A one-one mapping of a set S onto itself is sometimes called a permutation of the set S.

Inverse Function

Let f be a bijective function from the set A to the set B. The inverse function of f is the function that is assigned to an element $b \in B$ the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence $f^{-1}(b) = a$, when $f(a) = b$ (Refer Figure 3.3).

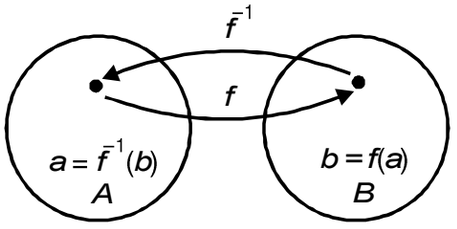


Fig. 3.3 *Inverse Function*

The function f^{-1} is the inverse function of f.

Note: A bijective function is called invertible since it can be defined as an inverse of this function.

Example 3.34: (i) Define $f: Z \to Z$ by $f(n) = n + 1$. Is f invertible, and if it is what is its inverse?

Solution: The function f has an inverse, since it is a bijective function. Let y be the image of x, so that $y = x + 1$. Then $x = y - 1$, i.e., $y - 1$ is the unique element of Z that is sent to y by f. Hence $f^{-1} = y - 1$.

(ii) Let $A = \{a, b, c\}$, and $B = \{5, 6, 7\}$. Define $F: A \to B$ as $f(a) = 5$; $f(b) = 6$; $f(c) = 7$. Is f invertible, and if it is what is its inverse?

Solution: Clearly the given function is bijective. The inverse function f^{-1} of f is given as $f^{-1}(5) = a; f^{-1}(6) = b; f^{-1}(7) = c$.

(*iii*) Define $f : Z \to Z$ by $f(x) = x^2$. Is f invertible?

Solution: Since $f(-2) = f(2) = 4$, f is not 1–1. If an inverse function were defined, it would have to assign two elements to 2. Hence f is not invertible.

Compositions of Functions

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the functions f and g denoted by $(f \circ g)$ is given in Figure 3.4 in such a way a that:

$$(f \circ g)(x) = f(g(x)) \quad \forall\, x \in A$$

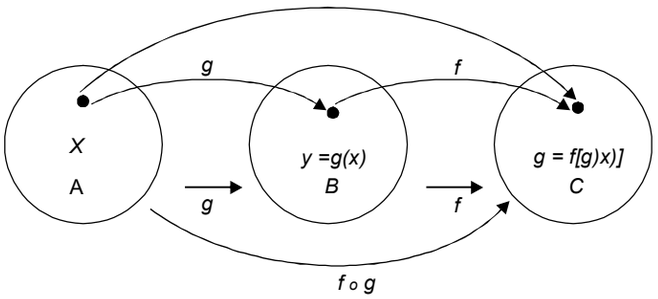


Fig. 3.4 *Composition of Function*

Example 3.35: Let $f : Z \to Z$ be a function defined by $f(x) = 2x + 3$. Let $g: Z \to Z$ be a function defined by $g(x) = 3x + 2$. Find (*i*) $f \circ g$ (*ii*) $g \circ f$.

Solution: Both $f \circ g$ and $g \circ f$ are defined. Further,

(*i*) $(f \circ g)(x) = f(g(x)) = f(3x + 2)$

$= 2(3x + 2) + 3 = 6x + 7$

(*ii*) $(g \circ f)(x) = g(f(x)) = g(2x + 3)$

$= 3(2x + 3) + 2 = 6x + 11$

Eventhough $f \circ g$ and $g \circ f$ are defined, $f \circ g$ and $g \circ f$ need not be equal, i.e., the commutative law does not hold for the composition of functions.

Example 3.36: Let $A = \{1, 2, 3\}$, $B = \{x, y\}$, $C = \{a\}$. Let $f: A \to B$ be defined by $f(1) = x; f(2) = y; f(3) = x$. Let $g: B \to C$ be defined by $g(x) = a$; $g(y) = a$.

Find (*i*) $f \circ g$, if possible (*ii*) $g \circ f$, if possible.

Solution: The solution is obtained as follows:

(*i*) $(f \circ g)(x) = f(g(x))$, but f cannot be applied on C and hence $f \circ g$ is meaningless.

(*ii*) $(g \circ f) : A \to C$ is meaningful. Now $(g \circ f)(x) = g(f(x))$, $\forall\, x \in A$.

$\therefore \quad (g \circ f)(1) = g(f(1)) = g(x) = a$

$(g \circ f)(2) = g(f(2)) = g(y) = a$

$(g \circ f)(3) = g(f(3)) = g(x) = a$

NOTES

Result: If $f : A \to B$, $g: B \to C$ and $h: C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof: $[(h \circ g) \circ f](x) = (h \circ g)(f(x))$

$$= h[(g(f(x)] \quad ...(3.1)$$

and $[h \circ (g \circ f)](x) = h[(g \circ f)(x)]$

$$= h[g(f(x))] \quad ...(3.2)$$

From Equations (3.1) and (3.2), $(h \circ g) \circ f = h \circ (g \circ f)$

Result: Let $f : A \to B$ and $g : B \to C$. Then,

(*i*) $g \circ f$ is onto, if both f and g are onto.

(*ii*) $g \circ f$ is 1 – 1, if both f and g are 1 – 1.

Proof:

(*i*) Let $z \in C$. Since $g : B \to C$ is onto, an element $y \in B$ such that $g(y) = z$. Since $f : A \to B$ is onto, for an element $x \in B$, such that $f(x) = y$.

$\therefore (g \circ f)(x) = g(f(x)) = g(y) = z$.

$\therefore (g \circ f)$ is onto.

(*ii*) Let $x_1 \neq x_2$ be two elements in A. Since $f : A \to B$ is one-one, and $f(x_1) \neq (x_2)$, $g(f(x_1)) = g(f(x_2))$. Thus, $g \circ f$ is one-one. In B, since $g: B \to C$ is one-one and $f(x_1) \neq (x_2)$.

3.7.1 Graph of the Function

Functions were originally the idealization of how a varying quantity depends on another quantity. The concept of a function was formalized at the end of the 19th century in terms of set theory, and this greatly enlarged the domains of application of the concept.

A **function** is a process or a relation that associates each element x of a set X, the **domain** of the function, to a single element y of another set Y (possibly the same set), the **codomain** of the function. It is customarily denoted by letters, such as f, g and h.

If the function is called f, then this relation is denoted by $y = f(x)$ and is read as "f of x", where the element x is the argument or input of the function, and y is the value of the function, the output or the image of x by f. The symbol that is used for representing the input is the variable of the function, for example f is a function of the variable x.

A function is uniquely represented by the set of all pairs $(x, f(x))$, called the graph of the function. When the domain and the codomain are sets of real numbers, each such pair may be thought of as the Cartesian coordinates of a point in the plane. The set of these points is termed as the graph of the function and is a standard means of illustrating the function.

Consequently, a function is a process that associates each element of a set X, to a single element of a set Y.

Range of a function, a set containing the output values produced by a function.

In mathematics, the range of a function may refer to either of two closely related concepts – (*i*) The Codomain of the Function and (*ii*) The Image of the Function. The image of a function is always a subset of the codomain of the function.

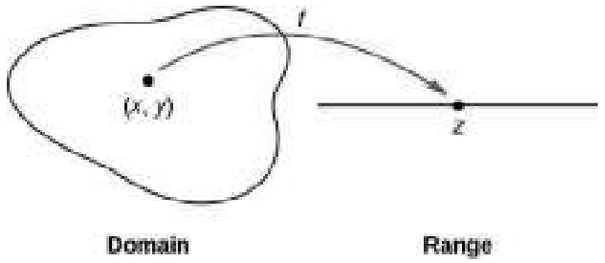
If $f : X \to Y$ then the set X is called the domain of definition or simply the domain of the function f.

The set of all elements $y \in Y$ which corresponds to some $x \in X$, is called the range of the function f, and is denoted by $f(X)$, i.e., $f(X) = \{f(x) : x \in X\} \subset Y$. The set Y whose subset is $f(X)$ is called the codomain of f.

The domain is represented by the symbols $D(f)$ and Df, while the range of function is written as $R(f)$ or Rf.

Domain and Range of a Function of Two Variables

Characteristically, if a function of two variables $z = (x, y)$ specifically maps each ordered pair (x, y) in a subset D of the real plane R^2 to a unique real number z, then the set D is termed as the **domain** of the **function**. The **range** of '*f*' is defined as the set of all real numbers z that has at least one ordered pair of the form $(x, y) \in D$ such that $f(x, y) = z$ as shown below in the given figure.

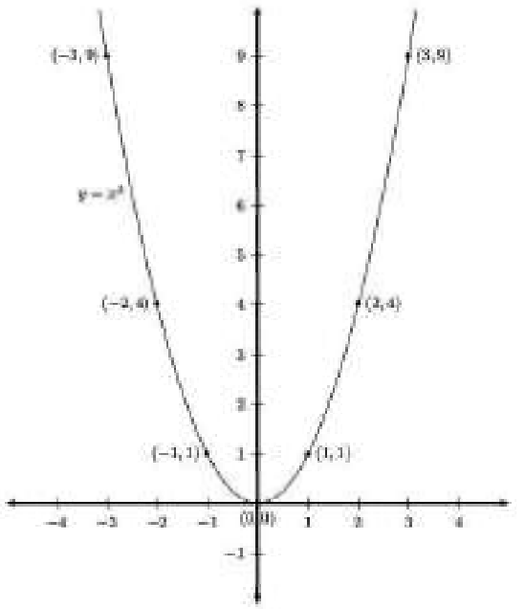


The above figure illustrates the domain of a function of two variables which consists of ordered pairs (x, y).

Graphing Functions of Two Variables

A **graph** is referred as a structure which typically represents a set of objects in which certain pairs of the objects are somehow related. The objects resemble to mathematical abstractions termed as vertices or nodes or points and each of the related pairs of vertices is termed as an edge or link or line. Usually, a graph can be accurately depicted in the diagrammatic form either as a set of dots or circles for the vertices that are joined by lines or curves for the edges.

Typically, the graph of a function f is the set of all points (x, y) that uniquely satisfies $y = f(x)$. Alternatively, we can state that at each x-value we can connect the function for determining the corresponding y-value. For example, the graph of $f(x) = x^2$ can be drawn for evaluating the function at a few specified points. Then, we plot each point (x, x^2) on the coordinate plane by means of connecting the dots through a smooth curve as shown below in the given graph.



3.8 COUNTABLE AND UNCOUNTABLE SETS

In this section we will talk about the concept of countable and uncountable sects. The simple but profound definition is that a set is countable if its elements can be matched up with the natural number, also referred to as the counting numbers, i.e, the infinite set 1, 2, 3, 4, 5... A set is uncountable if it is not countable.

Countable Sets

A countable set in mathematics has some cardinality, which means it has some finite number of elements that can be counted. It is a subset of natural numbers. A set in which number of its elements can not be counted are termed as uncountable. There is some difference of opinion on this. According to definition, a set S is termed **countable** if there is a function which is injective and symbolically it can be written as, $f: S \to N$, i.e., from a set S to the set of natural numbers $N = \{0, 1, 2, 3, \ldots.\}$. In case f is also onto, then it is a bijective function and the set S is termed as **countably infinite.** The following theorems define the various types of countable sets.

Theorem 3.1: In a set S, the following statements are equivalent:

1. If S is countable, then an injective function exists, which is given as:
   $$f: S \to N$$
2. Either S is empty set or there exists a surjective function then it is given as:
   $$g: N \to S$$
3. Either S is finite or a bijection exists then it is given as:
   $$h: N \to S$$

Theorem 3.2: The Cartesian product of finitely many countable sets is countable.

Theorem 3.3: Every subset of a countable set is countable. Basically, every infinite subset of a countably infinite set is countably infinite.

The set of prime numbers is countable by mapping the nth prime number to n.

Theorem 3.4: *Q,* the set of all rational numbers is countable.

Q is the set of all fractions a/b. Here, a and b are integers and $b > 0$. We can map this onto, the subset of ordered triples of natural numbers (a, b, c) such that $a \geq 0$, $b > 0$, where a and b are coprime.

Theorem 3.5: The union of countably many countable sets is countable. (Assuming the axiom of countable choice).

This works, only if, the sets $a, b, c, \ldots$ are disjoint, else the union is even smaller and is therefore, also countable.

Theorem 3.6: The set of all sequences of finite length of natural numbers is countable.

This is a set which is the union of sequences of Length 1, Length 2, Length 3, etc., and each one of these is a countable set. So, this is a countable union of countable sets and thus, countable.

Theorem 3.7: The set of all finite subsets of the natural numbers is countable.

If there is a finite subset, elements can be ordered into a finite sequence. Thus, this constitute countably many finite sequences, and hence, countably many finite subsets.

Uncountable Set

In mathematics, an **uncountable set** is an infinite set containing too many elements to be countable. The uncountability is closely related to its cardinal number. A set is uncountable if the cardinal number of the set is more than that of the natural numbers.

Uncountability has many equivalent characterizations. Let there be a set X. This set is uncountable iff any of the following conditions holds:

- There is no injective function $f: X \to N$, where N is the set of natural numbers.
- X is not null and any ω-sequence of elements of X has not even one element of X. In other words, there is no surjective function $g: N \to X$.
- The cardinality of X is neither finite nor equal to $\aleph_0$ (this symbol is called aleph-null, and is called the cardinality of the natural numbers).
- The set X has cardinality strictly more than $\aleph_0$.

Finite and Infinite Sets

A set is finite, if it has a finite number of elements. The elements of such a set can be counted by a finite number. The number of elements in a finite set A is denoted by $n(A)$. Here, n is a finite positive integer.

If a set has an infinite number of elements it is an infinite set. The elements of such a set cannot be counted by a finite number. A set of points along a line or in a plane is called a point set. A finite set has a finite subset. An infinite set may have an infinite subset.

Example 3.37: A set is given as $F = \{a, b, x, 0, 1, 8, p\}$. Find if it is a finite set.

Solution: Yes, it is a finite set because there are 7 elements in the set, $n(A) = 7$.

Example 3.38: There is a set defined as $S = \{x: x \text{ is a grain of sand on the sea-shore}\}$. Is it a finite set?

Solution: Yes. Although counting grains of sand is not practical, but it can be counted indirectly. There is a definite number, howsoever large it may be.

Example 3.39: Is set $R = \{x: x \text{ is a natural number}\}$ a finite set?

Solution: No. Set of natural numbers are $\{1, 2, 3, \ldots..\}$. This is an infinite set.

Example 3.40: A set is given as $P = \{x: x \text{ is a real number between 2 and 3}\}$. Is P a finite set?

Solution: No. The two numbers are finite but real numbers lying between these numbers are infinite.

Example 3.41: Is set $D = \{x: x \text{ is a multiple of 2}\}$ an infinite set?

Solution: Yes. There can be infinite numbers that are multiple of 2.

Example 3.42: A set is formed by English alphabets. Is it an infinite set?

Solution: No. Because English alphabets are 26 in numbers which is finite number.

Example 3.43: A set is given as set of points on number line in between 10 to 20. Is it a finite set?

Solution: No. There are infinite numbers of points and this point set is infinite.

Example 3.44: A point set in a plane is shown by the set of points in a plane figure. Is it a finite set?

Solution: Yes. There are infinite number of points.

3.9 GROUPS

Definition: A non empty set G, together with a binary compsition $*$ (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 $e \in G$, such that,

$$a * e = e * a = a \quad \text{for all } a \in G$$

(e is then called *identity*)

(*iii*) *Existence of Inverse* : For every $a \in G$, $\exists\ a' \in G$ (depending upon a) such that,

$$a * a' = a' * a = e$$

(a' is then called inverse of a)

Notes:

1. 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*.
2. If, in addition to the above postulates, G also satisfies the *commutative law*

   $a * b = b * a$ for all $a, b \in G$

   then G is called an **Abelian group** or *a* **commutative group**.
3. 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 an *infinite 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 cases of systems that form groups (or do not form groups).

Case 1: The set **Z** of integers forms an Abelian group with respect to 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 inverse elements. Commutativity again being obvious.

Case 2: One can easily check, as in the previous case, that sets **Q** of rationals, **R** of real numbers would also form Abelian groups with respect to addition.

Case 3: Set of integers, with respect to usual multiplication does not form a group, although closure, associativity, identity conditions hold.

Note 2 has no inverse with respect to multiplication as there does not exist any integer a such that, $2 . a = a . 2 = 1$.

Case 4: The set G of all +ve irrational numbers together with 1 under multiplication does not form a group as closure does not hold. Indeed $\sqrt{3} . \sqrt{3} = 3 \notin G$, although one would notice that other conditions in the definition of a group are satisfied here.

Case 5: 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.

Case 6: Set of all 2×2 matrices over integers under matrix addition would be another example of an Abelian group.

Case 7: 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,

$$\frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2}$$ will be inverse of $a + ib$.

Note: $a + ib$ non-zero means that not both a and b are zero. Thus $a^2 + b^2 \neq 0$.

Case 8: The set G of all nth 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 $r = 1, 2, ..., n$ 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 is an nth root of unity

$\Rightarrow$ $ab \in G \Rightarrow$ closure holds.

Associativity of multiplication is true in complex numbers.

Again, since $1.\ a = a\ .\ 1 = a$, 1 will be identity.

Also for any $a \in G$, $\frac{1}{a}$ will be its inverse as $\left(\frac{1}{a}\right)^n = \frac{1}{a^n} = 1$.

So, inverse of $e^2\pi^{ir/n}$ is $e^{2\pi i(n-r)/n}$ and identity is $e^2\pi^{i0/n} = 1$

Commutativity being obvious, we find G is an Abelian group.

As a particular case, if $n = 4$ then G is $\{1, -1, i, -i\}$

Case 9: (*i*) Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Define product on G by usual multiplication together with

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

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*)).

Case 10: Let $G =$ $\{(a, b) \mid a, b$ 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 $(1/a, -b/a)$ will be inverse of any element (a, b).

G is not Abelian as

$$(1, 2) * (3, 4) = (3, 4 + 2) = (3, 6)$$
$$(3, 4) * (1, 2) = (3, 6 + 4) = (3, 10).$$

Case 11 (a): 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.

It is called the general linear group of 2×2 matrices over reals and is denoted by $GL(2, \mathbf{R})$.

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 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

One can generalize and prove

(b) If G be the set of all $n \times n$ invertible matrices over reals, then G forms a group under matrix multiplication.

Case 12: Let $G = \{2^r \mid r = 0, \pm 1, \pm 2, ...\}$

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.

Case 13: *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 negative 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 generalize this result to

$$G = \{0, 1, 2, ..., n - 1\}$$

under addition modulo n where 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 $\mathbf{Z}_n$.

Case 14: 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 number p such that, $p \mid c$ 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, n 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 $\quad a \otimes b = r_1$ means

$$ab = q_1 n + r_1$$

Thus $\quad ab - q_1 n = r_1$

$$\Rightarrow (ab - q_1 n)c = r_1 c = nq_2 + r_2$$

$$\Rightarrow \quad (ab)c = r_2 + nq_2 + nq_1 c = n(q_1 c + q_2) + r_2$$

Or that r_2 is the least non-negative remainder got by dividing $(ab)c$ by n.

Similarly, if $a \otimes (b \otimes c) = r_3$ then we can show that r_3 is the least non negative 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

$$a \otimes 1 = 1 \otimes a = a \quad \text{for all } a \in G$$

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 such that, $ax + ny = 1$

By division algorithm, we can write

$$x = qn + r, \quad \text{where } 0 \le r < n$$

$$\Rightarrow \quad ax = aqn + ar$$

$$\Rightarrow \quad ax + ny = aqn + ar + ny$$

$$\Rightarrow \quad 1 = aqn + ar + ny$$

Or that $\quad ar = 1 + (-aq - y)n$

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 such that, $p \mid r$, $p \mid n$

$$\Rightarrow p \mid qn \text{ and } p \mid r$$

$$\Rightarrow p \mid qn + r$$

$$\Rightarrow p \mid x$$

$$\Rightarrow p \mid ax \text{ also } p \mid ny$$

$$\Rightarrow p \mid ax + ny = 1$$

Which is not possible. Thus r, n are coprime 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 U_n or $U(n)$ and call it the group of integers under multiplication modulo n.

Note: Suppose $n = p$, a prime, then since all the integers 1, 2, 3, ..., $p - 1$ are co-prime to p, these will all be members of G. One can show that

$$G = \{2, 4, 6, ..., 2(p - 1)\}$$

Where $p > 2$ is a prime forms an Abelian group under multiplication modulo $2p$.

Case 15: 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 $1 * (1 * 2) = 1 * 1 = 0$

But $(1 * 1) * 2 = 0 * 2 = 2$

Case 16: Let $S = \{1, 2, 3\}$ and let $S_3 = A(S)$ = set all permutations of S. 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 $fog \neq gof$. This would, in fact, be the smallest non Abelian group.

Note: 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* 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,

$$e'e = ee' = e$$

NOTES

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
$$\begin{aligned}(ab)\,(b^{-1}a^{-1}) &= [(ab)\,b^{-1}]\,a^{-1}\\ &= [(a(bb^{-1})]\,a^{-1}\\ &= (ae)\,a^{-1} = aa^{-1} = e\end{aligned}$$

Similarly, $(b^{-1}a^{-1})\,(ab) = e$

and thus the result follows.

(5) Let $ab = ac$, then

$$\begin{aligned}b &= eb = (a^{-1}a)b\\ &= a^{-1}(ab) = a^{-1}\,(ac)\\ &= (a^{-1}\,a)c = ec = c\end{aligned}$$

Thus $ab = ac \Rightarrow b = c$

Which is called the left cancellation law.

One can similarly, prove the right cancellation law.

Case 17 (*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 then to verify that $fog = goh$

But $f \neq h$.

(*b*) If we consider the group in case 10, we find

$$(1, 2) * (3, 4) = (3, 6) = (3, 0) * (1, 2)$$

But $(3, 4) \neq (3, 0)$

Hence, we notice, cross cancellations *may not* hold in a group.

Theorem 3.8: 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 $ax = b$

$$\Rightarrow \quad a^{-1}(ax) = a^{-1}b$$
$$\Rightarrow \quad ex = a^{-1}b$$

Or $x = a^{-1}b$

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

$$ax_1 = b \text{ and } ax_2 = b$$

$$\Rightarrow \quad ax_1 = ax_2$$

$$\Rightarrow \quad x_1 = x_2 \quad \text{by left cancellation}$$

Showing that the solution is unique.

Similarly, $y = ba^{-1}$ will be unique solution of the equation $ya = b$.

Theorem 3.9: 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 $\exists\ e, f \in G$, such that, $ae = a$

$$fa = a$$

Let now $b \in G$ be *any* element then again by (2) $\exists$ some x, y in G such that,

$$ax = b$$

$$ya = b.$$

Now $ax = b \quad \Rightarrow f.(a\,.\,x) = f\,.\,b$

$$\Rightarrow (f\,.\,a)\,.\,x = f\,.\,b$$

$$\Rightarrow a\,.\,x = f\,.\,b$$

$$\Rightarrow b = f\,.\,b$$

Again $y\,.\,a = b \quad \Rightarrow (y\,.\,a)\,.\,e = b\,.\,e$

$$\Rightarrow y\,.\,(a\,.\,e) = b\,.\,e$$

$$\Rightarrow y\,.\,a = be$$

$$\Rightarrow b = be$$

Thus we have $b = fb$ ...(3.3)

$b = be$ ...(3.4)

For any $b \in G$

Putting $b = e$ in Equation (3.3) and $b = f$ in Equation (3.4) we get

$$e = fe$$

$$f = fe$$

$$\Rightarrow \quad e = f.$$

Hence $ae = a = fa = ea$

i.e., $\exists\ e \in G$, such that, $ae = ea = a$

$\Rightarrow$ e is identity.

Again, for any $a \in G$, and (the identity) $e \in G$, the equations $ax = e$ and $ya = e$ have solutions.

NOTES

Let the solutions be $x = a_1$, and $y = a_2$

Then $aa_1 = e, \quad a_2a = e$

Now $a_1 = ea_1 = (a_2a)a_1 = a_2(aa_1) = a_2e = a_2.$

Hence $aa_1 = e = a_1a$ 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.

Note: 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

$a \,.\, (b \,.\, c) = (a \,.\, b) \,.\, c$ 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 Case 15 is not a semi group.

Theorem 3.10: 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 3.11: A finite semi-group in which cancellation laws hold is a group.

Proof: Let $G = \{a_1, a_2, ..., a_n\}$ be a finite semi-group in which cancellation laws hold.

Let $a \in G$ be any element, then by closure property

$aa_1, aa_2, ..., aa_n$

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 $aa_1, aa_2, ..., aa_n$ 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 3.2).

Note: 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 3.12: A finite semi-group is a group if and only if it satisfies cancellation laws.

Proof: Follows by previous theorem.

Definition: A non empty set G together with a binary composition '.' is said to form a *monoid* if

(*i*) $a(bc) = (ab)c \quad \forall\ a, b, c \in G$
(*ii*) $\exists$ an element $e \in G$ such that, $ae = ea = a \quad \forall\ a \in G$

e is then called identity of G. It is easy to see that e is unique.
So all groups are monoids and all monoids are semi groups.

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 3.13: A system $< G, . >$ forms a group if and only if

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$
(*ii*) $\exists\ e \in G$, *such that*, $ae = a$ *for all* $a \in G$
(*iii*) *for all* $a \in G$, $\exists\ a' \in G$, *such that*, $aa' = e$.

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*) $\exists\ a' \in G$, such that, $aa' = e$
$\therefore$ For $a' \in G$, $\exists\ a'' \in G$, such that, $a'a'' = e$ (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 $a \in G$, $\exists\ a' \in G$, such that, $aa' = a'a = e$
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.

Theorem 3.14: A system $< G, . >$ forms a group if and only if

(*i*) $a(bc) = (ab)c$ *for all* $a, b, c \in G$

(*ii*) $\exists\ e \in G$, *such that,* $ea = a$ *for all* $a \in G$

(*iii*) *for all* $a \in G$, $\exists$ *some* $a' \in G$, *such that*, $a'a = e$.

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?

Proof: The answer to which is provided by the following illustration.

Let G be a finite set having at least two elements. Define '.' on G by

$$ab = b \quad \text{for all } a, b \in G$$

Then clearly associativity holds in G.

Let $e \in G$ by any fixed element.

Then as $ea = a$ 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 negative integer then $n = -m$, where m is positive and we define $na = -ma = (-a) + (-a) + \ldots + (-a)$ m times.

Example 3.45: If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \le r \le n$, such that, $a^r = e$.

Solution: Since $o(G) = n$, G has n elements.

Let $a \in G$ be any element. By closure property $a^2, a^3, \ldots$ all belong to G.

Consider $e, a, a^2, \ldots, a^n$

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 $a, a^2, \ldots, a^n$ 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 $a^i = a^j$

$\Rightarrow$ $a^i \,.\, a^{-j} = a^j \,.\, a^{-j}$

$\Rightarrow \quad a^{i-j} = e$ where $1 \le i - j \le n$.

Putting $i - j = r$ gives us the required result.

Example 3.46: 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.

Example 3.47: 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 show that G is Abelian.

Solution: Let $n, n+1, n+2$ be three consecutive integers for which the given condition holds. Then for any $a, b \in G$,

$$(ab)^n = a^n b^n \quad ...(1)$$

$$(ab)^{n+1} = a^{n+1} b^{n+1} \quad ...(2)$$

$$(ab)^{n+2} = a^{n+2} b^{n+2} \quad ...(3)$$

Now $(ab)^{n+2} = a^{n+2} b^{n+2}$

$\Rightarrow (ab)(ab)^{n+1} = a^{n+2}\ b^{n+2}$

$\Rightarrow (ab)(a^{n+1} b^{n+1}) = a^{n+2}\ b^{n+2}$

$\Rightarrow ba^{n+1} = a^{n+1} b$ (using cancellation) ...(4)

Similarly $(ab)^{n+1} = a^{n+1} b^{n+1}$

Gives $(ab)(ab)^n = a^{n+1} b^{n+1}$

i.e., $(ab)(a^n b^n) = a^{n+1} b^{n+1}$

$\Rightarrow ba^n = a^n b$

$\Rightarrow ba^{n+1} = a^n ba$

$\Rightarrow a^{n+1} b = a^n ba$ using Equation (4)

$\Rightarrow ab = ba.$

Hence G is Abelian.

Note: 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.

Example 3.48: Suppose $(ab)^n = a^n b^n$ for all $a, b \in G$ where $n > 1$ is a fixed integer.

Show that (*a*) $(ab)^{n-1} = b^{n-1} a^{n-1}$

(*b*) $a^n\ b^{n-1} = b^{n-1} a^n$

(*c*) $(aba^{-1}b^{-1})^{n(n-1)} = e$ *for all* $a, b \in G$

Solution: (*a*) We have

$$[b^{-1}(ba)b]^n = b^{-1}(ba)^n b$$

And $[b^{-1}(ba)b]^n = (ab)^n$

$(ab)^n = b^{-1}(ba)^n b$

$\Rightarrow \quad (ab)^{n-1}ab = b^{-1}(b^n a^n)b$

$\Rightarrow \quad (ab)^{n-1} = b^{n-1}a^{n-1}$ for all $a, b \in G$

(*b*) Now $(a^{-1}b^{-1}ab)^n = a^{-n}b^{-n}a^n b^n$

And $(a^{-1}b^{-1}ab)^n = a^{-n}(b^{-1}ab)^n$

$= a^{-n}b^{-1}a^n b$

$\therefore \quad a^{-n}b^{-n}a^n b^n = a^{-n}b^{-1}a^n b$

$\Rightarrow \quad a^n b^{n-1} = b^{n-1}a^n$ for all $a, b \in G$

(*c*) Consider $(aba^{-1}b^{-1})^{n(n-1)}$

$= [(aba^{-1}b^{-1})^{n-1}]^n$

$= [(ba^{-1}b^{-1})^{n-1}a^{n-1}]^n$ by (*i*)

$= [ba^{-(n-1)}b^{-1}a^{n-1}]^n = [b(a^{-(n-1)}b^{-1}a^{n-1})]^n$

$= b^n(a^{-(n-1)}b^{-1}a^{n-1})^n = b^n a^{-(n-1)}b^{-n}a^{n-1}$

$= a^{-(n-1)}b^n b^{-n}a^{n-1}$ by (*ii*)

$= e$ for all $a, b \in G$.

Example 3.49: 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

$(a^m b^n)^{mx} = (a^m b^n)(a^m b^n).....(a^m b^n)$ mx times

$= a^m(b^n a^m b^n.....b^n a^m)b^n$

$= a^m(b^n a^m)^{mx-1}b^n$

$= a^m(b^n a^m)^{mx}(b^n a^m)^{-1}b^n$

$= a^m c^m(b^n a^m)^{-1}b^n$ 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 $(a^m b^n)^{mx+ny} = (b^n a^m)^{mx+ny}$

$\Rightarrow \quad a^m b^n = b^n a^m$ for all $a, b \in G$ ...(1)

Now $ab = a^{mx+ny}\ b^{mx+ny}$

$= a^{mx} . (a^{ny}\ b^{mx})b^{ny}$

$= a^{mx}(a^m\ k^m)b^{ny}$ where $d = a^y$, $k = b^x$

$= a^{mx}(k^m\ d^n)b^{ny}$ 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.

Note: In the following Theorem, we give another proof to Theorem 3.13 done earlier.

3.9.1 Properties of Groups

A **group** G is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property. The operation with respect to which a group is defined is often called the *group operation*, and a set is said to be a group 'Under' this operation. Elements A, B, C, ... with binary operation between A and B denoted AB form a group iff:

1. **Closure:** If A and B are two elements in G, then the product AB is also in G.
2. **Associativity:** The defined multiplication is associative, i.e., for all $A,B, C \in G$, $(AB)C = A(BC)$.
3. **Identity:** An identity For every element $A \in G$.
4. **Inverse:** For each element A of G, the set contains an element $B=A^{-1}$.

A group is a monoid each of whose elements is invertible. A group must contain at least one element, with the unique (up to isomorphism) single-element group known as the trivial group.

The study of groups is known as *group theory*. If there are a finite number of elements, the group is called a *finite group* and the number of elements is called the group order of the group. A subset of a group that is closed under the group operation and the inverse operation is called a subgroup. Subgroups are also groups, and many commonly encountered groups are in fact special subgroups of some more general larger group.

Theorem 3.15: Identity element of a group is unique.

Proof: Consider a group (G, *). Let e_1 and e_2 be two identity elements of this group.

$\therefore\ e_1 * e_2 = e_2 = e_2 * e_1$ [$\because e_1$ is the identity element.]

And $e_1 * e_2 = e_1 = e_2 * e_1$ [$\because e_2$ is the identity element.]

Thus, $e_1 = e_2$

$\Rightarrow$ The identity element of group is unique.

Theorem 3.16: Inverse of each element of a group is always unique.

Proof: Consider a group (G, $*$) with the identity element e and let a be arbitrary element of G.

$\therefore\ a^{-1} \in G$ [$\because$ G is a group]

If possible suppose b_1 and b_2 are two inverses of a.

$\therefore\ a * b_1 = e = b_1 * a$ and $a * b_2 = e = b_2 * a$

Now, $b_1 = b_1 *$ [$\because e$ is the identity of G]

$= b_1 * (a * b_2) = (b_1 * a) * b_2 = e * b_2 = b_2$

$\therefore$ Each element of a group has unique inverse.

Theorem 3.17: The inverse of the product of two elements of a group is equal to the product of their inverses taken in the reverse order.

Proof: Let $a, b \in G$ and a^{-1} and b^{-1} be the inverses of a and b respectively.

NOTES

Then,

$a\,a^{-1} = e = a^{-1}a$ and $b\,b^{-1} = e = b^{-1}b$

Consider, $(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1}$ [By Associativity]

$= a(e)\,a^{-1} = a\,a^{-1} = e$ [$\because b\,b^{-1} = e$]

Again consider, $\left(b^{-1}a^{-1}\right)(ab) = b^{-1}(a^{-1}a)\,b$

$= b^{-1}(e)\,b = b^{-1}b = e$ [$\because a\,a^{-1} = e$ and $b\,b^{-1} = e$]

Hence, $(ab)^{-1} = b^{-1}a^{-1}$

Theorem 3.18: If $a, b, c \in$ G and * is the binary operation defined on G, then

(i) $a * b = a * c \Rightarrow b = c$ if $a \neq 0$ [Left cancellation law]

(ii) $b * a = c * a \Rightarrow b = c$ if $a \neq 0$ [Right cancellation law]

Proof: (i) As G is a group defined with binary operation * and $a \in$ G, thus a^{-1} exist.

Consider $a * b = a * c$

$\Rightarrow a^{-1} * (a * b) = a^{-1} * (a * c)$ [Pre-multiplying both sides by a^{-1}]

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ [By Associativity]

$\Rightarrow e * b = e * c \Rightarrow b = c$

Similarly we can prove (ii).

Theorem 3.19: If (G, .) is a group, then the equations $a.x = b$ and $y.a = b$ have unique solution for all $a, b, x, y \in$ G.

Addition Modulo *m*: If a and b are any integers and m is a fixed positive integer, then **addition modulo *m*** is defined as $a +_m b = r$, where $0 \leq r < m$ and r is the least non-negative remainder when $a + b$ is divided by m. For example, $10 +_6 4 = 2$, as 2 is the remainder when $10 + 4 = 14$ is divided by 6.

Multiplication Modulo *m*: If a and b are any integers and m is a fixed positive integer, then **multiplication modulo *m*** is defined as $a \times_m b = r$, where $0 \leq r < m$ and r is the least non-negative remainder when ab is divided by m. For example, $7 \times_5 4 = 3$, as 3 is the remainder when $7 \times 4 = 28$ is divided by 5.

Example 3.50: Show that the set G = $\{a + b\sqrt{2} : a, b \in \text{Q}\}$ is a group under addition.

Solution: (i) Closure: Let $x, y \in$ G $\Rightarrow x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$ where $a, b, c, d \in$ Q.

$\therefore x + y = \left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = (a + c) + (b + d)\sqrt{2}$

$\Rightarrow x + y \in$ G for all $x, y \in$ G [$\because a, c \in$ Q $\Rightarrow a + c \in$ Q.

Similarly $b + d \in$ Q]

Thus, G is closed with respect to addition.

(ii) Associativity: G is associative under addition as the set of all the real numbers, R is associative under addition and G $\subset$ R.

(iii) Existence of identity: There exists $0 \in G$, such that $x + 0 = a + b\sqrt{2} + 0 = a + b\sqrt{2} = x$

Similarly, $0 + x = 0 + a + b\sqrt{2} = a + b\sqrt{2} = x$. Therefore, 0 is the identity element of G.

(iv) Existence of inverse: Let $x \in G \Rightarrow x = a + b\sqrt{2} \in G$ where $a, b \in Q$.
As $a, b \in Q \Rightarrow -a, -b \in Q$

$\therefore -x = -a + (-b)\sqrt{2} \in G$

We have $x + (-x) = (a + b\sqrt{2}) + \left(-a + (-b)\sqrt{2}\right) = 0 + 0\sqrt{2} = 0$

Similarly, $-x + x = 0 \Rightarrow -x$ is the inverse x and also $-x \in G$. Hence G is a group with respect to addition.

Example 3.51: Show that the set $G = \{-1, 1, -i, i\}$ is a group with respect to multiplication.

Solution: Firstly, we make the composition table:

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(i) Closure: G is closed with respect to multiplication as all the entries in the composition table are elements of G.

(ii) Associativity: The elements of G are complex numbers and the complex numbers are associative under multiplication.

(iii) Existence of identity: 1 is the identity of G as $1 \in G$ and $a.1 = a = 1.a$ for all $a \in G$.

(iv) Existence of inverse: From the table, the inverse of $1, -1, i$ and $-i$ are the elements $1, -1, -i$ and i respectively and all of them belongs to G. Thus, inverse exists.

Hence, $(G, \times)$ is a group.

Order of an Element

Let $(G, \cdot)$ be a group with identity element e and $a \in G$. If for $a \in G$, there is least positive integer m satisfying $a^m = e$ then m is called the **order** of a. It is denoted by $o(a)$.

Notes: 1. The order of a is said to be infinite or zero if there does not exists any positive integer m such that $a^m = e$.

2. If there exists a positive integer m such that $a^m = e$, then $o(a) \leq m$.

3. The only element of order one is the identity element.

NOTES

3.10 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 the following definition:

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 subsets $\{e\}$ 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).

Notice that $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ Mod 5 is not a subgroup of **Z** under addition as addition modulo 5 is not the composition of **Z**. Similarly, $\mathbf{Z}_5$ is not a subgroup of $\mathbf{Z}_6$, etc.

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 3.20: 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 $a, b, c \in H \Rightarrow a, b, c \in G \quad \Rightarrow \quad a(bc) = (ab)c$

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 3.21: 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 (If $f: A \to B$ is one-one and onto, then $f^{-1} : B \to A$ is also one-one and onto).

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.

Note: 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 3.22: 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 such that,

$$a, b \in H \Rightarrow ab \in H$$

Now $a, b, c \in H \Rightarrow a, b, c \in G$

$$\Rightarrow a(bc) = (ab)c$$

$\therefore$ 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.

Aliter: Let H be a finite subset such that, $a, b \in H \Rightarrow ab \in H$

We show $a \in H \Rightarrow a^{-1} \in H$.

If $a = e$ then $a^{-1} = a \in H$

Let $a \neq e$, then by closure $a, a^2, a^3 \ldots \in H$

Since H is finite, for some n, m, $a^n = a^m$, $n > m$

i.e., $a^{n-m} = e$, $n - m > 1$ as $a \neq e$

i.e., $a^{n-m-1}.\ a = e$

$$\Rightarrow a^{n-m-1} = a^{-1}$$

where $n-m-1 \geq 1$ and therefore,

NOTES

$a^{n-m-1} \in H$. Hence, $a \in H \Rightarrow a^{-1} \in H$ and thus H is a subgroup of G.

Definition: Let G be a group. Let

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$$

then $Z(G)$ is called centre of the group G.

Theorem 3.23: 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, $x, y \in Z(G) \Rightarrow xg = gx$

$yg = gy$ (for all $g \in G$)

$\Rightarrow g^{-1} x^{-1} = x^{-1} g^{-1}$

$g^{-1} y^{-1} = y^{-1} g^{-1}$ (for all $g \in G$)

Now $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1}$

$= (xg)y^{-1}(g^{-1}g)$

$= xg(y^{-1} g^{-1})g = xg(g^{-1} y^{-1})g$

$= x(gg^{-1})y^{-1}g$

$= (xy^{-1})g$ for all $g \in G$

$\Rightarrow \quad xy^{-1} \in Z(G)$

Hence, $Z(G)$ is a subgroup.

Note: 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.

Theorem 3.24: 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 $ab^{-1} \in HK$

$a, b \in HK \Rightarrow \quad a = h_1 k_1$ for some $h_1, h_2 \in H$

$b = h_2 k_2 \qquad k_1, k_2 \in K$

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.

Notes:

1. $HK = KH$ 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 $h_1 \in H$.
2. If G has binary composition +, we define $H + K = \{h + k \mid h \in H, k \in K\}$.

3.11 CYCLIC GROUPS

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 $G = < a >$ or $G = (a)$.

Thus, G is called cyclic if $\exists$ an element $a \in G$ such that,

$G = \{a^n \mid n \in \mathbf{Z}\}$.

Again, if binary composition of G is denoted by +, the words 'Power of a' would mean multiple of 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 3.25: Order of a cyclic group is equal to the order of its generator.

Proof: Let $G = < a >$, 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 such that, $a^n = e$.

Consider the elements $a^0 = e, a, a^2, ..., a^{n-1}$

These are all elements of G and are n in number.

Suppose any two of the above elements are equal

say $a^i = a\text{j}$ with $i > \text{j}$

then $a^i \cdot a^{-}\text{j} = e \Rightarrow a^{i-}\text{j} = e$

But $0 < i - \text{j} \leq n - 1 < n$, thus $\exists$ a +ve integer $i - \text{j}$, such that, $a^{i-\text{j}} = e$ and $i - \text{j} < n$, 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 $x = a^m$

NOTES

By division algorithm, we can write

$m = nq + r$ where $0 \le r < n$

Now $a^m = a^{nq+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$

$\Rightarrow x = a^r$ where $0 \le r < n$

i.e., x is one of $a^0 = e, a, a^2, ..., a^{n-1}$

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 $n - m$ such that, $a^{n-m} = e$ meaning thereby that a has finite order.

Hence, no two powers of a can be equal. In other words, G would contain infinite number of elements.

Theorem 3.26: A subgroup of a cylic group is cyclic.

Proof: Let $G = < a >$ 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 such that, $a^m \in H$. We claim $H = < a^m >$.

Let $x \in H$ be any element. Then $x = a^k$ for some k. By division algorithm, $k = mq + r$ where $0 \le r < m$

$\Rightarrow r = k - mq$

$\Rightarrow a^r = a^k \cdot a^{-mq} = x \cdot (a^m)^{-q} \in H$

But m is the least +ve integer such that, $a^m \in H$, 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.

Note: 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 $n\mathbf{Z} = < n >$.

Also $m\mathbf{Z} \subseteq n\mathbf{Z}$ if and only if $n \mid m$. So $m\mathbf{Z} = n\mathbf{Z}$ if and only if $m = \pm n$.

Theorem 3.27: 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 $xy = a^n \cdot a^m = a^{n+m} = a^{m+n} = a^m \cdot a^n = y \cdot x$

Hence, G is Abelian.

Note: In view of the above result, all non-Abelian groups are non-cyclic. $< \boldsymbol{Q}, + >$ the group of rationals under addition serves as an example of an Abelian group which is not cyclic. For, suppose $\frac{m}{n} \in \boldsymbol{Q}$ is a generator of $\boldsymbol{Q}$,

then any element of $\boldsymbol{Q}$ should be a multiple of $\frac{m}{n}$. Now $\frac{1}{3n} \in \boldsymbol{Q}$, 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 $\boldsymbol{Q}$.

Klein's four group would be an example of a finite Abelian group which is not cyclic. It is the group of matrices $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}$ and $\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$ under matrix multiplication.

Theorem 3.28: 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

$$x, y \in H \Rightarrow x = a^n, y = a^m$$

$$\therefore \quad xy^{-1} = a^n \,.\, a^{-m} = a^{n-m} \in H$$

By Lagrange's theorem $o(H) \mid o(G)$. But $o(H) = o(a)$

$$\therefore \quad o(a) \mid o(G).$$

Corollary: 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 (which is less than or equal to the order of the group). Its converse is, however, not true.

Theorem 3.29: 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 $< a^k >$ where k is a divisor of n and $< a^{n/m} >$ is the unique subgroup of order m. As a particular case, suppose $G = < a >$ has order 30. Since divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30, $\exists$ eight subgroups of G, namely

$< a > = \{e, a, a^2, ..., a^{29}\} = G$

$< a^2 > = \{e, a^2, a^4, ..., a^{28}\}$

$< a^3 > = \{e, a^3, a^6, ..., a^{27}\}$

$< a^5 >, < a^6 >, < a^{10} >, < a^{15} >$ and $< a^{30} > = \{e\}$ having order 30, 15, 10, 6, 5, 3, 2, 1.

Consider again, the cyclic group $\mathbf{Z}_{30} = \{0, 1, 2, ..., 29\}$ under addition modulo 30 . $o(\mathbf{Z}_{30}) = 30$ and as 30 has 8 divisors 1, 2, 3, 5, 6, 10, 15, 30, $\mathbf{Z}_{30}$ will have eight subgroups namely

$< 1 > = \{0, 1, 2, ..., 29\} = \mathbf{Z}_{30}$

$< 2 > = \{0, 2, 4, ..., 28\}$

$< 3 > = \{0, 3, 6, ..., 27\}$

$< 5 >, < 6 >, < 10 >, < 15 >, < 30 > = \{0\}$

having order 30, 15, 10, 6, 5, 3, 2, 1.

In view of the this theorem, these would be the only subgroups of $\mathbf{Z}_{30}$.

Theorem 3.30: 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 $a \in G$, $a \neq e$

and let $H = \{a^n \mid n \text{ an integer}\}$ then H is a cyclic subgroup of G.

$\therefore \quad o(H) \mid o(G) \Rightarrow o(H) = 1 \text{ or } p$

But $\quad o(H) \neq 1$ as $a \in H$, $a \neq e$,

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.

Corollary: A group of prime order is Abelian.

Theorem 3.31: 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 $\quad o(H) = 1 \text{ or } p$

i.e., $\quad H = \{e\} \text{ or } H = G$.

Theorem 3.32: A group of finite composite order has at least one non-trivial subgroup.

Proof: Let $o(G) = n = rs \qquad$ 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 $\quad 1 < k \leq r < n \qquad (k > 1, \text{ as } a \neq e)$

Let $\quad H = \{a, a^2, a^3, ..., a^k = e\}$

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 $K = \{a^r, a^{2r}, ..., a^{tr} = e\}$ 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 3.33: 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 $a \in G$, such that, $a \neq e$.

Let $H = < a >$, then H is a cyclic subgroup of G and $H \neq \{e\}$. But G has no non-trivial subgroups.

Thus $H = G$

$\Rightarrow G = < a >$

Consider now the subgroup $K = < a^2 >$

Now $a \notin < a^2 >$, because if $a \in < a^2 >$ 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 $a \notin < a^2 >$.

Again $< a^2 > \neq \{e\}$, because then $a^2 = e$ would again mean that $o(a)$ is finite (≤ 2).

Thus $< a^2 >$ 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.

Theorem 3.34: 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:

Theorem 3.35: An infinite cyclic group has precisely two generators.

Proof: Let $G = < a >$ 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

$\Rightarrow a = b^m = (a^n)^m = a^{nm}$

$\Rightarrow a^{nm-1} = e \Rightarrow o(a)$ is finite and $\leq nm - 1$

Since $o(G) = o(a)$ is infinite, the above can hold only if

$nm - 1 = 0 \Rightarrow nm = 1$

$\Rightarrow m = \frac{1}{n}$ or $n = \pm 1$ as m, n are integers.

i.e., $b = a$ 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 then 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 $p_1, p_2, ..., p_n$ are distinct prime factors of n (>1), then

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right) \ldots \left(1-\frac{1}{p_k}\right)$$

(*ii*) If m, n are coprime then

$\varphi(mn) = \varphi(m)\ \varphi(n)$, $(m, n \geq 1)$

Theorem 3.36: 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 $d \mid n$.

Define $A(d) = \{x \in G \mid o(x) = d\}$

Suppose $A(d) \neq \varphi$. Then $\exists\ x \in G$ such that, $o(x) = d$.

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 $\exists\ y \in G, y \notin H$ such that, $o(y) = d$, 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 $d \mid n$

Clearly, $G = \underset{d|n}{\cup} A(d)$

Let $d_1, ..., d_s$ be all divisors of n.

Suppose $A(d_1) = \varphi, ..., A(d_i) = \varphi$

and $A(d_{i+1}) \neq \varphi, ..., A(d_s) \neq \varphi$

[Note, if $A(d) = \varphi$ for all $d \mid n$, then $o(G) = 0$, a contradiction. So, $A(d) \neq \varphi$ for some $d \mid n$]

$\therefore$ $o[A(d_1)] = ... = o[A(d_i)] = 0$

and $o[A(d_{i+1})] = \varphi(d_{i+1}) ..., o[A(d_s)] = \varphi(d_s)$

Now $G = \underset{d|n}{\cup} A(d) \Rightarrow o(G) = \sum_{d|n} o[A(d)]$

$$\Rightarrow n = \varphi(d_{i+1}) + ... + \varphi(d_s)$$

we know that, $n = \sum_{d|n} \varphi(d)$

$$\Rightarrow \varphi(d_1) + ... + \varphi(d_i) + \varphi(d_{i+1}) + ... + \varphi(d_s) = \varphi(d_{i+1}) + ... + \varphi(d_s)$$

$$\Rightarrow \varphi(d_1) + ... + \varphi(d_i) = 0, \text{ a contradiction}$$

So, $A(d) \neq \varphi$ for all $d \mid n$. In particular

$A(n) \neq \varphi \Rightarrow \exists\ x \in A(n) \Rightarrow \exists\ x \in G$ such that, $o(x) = n = o(G) \Rightarrow G$ is a cyclic group.

3.12 HOMOMORPHISMS

NOTES

In this section we will discuss about an isomorphism which can 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,

$$f(a * b) = f(a)\ o\ f(b) \quad a, b \in G$$

We can use the same symbol '.' for both binary compositions.

With that as notation we find a map

$f: G \to G'$ 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 $G \cong G'$.

Also clearly then,

$$f(a_1 a_2 \ldots\ldots a_n) = f(a_1) f(a_2) \ldots\ldots f(a_n)$$

holds under an isomorphism (homomorphism)

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.

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.,

$$f(x) = 2x \quad \text{for all } x \in \mathbf{Z}$$

Then f is well defined as $x = y \Rightarrow 2x = 2y \Rightarrow f(x) = f(y)$ such 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.

Example 3.52: Let f be a mapping from $< \mathbf{Z}, + >$ the group of integers to the group $G = \{1, -1\}$ under multiplication defined as

$f: \mathbf{Z} \to G$, s.t.,

$f(x) = 1$ if x is even

$= -1$ if x is odd

NOTES

Then f is clearly well defined. Verify, if it is a homomorphism.

Solution: Let $x, y \in \mathbf{Z}$ be any elements.

Case (*i*): x, y are both even, then $x + y$ is even and as

$$f(x + y) = 1, f(x) = 1, f(y) = 1$$

Then $f(x + y) = 1 = 1.1 = f(x) \,.\, f(y)$

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 $f(x + y) = f(x)\, f(y)$

This proves that f is a homomorphism.

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 3.53: Let $\mathbf{R}^+$ be the group of positive real numbers under multiplication and $\mathbf{R}$ the group of all real numbers under addition. Then show that the map

$$\theta : \mathbf{R}^+ \to \mathbf{R}, \text{ s.t.,}$$
$$\theta(x) = \log x$$

is an isomorphism.

Solution: θ is clearly well defined.

$$\theta(x) = \theta(y)$$
$$\Rightarrow \log x = \log y$$
$$\Rightarrow e^{\log x} = e^{\log y}$$
$$\Rightarrow x = y$$

This shows that θ is one-one.

Since, $\theta(xy) = \log xy = \log x + \log y = \theta(x) + \theta(y)$

We find θ is a homomorphism.

Finally, if $y \in \mathbf{R}$ be any member, then

Since $e^y \in \mathbf{R}^+$ and $\theta(e^y) = y$, we gather that θ is onto and hence on isomorphism. The map $f : \mathbf{R} \to \mathbf{R}^+$, such that, $f(a) = e^a$ can also be considered.)

Theorem 3.37: 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 and G', respectively.

Proof: (*i*) We have

$$e \,.\, e = e$$
$$\Rightarrow f(e \,.\, e) = f(e)$$
$$\Rightarrow f(e) \,.\, f(e) = f(e)$$
$$\Rightarrow f(e) \,.\, f(e) = f(e) \,.\, e'$$
$$\Rightarrow f(e) = e' \text{ (cancellation)}$$

(*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.

$$f(x^n) = \underset{(n \text{ times})}{f(x \,.\, x \,.....x)}$$
$$= f(x)\,.\,f(x)\,.....\,f(x) \quad (n \text{ times})$$
$$= (f(x))^n.$$

If $n = 0$, we have the result by (*i*). In case n is –ve integer, result follows by using (*ii*).

Example 3.54: Show that $< \mathbf{Q}, + >$ cannot be isomorphic to $< \mathbf{Q}^*, \cdot >$, where $\mathbf{Q}^* = \mathbf{Q} - \{0\}$ and $\mathbf{Q}$ = Rational.

Solution: Suppose f is an isomorphism from $\mathbf{Q}$ to $\mathbf{Q}^*$. Then as $2 \in \mathbf{Q}^*$, f is onto, $\exists\ \alpha \in < \mathbf{Q}, + >$, such that, $f(\alpha) = 2$.

$$\Rightarrow \quad f\left(\frac{\alpha}{2} + \frac{\alpha}{2}\right) = 2$$

$$\text{or} \quad f\left(\frac{\alpha}{2}\right) f\left(\frac{\alpha}{2}\right) = 2$$

$$\Rightarrow \quad x^2 = 2 \quad \text{where } x = f\left(\frac{\alpha}{2}\right) \in \mathbf{Q}^*$$

But that is a contradiction as there is no rational no. x such that, $x^2 = 2$. Hence the result follows.

Example 3.55: Find all the homomorphisms from $\frac{\mathbf{Z}}{4\mathbf{Z}}$ to $\frac{\mathbf{Z}}{6\mathbf{Z}}$.

Solution: Let $f : \frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}}$ be a homomorphism.

Then $f(4\mathbf{Z} + n) = n\, f(4\mathbf{Z} + 1)$

So, f is completely known if $f(4\mathbf{Z} + 1)$ is known.

Now order of $(4\mathbf{Z} + 1)$ is 4 and so $o(f(4\mathbf{Z} + 1))$ divides 4.

Also $o(f(4\mathbf{Z} + 1))$ divides 6 and thus $o(f(4\mathbf{Z} + 1)) = 1$ or 2

If $o(f(4\mathbf{Z} + 1)) = 1$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z}$ = zero of $\frac{\mathbf{Z}}{6\mathbf{Z}}$

Hence $f(4\mathbf{Z} + n) = \text{zero}$

If $o(f(4\mathbf{Z} + 1)) = 2$, then $f(4\mathbf{Z} + 1) = 6\mathbf{Z} + 3$

$\Rightarrow f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$

Also $f(4\mathbf{Z} + n + 4\mathbf{Z} + m) = f(4\mathbf{Z} + n + m)$
$= 6\mathbf{Z} + 3(n + m)$
$= (6\mathbf{Z} + 3n) + (6\mathbf{Z} + 3m)$
$= f(4\mathbf{Z} + n) + f(4\mathbf{Z} + m)$

Thus there are two choices for f and it can be defined as,

$$f : \frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}} \text{ s.t.,}$$

$$f(4\mathbf{Z} + n) = 6\mathbf{Z} + 3n$$

Notice $4\mathbf{Z} + n = 4\mathbf{Z} + m$

$$\Rightarrow n - m \in 4\mathbf{Z}$$

$$\Rightarrow 3(n - m) \in 12\mathbf{Z} \subseteq 6\mathbf{Z}$$

$$\Rightarrow 3(n - m) \in 6\mathbf{Z}$$

$$\Rightarrow 6\mathbf{Z} + 3n \in 6\mathbf{Z} + 3m$$

i.e., f is well defined.

So there are two homomorphisms from $\frac{\mathbf{Z}}{4\mathbf{Z}} \to \frac{\mathbf{Z}}{6\mathbf{Z}}$. In fact, in general, there are d homomorphisms from $\frac{\mathbf{Z}}{m\mathbf{Z}} \to \frac{\mathbf{Z}}{n\mathbf{Z}}$ where $d = \text{g.c.d.}(m, n)$

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 3.38: 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 $f(xy^{-1}) = f(x)\, f(y^{-1}) = f(x)(f(y))^{-1} = e' \,.\, e'^{-1} = e'$

$$\Rightarrow xy^{-1} \text{ Ker } f$$

Hence, it is a subgroup of G.

Again, for any $g \in G$, $x \in \text{Ker } f$

$$f(g^{-1}xg) = f(g^{-1}) f(x) f(g)$$

$$= (f(g))^{-1} f(x)\, f(g) \qquad = (f(g))^{-1}\, e'\, f(g)$$

$$= (f(g))^{-1} f(g) = e'$$

$$\Rightarrow g^{-1}xg \in \text{Ker } f$$

Also it is a normal subgroup of G.

Theorem 3.39: 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 $f(x) = e'$ and as $f(e) = e'$

$f(x) = f(e) \Rightarrow x = e$ as f is 1-1

Hence Ker $f = \{e\}$.

Conversely, let Ker f contain only the identity element.

Let $f(x) = f(y)$

Then $f(x)\ (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow xy^{-1} \in \text{Ker } f = \{e\}$

$\Rightarrow xy^{-1} = e$

$\Rightarrow x = y$ or that f is one-one.

Example 3.56: 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 $o(a) = n$

We obtain $a^n = e \Rightarrow f(a^n) = f(e)$

$\Rightarrow f(a\ .\ a\ .....\ a) = f(e)$

$\Rightarrow (f(a))^n = e$

$\Rightarrow o(f(a)) \mid n = o(a)$

Again, let f be 1-1.

Since $o(f(a)) = m$

We obtain $(f(a))^m = e'$

$\Rightarrow f(a)\ .\ f(a)\ .....\ f(a) = e'$

$\Rightarrow f(a\ .\ a\ .....\ a) = e'$

$\Rightarrow f(a^m) = e' = f(e)$

$\Rightarrow a^m = e$ (f is 1-1)

i.e., $o(a) \mid m$ or $n \mid m$, but already $m \mid n$

Hence $m = n$.

Conversely, let $o(a) = o(f(a))$.

Then $f(x) = f(y)$

$\Rightarrow f(x)\ (f(y))^{-1} = e'$

$\Rightarrow f(xy^{-1}) = e'$

$\Rightarrow o(f(xy^{-1})) = 1$

$\Rightarrow o\ (xy^{-1}) = 1 \Rightarrow xy^{-1} = e \Rightarrow x = y$

$\Rightarrow f$ is 1-1.

Note: Under an isomorphism, order of any element is preserved.

Example 3.57: Show that the group (**R**, +) of real numbers cannot be isomorphic to the group R' of non zero real numbers under multiplication.

Solution: $-1 \in R'$ and order of -1 is 2 as $(-1)^2 = 1$. But **R** has no element of order 2. As if $x \in \mathbf{R}$ is of order 2 then $2x = x + x = 0$. But this does not hold in (**R**, +) for any x except $x = 0$.

By above remark, under an isomorphism order of an element is preserved. Thus there cannot be any isomorphism between **R** and R'.

NOTES

Example 3.58: Let G be a group and $f: G \to G$ such that, $f(x) = x^{-1}$ *be a* homomorphism. Show that G is Abelian.

Solution: Let $x, y \in G$ be any elements.

$$\begin{aligned} xy &= (y^{-1}x^{-1})^{-1} = f(y^{-1}x^{-1}) \\ &= f(y^{-1})\, f(x^{-1}) \\ &= yx, \text{ hence } G \text{ is Abelian.} \end{aligned}$$

Theorem 3.40: (Fundamental Theorem of Group Homomorphism).

If $f: G \to G'$ be an onto homomorphism with $K = Ker\, f$, then $\frac{G}{K} \cong G'$.

In other words, every homomorphic image of a group G is isomorphic to a quotient group of G.

Proof: Define a map $\varphi : \frac{G}{K} \to G'$, such that,

$$\varphi(Ka) = f(a), \quad a \in G$$

We show φ is an isomorphism.

That φ is well defined follows by,

$$\begin{aligned} & Ka = Kb \\ \Rightarrow\ & ab^{-1} \in K = \text{Ker } f \\ \Rightarrow\ & f(ab^{-1}) = e' \\ \Rightarrow\ & f(a)(f(b))^{-1} = e' \\ \Rightarrow\ & f(a) = f(b) \\ \Rightarrow\ & \varphi(Ka) = \varphi(Kb) \end{aligned}$$

By retracing 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 obtain that φ is a homomorphism.

To check that φ is onto, let $g' \in G'$ be any element. Since $f: G \to G'$ is onto, $\exists\ g \in G$, such that,

$$f(g) = g'$$

Now $\varphi(Kg) = f(g) = g'$

Showing thereby that Kg is the required pre-image of g' under φ.

Hence φ is an isomorphism.

Note: The above theorem is also called first theorem of isomorphism.

Direct Products

The reader is well acquainted 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 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 $G_1 \times G_2 \times ... \times G_n$ of arbitrary groups G_1, G_2..., G_n as

$$G_1 \times ... \times G_n = \{(g_1,..., g_n) \mid g_i \in G_i\}$$

where compostion is component wise multiplication.

Let $G = G_1 \times ... \times G_n$ = direct product of G_1,..., G_n.

Define $H_1 = \{g_1, e_2,..., e_n\} \mid g_1 \in G_1, e_i$ = identity of $G_i\}$

$H_2 = \{(e_1, g_2, e_3..., e_n) \mid g_2 \in G_2\}$.

.....

$H_n = \{(e_1, e_2, e_3..., g_n) \mid g_n \in G_n\}$

We show that H_1 is normal in G.

$H_1 \neq \varphi$ as $(e_1, e_2,..., e_n) \in H_1$

Let $(g_1, e_2,..., e_n)\ (g'_1, e_2,..., e_n) \in H_1$

Then $(g_1, e_2,..., e_n)\ (g'_1, e_2,..., e_n)^{-1}$

$= (g_1, e_2,..., e_n)\ (g_1^{-1}, e_2,...e_n)$

$= (g_1 g_1^{-1}, e_2,...e_n) \in H_1$

Thus $H_1 \leq G$

Let $g = (g_1.....g_n) \in G$

$x = (x_1, e_2,..., e_n) \in H_1$

Then $gxg^{-1} = (g_1,..., g_n)\ (x_1, e_2..., e_n)\ (g_1^{-1},..., g_n^{-1})$

$= (g_1 x_1 g_1^{-1}, e_2,...e_n) \in H_1$

$\therefore$ H_1 is normal in G.

Similarly, each H_i is normal in G for all $i = 1,..., n$.

Let $g = (g_1,..., g_n) \in G$

Then $g = (g_1, e_2,..., e_n)\ (e_1, g_2, e_3...e_n)...(e_1, e_2 ,..., e_{n-1}, g_n) \in H_1 H_2...H_n$

Suppose $g = h_1 h_2...h_n = h'_1 h'_2,...,h'_n$, $h_i, h'_i \in H_i$

Then $(g_1, e_2,..., e_n)$ ... $(e_1,... e_{n-1}, g_n) = (g'_1,..., e_n)...(e_1,...e_{n-1}, g'_n)$

$\Rightarrow (g_1,..., g_n) = (g'_1...g'_n)$

$\Rightarrow g_i = g'_i$ for all $i = 1,..., n$

$\Rightarrow h_i = h'_i$ for all $i = 1,..., n$

So, $g \in G$ can be written uniquely as product of elements from H_1,..., H_n.

We summarize this through the following definition.

Let H_1 ,..., H_n be normal subgroups of G. G is said to be an Internal Direct Product (IDP) of H_1,..., H_n if $G = H_1 H_2... H_n$ and each $g \in G$ can be written uniquely as product of elements from H_1,..., H_n.

Consider the groups $\mathbf{Z}_2 = \{0, 1\}$, $\mathbf{Z}_3 = \{0, 1, 2\}$ under addition modulo. Here $\mathbf{Z}_2 \times \mathbf{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0) (1, 1), (1, 2)\}$ will form a group under element wise multiplication (addition).

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, we must have $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.

On the other hand one can show that $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not isomorphic to $\mathbf{Z}_4$. In fact $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic (whereas $\boldsymbol{Z}_4$ is). If $\mathbf{Z}_2 \times \mathbf{Z}_2$ is cyclic then it has a generator whose order should be same as $o(\mathbf{Z}_2 \times \mathbf{Z}_2) = 4$. But no element of $\mathbf{Z}_2 \times \mathbf{Z}_2$ has order 4. Notice, $2(1, 1) = (0, 0)$, i.e., order of $(1, 1)$ is less then or equal to 2 etc. Hence no element can be generator of $\mathbf{Z}_2 \times \mathbf{Z}_2$. One can show that $\mathbf{Z}_n \times \mathbf{Z}_m \cong \mathbf{Z}_{nm}$ iff n and m are relatively prime.

Theorem 3.41: 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*) $H_1 \cap H_2 = \{e\}$.

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 $G \subseteq H_1H_2$. But $H_1H_2 \subseteq G$

$\Rightarrow$ $G = H_1H_2$

Let $g \in H_1 \cap H_2 \Rightarrow g \in H_1, g \in H_2$

$\therefore$ $g = ge = eg$ is written in 2 ways as product of elements from H_1 and H_2.

$\therefore$ $g = e \Rightarrow H_1 \cap H_2 = \{e\}$.

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 $g = h_1h_2 = h'_1h'_2$, $h_1, h'_1 \in H_1, h_2, h'_2 \in H_2$

$\Rightarrow h_1^{-1} h'_1 = h_2h_2^{-1} \in H_1 \cap H_2 = \{e\}$

$\Rightarrow h_1 = h'_1, h_2 = h'_2$

$\therefore$ G is an IDP of H_1 and H_2.

For example, let $G = < a >$ 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 3.42: Let $H_1, H_2, ..., H_n$ be normal in G. Then G is an IDP of H_1, $H_2, ..., H_n$ if and only if

(*i*) $G = H_1H_2 ... H_n$

(*ii*) $H_i \cap H_1H_2 ... H_{i-1} H_{i+1} ... H_n = \{e\}$

for all $i = 1, ... n$

NOTES

Proof: Suppose G is an IDP of $H_1,...,H_n$. Then (i) follows from the definition of IDP

Let $g \in H_i \cap H_1 ... H_{i-1}\ H_{i+1} ... H_n$

Then $g = h_i,\ h_i \in H_i$ and $g = h_1 h_2 ... h_{i-1}\ h_{i+1} ... h_n,\ h_j \in H_j$

$\Rightarrow g = ee ... h_i ... e$

$g = h_1 h_2 ... h_{i-1}\ e\ h_{i+1} ... h_n$

Since this representation of g should be unique we get $e = h_1, e = h_2,..., h_i = e,...$

or that $g = e$, which proves the result.

Conversely, let $g \in G$ then $g \in H_1 ... H_n \Rightarrow g = h_1 ... h_n,\ h_i \in H_i$

We show this representation is unique.

Let $g = h'_1 ..... h'_n,\ h'_i \in H_i$

$\therefore$ $h_1 ..... h_n = h'_1 ..... h'_n$

By (ii) $H_i \cap H_j = \{e\}$ for all $i \neq j$ because if $x \in H_i \cap H_j$

Then $x \in H_i,\ x \in H_j.\ (j \neq i)$

$x \in H_j \Rightarrow x \in H_1 ... H_j ... H_{i-1}\ H_{i+1} ... H_n$

as $x = e ... x ... e.\ e ... e$

$\Rightarrow x \in H_i \cap H_1 ... H_{i-1}\ H_{i+1} ... H_n = \{e\}$

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 $i \neq j$

$\therefore$ $h_1 ..... h_n = h'_1 ..... h'_n$

$\Rightarrow$ $h_n = (h_1^{-1}\ h'_1)\ (h_2^{-1}\ h'_2) ..... (h_{n-1}^{-1}\ h'_{n-1})\ h'_n$

$\therefore\ h_n\ h_n^{'-1} = (h_1^{-1}\ h'_1) ..... (h_{n-1}^{-1}\ h'_{n-1}) \in H_1 ..... H_{n-1} \cap H_n = \{e\}$

$\therefore$ $h_n = h'_n$

Similarly $h_{n-1} = h'_{n-1},....., h_1 = h'_1$

Hence G is an IDP of $H_1,....., H_n$.

Note: If G is an IDP of $H_1, H_2,....., H_n$ 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).

Example 3.59: Let G be a finite Abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.

Solution: Let $o(G) = p_1^{\alpha 1} ... p_r^{\alpha r}$

Where $p_1,..., p_r$ are distinct primes.

Since G is Abelian, each Sylow subgroup H_i of G is normal. $o(H_i) = p_i^{\alpha i}$.

Let $g \in H_i \cap H_1 ... H_{i-1}\ H_{i+1} ... H_r$

$\Rightarrow g \in H_i, g \in H_1 ... H_{i-1}\ H_{i+1} ... H_r$

Let $t = p_1^{\alpha 1} ... p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha i+1} ... p_r^{\alpha r}$

$g \in H_1 ... H_{i-1}\ H_{i+1} .. H_r$

$\Rightarrow g = h_1 ... h_{i-1}\ h_{i+1} ... h_r,\ h_j \in H_j$

$\Rightarrow g^t = h_1^t ... h_{i-1}^t\ h_{i+1}^t ... h_r^t = e$ as $h_j^t = e$ for all $j \neq i$

$\Rightarrow o(g) \mid t$

NOTES

But $g \in H_i \Rightarrow o(g) \mid o(H_i) = p_i^{\alpha i}$

$\Rightarrow o(g) = p_i^{\beta i}, \ \beta_i \geq 0$

$\therefore \quad p_i^{\beta i} \mid t$

$\Rightarrow p_i^{\beta i} \mid p_1^{\alpha 1} \ldots p_{i-1}^{\alpha i-1} \ p_{i+1}^{\alpha i+1} \ \ldots \ p_r^{\alpha r}$

$\Rightarrow \beta i = 0$

$\Rightarrow o(g) = 1 \Rightarrow g = e.$

$\therefore \ H_i \cap H_1 \ldots H_{i-1} \ H_{i+1} \ldots H_r = \{e\}$ for all $i = 1, \ldots, r$

Now $o(H_1 \ldots\ldots H_r) = \dfrac{o(H_1)\, o(H_2 \ldots H_r)}{o(H_1 \cap H_2 \ldots H_r)} = o(H_1)\, o(H_2 \ldots\ldots H_r)$

Again, $\quad o(H_2 H_3 \ldots H_r) = \dfrac{o(H_2).\, o(H_3 \ldots H_r)}{o(H_2 \cap H_3 \ldots H_r)}$

Now $\quad x \in H_2 \cap H_3 \ldots H_r$

$\Rightarrow x \in H_2$ and $x \in H_3 \ldots\ldots H_r \subseteq H_1 H_3 \ldots\ldots H_r$

$\Rightarrow x \in H_2 \cap H_1 H_3 \ldots H_r = \{e\}$

So $x = e$

$\therefore \quad o(H_2 \ldots\ldots H_r) = o(H_2)\, o(H_3 \ldots\ldots H_r)$

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 3.42, G is an IDP of $H_1, \ldots\ldots H_r$ and so isomorphic to EDP of $H_1, \ldots, H_r$.

Note: If G is a finite group and all its Sylow subgroups are normal then G is direct product of its Sylow subgroups.

Example 3.60: Show that if G is a group of order 45, it is IDP of its Sylow subgroups.

Solution: $o(G) = 45 = 3^2 \times 5$.

Number of Sylow 5-subgroups is $(1 + 5k)$, s.t., $(1 + 5k) \mid 9$ which gives $k = 0$

i.e., $\exists$ a unique normal Sylow 5-subgroup H of G where $o(H) = 5$.

Similarly, $\exists$ *a* unique normal Sylow 3-subgroup K of order 9.

Since $o(H \cap K) \mid 9, 5$, we find $o(H \cap K) = 1 \Rightarrow H \cap K = \{e\}$

Also $\quad o(HK) = \dfrac{5 \times 9}{1} = 45 = o(G) \Rightarrow G = HK$

Hence G is IDP of its sylow subgroups H & K.

Example 3.61: 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. So $nh = hn$ for all $n \in N$, $h \in H$ and $nk = kn$ for all $n \in N$, $k \in K$.

Let $n_1, n_2 \in N$.

$$n_2 \in N \Rightarrow n_2 \in G \Rightarrow n_2 = h_2k_2,\ \ h_2 \in H, k_2 \in K$$

$$\therefore \quad n_1n_2 = n_1h_2k_2$$
$$= h_2n_1k_2$$
$$= h_2k_2n_1$$
$$= n_2n_1$$

So, N is Abelian.

Example 3.62: 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 $F_3 = \{0, 1, 2\}$ mod 3.

Then one can check that G forms a non-Abelian group. In fact, it would be a subgroup of the groups 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 $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^3$.

If we consider the group $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$, 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 $\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ cannot be isomorphic as one is Abelian and the other a non-Abelian group.

Check Your Progress

12. Define the function.
13. What do you understand by graph of function?
14. What is countable set?
15. State the uncountable set.
16. Define the group.
17. What is subgroup?
18. State the cyclic group.
19. What is automorphism?

3.13 ANSWERS TO 'CHECK YOUR PROGRESS'

1. A mapping $f : A \to B$ is said to be onto if given $b \in B$ there exists $a \in A$ such that $f(a) = b$. It is also sometimes called surjective mapping.

NOTES

2. A relation R on a set A is called a partial order relation, if it is reflexive, anti-symmetric and transitive.
3. A binary relation R from a set A to a set B is a subset R of the Cartesian product $A \times B$.
4. Let R be a binary relation from the set A to the set B and S be a binary relation from the set B to the set C, then the ordered pair (R, S) is said to be composable. If (R, S) is a composable pair of binary relations, the composite $R\ O\ S$ and R and S, is a binary relation from the set A to the set C, such that, for $a \in A$ and $c \in C$, $a\ (R\ O\ S)c$ if for some $b \in B$, both aRb and bSc are binary relations.
5. In mathematics, the inverse relation of a binary relation is the relation written 'Backwards'. In formal terms, if $L: X \rightarrow Y$ is a binary relation, then the inverse relation is $L^{-1}: Y \rightarrow X$.
6. In mathematics, especially order theory, a partially ordered set (also termed as poset) formalizes and generalizes the intuitive concept of an ordering, sequencing, or arrangement of the elements of a set.
7. Let A and B be two sets. The set of all ordered pairs (a, b) such that $a \in A$, $b \in B$ is called the Cartesian product of A and B and is denoted by $A \times B$.
8. A relation R on a set A is called an equivalence relation if R is reflexive, symmetric and transitive.
9. Given an equivalence relation on set A, the collection of equivalence classes forms a partition of set A. The converse is also true, given a partition on set A, the relation "Induced by the Partition" is an equivalence relation.
10. In mathematics, an algebraic structure consists of a non-empty set A, termed as the underlying set, carrier set or domain. It is a collection of operations on A of finite arity, typically binary operations, and a finite set of identities, known as axioms that these operations must satisfy.
11. In mathematics, a Hopf algebra, named after Heinz Hopf, is a structure that is simultaneously a (unital associative) algebra and a (counital coassociative) coalgebra, with these structures' compatibility making it a bialgebra, and that moreover is equipped with an antiautomorphism satisfying a certain property.
12. In mathematics, a function is a binary relation between two sets that associates every element of the first set to exactly one element of the second set.
13. A function is uniquely represented by the set of all pairs $(x, f(x))$, called the graph of the function. When the domain and the codomain are sets of real numbers, each such pair may be thought of as the Cartesian coordinates of a point in the plane. The set of these points is termed as the graph of the function and is a standard means of illustrating the function.

14. A countable set in mathematics has some cardinality, which means it has some finite number of elements that can be counted. It is a subset of natural numbers. A set in which number of its elements can not be counted are termed as uncountable.
15. In mathematics, an uncountable set is an infinite set containing too many elements to be countable. The uncountability is closely related to its cardinal number. A set is uncountable if the cardinal number of the set is more than that of the natural numbers.
16. A non-empty set G, together with a binary compsition * (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 $e \in G$, such that,
    $a * e = e * a = a$ 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) such that,
    $a * a' = a' * a = e$
    (a' is then called inverse of a)
17. 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.
18. 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 $G = < a >$ or $G = (a)$.
19. An isomorphism from a group G to itself is called automorphism of G.

3.14 SUMMARY

- Let A and B be two sets. A relation R from A to B is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, then it is also denoted by aRb and conversely aRb means $(a, b) \in R$. The symbol aRb is read as 'a is related to b'. If $A = B$, we shall say R is a relation in A instead of 'from A to A'.
- 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.
- Sometimes, a relation is represented by a matrix, where, first we draw a table. Suppose R is a relation from a finite set A to a finite set B.
- A relation is represented with the help of a diagram called the graph of the relation.
- A binary relation R from a set A with n elements to a set B with m elements is represented as an $n \times m$ array M_R by marking the positions in M_R. The positions which correspond to the pairs belong to R with 1 and 0 elsewhere.

- A relation is a subset of Cartesian product of two sets. A relation shows relationship of a member of one set to that of another set. Thus, a relationship is shown as an ordered pair and is also called binary relation.
- Formally, a partial order is any binary relation that is reflexive (each element is comparable to itself), antisymmetric (no two different elements precede each other), and transitive (the start of a chain of precedence relations must precede the end of the chain).
- A poset can be visualized through its Hasse diagram, which depicts the ordering relation.
- Two elements of a poset $(S, \leq)$ are said to be comparable if $a \leq b$ or $b \leq a$. Otherwise a and b are said to be incomparable.
- Let A and B be two sets. A relation R from A to B is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, then it is also denoted by aRb and conversely, aRb means $(a, b) \in R$. The symbol aRb is read as 'a is related to b'. If $A = B$, we shall say that R is a relation in A instead of 'from A to A'.
- In mathematics, an equivalence relation is a binary relation that is reflexive, symmetric and transitive. The relation "Is Equal To" is the canonical example of an equivalence relation. Each equivalence relation provides a partition of the underlying set into disjoint equivalence classes. Two elements of the given set are equivalent to each other, if and only if they belong to the same equivalence class.
- Given an equivalence relation on set A, the collection of equivalence classes forms a partition of set A. The converse is also true, given a partition on set A, the relation "Induced by the Partition" is an equivalence relation.
- An algebraic structure may be based on other algebraic structures with operations and axioms involving several structures. For example, a vector space involves a second structure termed as a field, and an operation termed as the scalar multiplication between elements of the field called scalars, and elements of the vector space called vectors.
- The properties of specific algebraic structures are studied in abstract algebra. The general theory of algebraic structures has been formalized in universal algebra.
- Lattice structures can be defined on the basis of two or more binary operations, which typically include operations termed as meet and join, connected by the absorption law.
- Algebraic structures are defined through different configurations of axioms. Universal algebra abstractly studies such objects. One major dichotomy is between structures that are axiomatized entirely by identities and structures that are not. If all axioms defining a class of algebras are identities, then this class is a variety and it must not to be confused with algebraic varieties of algebraic geometry.
- A function is a relation from a set of inputs to a set of possible outputs where each input is related to exactly one output. This means that if the

object x is in the set of inputs (called the domain) then a function f will map the object x to exactly one object $f(x)$ in the set of possible outputs (called the codomain).

- The modern definition of function was first given in 1837 by the German mathematician Peter Dirichlet, "If a variable y is so related to a variable x that whenever a numerical value is assigned to x, there is a rule according to which a unique value of y is determined, then y is said to be a function of the independent variable x".
- A function is a process or a relation that associates each element x of a set X, the domain of the function, to a single element y of another set Y (possibly the same set), the codomain of the function. It is customarily denoted by letters, such as f, g and h.
- A countable set in mathematics has some cardinality, which means it has some finite number of elements that can be counted. It is a subset of natural numbers. A set in which number of its elements can not be counted are termed as uncountable.
- A set is finite, if it has a finite number of elements. The elements of such a set can be counted by a finite number. The number of elements in a finite set A is denoted by $n(A)$. Here, n is a finite positive integer.
- 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).
- If G is a group with identity element e then the subsets $\{e\}$ 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).
- 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 $G = < a >$ or $G = (a)$.
- A homomorphism from a group G to itself is called an endomorphism of G.

3.15 KEY TERMS

- **Binary composition:** A binary composition on a set S, is a rule which assigns to each pair of elements a, b of S a unique element c of S.
- **Partially ordered set:** A partially ordered set (also termed as poset) formalizes and generalizes the intuitive concept of an ordering, sequencing, or arrangement of the elements of a set.
- **Equivalence relation:** A relation R on a set A is called an equivalence relation if R is reflexive, symmetric and transitive.
- **Algebraic structure:** An algebraic structure consists of a non-empty set A, termed as the underlying set, carrier set or domain. An algebraic structure may be based on other algebraic structures with operations and axioms involving several structures.

NOTES

- **Subgroups:** 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.

3.16 SELF-ASSESSMENT QUESTIONS AND EXERCISES

Short-Answer Questions

1. Define the term relation.
2. How will you representation of a relation by matrix?
3. Define the binary relation.
4. Give the properties of equivalence relation.
5. What is partition of set?
6. Differentiate between the countable and uncountable set.
7. What is an algebraic structure?
8. Define the group.
9. Give the concept of semi group.
10. State the theorem of subgroup.
11. Define the Kernel of *f*.

Long-Answer Questions

1. Discuss the significance of relations and ordering properties giving appropriate examples.
2. Elaborate on the relation and their types with examples.
3. Explain in detail about the equivalence relation with their classes.
4. Discuss the algebraic structures by giving axioms and appropriate examples.
5. Describe the function by giving important theorems and examples.
6. Elaborate on the countable and uncountable set.
7. Discuss the group, subgroup and cyclic group.
8. Analyse the homomorphism and also prove the fundamental theorem of homomorphism.

3.17 FURTHER READING

Hazarika, Padmalochan. 2003. *A Class Textbook of Business Mathematics*. New Delhi: S. Chand & Company Ltd.

Tremblay, Jean Paul and R. Manohar. 2004. *Discrete Mathematical Structures With Applications To Computer Science*. New York: McGraw-Hill Higher Education.

Ramaswamy, V. 2006. *Discrete Mathematical Structures with Applications to Combinatorics*. Hyderabad: Universities Press.

Kolman, Bernand, Roberty C. Busby and Sharn Cutter Ross. 2006. *Discrete Mathematical Structures*. London (UK): Pearson Education.

Liu, C. L. 1985. *Elements of Discrete Mathematics*, 2nd Edition. New York: McGraw-Hill Higher Education.

Arumugam, S. and Thangapandi Isaac. 2008. *Modern Algebra*. Chennai: Scitech Publications (India) Pvt. Ltd.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. New Delhi: Cambridge University Press.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

UNIT 4 RINGS AND FIELDS

NOTES

Structure

4.0 INTRODUCTION

In linear algebra, the quotient of a vector space V by a subspace N is a vector space obtained by 'Collapsing' N to zero. The space obtained is called a 'Quotient Space' and is denoted V/N. A ring is a set which prepared with two operations (usually referred to as addition and multiplication) that satisfy certain properties: there are additive and multiplicative identities and additive inverses, addition is commutative, and the operations are associative and distributive. In mathematics, a subring of R is a subset of a ring that is itself a ring when binary operations of addition and multiplication on R are restricted to the subset, and which shares the same multiplicative identity as R.

In mathematics, a field is a set on which addition, subtraction, multiplication, and division are defined and behave as the corresponding operations on rational and real numbers do. A field is thus a fundamental algebraic structure, which is widely used in algebra, number theory, and many other areas of mathematics. Whereas the many subfields that fall under the umbrella of discrete mathematics, there is combinatorics, graph theory and coding theory.

A vector space is a space in which the elements are sets of numbers themselves. Each element in a vector space is a list of objects that has a specific length, which said to be vectors. A linear transformation is a function from one

NOTES

vector space to another that preserves the operations of addition and scalar multiplication. i.e., under a linear transformation, the image of a linear combination of vectors is the linear combination of the images of the vectors having the same coefficients. In mathematics, a set B of vectors in a vector space V is called a basis if every element of V may be written in a unique way as a finite linear combination of elements of B. In the theory of vector spaces, a set of vectors is said to be linearly dependent if there is a non-trivial linear combination of the vectors that equals the zero vector. If no such linear combination exists, then the vectors are said to be linearly independent.

Vector spaces are the subject of linear algebra and are well categorised by their dimension, which, roughly speaking, specifies the number of independent directions in the space.

The algebra of Quaternions is a structure first studied by the Irish mathematician William Rowan Hamilton which extends the two-dimensional complex numbers to four dimensions. Multiplication is non-commutative in quaternions, a feature which enables its representation of three-dimensional rotation.

In this unit, you will study about the quotient space, fields, rings, subring and subfield, vector space, linear combination, linear dependence and independence, basis of vector space, vector space of linear transformation, linear algebra, and algebra of Quaternions.

4.1 OBJECTIVES

After going through this unit, you will be able to:

- Explain the meaning of quotient space
- Analyse the fields
- Describe the rings and their classes
- Discuss the vector space
- Interpret the linear combination
- Discuss the linear dependence and independence
- Describe the basis of vector space
- Elaborate on the vector space of linear transformation
- Explain the linear algebra, and algebra of Quaternions

4.2 QUOTIENT SPACES

In linear algebra, the quotient of a vector space V by a subspace N is a vector space obtained by 'Collapsing' N to zero. The space obtained is called a **quotient space** and is denoted V/N.

Definition: Let V be a vector space over a field K, and let N be a subspace of V. We define an equivalence relation $\sim$ on V by stating that $x \sim y$ if $x - y \in N$. That is, x is related to y if one can be obtained from the other by adding an element of

N. From this definition, one can deduce that any element of *N* is related to the zero vectors; more precisely, all the vectors in *N* get mapped into the equivalence class of the zero vector.

The equivalence class – or, in this case, the coset – of *x* is often denoted

$$[x] = x + N$$

Since it is given by,

$$[x] = \{x + n : n \in N\}.$$

The quotient space *V*/*N* is then defined as *V*/~, the set of all equivalence classes over *V* by ~. Scalar multiplication and addition are defined on the equivalence classes by

- $\alpha[x] = [\alpha x]$ for all $\alpha \in K$, and
- $[x] + [y] = [x + y]$.

It is not hard to check that these operations are well-defined (i.e., do not depend on the choice of representatives). These operations turn the quotient space *V*/*N* into a vector space over *K* with *N* being the zero class, [0].

The mapping that associates to $v \in V$ the equivalence class [*v*] is known as the *quotient map*.

Alternatively phrased, the quotient space *V*/*N* is the set of all affine subsets of *V* which are parallel to *N*.

For examples Let $X = \mathbf{R}^2$ be the standard Cartesian plane, and let *Y* be a line through the origin in *X*. Then the quotient space *X*/*Y* can be identified with the space of all lines in *X* which are parallel to *Y*. That is to say that, the elements of the set *X*/*Y* are lines in *X* parallel to *Y*. Note that the points along any one such line will satisfy the equivalence relation because their difference vectors belong to *Y*. This gives a way to visualize quotient spaces geometrically. (By re-parameterising these lines, the quotient space can more conventionally be represented as the space of all points along a line through the origin that is not parallel to *Y*. Similarly, the quotient space for $\mathbf{R}^3$ by a line through the origin can again be represented as the set of all co-parallel lines, or alternatively be represented as the vector space consisting of a plane which only intersects the line at the origin.)

Another example is the quotient of $\mathbf{R}^n$ by the subspace spanned by the first ***m*** standard basis vectors. The space $\mathbf{R}^n$ consists of all *n*-tuples of real numbers $(x_1, ..., x_n)$. The subspace, identified with $\mathbf{R}^m$, consists of all *n*-tuples such that the last $n - m$ entries are zero: $(x_1, ..., x_m, 0, 0, ..., 0)$. Two vectors of $\mathbf{R}^n$ are in the same equivalence class modulo the subspace if and only if they are identical in the last $n - m$ coordinates. The quotient space $\mathbf{R}^n/\mathbf{R}^m$ is isomorphic to $\mathbf{R}^{n-m}$ in an obvious manner.

More generally, if *V* is an (internal) direct sum of subspaces *U* and *W*,

$$V = U \oplus W$$

Then the quotient space *V*/*U* is naturally isomorphic to *W*.

An important example of a functional quotient space is a **L^p space**.

NOTES

Properties

There is a natural epimorphism from V to the quotient space V/U given by sending x to its equivalence class $[x]$. The kernel (or nullspace) of this epimorphism is the subspace U. This relationship is neatly summarized by the short exact sequence,

$$0 \to U \to V \to V/U \to 0.$$

If U is a subspace of V, the dimension of V/U is called the codimension of U in V. Since a basis of V may be constructed from a basis A of U and a basis B of V/U by adding a representative of each element of B to A, the dimension of V is the sum of the dimensions of U and V/U. If V is finite-dimensional, it follows that the codimension of U in V is the difference between the dimensions of V and U:

$$\operatorname{codim}(U) = \dim(V/U) = \dim(V) - \dim(U).$$

Let T: $V \to W$ be a linear operator. The kernel of T, denoted $\ker(T)$, is the set of all x in V such that $T_x = 0$. The kernel is a subspace of V. The first isomorphism theorem for vector spaces says that the quotient space $V/\ker(T)$ is **isomorphic** to the image of V in W. An immediate corollary, for finite-dimensional spaces, is the rank–nullity theorem: the dimension of V is equal to the dimension of the kernel (the nullity of T) plus the dimension of the image (the rank of T).

The cokernel of a linear operator $T: V \to W$ is defined to be the quotient space $W/\operatorname{im}(T)$.

In abstract algebra, the **field of fractions** or **field of quotients** of an integral domain is the smallest field in which the integral domain can be embedded. The elements of the field of fractions of the integral domain R have the form a/b with a and b in R and b 0. The field of fractions of the ring R is denoted by $\operatorname{Quot}(R)$ or $\operatorname{Frac}(R)$. This is referred as the quotient field, field of fractions or fraction field.

If R is any commutative ring without zero divisors and at least one non-zero element e, then one can construct the field of fractions $\operatorname{Quot}(R)$ of R as the set of equivalence classes of pairs (n, d), where n and d are elements of R and d is not 0, and the equivalence relation given by (n, d) is equivalent to (m, b) if and only if $nb=md$. The sum of the equivalence classes of (n, d) and (m, b) is the class of $(nb + md, db)$ and their product is the class of (mn, db). The embedding is given by mapping n to the equivalence class of (en, e). This embedding does not depend on the choice of e. If R is an integral domain then (en, e) will be equivalent to $(n, 1)$.

The field of fractions of R is characterized by the universal property that if $f : R \to F$ is an injective ring homomorphism from R into a field F then there exists a unique ring homomorphism $g : \operatorname{Quot}(R) \to F$ which extends f.

Example 4.1: 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 $\{a_1, ..., a_r\}$ be a basis of D over F.

Let $0 \neq a \in D$. We show that a is invertible. Consider $\{aa_1, ..., aa_r\}$.

Let $\alpha_1(aa_1) + ... + \alpha_r(aa_r) = 0$, $\alpha_i \in F$.

Then $a(\alpha_1 a_1 + ... + \alpha_r a_r) = 0$

$\Rightarrow \alpha_1 a_1 + ... + \alpha_r a_r = 0$, as $a \neq 0$ and D is an integral domain.

$\Rightarrow \alpha_i = 0$ for all $i = 1, ..., r$ as $\{a_1, ..., a_r\}$ is linearly independent over F.

NOTES

$\Rightarrow \{aa_1, ..., aa_r\}$ is linearly independent over F.

But $[D : F] = r \Rightarrow \{aa_1, ..., aa_r\}$ is a basis of D over F.

$\therefore \quad 1 \in D \Rightarrow 1 = \beta_1 aa_1 + ... + \beta_r aa_r, \quad \beta_i \in F$

$= a(\beta_1 a_1 + ... \beta_r a_r)$

$= ab, \quad b = \beta_1 a_1 + ... + \beta_r a_r \in D$

$\Rightarrow a$ is invertible.

$\Rightarrow D$ is a field.

Algebraic Extensions

Suppose K is an extension of F and $a \in K$.

Let $F[a] = \{f(a) \mid f(x) = a_0 + a_1 x + ... + a_n x^n \in F[x]\}, \quad a_i \in F$

then as $f(a) = a_0 + a_1 a + ... + a_n a^n \in K$, we find $F[a] \subseteq K$

One can show that $F[a]$ is an integral domain.

Let E be its field of quotients. Then E is the smallest field containing $F[a]$. We show

$$F[a] \subseteq F(a) \subseteq E.$$

Now $x = 0 + 1.x + 0.x^2 + ... \in F[x]$ and so

$a = 0 + 1.a + 0.a^2 + ... \in F[a]$

i.e., $a \in F[a] \subseteq E$

Again if $\alpha \in F$ be any element then

$$\alpha = \alpha + 0x + 0x^2 + ... \in F[x]$$

gives $\alpha \in F[a]$ or that $F \subseteq F[a] \subseteq E$

Hence $F(a) \subseteq E$, as $F(a)$ is the smallest field containing F and a.

If $f(a) \in F[a]$ be any member where

$$f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_n a^n, \ \alpha_i \in F$$

then as $a \in F(a)$, $\alpha_i \in F \subseteq F(a)$, we find $f(a) \in F(a)$

Hence $F[a] \subseteq F(a)$ and so

$$F[a] \subseteq F(a) \subseteq E$$

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, $F(a) = \left\{ \dfrac{f(a)}{g(a)} \middle| g(a) \neq 0, f(x), g(x) \in F[x] \right\}$

In general, one can show that

$$F(a_1, ..., a_n) = \left\{ \frac{f(a_1, ..., a_n)}{g(a_1, ..., a_n)} \middle| g(a_1, ..., a_n) \neq 0, \begin{matrix} f(x_1, ..., x_n) \in F[x] \\ g(x_1, ..., x_n) \in F[x] \end{matrix} \right\}$$

NOTES

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 4.1: A field is an integral domain.

Proof: Let $< R, +, . >$ 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 $ab = 0$

$\Rightarrow a^{-1}(ab) = a^{-1}0$

$\Rightarrow b = 0.$

which shows that R is an integral domain.

Remark: Similarly we can show that a division ring is an integral domain and thus has no zero divisiors.

A 'partial converse' of the above result also holds.

Theorem 4.2: 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. Note closure holds in R' as R is an integral domain.

In other words $< R, +, \cdot >$ is a field (it being commutative as it is an integral domain).

Aliter: Let $R = \{a_1, a_2, ..., a_n\}$ be a finite non-zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, ..., aa_n$ 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 $aa_1, aa_2, ..., aa_n$ 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 $ax = (aa_i)x = a(a_ix)$

i.e., $x = a_ix$

Hence using commutativity we find

$$x = a_ix = xa_i$$

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 4.2: 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 $x \in R$.

4.3 FIELDS

A commutative division ring is known as a **field**. For example, set of rational numbers, set of real numbers and set of complex numbers under operation of addition and multiplication are field.

Note: Every non-zero elements of set of integers Z has no multiplicative inverse in Z. So set of integers is not a field.

Suppose F is a non-empty set having atleast two elements together with two binary operations defined by addition and multiplication. Then, (F, +, .) is said to be a field if the following properties hold true for all $a, b, c \in$ F

(i) F is closed with respect to addition, i.e., $a + b \in$ F

(ii) Addition is associative. i.e., $(a + b) + c = a + (b + c)$

(iii) Existence of additive identity, i.e., for all $a \in$ F, there exists an additive identity $0 \in$ F such that $0 + a = a + 0 = a$

(iv) Addition is commutative, i.e., $a + b = b + a$

(v) Existence of additive inverse, i.e., for every $a \in$ F, there exists $-a \in$ F such that $a + (-a) = -a + a = 0$

(vi) F is closed with respect to multiplication, i.e., $a.b \in$ F

(vii) Multiplication is associative, i.e., $a.(b.c) = (a.b).c$

(viii) Multiplication is distributive with respect to addition, i.e.,

$a.(b + c) = a.b + a.c$ and $(b + c).\ a = b.a + c.a$

NOTES

(ix) Multiplication is commutative, i.e., $a.b = b.a$

(x) Existence of multiplicative identity, i.e., for all $a \in F$ there exists multiplication identity $1 \in F$ such that $a.1 = 1.a = a$

(xi) Existence of multiplicative inverse, i.e., for every non-zero $a \in F$, there exists $\frac{1}{a} \in F$ such that $a.\frac{1}{a} = \frac{1}{a}.a = 1$.

Theorem 4.3: Every field is an integral domain.

Proof: Let (R, *f*, .) be a field. Then R is a commutative ring. Let $a \neq 0$. Then, a^{-1} exists (by definition of field)

$\therefore ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow (1b) = 0 \Rightarrow b = 0$

Suppose $b \neq 0$ and $ab = 0$, then

$ab = 0 \Rightarrow (ab)b^{-1} = 0.b^{-1} \Rightarrow a(bb^{-1}) = 0 \Rightarrow a.1 = 0 \Rightarrow a = 0$

$\therefore$ In a field, $ab = 0 \Rightarrow a = 0$ or $b = 0$

Thus, a field has no zero divisors and hence every field is an integral domain.

Note: Every integral domain is not a field since ring of integers is an integral domain but it is not a field.

Theorem 4.4: A skew field or a division ring has no zero divisors.

Proof: Suppose F is a skew field. Thus, F is a ring which has unit element and its non-zero elements have multiplicative inverse. Let F have two elements *a*, *b* such that $ab = 0$.

Case I: When $a \neq 0$

$\therefore a^{-1}$ exists and $a^{-1} \in F$

Pre-multiplying $ab = 0$ by a^{-1}, we get

$a^{-1}.ab = a^{-1}.0 \Rightarrow 1.b = 0 \Rightarrow b = 0$

Thus, $b = 0$ when $a \neq 0$

Case II: When $b \neq 0$

$\therefore b^{-1}$ exists and $b^{-1} \in F$

Post-multiplying $ab = 0$ by b^{-1}, we get

$(ab).b^{-1} = 0.b^{-1} \Rightarrow a.bb^{-1} = 0 \Rightarrow a.1 = 0 \Rightarrow a = 0$

Hence, $ab = 0 \Rightarrow a = 0$ or $b = 0$

Therefore, a skew field has no zero divisors.

Example 4.3: Give an example of a ring which is not an integral domain.

Solution: The set $(\{0, 1, 2, 3, 4, 5\}, +_6, \times_6)$ is a commutative ring. Let R = {0, 1, 2, 3, 4, 5}

Composition table for $+_6$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Composition table for $\times_6$

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Closure law: (i) Since all the entries in the composition table of addition are element of R, hence R is closed under addition modulo 6.

(ii) Since all the entries in the composition table of multiplication are element of R, hence R is closed under multiplication modulo 6.

Associative law: (i) Let a, b, c are any three elements of R. Then

$a +_6(b +_6 c) = a +_6(b + c)$

= least non-negative remainder when $a + (b + c)$ is divided by 6.

= least non-negative remainder when $(a + b) + c$ is divided by 6.

$= (a + b) +_6 c = (a +_6 b) +_6 c$

Thus the composition $+_6$ is associative.

(ii) Let a, b, c are any three elements of R. Then

$a \times_6 (b \times_6 c) = a \times_6 (bc)$

= least non-negative remainder when $a(bc)$ is divided by 6.

= least non-negative remainder when $(ab)c$ is divided by 6.

$= (ab) \times_6 c = (a \times_6 b) \times_6 c$

Thus the composition $\times_6$ is associative.

Existence of identity: Since $0 +_6 a = a = a +_6 0$ for all $a \in$ R, therefore $0 \in$ R is an additive identity.

Existence of inverse: We can easily observe from the table that the inverses of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively. Thus, the additive inverse exists.

NOTES

Commutative law: $a +_6 b = b +_6 a$ for all $a, b \in R$.

Distributive law: Let a, b, c be any three elements of R. Then

$a \times_6 (b +_6 c) = a \times_6 (b + c)$

= least non-negative remainder when $a(b + c)$ is divided by 6.

= least non-negative remainder when $ab + ac$ is divided by 6.

$= (ab) +_6 ac = (a \times_6 b) +_6 (a \times_6 c)$

Similarly, $(b +_6 c) \times_6 a = (b \times_6 a) +_6 (c \times_6 a)$

Thus R is a ring with respect to the given composition.

From the table, we have $a \times_6 b = b \times_6 a$ for all $a, b \in R$. Thus, R is a commutative ring.

Also, we have $1 \times_6 a = a = a \times_6 1$ for all $a \in R$. Thus, R is a commutative ring with unity.

Again from the table, $2 \times_6 3 = 0$ but $2 \neq 0$ and $3 \neq 0$ in R. Thus, R is not an integral domain.

Example 4.4: Give an example of a skew field which is not a field.

Solution: Let M be a set of matrices of form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where a, b, c, d are real numbers.

Closure law: (i) The closure law of addition is satisfied because the sum of two members of M is also a member of M.

(ii) The closure law of multiplication is satisfied because the product of two matrices of type 2×2 is a matrix of type 2×2, i.e., $A, B \in M \Rightarrow A.B \in M$

Associative law: (i) $A + (B + C) = (A + B) + C$

(ii) $A(BC) = (AB)C$ for all $A, B, C \in M$

Existence of Identity: (i) For $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M, A \in M$

$O + A = A + O = A$. Therefore, identity for addition exists.

(ii) For $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M, A \in M$

$I.A = A.I = A$. Therefore, identity for multiplication exists.

Existence of inverse: (i) There exists a matrix $-A \in M$ for every $A \in M$ such that $-A + A = O_{2 \times 2}$

(ii) Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a non singular matrix for which $A^{-1} \in M$ exists.

Also, $A^{-1}.A = A.A^{-1} = I$.

Thus, each non singular matrix possesses inverse.

Commutative law: For all A, B ∈ M, A + B = B + A

Distributive law: For all matrices A, B, C ∈ M,

A. (B + C) = A.B + A.C and (B + C).A = B.A + C.A

Hence (M, +, .) is a skew field.

Now, we know that matrix multiplication is not commutative, i.e., AB ≠ BA. Thus, (M, +, .) is a skew field but not a field.

NOTES

Example 4.5: Prove that ({0, 1, 2, 3, 4}, $+_5$, $\times_5$) is a field.

Solution: Composition table for addition modulo 5:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Composition table for multiplication modulo 5:

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Let A = {0, 1, 2, 3, 4}

Closure property: (i) We have $a +_5 b$ is a member of A for all $a, b \in$ A.

∴ A is closed under the composition addition modulo 5.

(ii) We have $a \times_5 b$ is a member of A for all $a, b \in$ A.

∴ A is closed under the composition multiplication modulo 5.

Associative law: (i) Let a, b, c are any three elements of A. Then

$a +_5 (b +_5 c) = a +_5 (b + c) = (a + b) +_5 c = (a +_5 b) +_5 c$

Thus the composition $+_5$ is associative.

(ii) Let a, b, c are any three elements of A. Then

$a \times_5 (b \times_5 c) = a \times_5 (bc) = (ab) \times_5 c = (a \times_5 b) \times_5 c$

Thus the composition $\times_5$ is associative.

Existence of identity: (i) For all $a \in$ A, we have $a +_5 0 = a = 0 +_5 a$

∴ $0 \in$ A is additive identity.

(ii) For all $a \in A$ and $1 \in A$, we have $a \times_5 1 = a = 1 \times_5 a$

$\therefore 1 \in A$ is multiplicative identity.

Existence of inverse: (i) As $0 +_5 0 = 0$,

NOTES

$1 +_5 4 = 0 = 4 +_5 1$,

$2 +_5 3 = 0 = 3 +_5 2$

Hence, additive inverse of each element exists.

(ii) As $1 \times_5 1 = 1$, $2 \times_5 3 = 1 = 3 \times_5 2$, $4 \times_5 4 = 1$

Hence, multiplicative inverse of each non-zero element of A exists.

Commutative law: Since the entries in the corresponding row and columns of both the table are identical, hence the compositions are commutative.

Distributive law: Let a, b, c are any three elements of A. Then

$a \times_5 (b +_5 c) = a \times_5 (b + c) = (ab) +_5 ac = (a \times_5 b) +_5 (a \times_5 c)$

Similarly, $(b +_5 c) \times_5 a = (b \times_5 a) +_5 (c \times_5 a)$

Thus, the set $(A, +_5, \times_5)$ is a field.

Example 4.6: Show that if $S = \left\{a + b\sqrt{3} : a, b \in Q\right\}$, then (S, +, .) is a field.

Solution: Closure law: (i) Let $p = a_1 + b_1\sqrt{3}$, where $a_1, b_1 \in Q$

$q = a_2 + b_2\sqrt{3}$, where $a_2, b_2 \in Q$

$\therefore \quad p + q = (a_1 + a_2) + (b_1 + b_2)\sqrt{3}$

Since, $a_1 + a_1, b_1 + b_2 \in Q$, therefore $p + q \in S$

Thus, S is closed under addition.

(ii) Let $p = a_1 + b_1\sqrt{3}$, where $a_1, b_1 \in Q$

$q = a_2 + b_2\sqrt{3}$, where $a_2, b_2 \in Q$

$\therefore \quad p.q = \left(a_1 + b_1\sqrt{3}\right).\left(a_2 + b_2\sqrt{3}\right) = (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}$

Now, since $a_1a_2 + 3b_1b_2$, $a_1b_2 + a_2b_1$ are rational numbers, therefore $p.q \in S$

Thus, S is closed under multiplication.

Existence of identity: (i) Let $p = a + b\sqrt{3}$

For $p \in S$, we have $\left(0 + 0\sqrt{3}\right) + \left(a + b\sqrt{3}\right) = a + b\sqrt{3} = \left(a + b\sqrt{3}\right) + \left(0 + 0\sqrt{3}\right)$

Thus, $0 + 0\sqrt{3}$ is the additive identity.

(ii) Let $p = a + b\sqrt{3}$ and $\left(1 + 0\sqrt{3}\right) \in S$

We have $\left(1 + 0\sqrt{3}\right).\left(a + b\sqrt{3}\right) = a + b\sqrt{3} = \left(a + b\sqrt{3}\right).\left(1 + 0\sqrt{3}\right)$

Thus, $1 + 0\sqrt{3}$ is the multiplicative identity.

Associative law: (i) As we know that elements of S are real numbers and addition of real numbers is associative. Thus, for all $p, q, r \in S, p + (q + r) = (p + q) + r$

(ii) As we know that elements of S are real numbers and multiplication of real numbers is associative. Thus, for all $p, q, r \in S, p.(qr) = (pq).r$

Existence of inverse: (i) Let $p = a + b\sqrt{3}$. Then for $x \in S$, there exists $-a - b\sqrt{3}$ such that $\left(a + b\sqrt{3}\right) + \left(-a - b\sqrt{3}\right) = 0 + 0\sqrt{3} = \left(-a - b\sqrt{3}\right) + \left(a + b\sqrt{3}\right)$

Thus, additive inverse exists.

(ii) Let $p = a + b\sqrt{3}$ be a non-zero element of S. Then atleast one of a and b is not 0.

Now, $$\frac{1}{p} = \frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{\left(a + b\sqrt{3}\right)\left(a - b\sqrt{3}\right)} = \frac{a - b\sqrt{3}}{a^2 - 3b^2}$$

$$= \frac{a}{a^2 - 3b^2} - \frac{b\sqrt{3}}{a^2 - 3b^2} \neq 0$$

$\therefore$ $$p.\frac{1}{p} = \left(a + b\sqrt{3}\right).\left(\frac{a}{a^2 - 3b^2} - \frac{b\sqrt{3}}{a^2 - 3b^2}\right)$$

$$= \frac{a^2 - 3b^2}{a^2 - 3b^2} = 1 = 1 + 0\sqrt{3} = \text{identity element}$$

Commutative law: For all $p, q \in S, p + q = q + p$ and $p.q = q.p$

Thus, each non-zero element of S has a multiplicative inverse.

Distributive law: As we know that elements of S are real numbers and real numbers follow distributive law. Thus, for all $p, q, r \in S, p.(q + r) = p.q + p.r$ and $(q + r).p = q.p + r.p$

Thus, (S, +, .) is a field.

Example 4.7: Let $R = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a, b \in R\right\}$. Prove that R is non-commutative ring without identity under usual addition and multiplication.

Solution: Closure law: (i) Let $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in R$, $a, b, c, d \in R$

Then, $$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a + b & c + d \\ 0 & 0 \end{bmatrix}$$

Since $a + b, c + d \in R \Rightarrow \begin{bmatrix} a + b & c + d \\ 0 & 0 \end{bmatrix} \in R$

NOTES

(ii) Let $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in R$, $a, b, c, d \in R$

Then, $AB = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$

Since $ac, ad \in R \Rightarrow \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \in R$

Existence of identity: (i) $O + A = A = A + O$ for all $A \in R$

$\therefore$ Null matrix O of type 2×2 is an additive identity of R.

(ii) The multiplicative identity of R, unit matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin R$

$\therefore$ Multiplicative identity does not exist in R.

Existence of inverse: $(-A) + A = O_{2\times 2} = A + (-A)$

$\therefore$ For every $A \in R$, inverse $(-A)$ exists.

Associative law: (i) If $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$, $C = \begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}$,

then, $A + (B + C) = (A + B) + C$

Thus, associative law exists for addition of matrices.

(ii) For all $A, B, C \in R$, $A(BC) = (AB)C$

Thus, matrix multiplication is associative

Commutative law: (i) For all $A, B \in R$, it can be easily seen that $A + B = B + A$.

Thus, commutative law exists for the addition of matrices.

(ii) Let $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \in R$, $a, b, c, d \in R$

Then, $AB = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}$

$BA = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & bc \\ 0 & 0 \end{bmatrix}$

$\therefore AB \neq BA$

Distributive law: $A.(B + C) = A.B + A.C$ and $(B + C).A = B.A + C.A$ for A, B, $C \in R$

Thus, R is a non-commutative ring without identity under usual addition and multiplication.

Example 4.8: Prove that the set R of all real valued continuous functions defined on the closed interval [0, 1] is commutative ring with unity with respect to the addition and multiplication of functions defined point wise as follows:

$(a + b)(x) = a(x) + b(x)$

$(ab)(x) = a(x).b(x)$, where a, b are two members of R.

Solution: Let a be a real valued function defined on [0, 1]. Then $a(x)$ will also be a real number when $x \in [0, 1]$.

Properties Under Addition

Closure Law: (i) We have for all $a, b \in R$, $(a + b)(x) = a(x) + b(x)$ = Sum of two real numbers = Real number

Also, given that $a + b$ is a continuous function on [0, 1]. Thus, $(a + b) \in R$ and hence R is closed with respect to addition.

(ii) We have for all $a, b \in R$ $(a.b)(x) = a(x).b(x)$ = Product of two real numbers = Real number

Also, given that $a. b$ is a continuous function [0, 1]. Thus, R is closed under multiplication.

Existence of Identity: (i) Let $c \in R$ be a function such that for all $x \in [0, 1]$, $c(x) = 0$

$\therefore (a + c)(x) = a(x) + c(x) = a(x) + 0 = a(x)$ for each $a \in R$

Similarly $(c + a)(x) = a(x)$. Thus, $c + a \equiv a \equiv a + c$

$\Rightarrow c \in R$ is additive identity.

(ii) Let $t(x) = 1$ be a function for all $x \in [0, 1]$

t is a continuous and real valued function defined on [0, 1].

$\therefore t \in R$ and for each $a \in R$, we have

$(a.t)x = a(x).t(x) = a(x).1 = a(x) = (t.a)x$

$\therefore t \in R$ is a multiplicative identity of R.

Associative Law: (i) For $x \in [0, 1]$ and $a, b, c \in R$, we have

$[(a + b) + c](x) = (a + b)x + c(x)$

$= a(x) + b(x) + c(x) = a(x) + [b(x) + c(x)] = [a + (b + c)]x$

Thus, $[(a + b) + c] = [a + (b + c)]$

(ii) For all $x \in [0, 1]$ and $a, b, c \in R$, we have

$[a\ (bc)](x) = a(x).(bc)(x)$

$= a(x).b(x).c(x) = [a.b](x).c(x) = [(a.b).c)](x)$

$\therefore a(bc) \equiv (ab)c$ Thus, R is associative under multiplication

Existence of Inverse: Let function $-a$ be such that $(-a)(x) = -a(x)$ for all $x \in [0, 1]$

$\therefore -a \in R$ and hence for each $a \in R$, there exists $-a \in R$ such that

$(-a + a)(x) = -a(x) + a(x) = 0 = c(x)$

$\therefore -a + a \equiv c \equiv a + (-a)$

NOTES

Thus, $(-a)$ is additive inverse of a.

Commutative Law: For all $a, b \in R$, we have

$(a.b)(x) = a(x).b(x) = b(x).a(x) = (b.a)(x)$

$\therefore a.b \equiv b.a$

Thus, R is commutative with respect to multiplication.

Distributive Law: For all $a, b, c \in R$, $[a.(b + c)](x) = a(x).(b + c)(x)$

$= a(x).[b(x) + c(x)]$

$= a(x).\ b(x) + a(x).\ c(x) = ab(x) + ac(x) = (ab + ac)(x)$

$\Rightarrow a.(b + c) \equiv a.b + a.c$

Similarly we can prove that $(b + c).\ a \equiv b.a + c.a$

Thus, R is a commutative ring with unity.

Definition: (Field Axioms) *A* field is a set F with two operations, called **addition** and **multiplication** which satisfy the following axioms (A1–5), (M1–5) and (D).

(A) Axioms for Addition

(A1) $x, y \in F \Rightarrow x + y \in F$

(A2) $x + y = y + x$ for all $x, y \in F$ (Addition is commutative)

(A3) $(x + y) + z = x + (y + z)$ for all $x, y, z \in F$ (Addition is associative)

(A4) F contains an element 0 such that $0 + x = x$ for every $x \in F$.

(A5) For each $x \in F$ there is an element $-x \in F$ such that $x + (-x) = 0$.

(M) Axioms for Multiplication

(M1) $x, y \in F \Rightarrow xy \in F$

(M2) $xy = yx$ for all $x, y \in F$ (Multiplication is commutative)

(M3) $(xy)z = x(yz)$ for all $x, y, z \in F$ (Multiplication is associative)

(M4) F contains an element $1 \neq 0$ such that $1x = x$ for every $x \in F$.

(M5) For each $0 \neq x \in F$ there is an element $1/x \in F$ such that $x\ (1/x) = 1$.

4.4 RINGS

Definition: A non empty set R, together with two binary compositions + and . 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 $a, b \in R$

(*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 . 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 ., 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 . defined on it and satisfies the above axioms.

(*c*) Axiom (*v*) is named associativity w.r.t. . and axiom (*vi*) is referred to as distributivity (left and right) w.r.t. . 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.,

$$ae = ea = a \quad \text{for all } a \in R$$

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 $a + a + ...+ a$ (*n* times), *n* being an integer.

Example 4.9: Sets of real numbers, rational numbers, integers form rings w.r.t. usual addition and multiplication. These are all commutative rings with unity.

Example 4.10: Set **E** of all even integers forms a commutative ring, without unity (under usual addition and multiplication).

Example 4.11: (*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 4.12: The set $\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ forms a ring under addition and multiplication modulo 7. (In fact, we could take *n* in place of 7).

Example 4.13: The set $R = \{0, 4, 6\}$ under addition and multiplication modulo 6 forms a commutative ring with unity. The composition tables are

$\oplus$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\odot$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

NOTES

Since $0 \odot 4 = 0$, $2 \odot 4 = 2$, $4 \odot 4 = 4$, we notice 4 is unity of R.

Example 4.14: 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 $f, g \in F$

$(f + g)x = f(x)$ for all $x \in \mathbf{R}$

$(f\,g)x = f(x)g(x)$ for all $x \in \mathbf{R}$

zero of this ring is the mapping $O : \mathbf{R} \to \mathbf{R}$, s.t.,

$O(x) = 0$ for all $x \in \mathbf{R}$

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 $x \in \mathbf{R}$.

Remark: Although the same notation fg has been used for product here it should not be mixed up with fog defined earlier.

Example 4.15: 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.

We can similarly get $\mathbf{Z}_n[i]$ the ring of Gaussian integers modulo n. For instance,

$$\mathbf{Z}_3[i] = \{a + ib \mid a, b \in \mathbf{Z}_3 = \{0, 1, 2\} \bmod 3\}$$
$$= \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$$

Example 4.16: 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 $\cdot$ 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 4.17: 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 4.18: Let $R = \{0, a, b, c\}$. Define + and . 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 it is an example of the smallest non commutative ring.

4.4.1 Some Special Classes of Rings

Theorem 4.5: *In a ring R, the following results hold*

(*i*) $a \cdot 0 = 0 \cdot a = 0$ *for all* $a \in R$

(*ii*) $a(-b) = (-a)b = -ab$ *for all* $a, b \in R$

(*iii*) $(-a)(-b) = ab$. $\forall\ a, b \in R$

(*iv*) $a(b - c) = ab - ac$. $\forall\ a, b, c \in R$

Proof: (*i*) $a \cdot 0 = a \cdot (0 + 0)$

$\Rightarrow \quad a \cdot 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow \quad a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$

$\Rightarrow \quad 0 = a \cdot 0$

using cancellation w.r.t + in the group $< R, + >$.

(*ii*) $a \cdot 0 = 0$

$\Rightarrow \quad a(-b + b) = 0$

$\Rightarrow \quad a(-b) + ab = 0$

$\Rightarrow \quad a(-b) = -(ab)$

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

$$n(a + b) = na + nb$$

$$(n + m)a = na + ma$$

NOTES

$(nm)a = n(ma)$

$a^m\ a^n = a^{m+n}$

$(a^m)^n = a^{mn}$ (see under groups).

NOTES

Example 4.19: Let $<R, +, .>$ be a ring where the group $<R, +>$ is cyclic. Show that R is a commutative ring:

Solution: Let $< R, + >$ be generated by a. Let $x, y \in R$ be any two elements, then $x = ma$, $y = na$ for some integers m, n.

Now $xy = (ma)(na)$

$= (a + a + ... + a)(a + a + ... + a)$

m times n times

$= (mn)a^2 = (nm)a^2 = (na)(ma) = yx$

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 1: 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 2: 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. Again, $\mathbf{Z} \times \mathbf{Z}$ will not be an integral domain.

Remark: Some authors do not insist upon the condition of commutativity as a part of the definition of an integral domain. One can have (see examples 4.20, 4.21 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 4.6: 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 $ab = ac$ $(a \neq 0)$

Then $ab - ac = 0$

$\Rightarrow$ $a(b - c) = 0$

$\Rightarrow$ $a = 0$ or $b - c = 0$

NOTES

Since $a \neq 0$, we get $b = c$.

Conversely, let the given condition hold.

Let $a, b \in R$ be any elements with $a \neq 0$.

Suppose $ab = 0$

then $ab = a.0$

$\Rightarrow$ $b = 0$ 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 1: 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 2: 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 3: 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.

Example 4.20: 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 $\begin{bmatrix} \frac{x-iy}{k} & -\frac{u+iv}{k} \\ \frac{u-iv}{k} & \frac{x+iy}{k} \end{bmatrix}$

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

NOTES

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

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 4.21: 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.

Two elements $a + bi + cj + dk$ and $a' + b'i + c'j + d'k$ are equal iff $a = a'$, $b = b'$, $c = c'$, $d = d'$.

Addition and multiplication on D are defined by

$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$

And

$(a + bi + cj + dk)\,(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' - bd' + ca' - db')j + (ad' + bc' - ab' + da')k$

The symbol + in the elements of D is just a notation and is not to be a confused with addition in real numbers. We identify element $o + 1i + oj + ok$ by i and so on.

Thus since $i = 0 + 1i + 0j + 0k$

$j = 0 + 0i + 1j + 0k$

We have $ij = k, ji = -k$, etc., In fact that shows that D is non commutative. 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.

The elements of D can also be written as quadruples (a, b, c, d).

This ring D is called the *ring of quaternions*.

Theorem 4.7: A field is an integral domain.

Proof: Let $< R, +, . >$ 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 $ab = 0$

$\Rightarrow\ a^{-1}(ab) = a^{-1}0$

$\Rightarrow\ b = 0.$

which shows that R is an integral domain.

Remark: Similarly we can show that a division ring is an integral domain and thus has no zero divisiors.

A 'partial converse' of the above result also holds.

Theorem 4.8: 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. Note closure holds in R' as R is an integral domain.

In other words $< R, +, \cdot >$ is a field (it being commutative as it is an integral domain).

Aliter: Let $R = \{a_1, a_2, ..., a_n\}$ be a finite non zero integral domain. Let $0 \neq a \in R$ be any element then $aa_1, aa_2, ..., aa_n$ 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 $aa_1, aa_2, ..., aa_n$ 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 $ax = (aa_i)x = a(a_ix)$

i.e., $x = a_ix$

Hence using commutativity we find

$$x = a_ix = xa_i$$

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 4.22: 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 4.23: The ring $\{0, 1\}$ under addition and multiplication mod 2 forms a Boolean ring.

Example 4.24: Show that a Boolean ring is commutative.

Solution: Let $a, b \in R$ be any elements

Then $a + b \in R$ (closure)

By given condition

$$(a + b)^2 = a + b$$

$$\Rightarrow \quad a^2 + b^2 + ab + ba = a + b$$

$$\Rightarrow \quad a + b + ab + ba = a + b$$

NOTES

NOTES

$$\Rightarrow \quad ab + ba = 0$$

$$\Rightarrow \quad ab = -ba \qquad ...(1)$$

$$\Rightarrow \quad a(ab) = a(-ba)$$

$$\Rightarrow \quad a^2b = -aba$$

$$\Rightarrow \quad ab = -aba \qquad ...(2)$$

Again Equation (1) gives

$$(ab)a = (-ba)a$$

$$\Rightarrow \quad aba = -ba^2 = -ba \qquad ...(3)$$

Equations (2) and (3) give

$$ab = ba \ (= -aba)$$

or that R is commutative.

Example 4.25: Show that order of a finite Boolean ring is of the type 2^n, $n = 0, 1, 2,....$

Solution: Let $< R, +, . >$ be a finite Boolean ring. Then $a^2 = a \ \ \forall \ a \in R$,

Thus $(a + a)^2 = a + a$

$\Rightarrow a^2 + a^2 + 2aa = a + a$

$\Rightarrow 2a^2 = 0$ or that $2a = 0 \quad \forall \ a \in R$

Thus each non zero element in the group $< R, + >$ has order 2.

By Cauchy's theorem in groups, we know if p is any prime dividing $o(R)$ then $\exists$ $x \in R$, s.t., $o(x) = p$. But order of each non zero element is 2 and thus 2 is the only prime dividing $o(R)$. Hence $o(R) = 2^n$.

Example 4.26: (a) Show that a non zero element a in $\mathbf{Z}_n$ is a unit iff a and n are relatively prime.

(b) If a is not a unit then it is a zero divisor.

Solution: (a) $\mathbf{Z}_n = \{0, 1, 2, ..., n - 1\}$ mod n

Let $a \in \mathbf{Z}_n$ be a unit, then $\exists\ b \in \mathbf{Z}_n$ s.t.,

$$a \otimes b = 1$$

i.e., when ab is divided by n, remainder is 1, in other words,

$$ab = nq + 1$$

Or $\quad ab - nq = 1$

$\Rightarrow$ a and n are relatively prime.

Conversely, let $(a, n) = 1$, then $\exists$ integers u, v, s.t.,

$$au + nv = 1$$

$$\Rightarrow \quad au = n(-v) + 1$$

Suppose, $u = nq + r, \quad 0 \le r < n, \quad r \in \mathbf{Z}_n$,

Then $\quad au = anq + ar \ = n\ (-v) + 1$

$$\Rightarrow \quad ar \ = n\ (-v - aq) + 1, \quad r \in \mathbf{Z}_n$$

i.e., $a \otimes r = 1, \quad r \in \mathbf{Z}_n$

i.e., a is a unit.

(b) Let a be not a unit and suppose g.c.d$(a, n) = d > 1$

Since $d \mid a$, $a = dk$ for some k. Also $d \mid n \Rightarrow n = dt$

$\Rightarrow a.t = dk \ \frac{n}{d} = kn = 0 \bmod n$

i.e., a is a zero divisor.

Remark: In $\mathbf{Z}_n$, the set of units is U_n. Thus for instance, in $\mathbf{Z}_8$ 1, 3, 5, 7 are units.

Example 4.27: Show that $\mathbf{Z}_p = \{0, 1, 2, ..., p-1\}$ modulo p is a field iff p *is* a prime.

Solution: Let $\mathbf{Z}_p$ 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 $\Rightarrow \mathbf{Z}_p$ has zero divisors.

i.e., $\mathbf{Z}_p$ is not an integral domain, a contradiction as $\mathbf{Z}_p$ being a field is an integral domain.

Hence p is prime.

Conversely, let p be a prime. We need show that $\mathbf{Z}_p$ is an integral domain (it being finite will then be a field).

Let $a \otimes b = 0 \quad a, b \in \mathbf{Z}_p$

Then ab is a multiple of p

$\Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$ (p being prime)

$\Rightarrow a = 0$ or $b = 0$ (Notice $a, b \in \mathbf{Z}_p \Rightarrow a , b < p$)

$\Rightarrow \mathbf{Z}_p$ is an integral domain and hence a field.

Remark : (*i*) We can also use problem 4 to prove this result.

(*ii*) Since $\mathbf{Z}_p$ is a field, all its non zero elements are units by definition of a field.

Example 4.28: 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 $y + 1 \in R$ as $1 \in R$

By given condition

$$(x(y + 1))^2 = x^2 (y + 1)^2$$

$$\Rightarrow (xy + x)^2 = x^2 (y + 1)^2$$

$$\Rightarrow (xy)^2 + x^2 + xyx + xxy = x^2(y^2 + 1 + 2y)$$

$$\Rightarrow x^2y^2 + x^2 + xyx + xxy = x^2y^2 + x^2 + 2x^2y$$

$$\Rightarrow xyx = x^2y \qquad ...(1)$$

Since Equation (1) holds for all x, y in R, it holds for $x + 1$, y also. Thus replacing x by $x + 1$, we get

NOTES

$$(x + 1)\, y(x + 1) = (x + 1)^2 y$$

$$\Rightarrow (xy + y)\,(x + 1) = (x^2 + 1 + 2x)y$$

$$\Rightarrow xyx + xy + yx + y = x^2y + y + 2xy$$

$$\Rightarrow yx = xy \text{ using Equation (1)}$$

Hence R is commutative.

Example 4.29: 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

$$f(x) = \frac{1}{2} - x, \quad 0 \le x \le \frac{1}{2}$$

$$= 0, \quad \frac{1}{2} \le x \le 1$$

and $$g(x) = 0, \quad 0 \le x \le \frac{1}{2}$$

$$= x - \frac{1}{2}, \quad \frac{1}{2} \le x \le 1$$

then f and g are continuous functions and $f \neq 0$, $g \neq 0$

whereas $$g f(x) = g(x)\, f(x) = 0 \cdot \left(\frac{1}{2} - x\right) \text{ if } 0 \le x \le \frac{1}{2}$$

$$= \left(x - \frac{1}{2}\right).0 = 0 \text{ if } \frac{1}{2} \le x \le 1$$

i.e., $g f(x) = 0$ for all x

i.e., $g f = 0$ but $f \neq 0$, $g \neq 0$.

Subrings

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 $< \mathbf{Z}, +, . >$ 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 4.9: 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 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 Subrings

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

NOTES

$$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}2 & 2\\ 2 & 0\end{bmatrix} = \begin{bmatrix}4 & 2\\ 2 & 2\end{bmatrix} \notin S + T.$$

NOTES

4.4.2 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.

Thus it is the smallest positive integer n such that $1 + 1 + ...+ 1 = 0$ in R.
n times

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.

Example 4.30: (a) Rings of integers, even integers, rationals, reals, complex numbers 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 $1 \,.\, 1 = 1 \neq 0$

Product of Rings

Let R_1 and R_2 be two rings.

Let $R = R_1 \times R_2 = \{(a, b) \mid a \in R_1, b \in R_2\}$, then it is easy to verify that R forms a ring under addition and multiplication defined by

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$(a_1, b_1) \,.\, (a_2, b_2) = (a_1a_2, b_1b_2)$$

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.

Theorem 4.10: The characteristic of an integral domain is either zero or a prime number.

Proof: Let a be any non-zero element of an integral domain R.

Assume that the order of a, i.e., $o(a) = 0$. Then the characteristic of R is 0.

Now, suppose that order of a, i.e., $o(a) = p, p \neq 0$. Then the characteristic of R is p.

Let us assume that p is a composite number. Then $p = p_1p_2$, $0 < p_1$, $p_2 < p$

As $a \neq 0$ and R is integral domain, thus $a^2 = a.a \neq 0$

So, a^2 is a non-zero member of R.

$\therefore o(a^2) = p \Rightarrow pa^2 = 0$

$\Rightarrow (p_1p_2)\, a^2 = 0 \Rightarrow (p_1a)(\, p_2a) = 0 \Rightarrow$ Either $p_1a = 0$ or $p_2a = 0$

But we have $o(a) = p \Rightarrow$ Either $p_1 > p$ or $p_2 = p$,

which is a contradiction. Hence our assumption that p is a composite number is wrong.

Thus, p must be a prime number.

Theorem 4.11: The characteristic of a ring with identity (unity) is zero or greater than zero according as the identity element of the ring regarded as a member of the additive group of the ring has the order zero or greater than zero.

Proof: Suppose (R, +, .) is a ring with identity 1.

Case I: Order of 1 is 0.

As the order of 1 is 0, hence the characteristic of R is 0.

Case II: Order of 1 is $n \neq 0$.

As the order of 1 is n, hence 1 * 1 * 1 * 1 * …. * 1 = 0

i.e, 1 + 1 + 1 + …. upto n terms = 0 i.e., $n.1 = 0$

If $a \in$ R, then $na = a + a + \ldots + a = 1.a + 1.a + \ldots + 1.a$

$= (1 + 1 + \ldots + 1)a = (n.1)a = 0.a = 0$

Thus, the characteristic of the ring is n.

Theorem 4.12: The order of each element of an integral domain (regarding elements as the members of additive group) is same.

Proof: Let a be any non-zero element of an integral domain R and n be the order of it as an element of the group (R, +). Suppose b is the other non-zero element of R.

Case I: When $n = 0$.

$\therefore$ No positive integer K exists such that $Ka = 0$

Assume that the order of b, i.e., $o(b) = m$ and $m > 0$.

$\therefore mb = 0 \Rightarrow a(mb) = 0$

$\Rightarrow a(b + b + \ldots + m \text{ times}) = 0$

$\Rightarrow ab + ab + \ldots + m \text{ times} = 0$

$\Rightarrow (a + a + \ldots + m \text{ times})b = 0$

$\Rightarrow (ma)b = 0 \Rightarrow ma = 0$ $[\because b \neq 0$ and R is an integral domain$]$

$\Rightarrow a$ is of non-zero order. But this not possible and hence our assumption is wrong.

Thus, $o(b) = o(a) = 0$

Case II: When $n > 0$.

$\therefore na = 0$ $[\because n$ is order of $a]$

$\Rightarrow (na)b = 0$

$\Rightarrow (a + a + \ldots\ldots + n \text{ times})b = 0$

NOTES

NOTES

$\Rightarrow ab + ab + \ldots\ldots\ldots + n$ times $= 0$

$\Rightarrow a(b + b + \ldots\ldots\ldots + n$ times$) = 0$

$\Rightarrow a(nb) = 0 \Rightarrow nb = 0$ $[\because a \neq 0$ and R is an integral domain$]$

$\Rightarrow o(a) \leq 0$

Let $o(b) = m < n$. Then $mb = 0$

$\Rightarrow a(mb) = 0$

$\Rightarrow a(b + b + \ldots\ldots\ldots + m$ times$) = 0$

$\Rightarrow ab + ab + \ldots\ldots\ldots + m$ times $= 0$

$\Rightarrow (a + a + \ldots\ldots\ldots + m$ times$)b = 0$

$\Rightarrow (ma)b = 0$

$\Rightarrow ma = 0$ $[\because b \neq 0$ and R is an integral domain$]$

$\Rightarrow o(a) \leq m \Rightarrow n \leq m$, which is impossible

$\therefore\ o(b) = n$

Theorem 4.13: The characteristic of an integral domain R is 0 or $n > 0$ according as the order of any non-zero element regarding as a member of additive group of R is 0 or n.

Proof: If the order of $a = 0$, characteristic of R will be zero. Let the order of a be n. Then $na = 0$.

Proceed in same way as in Case II of Theorem 4.12 till $nb = 0$. But $o(a) = n \Rightarrow n$ is the least positive integer such that $na = 0$.

Also $n.0 = 0$. Thus, n is the least positive integer such that $nx = 0$ for all $x \in$ R and hence characteristic of R is n.

Example 4.31: Show that the set $G = \left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in R\right\}$ is a subring of a ring

$M = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in R\right\}$ under usual addition and multiplication of matrices.

Solution: Given, $a \in$ R

$\therefore$ G is a non-empty subset of R

Let $A = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} \in$ G be any elements.

Then $A - B = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & 0 \end{bmatrix} \in G$

Also, $AB = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \in G$

Thus, G is a subring of M.

Example 4.32: Show that every finite ring has non-zero characteristic.

Solution: Let the characteristic of a finite ring R be 0 and a is any element of R.

Then, for all $a(\neq 0) \in R$ and $n \in N$, $na \neq 0$.

Therefore, $2a, 3a, 4a, \ldots\ldots \in R$

But it is given that R is a finite ring, hence it contains finite number of elements.

$\therefore$ We have,

$n_1 a = n_2 a$ for some positive integers n_1 and n_2 such that $n_1 > n_2$

$\Rightarrow n_1 a - n_2 a = n_2 a - n_2 a$

$\Rightarrow (n_1 - n_2)a = 0$

$\Rightarrow ma = 0$, where $m = (n_1 - n_2)$ is a positive integer

This contradicts our assumption that R is zero.

Thus, R has non-zero characteristic.

Check Your Progress

1. Define the quotient space.
2. What is field of fraction?
3. When R is called Boolean ring?
4. What do you understand by field?
5. State the existence of identity.
6. Give the closure property.
7. State the commutative law.
8. Define the term ring.

4.5 SUBRINGS

Let S be a non-empty subset of a ring (R, +, .), such that, (S, +, .) itself is a ring. Then S is called a **subring** of R. For example, (i) The ring of real numbers is a subring of the ring of complex numbers.

(ii) The ring of integers is a subring of the ring of rational numbers and ring of rational numbers is subring of ring of real numbers.

Note: Every ring R has {0} and R as two subrings which are called **improper subrings** of R and all other subrings, if any is called **proper subrings** of R.

4.5.1 Some Important Theorems on Subrings

Theorem 4.14: The necessary and sufficient conditions for a non-empty subset S of the ring R to be a subring of R are

(i) $a, b \in S \Rightarrow a - b = S$

(ii) $a, b \in S \Rightarrow a.b = S$

Proof: Necessary Condition: Suppose a ring (R, +, .) has a subring (S, +, .)

NOTES

NOTES

Let $a, b \in S$. Since $-b$ is additive inverse of b, therefore $-b \in S$.

Since S is closed under addition, therefore $a - b \in S$.

Also, S is closed under multiplication, therefore $a.b \in S$

Thus, $a, b \in S \Rightarrow a - b \in S$ and $a.b \in S$

Sufficient Condition: Suppose R has a non empty subset S such that for all $a, b \in S$, $a - b \in S$ and $a.b \in S$

Now, $a - a \in S$ [$\because a \in S$]

$\Rightarrow 0 \in S$, i.e., additive identity exists.

Also, $0 - a = -a \in S$, i.e., each element of S possesses additive inverse.

Again $a \in S, -b \in S \Rightarrow a - (-b) = a + b \in S$

Thus, S is closed under addition.

For all $a, b \in S \Rightarrow a.b \in S$ Thus, S is closed under multiplication.

The associativity and commutativity must hold in S as they hold in R because S is a subset of R. Also the distributive laws must hold in S as they hold in R. Thus, S is a subring of R.

Theorem 4.15: The intersection of two subrings is a ring.

Proof: Let a ring R has two subrings S_1 and S_2. Since, S_1 and S_2 has a common element 0 which is an additive identity, thus, $S_1 \cap S_2 \neq f$

Thus, $S_1 \cap S_2$ will be a subring if

(i) $a, b \in S_1 \cap S_2 \Rightarrow a - b \in S_1 \cap S_2$

(ii) $a, b \in S_1 \cap S_2 \Rightarrow a.b \in S_1 \cap S_2$

Let $S_1 \cap S_2$ has two elements a, b. Then $a, b \in S_1$ and $a, b \in S_2$

As S_1 and S_2 are subrings, thus $a - b \in S_1$ and $a - b \in S_2$

$a.b \in S_1$ and $a.b \in S_2 \Rightarrow a - b \in S_1 \cap S_2$ and $a.b \in S_1 \cap S_2$

Thus, $S_1 \cap S_2$ is a subring of R.

Theorem 4.16: An arbitrary intersection of subrings is a subring.

Proof: Let $\{S_i : i \in T\}$ be any family of subrings of a ring R such that for all $i \in T$, S_i is a subring of R. Suppose $S = \bigcap_{i \in T} S_i = \{x \in R : x \in S_i \text{ for all } i \in T\}$

R has an additive identity 0 which is also an element of S_i for each $i \in T$

$\therefore 0 \in S \Rightarrow S \neq f$

Let S has two elements a and b. Then $a, b \in S_i$ for all $i \in T$

As each S_i is a subring of R, thus

For all $i \in T$, $a - b \in S_i$ and $a.b \in S_i$

$\Rightarrow a - b \in \bigcap_{i \in T} S_i$ and $a.b \in \bigcap_{i \in T} S_i$

$\Rightarrow a - b \in S$ and $a.b \in S$

Thus, arbitrary intersection of subring is a subring.

4.5.2 Subfield

If a subset of the elements of a field satisfies the field axioms with the same operations of, then is called a *subfield*. In a finite field of field order, with a prime, there exists a subfield of field order for every dividing.

NOTES

In mathematics, mostly in *algebra*, a **field extension** is a pair of fields such that $E \subseteq F$ the operations of E are those of F restricted to E. In this case, F is an extension field of E and E is a subfield of F. For example, under the usual notions of addition and multiplication, the complex numbers are an extension field of the real numbers; the real numbers are a subfield of the complex numbers.

Field extensions are fundamental in algebraic number theory, and in the study of polynomial roots through **'Galois Theory'**, and are widely used in algebraic geometry.

A subfield of a field L is a subset K of L that is a field with respect to the field operations inherited from L. Equally, a subfield is a subset that contains 1, and is closed under the operations of addition, subtraction, multiplication, and taking the inverse of a non-zero element of K.

As $1 - 1 = 0$, the latter definition implies K and L have the same zero element.

For example, the field of rational numbers is a subfield of the real numbers, which is itself a subfield of the complex numbers. More generally, the field of rational numbers is (or is isomorphic to) a subfield of any field of characteristic 0.

The characteristic of a subfield is the same as the characteristic of the larger field.

A subfield E of a field F is a subset of F that is a field with respect to the field operations of F. Equivalently E is a subset of F that contains 1, and is closed under addition, multiplication, additive inverse and multiplicative inverse of a non-zero element. This means that $1 \in E$, that for all $a, b \in E$ both $a + b$ and $a \cdot b$ are in E, and that for all $a \neq 0$ in E, both $-a$ and $1/a$ are in E.

Field homomorphism's are maps $f: E \to F$ between two fields such that $f(e_1 + e_2) = f(e_1) + f(e_2)$, $f(e_1 e_2) = f(e_1) f(e_2)$, and $f(1_E) = 1_F$, where e_1 and e_2 are arbitrary elements of E. All field homomorphism's are injective. If f is also surjective, it is called an isomorphism (or the fields E and F are called isomorphic).

A field is called a prime field if it has no proper (i.e., strictly smaller) subfields. Any field F contains a prime field. If the characteristic of **F** is p (a prime number), the prime field is isomorphic to the finite field $\mathbf{F}_p$. Otherwise the prime field is isomorphic to **Q**.

4.6 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. You would recall that a vector is defined as a directed line segment, which in algebraic terms is defined as an ordered

NOTES

pair (a, b) being coordinates of the terminal point relative to a fixed coordinate system. Addition of vectors is given by the rule:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

You can easily verify that set of vectors under this forms an abelian group. Also, scalar multiplication is defined by the rule $\alpha (a, b) = (\alpha a, \alpha b)$ which satisfies certain properties. This concept is extended similarly to three dimensions. You can generalize the whole idea through the 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 $< F, +, \cdot >$ be a field. Define a function $\times$ (called scalar multiplication) from $F \times V \to V$, such that, for all $\alpha \in F$, $v \in V$, $\alpha \cdot v \in V$. 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*) $1 \cdot x = x$, 1 being unity of F.

Also then, members of F are called *scalars* and those of V are called *vectors*.

Note: You can use the same symbol + for the two different binary compositions of V and F, for convenience. Similarly, the 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, you can use different symbols like 0_v and 0_F, etc.

Since you generally work with a fixed field, you would only be writing V as 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).

You have defined the scalar multiplication from $F \times V \to V$. You 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 as 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 will consider about only vector spaces over F.

You can also talk about the above system when the scalars are allowed to take values in a ring instead of a field, which leads to the definition of modules.

Theorem 4.17: 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*) $(\alpha - \beta)x = \alpha x - \beta x$, $\alpha, \beta \in F$, $x \in V$

Proof: (*i*) $0.x = (0 + 0).x = 0.x + 0.x$

$\Rightarrow 0 + 0.x = 0.x + 0.x$

$\Rightarrow 0 = 0.x$ (cancellation in V)

(*ii*) $\alpha.0 = \alpha.(0 + 0) = \alpha.0 + \alpha.0 \Rightarrow \alpha.0 = 0$

(*iii*) $(-\alpha)x + \alpha x = [(-\alpha) + \alpha]x = 0 \ . \ x = 0$

$\Rightarrow (-\alpha x) = -\alpha x$

(*iv*) Follows from above.

The following examples illustrate Theorem 4.17

(i) If $< F, +, . >$ 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.

(ii) Let $< F, +, . >$ be a field

Let $V = \{(\alpha_1, \alpha_2) \mid \alpha_1, \alpha_2 \in F\}$

Define + and . (scalar multiplication) by

$$(\alpha_1, \alpha_2) + (\beta_1, \beta_2) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$
$$\alpha(\alpha_1, \alpha_2) = (\alpha\alpha_1, \alpha\alpha_2)$$

You 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 $(\alpha_1, \alpha_2, ..., \alpha_n)$, $\alpha_i \in F$ and define F^n or $F^{(n)} = \{(\alpha_1, \alpha_2, ..., \alpha_n) \mid \alpha_i \in F\}$ as a vector space over F.

(iii) 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 $\mathbf{C}(\mathbf{R})$, $\mathbf{C}(\mathbf{C})$, $\mathbf{R}(\mathbf{Q})$ would be some examples of vector spaces, where $\mathbf{C}$ = Complex Numbers., $\mathbf{R}$ = Reals and $\mathbf{Q}$ = Rationals.

(iv) Let V = set of all real valued continuous functions defined on [0, 1]. Then V forms a vector space over the field $\mathbf{R}$ of reals under addition and scalar multiplication defined by:

$$(f + g)x = f(x) + g(x) \quad f, g \in V$$
$$(\alpha f)x = \alpha f(x) \quad \alpha \in \mathbf{R} \quad \text{for all } x \in [0, 1]$$

It may be recalled here that sum of two continuous functions is continuous and scalar multiple of a continuous function is continuous.

(v) The set $F[x]$ of all polynomials over a field F in an indeterminate x forms a vector space over F with respect to, the usual addition of polynomials and the scalar multiplication defined by:

For $f(x) = a_0 + a_1x + ... + a_nx^n \in F[x], \quad \alpha \in F$

$$\alpha.(f(x)) = \alpha a_0 + \alpha a_1 x + ... + \alpha a_n x^n.$$

(vi) $M_{m \times n}(F)$, 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.

We use the notation $M_n(F)$ for $M_{n \times n}(F)$.

NOTES

NOTES

(vii) Let F be a field and X a non-empty set.

Let $F^X = \{f \mid f : X \to F\}$, the set of all mappings from X to F. Then F^X forms a vector space over F under addition and scalar multiplication defined as follows:

For $f, g \in F^X, \alpha \in F$

Define $f + g : X \to F, \alpha F : X \to, F$ such that

$$(f + g)(x) = f(x) + g(x)$$

$$(\alpha f)(x) = \alpha f(x) \qquad \forall\ x \in X$$

(viii) Let V be the set of all vectors in three dimensional space. Addition in V is taken as the usual addition of vectors in geometry and scalar multiplication is defined as:

$\alpha \in \mathbf{R}$, $\vec{v} \in V \Rightarrow \alpha \vec{v}$ is a vector in V with magnitude $|\alpha|$ times that of V. Then V forms a vector space over $\mathbf{R}$.

4.6.1 Properties of Vector Spaces

We come across different quantities in the study of physical phenomena, such as mass or volume of a body, time, temperature, speed, etc. All these quantities are such that they can be expressed completely by their magnitude, i.e., by a single number. For example, mass of a body can be specified by the number of grams and time by minutes, etc. Such quantities are called scalars. There are certain other quantities which cannot be expressed completely by their magnitude alone, such as velocity, acceleration, force, displacement, momentum, etc. These quantities can be expressed completely by their magnitude and direction and are called vectors.

Representation of Vectors

The best way to represent a vector is with the help of directed line segment.

Suppose A and B are two points, then by the vector $\vec{AB}$, we mean a quantity whose magnitude is the length AB and whose direction is from A to B (Refer Figure 4.1).

A and B are called the end points of the vector $\vec{AB}$. In particular, A is called the initial point and B is called the terminal point. Sometimes a vector $\vec{AB}$ is expressed by a single letter **a**, which is always written in bold type to distinguish it from a scalar. Sometimes, however, we write the vector **a** as $\vec{a}$ or $\overline{a}$.

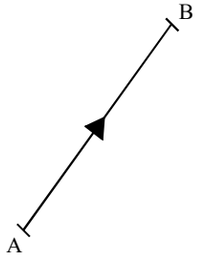


Fig. 4.1 *Vector* $\vec{AB}$

NOTES

Definitions

Modulus of a vector: The modulus or magnitude of a vector is the positive number measuring the length of the line representing it. It is also called the vector's absolute value. Modulus of a vector **a** is denoted by | **a** | or by the corresponding letter *a* in italics.

Unit Vector: A vector whose magnitude is unity is called a unit vector and is generally denoted by $\hat{\mathbf{a}}$. We will always use the symbols $\hat{\mathbf{i}}$, $\hat{\mathbf{j}}$, $\hat{\mathbf{k}}$ to denote the unit vectors along the *x*, *y* and *z* axis respectively in three dimensions.

If **a** is any vector, then $\mathbf{a} = a\,\hat{\mathbf{a}}$, where $\hat{\mathbf{a}}$ is a unit vector having the same direction as **a** (The idea would become clearer when we define the product of a vector with a scalar).

Zero Vector: A vector with zero magnitude and any direction is called a zero vector or a null vector. For example, if in Figure 4.1 the point *B* coincides with the point *A*, the vector $\vec{AB}$ becomes the zero vector $\vec{AB}$. The zero vector is denoted by the symbol **0**.

Equality of Two Vectors: Two vectors are said to be equal if and only if they have the same magnitude and the same direction.

Negative of a Vector: The vector which has the same magnitude as the vector **a**, but has the opposite direction is called negative of **a** and is denoted by –**a**.

Thus, $\vec{AB} = -\vec{BA}$ for any vector $\vec{AB}$.

Free vectors: A vector is said to be a free vector or a sliding vector if its magnitude and direction are fixed but position in space is not fixed.

Note: When we defined equality of vectors, it was assumed that the vectors are free vectors. Thus, two vectors $\vec{AB}$ and $\vec{CD}$ can be equal if *AB* = *CD* and *AB* is parallel to *CD*, although they are not coincident (Refer Figure 4.2).

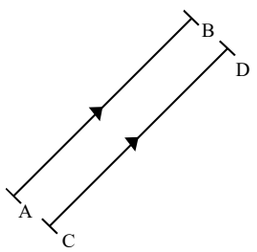


Fig. 4.2 *Equality of Two Vectors*

So, equality of two vectors does not mean that the two vectors are equivalent in all respects. For example, suppose we apply a certain force in a certain direction at two different points of a body, then although the vectors are same still they may have varying effects on the body.

Localized vector is that whose position in space is also fixed.

Coinitial vectors: Vectors having the same initial point are called coinitial vectors or concurrent vectors.

NOTES

Angle Between Two Vectors

Let $\vec{AB}$ = **a** and $\vec{CD}$ = **b** be any two vectors. Through a point *O*, take lines OA_1 and OC_1 parallel to $\vec{AB}$ and $\vec{CD}$ respectively (Refer Figure 4.3).

The angle θ between the lines OA_1 and OC_1 is called the angle between the vectors **a** and **b**, where $0 \le \theta \le \pi$.

If $\theta = 0$ or π, the two vectors are said to be parallel. Thus, parallelism only requires that the two vectors have the same or opposite direction and there is no necessity of relation between their magnitudes.

The vectors are said to be perpendicular if, $\theta = \frac{\pi}{2}$.

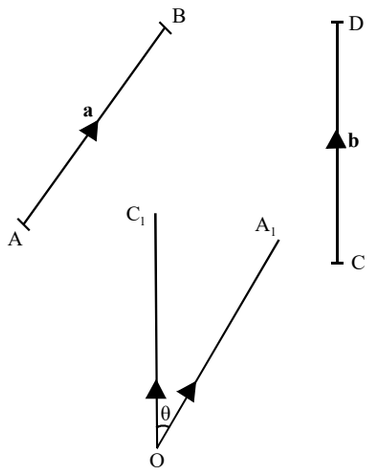


Fig. 4.3 *Angle Between Two Vector*

The Triangle Law

If there are two vectors **a** = $\vec{OA}$ and **b** = $\vec{AB}$, represented as two sides of a triangle, as shown in Figure 4.4, then the third side $\vec{OB}$, shown as **c** shows the resultant.

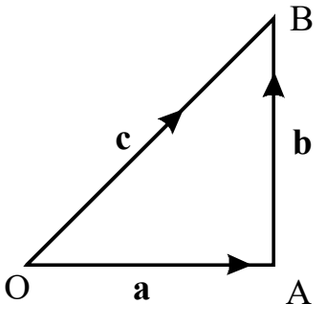


Fig.4.4 *Triangle Law*

The Parallelogram Law

Let **a** and **b** be any two vectors. Through a point *O*, take a line *OA* parallel to the vector **a** and of length equal to *a*. Then, $\vec{OA}$ = **a**. Again through *A,* take a line *AB* the vector ***b*** having length *b,* then $\vec{AB}$ = **b**.

We define the sum of **a** and **b** as (**a** + **b**) to be the vector $\vec{OB}$ and write,

$\mathbf{a} + \mathbf{b} = \vec{OB}$.

Similarly, the sum of three or more vectors can be obtained by repeated application of this definition.

NOTES

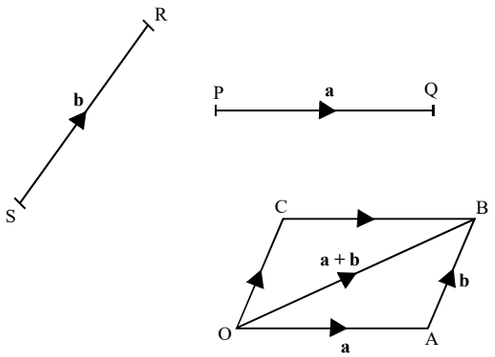


Fig. 4.5 *Parallelogram Law*

Notes: 1. The process by which we obtained an equal vector $\vec{OA}$ from **a** is sometimes referred to as translation of vectors. It is obtained by moving the line segment of **a** from its original position to the new position *OA*, without disturbing the direction.
2. This method of addition is called parallelogram law of addition.

Derivative of Sum

Vector Addition is Commutative

Let **a** and **b** be any two vectors. We get,

$$\vec{OB} = \mathbf{a} + \mathbf{b}$$ [Refer Figure 4.5]

Now complete the parallelogram *OABC*, then

$$\vec{OC} = \mathbf{b} \quad \text{and} \quad \vec{CB} = \mathbf{a}$$

Also, $\vec{OC} + \vec{CB} = \vec{OB}$ [By definition of addition]

$\Rightarrow$ $\mathbf{b} + \mathbf{a} = \vec{OB}$

Hence, $\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a} = \vec{OB}$

This proves the result.

Vector Addition is Associative

Let, $\mathbf{a} = \vec{OA}$

$\mathbf{b} = \vec{AB}$

$\mathbf{c} = \vec{BC}$

be three vectors.

NOTES

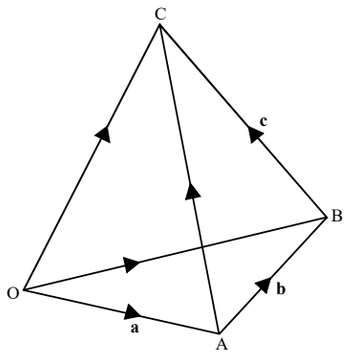


Fig. 4.6 *Vector Addition*

Then, $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = (\vec{OA} + \vec{AB}) + \vec{BC}$

$= \vec{OB} + \vec{BC}$

$= \vec{OC}$ ... (4.1)

And, $\mathbf{a} + (\mathbf{b} + \mathbf{c}) = \vec{OA} + (\vec{AB} + \vec{BC})$

$= \vec{OA} + \vec{AC}$

$= \vec{OC}$ ... (4.2)

Thus, from Equations (4.1) and (4.2), we have,

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$$

Hence proved.

Existence of Identity

If **a** is any vector and **0** is the zero vector then,

$$\mathbf{a} + \mathbf{0} = \mathbf{a}$$

In Figure 4.6, if *B* coincides with *A* then,

$$\vec{AB} = \vec{AA} = \mathbf{0}$$

By definition

$$\vec{OB} = \vec{OA} + \vec{AB}$$

$\Rightarrow$ $\vec{OA} = \vec{OA} + \vec{AA}$

$\Rightarrow$ $\mathbf{a} = \mathbf{a} + \mathbf{0}$

Hence, proved.

Existence of Inverse

If **a** is any vector, then a vector –**a**, is called inverse of **a** such that,

$$\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$$

Let, $\mathbf{a} = \vec{OA}$ [By Definition of Addition]

Then, by definition, $-\mathbf{a} = \vec{AO}$

Thus, $\vec{OA} + \vec{AO} = \vec{OO}$

$\Rightarrow$ $\mathbf{a} + (-\mathbf{a}) = \mathbf{0}$

In view of the above properties, we can say that the set V of vectors with addition of vectors as a binary composition forms an abelian group.

Subtraction of Vectors: By $\mathbf{a} - \mathbf{b}$ we mean $\mathbf{a} + (-\mathbf{b})$, where $-\mathbf{b}$ is inverse of $\mathbf{b}$ is also called negative of $\mathbf{b}$ as defined earlier.

NOTES

Multiplication of a Vector by a Scalar

Suppose $\mathbf{a}$ is a vector and n is a scalar. By $n\mathbf{a}$ we mean a vector whose magnitude is $|n||\mathbf{a}|$, i.e., $|n|$ times the magnitude of $\mathbf{a}$ and whose direction is that of $\mathbf{a}$ or opposite to that of $\mathbf{a}$ depending on n being positive or negative.

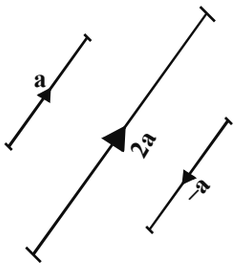


Fig. 4.7 *Scalar Multiplication and Negation of a Vector*

Generally, the scalar is written on the left of the vector, although one could write it on the right too.

Note: We do not put any sign (. or ×) between n and $\mathbf{a}$ when we write $n\mathbf{a}$.

The following results can be proved:

(i) $(mn)\mathbf{a} = m(n\mathbf{a})$

(ii) $0\mathbf{a} = \mathbf{0}$

(iii) $n(\mathbf{a} + \mathbf{b}) = n\mathbf{a} + n\mathbf{b}$

(iv) $(m + n)\mathbf{a} = m\mathbf{a} + n\mathbf{a}$

Proofs: (i) and (ii) are direct consequence of the definition and hardly need any further proof.

(iii) $n(\mathbf{a} + \mathbf{b}) = n\mathbf{a} + n\mathbf{b}$. Let n be positive.

Suppose $\mathbf{a} = \vec{OA}$, $\mathbf{b} = \vec{AB}$

Then, $\vec{OB} = \mathbf{a} + \mathbf{b}$

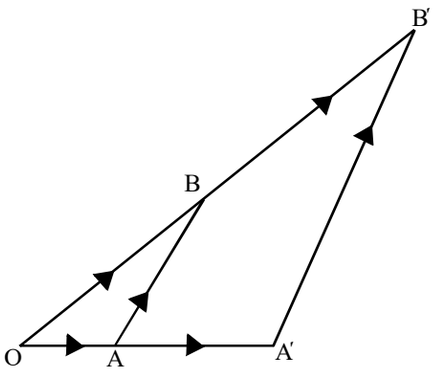


Fig. 4.8 *Graphical Representation of na + nb*

NOTES

Let A', B' be points on OA and OB (or OA and OB produced) respectively such that,

$$OA' = n \cdot OA$$

$$OB' = n \cdot OB$$

Then, $\overrightarrow{OA'} = n\overrightarrow{OA} = n\mathbf{a}$

$$\overrightarrow{OB'} = n\overrightarrow{OB} = n(\mathbf{a} + \mathbf{b})$$

Also, $A'B' = nAB$ (Where, OAB and $OA'B'$ are similar triangles)

$\Rightarrow$ $\overrightarrow{A'B'} = n\overrightarrow{AB}$

$$= n\mathbf{b}$$

Now, $\overrightarrow{OB'} = \overrightarrow{OA'} + \overrightarrow{A'B'}$

$\Rightarrow$ $n(\mathbf{a} + \mathbf{b}) = n\mathbf{a} + n\mathbf{b}$

This proves our assertion.

When n is negative, the figure would change in this case as now A and A' will lie on the opposite sides of O.

Proceeding as before, we get,

$$\overrightarrow{OA'} = n\mathbf{a}$$

$$\overrightarrow{A'B'} = n\mathbf{b}$$

$$\overrightarrow{OB'} = n(\mathbf{a} + \mathbf{b})$$

Which proves the result as $\overrightarrow{OB'} = \overrightarrow{OA'} + \overrightarrow{A'B'}$

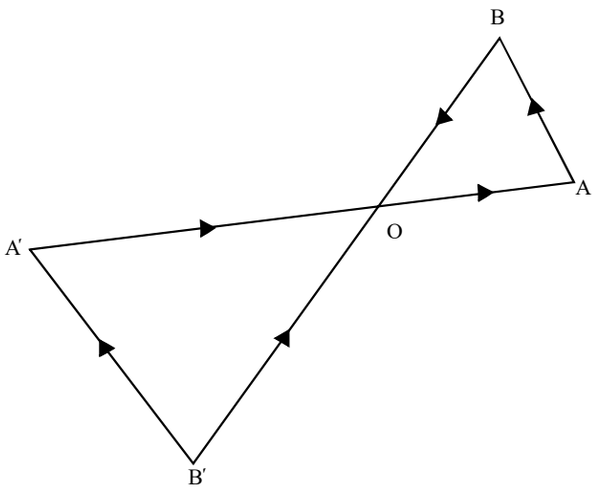


Fig. 4.9 *Graphical Representation of na + nb when n is Negative*

(*iv*) Suppose m and n are positive.

We show that, $(m + n)\mathbf{a} = m\mathbf{a} + n\mathbf{a}$

Let, $m + n = k$

Then,

LHS $= \mathbf{a} + \mathbf{a} + \mathbf{a} + \ldots + \mathbf{a}$ (k times)

Also, RHS $= m\mathbf{a} + n\mathbf{a}$

$$= \underbrace{(\mathbf{a}+\mathbf{a}+...+\mathbf{a})}_{(m \text{ times})} + \underbrace{(\mathbf{a}+\mathbf{a}+...+\mathbf{a})}_{(n \text{ times})}$$

$$= \mathbf{a}+\mathbf{a}+\ldots+\mathbf{a} \quad (m+n \text{ times})$$

$$\Rightarrow \quad \text{LHS} = \text{RHS} \quad (k \text{ times})$$

One can easily prove the result even if m or n is negative.

Aliter: Direction of the vector $(m+n)\mathbf{a}$ is same as that of $\mathbf{a}$, since $m+n>0$.

Also, directions of the vectors $m\mathbf{a}$ and $n\mathbf{a}$ are same as that of $\mathbf{a}$ and, therefore, direction of $m\mathbf{a}+n\mathbf{a}$ is also same as that of $\mathbf{a}$.

Now, magnitude of the vector $(m+n)\mathbf{a}$ is,

$$|m+n|\ |\boldsymbol{a}| = (m+n)a$$
$$= ma + na$$
$$= |m|\ |\mathbf{a}| + |n|\ |\mathbf{a}|$$
$$= |m\ \mathbf{a}| + |n\ \mathbf{a}| \text{ as they have same direction.}$$
$$= |m\mathbf{a} + n\mathbf{a}|$$

This is the magnitude of the vector $m\mathbf{a}+n\mathbf{a}$, i.e., the vector on the RHS.

Thus, the two vectors have same direction and magnitude and hence they are equal.

The different cases when either m or n is negative or both m and n are negative can be dealt with similarly.

Theorem 4.18: Two non-zero vectors $\mathbf{a}$ and $\mathbf{b}$ are parallel if and only if a scalar t is such that, $\mathbf{a} = t\mathbf{b}$.

Proof: Let $\mathbf{a}$ be parallel to $\mathbf{b}$. Then the direction of $\mathbf{a}$ and $\mathbf{b}$ is same or opposite.

Suppose direction of $\mathbf{a}$ and $\mathbf{b}$ is same.

If $a = b$, where a, b are the magnitudes of $\mathbf{a}$ and $\mathbf{b}$ respectively, then $t = 1$ serves our purpose, because then,

$$a = 1.\ b \ \Rightarrow\ \mathbf{a} = 1\mathbf{b}$$

If $a \neq b$, then we can always find a scalar t such that, $a = tb$

(Property of real numbers, indeed we take $t = a/b$)

For this t, we have,

$$\mathbf{a} = t\mathbf{b}$$

So, when direction of $\mathbf{a}$ and $\mathbf{b}$ is same, the result is true.

Now, let direction of $\mathbf{a}$ and $\mathbf{b}$ be opposite. The same scalar will do the job except that in this case we will take t with the negative sign.

Conversely, let $\mathbf{a}$ and $\mathbf{b}$ be two vectors such that, $\mathbf{a} = t\mathbf{b}$ for some scalar t.

By definition of equality of vectors this implies that $\mathbf{a}$ and $t\mathbf{b}$ have same direction.

Again, $\mathbf{a}$ and $t\mathbf{b}$ have same or opposite direction

[By definition of $t\mathbf{b}$]

$\Rightarrow$ $\mathbf{a}$ and $\mathbf{b}$ are two vectors having same or opposite direction.

$\Rightarrow$ $\mathbf{a}$ and $\mathbf{b}$ are parallel.

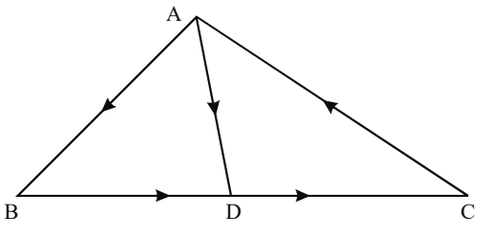
NOTES

NOTES

Hence proved.

Example 4.33: If ABC is a triangle and D is middle point of BC, show that $\overrightarrow{BD} = \frac{1}{2}\overrightarrow{BC}$.

Solution: In figure below, $\overrightarrow{BD}$ is a vector with magnitude $BD = \frac{1}{2}BC$ and $\overrightarrow{BC}$ is a vector with magnitude BC.



Since directions of $\overrightarrow{BC}$ and $\overrightarrow{BD}$ vectors are same, it follows that $\overrightarrow{BD} = \frac{1}{2}\overrightarrow{BC}$

Example 4.34: Show that the vector equation, $\mathbf{a} + \mathbf{x} = \mathbf{b}$ has a unique solution.

Solution: We know that,

$$\mathbf{a} + [-\mathbf{a} + \mathbf{b}] = [\mathbf{a} + (-\mathbf{a})] + \mathbf{b} \quad \text{[By Associativity Law]}$$
$$= \mathbf{0} + \mathbf{b} \quad \text{[By Identity Law]}$$
$$= \mathbf{b}$$

$\Rightarrow$ $-\mathbf{a} + \mathbf{b}$ is a solution of $\mathbf{a} + \mathbf{x} = \mathbf{b}$.

Suppose that $\mathbf{y}$ is any other solution of this equation.

Then,
$$\mathbf{y} = \mathbf{0} + \mathbf{y}$$
$$= [(-\mathbf{a}) + \mathbf{a}] + \mathbf{y}$$
$$= (-\mathbf{a}) + (\mathbf{a} + \mathbf{y})$$
$$= -\mathbf{a} + \mathbf{b}, \text{ as } \mathbf{y} \text{ is a solution.}$$

$\Rightarrow$ $-\mathbf{a} + \mathbf{b}$ is the unique solution.

Position Vector

Let O be a fixed point, called origin. If P is any point in space and the vector $\overrightarrow{OP} = \mathbf{r}$, we say that position vector of P is $\mathbf{r}$ with respect to the origin O, and express this as $P(\mathbf{r})$.

Whenever we talk about some points with position vectors it is to be understood that all those vectors are expressed with respect to the same origin. To prove that:

If A and B are any two points with position vectors $\mathbf{a}$ and $\mathbf{b}$ then,

$$\overrightarrow{AB} = \mathbf{b} - \mathbf{a}$$

If O is the origin, then it is given that,

$$\overrightarrow{OA} = \mathbf{a}$$

$\vec{OB} = \mathbf{b}$

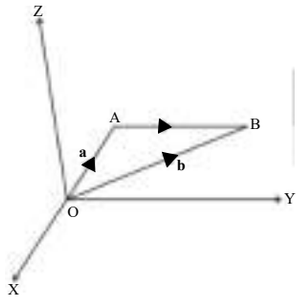


Fig. 4.10 *Position Vector*

Also, $\vec{OA} + \vec{AB} = \vec{OB}$ [By Addition Law]

$\Rightarrow \quad \vec{AB} = \vec{OB} - \vec{OA}$

$\Rightarrow \quad \vec{AB} = \mathbf{b} - \mathbf{a}$

Components of a Vector

Let P be any point in space with coordinates x, y, z. Complete the parallelopiped as shown in Figure 4.11.

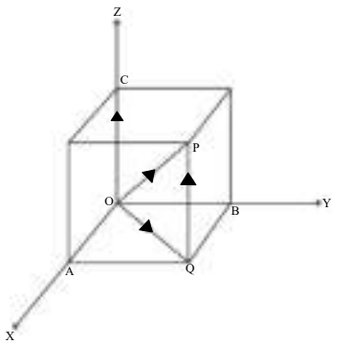


Fig. 4.11 *Components of a Vector*

Then, co-ordinates of the points A, B, C are $(x, 0, 0), (0, y, 0), (0, 0, z)$ respectively.

Suppose that position vector of P is $\mathbf{r}$,

i.e., $\vec{OP} = \mathbf{r}$

Also, let $\hat{\mathbf{i}}$, $\hat{\mathbf{j}}$, $\hat{\mathbf{k}}$, be the unit vectors along the three coordinates x, y and z-axis.

Now, $OA = x$

$\Rightarrow \quad \vec{OA} = x\hat{\mathbf{i}}$

Note: $x\hat{\mathbf{i}}$ is a vector whose magnitude is 1. $x = x$ and whose direction is that of the x-axis and this is precisely the vector $\vec{OA}$.

Similarly, $\vec{OB} = y\hat{\mathbf{j}}$

$\vec{OC} = z\hat{\mathbf{k}}$

NOTES

From the triangle OPQ,

$$\mathbf{r} = \overrightarrow{OP} = \overrightarrow{OQ} + \overrightarrow{QP}$$

$$= \overrightarrow{OQ} + \overrightarrow{OC}$$

Also from the triangle OAQ,

$$\overrightarrow{OQ} = \overrightarrow{OA} + \overrightarrow{AQ}$$

$$= \overrightarrow{OA} + \overrightarrow{OB}$$

Thus, $\mathbf{r} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC} = x\,\hat{\mathbf{i}} + y\,\hat{\mathbf{j}} + z\,\hat{\mathbf{k}}$.

Hence, if P is any point with position vector $\mathbf{r}$ and coordinates x, y, z then,

$$\mathbf{r} = x\,\hat{\mathbf{i}} + y\,\hat{\mathbf{j}} + z\,\hat{\mathbf{k}} \qquad \text{... (4.3)}$$

Which can be expressed by writing,

$$\mathbf{r} = (x, y, z) \qquad \text{... (4.4)}$$

Thus, Equations (4.3) and (4.4) mean exactly the same. x, y, z are called the components of the vector $\mathbf{r}$.

Note: $OP = |\mathbf{r}| = r$

Using geometry we find,

$$r^2 = OQ^2 + QP^2 = OA^2 + AQ^2 + QP^2$$

$$= OA^2 + OB^2 + OC^2$$

$$\Rightarrow \qquad r^2 = x^2 + y^2 + z^2$$

i.e., the square of the modulus of a vector is equal to the sum of the squares of its rectangular components.

Note: The vectors $\hat{\mathbf{i}}$, $\hat{\mathbf{j}}$, $\hat{\mathbf{k}}$ are said to form an orthonormal triad.

Angle Between Two Vectors: Let A and B be two points in space with position vectors $\mathbf{a}$ and $\mathbf{b}$, and the coordinates of A and B be respectively (a_1, a_2, a_3) and (b_1, b_2, b_3).

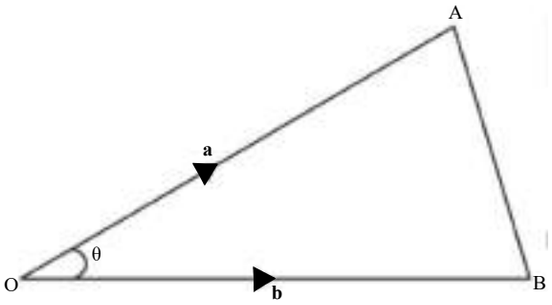


Fig. 4.12 *Angle Between Two Vectors*

Then,

$$\mathbf{a} = \overrightarrow{OA} = a_1\,\hat{\mathbf{i}} + a_2\,\hat{\mathbf{j}} + a_3\,\hat{\mathbf{k}}$$

$$\mathbf{b} = \overrightarrow{OB} = b_1\,\hat{\mathbf{i}} + b_2\,\hat{\mathbf{j}} + b_3\,\hat{\mathbf{k}}$$

$\Rightarrow$ $\mathbf{b} - \mathbf{a} = (b_1 - a_1)\,\hat{\mathbf{i}} + (b_2 - a_2)\,\hat{\mathbf{j}} + (b_3 - a_3)\,\hat{\mathbf{k}}$

Also, $\vec{AB} = \mathbf{b} - \mathbf{a}$

Thus, $AB^2 = (b_1 - a_1)^2 + (b_2 - a_2)^2 + (b_3 - a_3)^2$

NOTES

Let θ be the angle between **a** and **b**. When θ is the angle between OA and OB, we have,

$$AB^2 = OA^2 + OB^2 - 2\,OA\,.\,OB\cos\theta$$

$\Rightarrow$ $$\cos\theta = \frac{OA^2 + OB^2 - AB^2}{2\,OA\,.\,OB}$$

$$= \frac{(a_1^2 + a_2^2 + a_3^2) + (b_1^2 + b_2^2 + b_3^2) - \Sigma(b_1 - a_1)^2}{2\,a\,.\,b}$$

$\Rightarrow$ $$\cos\theta = \frac{a_1b_1 + a_2b_2 + a_3b_3}{\sqrt{a_1^2 + a_2^2 + a_3^2}\sqrt{b_1^2 + b_2^2 + b_3^2}}$$

$\because$ $a^2 = a_1^2 + a_2^2 + a_3^2$

And, $b^2 = b_1^2 + b_2^2 + b_3^2$

Example 4.35: Find the angle between the vectors

$$\mathbf{a} = \hat{\mathbf{i}} + 2\,\hat{\mathbf{j}} + 3\,\hat{\mathbf{k}}$$

$$\mathbf{b} = \hat{\mathbf{i}} - \hat{\mathbf{j}} + 2\,\hat{\mathbf{k}}$$

Solution: $\mathbf{a} = (1, 2, 3)$

$\mathbf{b} = (1, -1, 2)$

$\Rightarrow$ $a^2 = 1 + 4 + 9 = 14$

$b^2 = 1 + 1 + 4 = 6$

If θ is the angle between **a** and **b**, then

$$\cos\theta = \frac{1\times1 + 2\times(-1) + 3\times2}{\sqrt{14}\sqrt{6}} = \frac{5}{\sqrt{84}}$$

Hence, $\theta = \cos^{-1}\dfrac{5}{\sqrt{84}}$

Section Formula

To find the position vector of a point dividing the join of two given points in a given ratio.

Let A and B be the two given points with position vectors **a** and **b** respectively. Suppose the point $R(\mathbf{r})$ divides AB in the ratio $m : n$.

i.e., $AR : RB = m : n$

NOTES

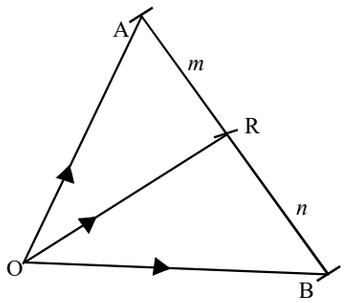


Fig. 4.13 *Section Formula*

Then, $$\frac{AR}{m} = \frac{RB}{n}$$

Or, $$nAR = mRB$$

$\Rightarrow$ $$n\overrightarrow{AR} = m\overrightarrow{RB}$$

$\Rightarrow$ $$n(\mathbf{r} - \mathbf{a}) = m(\mathbf{b} - \mathbf{r})$$

$\Rightarrow$ $$n\mathbf{r} + m\mathbf{r} = m\mathbf{b} + n\mathbf{a}$$

$\Rightarrow$ $$\mathbf{r} = \frac{n\mathbf{a} + m\mathbf{b}}{n + m}$$

This gives the required value of **r**.

Corollary. If R is the middle point of AB, then $\mathbf{r} = \frac{\mathrm{a} + \mathrm{b}}{2}$ as in this case $m = n$.

Theorem 4.19: Three distinct points A, B, R with position vectors a, b, r are collinear if and only if there exist three numbers x, y, z (not all zero) such that

$$x\mathbf{a} + y\mathbf{b} + z\mathbf{c} = 0$$

And $$x + y + z = 0$$

Proof*:* Let the three points A, B, R be collinear

Then, R divides AB in some ratio, say $m : n$.

Where, $$\mathbf{r} = \frac{n\mathbf{a} + m\mathbf{b}}{n + m}$$

$\Rightarrow$ $$(n + m)\mathbf{r} = n\mathbf{a} + m\mathbf{b}$$

Or, $$n\mathbf{a} + m\mathbf{b} - (n + m)\mathbf{r} = 0$$

Let, $$x = n, y = m, z = -(n + m)$$

Then, $$x\mathbf{a} + y\mathbf{b} + z\mathbf{r} = 0$$

Where, $x + y + z = n + m - (n + m) = 0$

Thus, all x, y, z can't be zero. Hence proved.

Conversely, Suppose $\exists\, x, y, z$, not all zero such that,

$$x\mathbf{a} + y\mathbf{b} + z\mathbf{r} = 0$$

And, $$x + y + z = 0$$

Let, $z \neq 0$

Then, $x + y + z = 0$

$\Rightarrow$ $x + y = -z$

$\Rightarrow$ $(x + y)\,\mathbf{r} = -z\,\mathbf{r}$

Also, $-z\,\mathbf{r} = x\mathbf{a} + y\mathbf{b}$

Thus, $x\mathbf{a} + y\mathbf{b} = (x + y)\,\mathbf{r}$

$\Rightarrow$ $\mathbf{r} = \dfrac{x\mathbf{a} + y\mathbf{b}}{x + y}$, as $x + y \neq 0$, otherwise $z = 0$

$\Rightarrow$ R divides AB in the ratio $x : y$

$\Rightarrow$ R lies on AB

$\Rightarrow$ A, B, R are collinear.

Hence proved.

Example 4.36: Show that the points with position vectors $3\mathbf{a} - 2\mathbf{b} + 4\mathbf{c}$, $\mathbf{a} + \mathbf{b} + \mathbf{c}$, and $-\mathbf{a} + 4\mathbf{b} - 2\mathbf{c}$ are collinear.

Solution: The three points will be collinear if and only if we can find x, y, z (not all zero) such that,

$$x(3\mathbf{a} - 2\mathbf{b} + 4\mathbf{c}) + y(\mathbf{a} + \mathbf{b} + \mathbf{c}) + z(-\mathbf{a} + 4\mathbf{b} - 2\mathbf{c}) = 0 \quad \ldots(4.5)$$

And, $x + y + z = 0$ $\ldots(4.6)$

Equation (4.5) can be written as,

$$(3x + y - z)\,\mathbf{a} + (-2x + y + 4z)\,\mathbf{b} + (4x + y - 2z)\mathbf{c} = 0$$

This gives,

$$3x + y - z = 0$$
$$-2x + y + 4z = 0$$
$$4x + y - 2z = 0$$

Also, we should have $x + y + z = 0$. One non-zero solution of these four equations is,

$$x = z = 1, \quad y = -2$$

We find that the three given points are collinear.

Symmetry in $\mathbf{a}, \mathbf{b}, \mathbf{c}$ implies that R will also be the point that divides BE and CF in the ratio 2 : 1. This in turn yields that R is the required point where the three medians meet and it also trisects them.

Coplanar Points

It can be proved that four points with position vectors $\mathbf{a}, \mathbf{b}, \mathbf{c}$ and $\mathbf{d}$ are coplanar if and only if we can find scalars (not all zero) x, y, z and t such that,

$$x\mathbf{a} + y\mathbf{b} + z\mathbf{c} + t\mathbf{d} = 0$$

And, $x + y + z + t = 0$

Example 4.37: Show that the points with position vectors $6\mathbf{a} - 4\mathbf{b} + 4\mathbf{c}$, $-\mathbf{a} - 2\mathbf{b} - 3\mathbf{c}$, $\mathbf{a} + 2\mathbf{b} - 5\mathbf{c}$, $-4\mathbf{c}$ are coplanar.

Solution: The four points will be coplanar if we can find scalars x, y, z and t (not all zero) such that,

$$x(6\mathbf{a} - 4\mathbf{b} + 4\mathbf{c}) + y(-\mathbf{a} - 2\mathbf{b} - 3\mathbf{c}) + z(\mathbf{a} + 2\mathbf{b} - 5\mathbf{c}) + t(-4\mathbf{c}) = 0 \quad ...(4.7)$$

And, $$x + y + z + t = 0 \quad ...(4.8)$$

Rearranging Equation (4.7), we get,

NOTES

$$(6x - y + z)\mathbf{a} + (-4x - 2y + 2z)\mathbf{b} + (4x - 3y - 5z - 4t)\,\mathbf{c} = 0$$

This equation suggests that,

$$6x - y + z = 0$$
$$-4x - 2y + 2z = 0$$
$$4x - 3y - 5z - 4t = 0$$

Also, we should have, $x + y + z + t = 0$

Which gives, $x = 0, y = 1, z = 1, t = -2$

This is a non-zero solution of the equations and thus the four points are coplanar.

Dot and Cross Product of Vectors

Product of two vectors is defined in two ways, the scalar product and the vector product.

Scalar Product or Dot Product

If **a** and **b** are two vectors, then their scalar product **a . b** (read as **a** dot **b**) is defined by,

$$\mathbf{a} \cdot \mathbf{b} = ab \cos \theta$$

Where, a and b are the magnitudes of the vectors **a** and **b** respectively and θ is the angle between the vectors **a** and **b**.

It is clear from definition that dot product of two vectors is a scalar quantity.

Hence proved.

Scalar Product is Commutative

$$\mathbf{a} \cdot \mathbf{b} = ab \cos \theta$$
$$= ba \cos \theta$$
$$= \mathbf{b} \cdot \mathbf{a}$$

Theorem 4.20: Two non-zero vectors **a** and **b** are perpendicular if and only if,

$$\mathbf{a} \cdot \mathbf{b} = 0$$

Proof: Let **a** and **b** be two non-zero perpendicular vectors. Then,

$$\mathbf{a} \cdot \mathbf{b} = ab \cos\left(\frac{\pi}{2}\right) = 0$$

Conversely, Let $\mathbf{a} \cdot \mathbf{b} = 0$

$\Rightarrow$ $ab \cos \theta = 0$

Where, θ is the angle between **a** and **b**.

$\Rightarrow$ $\cos \theta = 0$ [As **a** and **b** are non-zero]

$\Rightarrow$ $$\theta = \frac{\pi}{2}$$

$\Rightarrow$ **a** and **b** are perpendicular.

The following results are trivial:

$$\hat{\mathbf{i}} \cdot \hat{\mathbf{i}} = \hat{\mathbf{j}} \cdot \hat{\mathbf{j}} = \hat{\mathbf{k}} \cdot \hat{\mathbf{k}} = 1$$

$$\hat{\mathbf{i}} \cdot \hat{\mathbf{j}} = \hat{\mathbf{j}} \cdot \hat{\mathbf{k}} = \hat{\mathbf{k}} \cdot \hat{\mathbf{i}} = 0$$

Definition. By $\mathbf{a}^2$ we will always mean **a** . **a**.

Thus, $\mathbf{a} \cdot \mathbf{a} = a\,a \cos 0 = \mathbf{a}^2$.

Example 4.38: Show that **a**. (–**b**) = –**a** . **b**

Solution: We have,

$\mathbf{a}.(-\mathbf{b}) = ab \cos(\pi - \theta)$, where θ is angle between **a** and **b**.

$= -ab \cos\theta$

$= (-\mathbf{a}) \cdot \mathbf{b}$.

Distributive Law

Prove that, $\mathbf{a}.(\mathbf{b} + \mathbf{c}) = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{c}$.

Proof: Let, $\vec{OA} = \mathbf{a}$

$\vec{OB} = \mathbf{b}$

$\vec{BC} = \mathbf{c}$

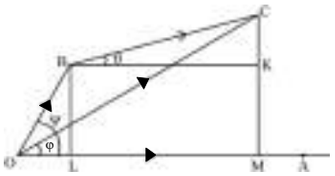


Fig. 4.14 *Distributive Law*

Let *BL* and *CM* be perpendiculars from *B* and *C* on $\vec{OA}$ respectively and *BK* be perpendicular from *B* on *CM*.

Then, $\mathbf{a} \cdot \mathbf{b} = ab \cos\psi = a \cdot OL$

$\mathbf{a} \cdot \mathbf{c} = ac \cos\theta = a \cdot BK = a \cdot LM$

$\Rightarrow$ RHS $= \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{c} = a \cdot OL + a \cdot LM = a(OL + LM)$

$= a \cdot OM$

Again, $\vec{OB} + \vec{BC} = \vec{OC}$

$\Rightarrow \mathbf{b} + \mathbf{c} = \vec{OC}$

$\Rightarrow$ LHS $= \mathbf{a}(\mathbf{b} + \mathbf{c}) = \mathbf{a} \cdot \vec{OC}$

$= a \cdot OC \cos\varphi$

$= a \cdot OM$

Hence, the result is analysed as follows:

An immediate consequence of the above result is,

$$(\mathbf{a} + \mathbf{b})^2 = (\mathbf{a} + \mathbf{b}) \cdot (\mathbf{a} + \mathbf{b})$$

NOTES

$$= \mathbf{a} \cdot \mathbf{a} + \mathbf{a} \cdot \mathbf{b} + \mathbf{b} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b}$$
$$= \mathbf{a}^2 + \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \cdot \mathbf{b} + \mathbf{b}^2$$
$$= \mathbf{a}^2 + 2\mathbf{ab} + \mathbf{b}^2$$

NOTES

Similarly, we can prove that,

$$(\mathbf{a} - \mathbf{b})^2 = \mathbf{a}^2 - 2\mathbf{ab} + \mathbf{b}^2$$
$$(\mathbf{a} + \mathbf{b}) \cdot (\mathbf{a} - \mathbf{b}) = \mathbf{a}^2 - \mathbf{b}^2$$

Scalar Product in Terms of the Components

Let, $\mathbf{a} = (a_1, a_2, a_3) = a_1 \hat{\mathbf{i}} + a_2 \hat{\mathbf{j}} + a_3 \hat{\mathbf{k}}$

$\mathbf{b} = (b_1, b_2, b_3) = b_1 \hat{\mathbf{i}} + b_2 \hat{\mathbf{j}} + b_3 \hat{\mathbf{k}}$

If **a** and **b** be any two vectors, then

$$\mathbf{a} \cdot \mathbf{b} = (a_1 \hat{\mathbf{i}} + a_2 \hat{\mathbf{j}} + a_3 \hat{\mathbf{k}}) \cdot (b_1 \hat{\mathbf{i}} + b_2 \hat{\mathbf{j}} + b_3 \hat{\mathbf{k}})$$
$$= a_1 b_1 \hat{\mathbf{i}} \cdot \hat{\mathbf{i}} + a_2 b_2 \hat{\mathbf{j}} \cdot \hat{\mathbf{j}} + a_3 b_3 \hat{\mathbf{k}} \cdot \hat{\mathbf{k}}$$

[Other terms being zero]

$$= a_1 b_1 + a_2 b_2 + a_3 b_3$$

Angle Between Two Vectors

Since, $\mathbf{a}.\mathbf{b} = ab \cos \theta$

$$\Rightarrow \quad \cos \theta = \frac{\mathbf{a}.\mathbf{b}}{ab}$$

$$= \frac{a_1 b_1 + a_2 b_2 + a_3 b_3}{\sqrt{a_1^2 + a_2^2 + a_3^2}\sqrt{b_1^2 + b_2^2 + b_3^2}}$$

This formula has been proved earlier.

Example 4.39: Show that the vectors **a**, **b**, **c** given by,

$$7\mathbf{a} = 2\hat{\mathbf{i}} + 3\hat{\mathbf{j}} + 6\hat{\mathbf{k}}$$

$$7\mathbf{b} = 3\hat{\mathbf{i}} - 6\hat{\mathbf{j}} + 2\hat{\mathbf{k}}$$

$$7\mathbf{c} = 6\hat{\mathbf{i}} + 2\hat{\mathbf{j}} - 3\hat{\mathbf{k}}$$

are of unit length and are mutually perpendicular.

Solution: The three vectors are,

$$\mathbf{a} = \left(\frac{2}{7}, \frac{3}{7}, \frac{6}{7}\right)$$

$$\mathbf{b} = \left(\frac{3}{7}, \frac{-6}{7}, \frac{2}{7}\right)$$

$$\mathbf{c} = \left(\frac{6}{7}, \frac{2}{7}, \frac{-3}{7}\right)$$

Now, $$a = \sqrt{\left(\frac{2}{7}\right)^2 + \left(\frac{3}{7}\right)^2 + \left(\frac{6}{7}\right)^2} = \frac{1}{7}\sqrt{4+9+36} = 1$$

$$b = \sqrt{\left(\frac{3}{7}\right)^2 + \left(\frac{-6}{7}\right)^2 + \left(\frac{2}{7}\right)^2} = 1$$

$$c = \sqrt{\left(\frac{6}{7}\right)^2 + \left(\frac{2}{7}\right)^2 + \left(\frac{-3}{7}\right)^2} = 1$$

This shows that the given vectors are of unit length.

Again,

$$\mathbf{a} \cdot \mathbf{b} = \frac{2}{7}\times\frac{3}{7} + \frac{3}{7}\times\left(\frac{-6}{7}\right) + \frac{6}{7}\times\frac{2}{7} = \frac{1}{49}(6 - 18 + 12) = 0$$

Thus, **a** and **b** are perpendicular:

Similarly, $$\mathbf{b} \cdot \mathbf{c} = \frac{3}{7}\times\frac{6}{7} + \left(\frac{-6}{7}\right)\times\frac{2}{7} + \frac{2}{7}\times\left(\frac{-3}{7}\right) = \frac{1}{49}(18 - 12 - 6) = 0$$

$$\mathbf{c} \cdot \mathbf{a} = \frac{6}{7}\times\frac{2}{7} + \frac{2}{7}\times\frac{3}{7} + \left(\frac{-3}{7}\right)\times\frac{6}{7} = \frac{1}{49}(12 + 6 - 18) = 0$$

This implies that **b** is perpendicular to **c** and **c** is perpendicular to **a**.

Thus, **a, b, c** are mutually perpendicular.

Cross Product of Two Vectors

Vector product is also termed as cross product. If **a** and **b** are two vectors, then their vector product **a** × **b** (read as **a** cross **b**) is defined by,

$$\mathbf{a} \times \mathbf{b} = ab \sin\theta\ \hat{\mathbf{n}}$$

Where, a and b are the magnitudes of the vectors **a** and **b**, θ is the angle between **a** and **b** and $\hat{\mathbf{n}}$ is a unit vector whose direction is along the normal to the plane of **a** and **b** in the direction from which rotation of **a** to **b** looks anti-clockwise. In other words, direction of $\hat{\mathbf{n}}$ is towards that side to which a right-handed screw will move if **a** is rotated towards **b**.

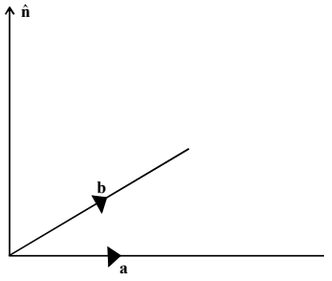


Fig. 4.15 *Cross Products of Two Vectors*

So, if **a** and **b** lie in the plane of the paper as shown in the Figure 4.15 then direction of $\hat{\mathbf{n}}$ is along the normal to the plane of the paper pointing towards the reader.

NOTES

It is proved from definition that the vector or cross products of two vectors is a vector.

Also according to the definition that $\mathbf{a} \times \mathbf{b}$ and $\mathbf{b} \times \mathbf{a}$ will have the same magnitude $ab \sin\theta$, but opposite directions.

Hence, $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$

Thus, vector product is not commutative.

Also, for any vector $\mathbf{a}$,

$$\mathbf{a} \times \mathbf{a} = a\, a \sin 0.\ \hat{\mathbf{n}} = 0$$

The following results are direct consequence of the definition:

$$\hat{\mathbf{i}} \times \hat{\mathbf{i}} = \hat{\mathbf{j}} \times \hat{\mathbf{j}} = \hat{\mathbf{k}} \times \hat{\mathbf{k}} = 0$$

$$\hat{\mathbf{i}} \times \hat{\mathbf{j}} = \hat{\mathbf{k}},\ \hat{\mathbf{j}} \times \hat{\mathbf{i}} = -\hat{\mathbf{k}}$$

$$\hat{\mathbf{j}} \times \hat{\mathbf{k}} = \hat{\mathbf{i}},\ \hat{\mathbf{k}} \times \hat{\mathbf{j}} = -\hat{\mathbf{i}}$$

$$\hat{\mathbf{k}} \times \hat{\mathbf{i}} = \hat{\mathbf{j}},\ \hat{\mathbf{i}} \times \hat{\mathbf{k}} = -\hat{\mathbf{j}}$$

Example 4.40: Show that $(m\mathbf{a}) \times \mathbf{b} = \mathbf{a} \times (m\mathbf{b}) = m(\mathbf{a} \times \mathbf{b})$

Solution: We have,

$$(m\mathbf{a}) \times \mathbf{b} = mab \sin\theta\ \hat{\mathbf{n}}$$
$$= amb \sin\theta\ \hat{\mathbf{n}}$$
$$= \mathbf{a} \times (m\mathbf{b})$$

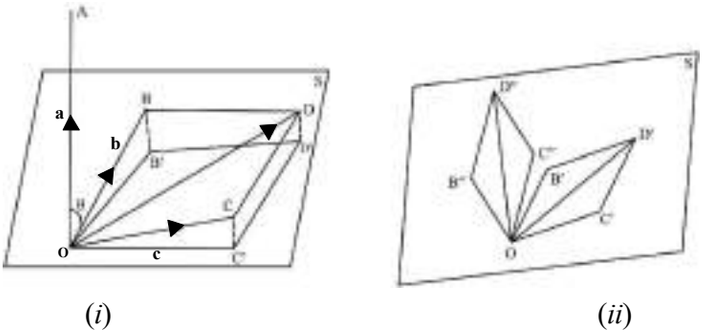
Similarly, $(m\mathbf{a}) \times \mathbf{b} = m(\mathbf{a} \times \mathbf{b})$

Distributive Law

Prove that, $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c}$

Proof: Through a point O, take vectors $\overrightarrow{OA} = \mathbf{a}$, $\overrightarrow{OB} = \mathbf{b}$ and $\overrightarrow{OC} = \mathbf{c}$. Let, S be a plane through O and perpendicular at $\overrightarrow{OA}$. Complete the parallelogram $OCDB$.

Such that, $\overrightarrow{OD} = \mathbf{b} + \mathbf{c}$



(*i*) (*ii*)

Fig. 4.16 *Distributive Law*

Let B', C', D' be the feet of perpendiculars from B, C, D respectively on the plane S.

Let, $\angle AOB = \theta$

Then, $\mathbf{a} \times \mathbf{b} = ab \sin\theta\ \hat{\mathbf{n}}$

Where, $\hat{\mathbf{n}}$ is a unit vector perpendicular to both OA and OB in the direction determined by motion of right-handed screw.

NOTES

Now, $\angle BOB' = \frac{\pi}{2} - \theta$

Thus, $\mathbf{b}' = \overrightarrow{OB}'$

Then, $|\mathbf{b}'| = b' = OB' = OB \cos\left(\frac{\pi}{2} - \theta\right) = b \sin\theta$

Again since OA, OB, OB' are in the same plane $AOB'B$, unit vector perpendicular to $\mathbf{a}$ and $\mathbf{b}$ is same as unit vector perpendicular to $\mathbf{a}$ and $\mathbf{b}'$.

Thus, $\mathbf{a} \times \mathbf{b}' = ab' \sin\left(\frac{\pi}{2}\right) \hat{\mathbf{n}}$

$= ab \sin\theta\ \hat{\mathbf{n}} = \mathbf{a} \times \mathbf{b}$

Similarly, $\mathbf{a} \times \mathbf{c} = \mathbf{a} \times \mathbf{c}'$

Where, $\mathbf{c}' = \overrightarrow{OC}'$

And, $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \overrightarrow{OD} = \mathbf{a} \times \overrightarrow{OD}'$

Since OA is perpendicular to plane S and OD' lies in it, the unit vector perpendicular to both $\overrightarrow{OA}$ and $\overrightarrow{OD}'$ will lie in the plane S, say along OD''. So, OD'' lies in the plane S and is perpendicular to both OA and OD'.

Draw lines, $OB'' \perp OB'$ and $OC'' \perp OC'$,

Such that, $OB'' = \overrightarrow{OA}\ .\ \overrightarrow{OB}'$

$OC'' = \overrightarrow{OA}\ .\ \overrightarrow{OC}'$

Also cut off, $OD'' = \overrightarrow{OA}\ .\ \overrightarrow{OD}'$

Then,

$\mathbf{a} \times \mathbf{b}' = \overrightarrow{OA} \times \overrightarrow{OB}' = \overrightarrow{OB}''$

$\mathbf{a} \times \mathbf{c}' = \overrightarrow{OA} \times \overrightarrow{OC}' = \overrightarrow{OC}''$

$\mathbf{a} \times \overrightarrow{OD}' = \overrightarrow{OA} \times \overrightarrow{OD}' = \overrightarrow{OD}''$

Also, $OC''\ D''\ B''$ will be a parallelogram as $OC'D'B'$ is a parallelogram. Hence,

$\overrightarrow{OD}'' = \overrightarrow{OB}'' + \overrightarrow{OC}''$

i.e., $\mathbf{a} \times \overrightarrow{OD}' = \mathbf{a} \times \mathbf{b}' + \mathbf{a} \times \mathbf{c}'$

i.e., $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c}$

(As proved earlier)

The above proof is sometimes referred to as the geometrical proof of the distributive law.

NOTES

Vector Product in Terms of Components

Let, $\mathbf{a} = (a_1, a_2, a_3) = a_1\hat{\mathbf{i}} + a_2\hat{\mathbf{j}} + a_3\hat{\mathbf{k}}$

$$\mathbf{b} = (b_1, b_2, b_3) = b_1\hat{\mathbf{i}} + b_2\hat{\mathbf{j}} + b_3\hat{\mathbf{k}}$$

Where, **a** and **b** be any two vectors. Then,

$$\mathbf{a} \times \mathbf{b} = (a_1\hat{\mathbf{i}} + a_2\hat{\mathbf{j}} + a_3\hat{\mathbf{k}}) \times (b_1\hat{\mathbf{i}} + b_2\hat{\mathbf{j}} + b_3\hat{\mathbf{k}})$$

$$= a_1b_1\hat{\mathbf{i}} \times \hat{\mathbf{i}} + a_1b_2\hat{\mathbf{i}} \times \hat{\mathbf{j}} + a_1b_3\hat{\mathbf{i}} \times \hat{\mathbf{k}} + a_2b_1\hat{\mathbf{j}} \times \hat{\mathbf{i}} + a_2b_2\hat{\mathbf{j}} \times \hat{\mathbf{j}}$$

$$+ a_2b_3\hat{\mathbf{j}} \times \hat{\mathbf{k}} + a_3b_1\hat{\mathbf{k}} \times \hat{\mathbf{i}} + a_3b_2\hat{\mathbf{k}} \times \hat{\mathbf{j}} + a_3b_3\hat{\mathbf{k}} \times \hat{\mathbf{k}}$$

$$= a_1b_2\hat{\mathbf{k}} - a_1b_3\hat{\mathbf{j}} - a_2b_1\hat{\mathbf{k}} + a_2b_3\hat{\mathbf{i}} + a_3b_1\hat{\mathbf{j}} - a_3b_2\hat{\mathbf{i}}$$

$$= \hat{\mathbf{i}}(a_2b_3 - a_3b_2) + \hat{\mathbf{j}}(a_3b_1 - a_1b_3) + \hat{\mathbf{k}}(a_1b_2 - a_2b_1)$$

$$= \begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$$

Example 4.41: If $\mathbf{a} = 2\hat{\mathbf{i}} - \hat{\mathbf{j}} + \hat{\mathbf{k}}$, $\mathbf{b} = 3\hat{\mathbf{i}} + 4\hat{\mathbf{j}} - \hat{\mathbf{k}}$, verify that $\mathbf{a} \times \mathbf{b}$ represents a vector perpendicular to both **a** and **b**.

Solution: We have,

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ 2 & -1 & 1 \\ 3 & 4 & -1 \end{vmatrix} = -3\hat{\mathbf{i}} + 5\hat{\mathbf{j}} + 11\hat{\mathbf{k}}$$

Now, $\mathbf{a}.(\mathbf{a} \times \mathbf{b}) = (2\hat{\mathbf{i}} - \hat{\mathbf{j}} + \hat{\mathbf{k}}) . (-3\hat{\mathbf{i}} + 5\hat{\mathbf{j}} + 11\hat{\mathbf{k}})$

$= 2 . (-3) + (-1) . 5 + 1 . 11 = 0$

$\Rightarrow$ **a** is perpendicular to $\mathbf{a} \times \mathbf{b}$.

Similarly, we can prove that **b** is also perpendicular to $\mathbf{a} \times \mathbf{b}$.

Theorem 4.21: Two vectors $\mathbf{a} = (a_1, a_2, a_3)$ and $\mathbf{b} = (b_1, b_2, b_3)$ are parallel if and only if,

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3}$$

Proof: Let **a** and **b** be parallel.

$\Rightarrow$ Angle θ between them is zero.

$\Rightarrow$ $\sin\theta = 0$

$\Rightarrow$ $\mathbf{a} \times \mathbf{b} = 0$

$\Rightarrow$ $\begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = 0$

$\Rightarrow (a_2b_3 - a_3b_2)\ \hat{\mathbf{i}} + (a_3b_1 - a_1b_3)\ \hat{\mathbf{j}} + (a_1b_2 - a_2b_1)\ \hat{\mathbf{k}} = 0 = 0\,\hat{\mathbf{i}} + 0\,\hat{\mathbf{j}} + 0\,\hat{\mathbf{k}}$

$\Rightarrow \quad a_2b_3 - a_3b_2 = 0$

$a_3b_1 - a_1b_3 = 0$

$a_1b_2 - a_2b_1 = 0$

$\Rightarrow \quad \frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3}$

Converse follows by simply retracing the steps back.

Vector Product as Area

Let *OABC* be a parallelogram such that,

$\overrightarrow{OA} = \mathbf{a}$

$\overrightarrow{OC} = \mathbf{b}$

and let θ be the angle between **a** and **b**.

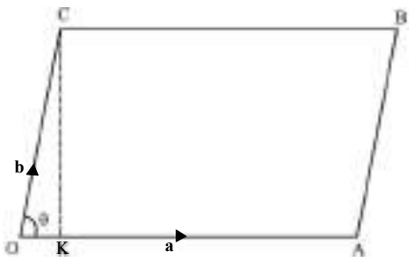


Fig. 4.17 *Vector Product as Area*

Now area of the parallelogram *OABC*,

$= OA \,.\, CK$ (Where, $CK \perp OA$)

$= ab \sin\theta$

Also, $\mathbf{a} \times \mathbf{b} = (ab \sin\theta)\ \hat{\mathbf{n}}$

Comparing the two we note that, $\mathbf{a} \times \mathbf{b}$ = Area of the parallelogram *OABC*, i.e., the magnitude of the vector product of two vectors is the area of the parallelogram whose adjacent sides are represented by these vectors.

Corollary: It is easy to see that the area of the triangle *OAC* is $\frac{1}{2}\ \mathbf{a} \times \mathbf{b}$.

Example 4.42: Find the area of the parallelogram whose adjacent sides are determined by the vectors $\mathbf{a} = \hat{\mathbf{i}} + 2\,\hat{\mathbf{j}} + 3\,\hat{\mathbf{k}}$, $\mathbf{b} = 3\,\hat{\mathbf{i}} - 2\,\hat{\mathbf{j}} + \hat{\mathbf{k}}$.

Solution: Required area = $|\mathbf{a} \times \mathbf{b}|$

Now, $\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \hat{\mathbf{i}} & \hat{\mathbf{j}} & \hat{\mathbf{k}} \\ 1 & 2 & 3 \\ 3 & -2 & 1 \end{vmatrix}$

$= \hat{\mathbf{i}}\,(2 + 6) - \hat{\mathbf{j}}\,(1 - 9) + \hat{\mathbf{k}}\,(-2 - 6)$

NOTES

$$= 8(\hat{\mathbf{i}} + \hat{\mathbf{j}} - \hat{\mathbf{k}})$$

$\Rightarrow$ $|\mathbf{a} \times \mathbf{b}| = \sqrt{64+64+64} = 8\sqrt{3}$ is the required area.

NOTES

Triple Product (Scalar, Vector)

Scalar Triple Product

The scalar triple product is defined as the dot product of one of the vectors with the cross product of the other two. Suppose **a**, **b**, **c** are three vectors. Then, $\mathbf{b} \times \mathbf{c}$ is again a vector and thus we can talk of $\mathbf{a}.(\mathbf{b} \times \mathbf{c})$, which would, of course, be a scalar. This is called scalar triple product of three vectors.

Let, $\mathbf{a} = (a_1, a_2, a_3)$

$\mathbf{b} = (b_1, b_2, b_3)$

$\mathbf{c} = (c_1, c_2, c_3)$

Then, $\mathbf{b} \times \mathbf{c} = (b_2c_3 - b_3c_2,\ b_3c_1 - c_3b_1,\ b_1c_2 - b_2c_1)$

$= (d_1, d_2, d_3) = \mathbf{d}$ (say)

Thus, $\mathbf{a} \cdot (\mathbf{b} \times \mathbf{c}) = \mathbf{a} \cdot \mathbf{d} = a_1d_1 + a_2d_2 + a_3d_3$

$= a_1(b_2c_3 - b_3c_2) + a_2(b_3c_1 - c_3b_1) + a_3(b_1c_2 - b_2c_1)$

$$= \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \quad \ldots(4.9)$$

Hence, this is the value of the scalar triple product $\mathbf{a}.(\mathbf{b} \times \mathbf{c})$.

Suppose we had started with $\mathbf{b} \cdot (\mathbf{c} \times \mathbf{a})$, it is easy to prove that the resulting determinant would have been,

$$\begin{vmatrix} b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \\ a_1 & a_2 & a_3 \end{vmatrix}$$

which is same as Equation (4.9) (As per the properties of determinants), and so,

$$\mathbf{a} \cdot (\mathbf{b} \times \mathbf{c}) = \mathbf{b} \cdot (\mathbf{c} \times \mathbf{a})$$

Similarly, $\mathbf{b} \cdot (\mathbf{c} \times \mathbf{a}) = \mathbf{c} \cdot (\mathbf{a} \times \mathbf{b})$

$\Rightarrow$ $\mathbf{a} \cdot (\mathbf{b} \times \mathbf{c}) = \mathbf{c} \cdot (\mathbf{a} \times \mathbf{b}) = (\mathbf{a} \times \mathbf{b}) \cdot \mathbf{c}$ [By Commutative Property]

Dot and cross can be interchanged in a scalar triple product and we write the scalar triple product as **[a, b, c]** or **[abc]**, where it is upto the reader where to put cross and dot.

Note: It can be verified that,

$$\mathbf{[abc] = -[bac]}$$

And, $\mathbf{[abc] = [bca] = [cab]}$

Example 4.43: Prove the distributive law $\mathbf{a} \times (\mathbf{b} + \mathbf{c}) = \mathbf{a} \times \mathbf{b} + \mathbf{a} \times \mathbf{c}$ using scalar triple product.

Solution: Let, $\mathbf{d} = \mathbf{a} \times (\mathbf{b} + \mathbf{c}) - \mathbf{a} \times \mathbf{b} - \mathbf{a} \times \mathbf{c}$

Then, it required to prove that, $\mathbf{d} = \mathbf{0}$

Let $\mathbf{e}$ be any vector, then,

$$\mathbf{e} \cdot \mathbf{d} = \mathbf{e} \cdot [\mathbf{a} \times (\mathbf{b} + \mathbf{c})] - \mathbf{e} \cdot (\mathbf{a} \times \mathbf{b}) - \mathbf{e} \cdot (\mathbf{a} \times \mathbf{c})$$

$$= (\mathbf{e} \times \mathbf{a}) \cdot (\mathbf{b} + \mathbf{c}) - (\mathbf{e} \times \mathbf{a}) \cdot \mathbf{b} - (\mathbf{e} \times \mathbf{a}) \cdot \mathbf{c}$$

[Interchanging dot and cross in the scalar triple products]

$$= (\mathbf{e} \times \mathbf{a}) \cdot [(\mathbf{b} + \mathbf{c}) - \mathbf{b} - \mathbf{c}]$$ [Distributivity of scalar product]

$$= (\mathbf{e} \times \mathbf{a}) \cdot 0 = 0$$

$\Rightarrow$ $\mathbf{e} \cdot \mathbf{d} = 0$ for all vectors $\mathbf{e}$

$\Rightarrow$ $\mathbf{d} = \mathbf{0}$ (We can take $\mathbf{e}$ to be a non-zero vector, not perpendicular to $\mathbf{d}$.)

Hence proved.

Vector Triple Product

A vector triple product is defined as the cross product of one vector with the cross product of the other two.

A product of the type $\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$ is called a vector triple product.

We prove,

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{a} \cdot \mathbf{c})\,\mathbf{b} - (\mathbf{a} \cdot \mathbf{b})\,\mathbf{c}$$

in the following way:

Let, $\mathbf{a} = (a_1, a_2, a_3)$

$\mathbf{b} = (b_1, b_2, b_3)$

$\mathbf{c} = (c_1, c_2, c_3)$

Then, $\mathbf{b} \times \mathbf{c} = (b_2c_3 - b_3c_2,\ b_3c_1 - b_1c_3,\ b_1c_2 - b_2c_1)$

$= (d_1, d_2, d_3) = \mathbf{d}$ (say)

Then,

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = \mathbf{a} \times \mathbf{d}$$

$$= (a_2d_3 - a_3d_2,\ a_3d_1 - a_1d_3,\ a_1d_2 - a_2d_1)$$

$$= (a_2d_3 - a_3d_2)\ \hat{\mathbf{i}} + (a_3d_1 - a_1d_3)\ \hat{\mathbf{j}} + (a_1d_2 - a_2d_1)\ \hat{\mathbf{k}}$$

$$= \Sigma(a_2d_3 - a_3d_2)\ \hat{\mathbf{i}}$$

$$= \Sigma[a_2(b_1c_2 - b_2c_1) - a_3(b_3c_1 - b_1c_3)]\ \hat{\mathbf{i}}$$

$$= \Sigma[a_2b_1c_2 - a_2b_2c_1 - a_3b_3c_1 + a_3b_1c_3 + a_1b_1c_1 - a_1b_1c_1]\ \hat{\mathbf{i}}$$

[Adding and subtracting $a_1b_1c_1$]

$$= [b_1(a_1c_1 + a_2c_2 + a_3c_3) - c_1(a_1b_1 + a_2b_2 + a_3b_3)]\ \hat{\mathbf{i}}$$

$$+ [b_2(a_1c_1 + a_2c_2 + a_3c_3) - c_2(a_1b_1 + a_2b_2 + a_3b_3)]\ \hat{\mathbf{j}}$$

$$+ [b_3(a_1c_1 + a_2c_2 + a_3c_3) - c_3(a_1b_1 + a_2b_2 + a_3b_3)]\ \hat{\mathbf{k}}$$

NOTES

$$= (a_1c_1 + a_2c_2 + a_3c_3)(b_1\hat{\mathbf{i}} + b_2\hat{\mathbf{j}} + b_3\hat{\mathbf{k}}) - (a_1b_1 + a_2b_2 + a_3b_3)(c_1\hat{\mathbf{i}} + c_2\hat{\mathbf{j}} + c_3\hat{\mathbf{k}})$$

$$= (\mathbf{a} \cdot \mathbf{c})\mathbf{b} - (\mathbf{a} \cdot \mathbf{b})\mathbf{c}$$

NOTES

This proves our assertion.

Note: There is neither a cross nor a dot between (**a** . **c**) and **b** in (**a** . **c**)**b** and between (**a** . **b**) and **c** in (**a** . **b**) **c**.

This is so, because (**a** . **c**) and (**a** . **b**) are scalars.

Example 4.44: Prove that, $\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) + \mathbf{b} \times (\mathbf{c} \times \mathbf{a}) + \mathbf{c} \times (\mathbf{a} \times \mathbf{b}) = \mathbf{0}$.

Solution: We know that,

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{a} \cdot \mathbf{c})\mathbf{b} - (\mathbf{a} \cdot \mathbf{b})\mathbf{c}$$

$$\mathbf{b} \times (\mathbf{c} \times \mathbf{a}) = (\mathbf{b} \cdot \mathbf{a})\mathbf{c} - (\mathbf{b} \cdot \mathbf{c})\mathbf{a}$$

$$\mathbf{c} \times (\mathbf{a} \times \mathbf{b}) = (\mathbf{c} \cdot \mathbf{b})\mathbf{a} - (\mathbf{c} \cdot \mathbf{a})\mathbf{b}$$

The result is computed using addition.

Check Your Progress

9. Define the subring.
10. When subfield is a subset that contains 1?
11. What do you understand by vector space?
12. How will you define the zero vector?

4.7 LINEAR COMBINATIONS

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 $v_1, v_2, ..., v_n$ 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 $< S >$. If $S = \varphi$, define $L(S) = \{0\}$.

Theorem 4.22: $L(S)$ 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 $x = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$

$y = \beta_1 v_1' + \beta_2 v_2' + ... + \beta_m v_m'$, $v_i, v_j' \in S$, $\alpha_i, \beta_j \in F$

Thus $\alpha x + \beta y = \alpha\alpha_1 v_1 + \alpha\alpha_2 v_2 + ... + \alpha\alpha_n v_n + \beta\beta_1 v_1' + ... + \beta\beta_m v_m'$.

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 4.23: 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

$\Rightarrow \Sigma\alpha_i v_i \in S_2 \Rightarrow x \in L(S_2)$

$\Rightarrow L(S_1) \subseteq L(S_2)$.

(*ii*) $S_1 \subseteq S_1 \cup S_2 \Rightarrow L(S_1) \subseteq L(S_1 \cup S_2)$

$S_2 \subseteq S_1 \cup S_2 \Rightarrow L(S_2) \subseteq L(S_1 \cup S_2)$

$\Rightarrow L(S_1) + L(S_2) \subseteq L(S_1 \cup S_2)$

Again, $S_1 \subseteq L(S_1) \subseteq L(S_1) + L(S_2)$

$S_2 \subseteq L(S_2) \subseteq L(S_1) + L(S_2)$

$\Rightarrow S_1 \cup S_2 \subseteq L(S_1) + L(S_2)$.

Hence $L(S_1 \cup S_2) \subseteq L(S_1) + L(S_2)$

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 $L(S_1 \cup S_2) = L(S_1) + L(S_2)$.

(*iii*) Let $L(S_1) = K$ then we show $L(K) = L(S_1)$

Now $K \subseteq L(K) \ \therefore\ L(S_1) \subseteq L(L(S_1))$

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

$\Rightarrow x \in L(S_1)$

Thus $L(L(S_1)) \subseteq L(S_1)$

Hence $L(L(S_1)) = L(S_1)$.

Theorem 4.24: 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 V containing W and W is itself a subspace.

$L(W) \subseteq W$

Hence $L(W) = W$.

NOTES

NOTES

Conversely, let $L(W) = W$

Let $x, y \in W, \alpha, \beta \in F$

Then $x, y \in L(W)$

$\Rightarrow$ 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 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 are, $V = L(S)$. We use notation FDVS for a Finite Dimensional Vector Space.

From the results, it is 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, $L(S_1 \cup S_2) = L(S_1) + L(S_2) = S_1 + S_2$.

Example 4.45: 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 $(2, 3) = \alpha(1, 4) + \beta(0, 3)$

$\Rightarrow$ $(2, 3) = (\alpha + 0, 4\alpha + 3\beta)$

$\Rightarrow$ $2 = \alpha, 4\alpha + 3\beta = 3$

$\Rightarrow$ $\alpha = 2, \beta = -\frac{5}{3}$

Hence $(2, 3) = 2\,(1, 4) - \frac{5}{3}\,(0, 3)$

Showing that $(2, 3) \in L(S)$.

Example 4.46: 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 $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \alpha(2, 0, 0\ 1) + \beta(-1, 0, 1, 0), \quad \alpha, \beta \in \mathbf{R}$

then $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (2\alpha - \beta, 0, \beta, \alpha)$

i.e., $L(S) = \{(2\alpha - \beta, 0, \beta, \alpha) \mid \alpha, \beta \in \mathbf{R}\}$

Example 4.47: Show that the vector space $F[x]$ is not finite dimensional.

Solution: Let $V = F[x]$ and suppose it is finite dimensional.

Then $\exists\ S \subseteq V$, such that, $V = L(S)$ and S is finite.

Suppose $S = \{p_1, p_2, ..., p_k\}$. We can assume $p_i \neq 0 \quad \forall i$

Let deg $p_i = r_i$ and let $t = \text{Max } \{r_1, r_2, ..., r_k\}$

Now $x^{t+1} \in V$ and since $V = L(S)$,

$$x^{t+1} = \alpha_1 p_1 + \alpha_2 p_2 + \ldots + \alpha_k p_k, \quad \alpha_i \in F$$

So $$0 = (-1)\, x^{t+1} + \alpha_1 p_1 + \ldots + \alpha_k p_k$$

Since x^{t+1} does not appear in $p_1, p_2, \ldots, p_k$

We get $-1 = 0$, a contradiction. Hence V is not FDVS over F.

Note if $S = \{1, x, \ldots, x^n, \ldots\}$ then $V = L(S)$.

NOTES

4.8 LINEAR INDEPENDENCE AND LINEAR DEPENDENCE

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 $\alpha_1, \alpha_2, \ldots \alpha_n \in F$, (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 (*LD*), these are called Linearly Independent (*LI*)

In other words, $v_1, v_2, \ldots, v_n$ are *LI* if

$$\Sigma \alpha_i v_i = 0 \Rightarrow \alpha_i = 0 \text{ for all } i$$

A finite set $X = \{x_1, x_2 \ldots, x_n\}$ is said to be *LD* or *LI* according as its n members are *LD* or *LI*

In general any subset Y of $V(F)$ is called *LI* if every finite non-empty subset of Y is *LI*, *otherwise* it is called *LD*

So, if some subsets are *LI* and some are *LD* then Y is called *LD*

Observations: (*i*) A non-zero vector is always *LI* as $v \neq 0$, $\alpha v = 0$ would mean $\alpha = 0$.

(*ii*) Zero vector is always *LD*

$$1 \cdot 0 = 0 \qquad 1 \neq 0,\ 1 \in F$$

Thus, any collection of vectors to which zero belongs is always *LD*

In other words, if $v_1, v_2, \ldots, v_n$ are *LI* then none of these can be zero. (But not conversely, see example ahead).

(*iii*) v is *LI* iff $v \neq 0$.

(*iv*) Any subset of a *LI* set is *LI*

(*v*) Any super set of a *LD* set is *LD*

(*vi*) Empty set φ is *LI* 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 *LI* We sometimes express it by saying that empty set is *LI* vacuously.

(*vii*) A set of vector is *LI* if and only if every finite subset of it is *LI*

Some examples of **linear dependence** and **independence** are given as follows:

(i) Consider $\mathbf{R}^2(\mathbf{R})$, $\mathbf{R}$ = reals.

NOTES

$v_1 = (1, 0), v_2 = (0, 1) \in \mathbf{R}^2$ are *LI*

as $\alpha_1 v_1 + \alpha_2 v_2 = 0$ for $\alpha_1, \alpha_2 \in \mathbf{R}$

$\Rightarrow \alpha_1(1, 0) + \alpha_2(0, 1) = (0, 0)$

$\Rightarrow (\alpha_1, \alpha_2) = (0, 0) \Rightarrow \alpha_1 = \alpha_2 = 0.$

(ii) 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 *LD*

(iii) In the vector space $F[x]$ of polynomials the vectors $f(x) = 1 - x$, $g(x) = x - x^2$, $h(x) = 1 - x^2$ are *LD* since $f(x) + g(x) - h(x) = 0$.

Example 4.48: Show that the vectors $v_1 = (0, 1, -2)$, $v_2 = (1, -1, 1)$, $v_3 = (1, 2, 1)$ are *LI in* $\mathbf{R}^3(\mathbf{R})$.

Solution: Let $\Sigma\alpha_i v_i = 0$ for $\alpha_i \in \mathbf{R}$

Then $\alpha_1(0, 1, -2) + \alpha_2(1, -1, 1) + \alpha_3(1, 2, 1) = (0, 0, 0)$

$\Rightarrow (0, \alpha_1, -2\alpha_1) + (\alpha_2, -\alpha_2, \alpha_2) + (\alpha_3, 2\alpha_3, \alpha_3) = (0, 0, 0)$

$\Rightarrow$

$$\begin{aligned} 0 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1 - \alpha_2 + 2\alpha_3 &= 0 \\ -2\alpha_1 + \alpha_2 + \alpha_3 &= 0 \end{aligned}$$

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

$\Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0 \Rightarrow v_1, v_2, v_3$ are *LI*

Example 4.49: Show that $\{f(x), g(x), h(x)\}$ is *LI* in $F[x]$, whenever. *deg* $f(x)$, *deg* $g(x)$, *deg* $h(x)$ are distinct.

Solution: Let

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_m x^m, \quad a_m \neq 0 \\ g(x) &= b_0 + b_1 x + \ldots + b_n x^n, \quad b_n \neq 0 \\ h(x) &= c_0 + c_1 x + \ldots + c_t x^t, \quad c_t \neq 0 \end{aligned}$$

Let $\alpha f(x) + \beta g(x) + \gamma h(x) = 0, \quad \alpha, \beta, \gamma \in F$

Let $m < n < t$ (without any loss of generality)

then $\gamma c_t = 0 \Rightarrow \gamma = 0$ as $c_t \neq 0$

$\therefore \quad \alpha f(x) + \beta g(x) = 0$

and so $\beta b_n = 0 \Rightarrow \beta = 0$ as $b_n \neq 0$

$\Rightarrow \alpha f(x) = 0 \Rightarrow \alpha a_m = 0 \Rightarrow \alpha = 0$ as $a_m \neq 0$

Hence $\{f(x), g(x), h(x)\}$ is *LI* in $F[x]$ over F.

Example 4.50: 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 *LD* in $\mathbf{R}^4(\mathbf{R})$.

NOTES

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 $(a, a, 2a, 4a) + (2b, -b, -5b, 2b) + (c, -c, -4c, 0)$

$$+ (2d, d, d, 6d) = (0, 0, 0, 0)$$

$$\Rightarrow \quad \begin{aligned} a + 2b + c + 2d &= 0 \\ a - b - c + d &= 0 \\ 2a - 5b - 4c + d &= 0 \\ 4a + 2b + 0c + 6d &= 0 \end{aligned}$$

$$\Rightarrow \quad \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & -1 & -1 & 1 \\ 2 & -5 & -4 & 1 \\ 4 & 2 & 0 & 6 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_2 \to R_2 - R_1,\ R_3 \to R_3 - 2R_1,\ R_4 \to R_4 - 4R_1$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \\ 0 & -3 & -2 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to \frac{1}{2} R_4,\ R_3 \to \frac{1}{3} R_3$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & -1 & -2/3 & -1/3 \\ 0 & -3/4 & -1 & -1/2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$R_4 \to R_4 - R_2,\ R_3 \to R_3 - R_2$

$$\begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & -3 & -2 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow \quad \begin{aligned} a + 2b + c + 2d &= 0 \\ -3b - 2c + d &= 0 \\ 3b + 2c + d &= 0 \end{aligned}$$

$a = -1,\ b = -1,\ c = 1,\ d = 1$ satisfy the equations.

Since coefficients are non-zero, the given vectors are *LD*

Example 4.51: Show that

(*i*) $\{1, \sqrt{2}\}$ is *LI* in **R** over **Q**.

(*ii*) $\{1, \sqrt{2}, \sqrt{3}\}$ is LI in **R** over **Q**.

(*iii*) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is LI in **R** over **Q**.

NOTES

Solution: (*i*) Suppose $a + b\sqrt{2} = 0,\ a, b \in \mathbf{Q}$

Suppose $b \neq 0$, then $\sqrt{2} = -\frac{a}{b} \in \mathbf{Q}$, a contradiction

Hence $b = 0$ and so $a = 0$. Thus $\{1, \sqrt{2}\}$ is *LI* in **R** over **Q**.

(*ii*) Let $a + b\sqrt{2} + c\sqrt{3} = 0, \quad a, b, c \in \mathbf{Q}$

Let $c \neq 0$, then

$$\sqrt{3} = -\frac{a}{c} - \frac{b}{c}\sqrt{2} = \alpha + \beta\sqrt{2}, \quad \alpha, \beta \in \mathbf{Q}$$

$$\Rightarrow \quad 3 = \alpha^2 + 2\beta^2 + 2\alpha\beta\sqrt{2}$$

$$\Rightarrow \quad \alpha\beta\sqrt{2} \in \mathbf{Q} \Rightarrow \alpha\beta = 0$$

Let $\alpha = 0$ then $\beta = \sqrt{\frac{3}{2}}$, a contradiction

So, $c = 0$ giving $a + b\sqrt{2} = 0 \Rightarrow a = b = 0$ by (*i*)

Hence the result follows.

(*iii*) Let $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0, \quad a, b, c, d \in \mathbf{Q}$

Then $(a + b\sqrt{2}) + \sqrt{3}(c + d\sqrt{2}) = 0$

Let $c + d\sqrt{2} \neq 0$

Then $$\sqrt{3} = \frac{-(a + b\sqrt{2})}{(c + d\sqrt{2})} = \frac{-(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2}$$

$$= \alpha + \beta\sqrt{2}, \quad \alpha, \beta \in \mathbf{Q}$$

$$\Rightarrow \quad \alpha.1 + \beta\sqrt{2} + (-1)\sqrt{3} = 0$$

$$\Rightarrow \quad -1 = 0 \text{ by } (ii), \text{ a contradiction}$$

$$\therefore \quad c + d\sqrt{2} = 0 \Rightarrow c = d = 0 \Rightarrow a + b\sqrt{2} = 0$$

$$\Rightarrow \quad a = b = 0$$

Hence the result follows.

Theorem 4.25: If $S = \{v_1, v_2, \ldots v_n\}$ is a basis of *V,* then every element of V can be expressed uniquely as a linear combination of $v_1, v_2, \ldots, v_n$.

Proof: Since, by definition of basis, $V = L(S)$, each element $v \in V$ can be expressed as linear combination of $v_1, v_2, \ldots, v_n$.

Suppose $v = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n, \quad \alpha_i \in F$

$v = \beta_1 v_1 + \beta_2 v_2 + \ldots + \beta_n v_n, \quad \beta_i \in F$

then $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n = \beta_1 v_2 + \beta_2 v_2 + \ldots + \beta_n v_n$

$\Rightarrow (\alpha_1 - \beta_1) v_1 + (\alpha_2 - \beta_2) v_2 + \ldots + (\alpha_n - \beta_n) v_n = 0$

$\Rightarrow \alpha_i - \beta_i = 0$ for all i ($v_1, v_2, \ldots v_n$ are *LI*)

$\Rightarrow \alpha_i = \beta_i$ for all i.

Theorem 4.26: Suppose *S* is a finite subset of a vector space *V* such that $V = L(S)$ [i.e., *V* is an FDVS] then there exists *a* subset of *S* which is a basis of *V.*

NOTES

Proof: If S consists of LI 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 finite).

Suppose $T = \{v_1, v_2, ..., v_n\}$

We show T is LI

Let $\Sigma\alpha_i v_i = 0, \quad \alpha_i \in F$

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 $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$

$\Rightarrow \alpha_1^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n) = 0$

$\Rightarrow v_1 = (-\alpha_1^{-1}\alpha_2)v_2 + (-\alpha_1^{-1}\alpha_3)v_3 + ... + (-\alpha_1^{-1}\alpha_n)v_n$

$= \beta_2 v_2 + \beta_3 v_3 + ... + \beta_n v_n \quad \beta_i \in F$

If $v \in V$ be any element then

$v = \gamma_1 v_1 + \gamma_2 v_2 + ... \gamma_n v_n \quad \gamma_i \in F$ as $V = L(T)$

$\Rightarrow v = \gamma_1(\beta_2 v_2 + ... + \beta_n v_n) + \gamma_2 v_2 + ... + \gamma_n v_n$

i.e., any element of V is a linear combination of $v_2, v_3, ..., v_n$

$\Rightarrow \{v_2, v_3, ...v_n\}$ spans V, which contradicts our choice of T (as T was such minimal)

Hence $\alpha_1 = 0$

or that $\alpha_i = 0$ for all i

$\Rightarrow v_1, v_2, ... v_n$ are LI

and thus T is a basis of V.

Corollary: An FDVS has a basis.

In fact, you can prove this result for any vector space, i.e., any vector space has a basis.

Theorem 4.27: Let V be an FDVS. Suppose S and T are two finite subsets of V such that S spans V and T is LI Then $o(T) \leq o(S)$.

Proof: Suppose $S = \{v_1, v_2, ..., v_n\}$

$T = \{w_1, w_2, ..., w_m\}$

Suppose $m > n$.

Since S spans V, we have

$$w_1 = a_{11} v_1 + a_{12} v_2 + ... + a_{1n} v_n$$
$$w_2 = a_{21} v_1 + a_{22} v_2 + ... + a_{2n} v_n$$
$$... \quad ... \quad ...$$
$$w_m = a_{m1} v_1 + a_{m2} v_2 + ... + a_{mn} v_n \qquad \text{where } a_{ij} \in F$$

Consider the system of equations

$$a_{11} x_1 + a_{21} x_2 + ... + a_{m1} x_m = 0$$
$$a_{12} x_1 + a_{22} x_2 + ... + a_{m2} x_m = 0$$
$$... \quad ... \quad ...$$

$$a_{1n}\, x_1 + a_{2n}\, x_2 + \ldots + a_{mn}\, x_m = 0$$

where $x_1, x_2, \ldots, x_m \in F$ are unknowns.

Since the mumber of equations is less than the number of unknowns, $\exists$ a non-zero solution $\alpha_1, \alpha_2, \ldots, \alpha_m$ (some $\alpha_i \neq 0$) in F such that,

NOTES

$$a_{11}\, \alpha_1 + \ldots + a_{m1}\, \alpha_m = 0$$
$$\ldots \qquad \ldots \qquad \ldots$$
$$a_{1n}\, \alpha_1 + \ldots + a_{mn}\, \alpha_m = 0$$

Thus $\alpha_1 (a_{11}\, v_1 + \ldots + a_{1n}\, v_n) + \ldots + \alpha_m (a_{m1}\, v_1 + \ldots + a_{mn}\, v_n) = 0$

$\Rightarrow \alpha_1\, w_1 + \alpha_2\, w_2 + \ldots + \alpha_m\, w_m = 0$

$\Rightarrow \alpha_i = 0\ \forall i$ as $w_1, w_2, \ldots, w_m$ are LI

which is a contradiction and thus $m \leq n$

i.e., $o(T) \leq o(S)$.

Corollary 1: Any basis of an FDVS is finite.

Proof: Let S be a basis of an FDVS V and suppose S is not finite.

Since V is finite dimensional, $\exists$ a finite subset T of V such that, $V = L(T)$. Suppose $o(T) = m$

Let S_1 be a LI subset of S such that, $o(S_1) = m + 1$

By above theorem then $o(T) \geq o(S_1)$ giving $m \geq m + 1$, a contradiction.

Hence S must be finite.

Corollary 2: Any two bases of an FDVS have same member of elements.

Proof: Let S and T be two bases of an FDVS V

By above corollary, S and T are finite and by the theorem $o(T) \leq o(S)$ and $o(S) \leq o(T)$

Hence $o(T) = o(S)$ with the result of corollary2 in our mind we make.

4.9 BASIS OF VECTOR SPACES

Definition: A FDVS 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 $\dim \mathbf{R}^n = n$

Corollary: If $\dim V = n$, then any $n + 1$ vectors in V are linearly dependent.

Proof: Let $T \subseteq V$ be an LI set such that, $o(T) = n + 1$

Let S be a basis of V. Then S spans V and $o(S) = n$.

$$o(T) \leq o(S)$$

giving $n + 1 \leq n$ a contradiction

Thus any $n + 1$ vectors in V are LD

NOTES

Theorem 4.28: A basis of a vector space is maximal linearly independent set and conversely, every maximal linearly independent set in a vector space is its basis.

Proof: Let S be a basis of a vector space V, then S is linearly independent set in V. Let T be a linearly independent set in V such that $S \subseteq T$. If $S \neq T$ then $\exists$ some $t \in T$ such that, $t \notin S$.

Now $t \in T \Rightarrow t \in V \Rightarrow t = \alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n$, $\alpha_i \in F$, $s_i \in S$ as S spans V

$\Rightarrow (-1)\ t + \alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n = 0$, where $t \neq s_i$ for any i

$\Rightarrow -1 = 0$

as $\{t, s_1, s_2, ..., s_n\} \subseteq T$ is a linearly independent set. So we get a contradiction.

Hence S is a maximal linearly independent set.

Conversely, let $S \subseteq V$ be a maximal linearly independent set. Let $v \in V$, and suppose $v \notin L(S)$

Then $S \not\subseteq S \cup \{v\}$ as $v \notin L(S) \Rightarrow v \notin S$

and so $S \cup \{v\}$ is an LD set and thus $\exists$ a finite subset of $S \cup \{v\}$ which is a LD set.

i.e., $\exists\ s_1, s_2, ... s_n \in S$ such that, $\{v, s_1, s_2, ..., s_n\}$ is an LD set.

i.e., $\alpha v + \alpha_1 s_1 + ... + \alpha_n s_n = 0$, $\alpha \in F$, $\alpha_i \in F$

where α or some α_i is not zero.

If $\alpha = 0$ then $\alpha_1 s_1 + \alpha_2 s_2 + ... + \alpha_n s_n = 0$

$\Rightarrow \alpha_i = 0\ \forall\ i$.

Thus $\alpha \neq 0$

So $v = (-\alpha^{-1}\alpha_1)s_1 + ... + (-\alpha^{-1}\alpha_n)\ s_n$

$\Rightarrow v \in L(S)$, (a contradiction)

Thus $V = L(S)$ and so S is a basis of V.

Corollary: Suppose n is the maximum number of LI vectors in any subset of a vector space V. Then dim $V = n$.

Proof: Let S be a LI subset of V such that $o(S) = n$

Then S is a maximal LI set in V. By above theorem then S is a basis of V. Hence dim $V = o(S) = n$.

Theorem 4.29: Let $V(F)$ be a vector space. A minimal generating set of V is a basis of V and conversely, every basis of V is a minimal generating set of V.

Proof: Let S be a minimal generating set of V

Then $V = L(S)$ and no proper subset of S generates V. We show S is LI set. Suppose it is not, then there exists a finite subset S_1, of S such that S_1 is not LI Thus $\exists\ s \in S_1$ such that, s is linear combination of elements of S_1, and so of S.

Let $T = S - \{s\}$

then $V = L(T)$ and $T \subseteq S$, a contradiction as S is minimal generating set of V.

Hence S is a basis of V.

NOTES

Conversely, let B be a basis of V. We show no proper subset of B generates V. Let $B' \subseteq B$ and $V = L(B')$. Then $\exists\ b \in B$, such that, $b \notin B'$

Now $b \in B \Rightarrow b \in V = L(B') \Rightarrow b = \sum_{1}^{n} \alpha_i b_i', \quad b_i' \in B'$

$\Rightarrow \quad 0 = (-1)\ b + \sum_{1}^{n} \alpha_i b'_i,\ b \neq b'_i$ *for any* i

$\Rightarrow \quad -1 = 0$ as $\{b, b'_1, ..., b'_n\} \subseteq B$ is an *LI* set, a contradiction.

Thus B is minimal generating set of V.

Theorem 4.30: If V is an FDVS and $\{v_1, v_2, ..., v_r\}$ is a LI 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 *LI* subset of V, containing $\{v_1, v_2, ..., v_r\}$.

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 *LD* 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 $\alpha_1 v_1 + ... + \alpha_n v_n = 0$

$\Rightarrow \quad \alpha_i = 0$ for all i as $v_1, v_2, ..., v_n$ are *LI*

$\therefore \quad \alpha = \alpha_i = 0$ for all i which is not true.

Hence $\alpha \neq 0$ and so α^{-1} exists.

Since $v = (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + ... + (-\alpha^{-1}\alpha_n)v_n$

v is a linear combination of $v_1, v_2, ..., v_n$

which proves our assertion.

Aliter: Let dim $V = n$ and $S = \{v_1, v_2, ..., v_r\}$. If S is maximal *LI* set in V then by Theorem 4.28, it is a basis of V. If S is not maximal *LI* set in V then $\exists$ a set $T \supseteq S$ such that T is *LI* set in V. Since an *LI* set cannot have more than n vectors, after finite number of steps, there would be a maximal *LI* set $B \supseteq S$ in V. B would be a basis of V. Hence S can be extended to form a basis B of V.

Note: This result can be proved even if the vector space is not finite dimensional.

Theorem 4.31: If *dim* $V = n$ and $S = \{v_1, v_2, ..., v_n\}$ spans V then S is a basis of V.

Proof: Since dim $V = n$, any basis of V has n elements. A subset of S will be a basis of V but as S contains n elements, it will itself form basis of V.

NOTES

Theorem 4.32: If *dim* $V = n$ and $S = \{v_1, v_2,...,v_n\}$ is *LI* subset of V then S is a basis of V.

Proof: Since $\{v_1, v_2,..., v_n\} = S$ is *LI* it can be extended to form a basis of V, but dim V being n it will itself be a basis of V.

Aliter: Let $v \in V$, then

$v, v_1, v_2,..., v_n$ will be *LD*. Thus $\exists\ \alpha, \alpha_1, \alpha_2,..., \alpha_n \in F$ such that,

$$\alpha v + \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$$

where some α_i or α is not zero.

If $\alpha = 0$, then

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$$

$$\Rightarrow \alpha_i = 0\ \forall i \text{ as } v_1, v_2 ..., v_n \text{ are } LI$$

Thus $\alpha \neq 0$ and so

$$v = (-\alpha^{-1}\alpha_1)v_1 + ... + (-\alpha^{-1}\alpha_n)v_n \in L(S)$$

$\Rightarrow V \subseteq L(S)$

$\Rightarrow V = L(S)$ and as S is *LI*, S is a basis of V.

Example 4.52: If $\{v_1, v_2,..., v_n\}$ is a basis of FDVS V of *dim* n and $v = \Sigma\alpha_i v_i$, $\alpha_r \neq 0$ then prove that $\{v_1, v_2,..., v_{r-1}, v, v_{r+1} ..., v_n\}$ is also a basis of V.

Solution: We have

$$v = \alpha_1 v_1 + ... + \alpha_r v_r + ... + \alpha_n v_n \quad \alpha_r \neq 0,\ \therefore\ \alpha_r^{-1} \text{ exists}$$

$$\Rightarrow v_r = (-\alpha_r^{-1}\alpha_1)\, v_1 + ... + (-\alpha_r^{-1}\, \alpha_{r-1})\, v_{r-1} + \alpha_r^{-1} v + ... + (-\alpha_r^{-1}\alpha_n)v_n$$

$$= \beta_1 v_1 + ... + \beta_{r-1} v_{r-1} + \beta_r v + \beta_{r+1}\, v_{r+1} + ... + \beta_n v_n.$$

If $x \in V$ be any element, then

$$x = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n \quad \alpha_i \in F$$

$$\Rightarrow x = a_1 v_1 + ... + a_{r-1} v_{r-1} + a_r(\beta_1 v_1 + ... + \beta_n v_n) + ... + a_n v_n$$

or that x is a linear combination of

$$v_1, ..., v_{r-1}, v, v_{r+1},..., v_n$$

and x being any element, we find V is spanned by $\{v_1,..., v_{r-1}, v, v_{r+1},... v_n\}$ and it forms a basis of V.

Theorem 4.33: 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 $\{v_1, v_2, .., v_n\}$ be a basis of V.

We claim $\{\theta(v_1), \theta(v_2), ..., \theta(v_n)\}$ is a basis of W.

Now $\sum_{i=1}^{n} \alpha_i\ \theta(v_i) = 0 \quad \alpha_i \in F,$

$$\Rightarrow \sum \theta(\alpha_i v_i) = 0 = \theta(0)$$

$$\Rightarrow \sum \alpha_i v_i = 0 \quad (\theta \text{ is } 1\text{–}1)$$

$\Rightarrow$ $\alpha_i = 0$ for all i as $v_1, v_2, ..., v_n$ are LI

$\Rightarrow$ $\theta(v_1), \theta(v_2), ..., \theta(v_n)$ are LI

Again, if $w \in W$ is any element, then as θ is onto, $\exists$ some $v \in V$ such that, $\theta(v) = w$

NOTES

Now $v \in V \Rightarrow v = \sum_{i=1}^{n} \alpha_i v_i$ for some $\alpha_i \in F$

$$\Rightarrow \quad w = \theta(v) = \theta\left(\sum \alpha_i v_i\right)$$

$$\Rightarrow \quad w = \sum \theta(\alpha_i v_i) = \alpha_1 \theta(v_1) + \alpha_1 \theta(v_2) + ... + \alpha_n \theta(v_n)$$

or that w is a linear combination of $\theta(v_1), \theta(v_2), ..., \theta(v_n)$

Hence $\theta(v_1), \theta(v_2),..., \theta(v_n)$ span W and therefore, form a basis of W showing that dim $W = n$.

Conversely, let dim V = dim $W = n$ and suppose. $\{v_1, v_2, ..., v_n\}$ and $\{w_1, w_2, ...,w_n\}$ are basis of V and W respectively.

Define a map $\theta : V \to W$ such that,

$$\theta(v) = \theta(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n)$$
$$= \alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_n w_n$$

then θ is easily seen to be well defined. (Indeed any $v \in V$ is unique linear combination of members of basis).

If $v, v' \in V$ be any elements then

$$v = \sum \alpha_i v_i, \; v' = \sum \beta_i v_i \quad \alpha_i, \beta_i \in F$$

$$\theta(v + v') = \theta\left(\sum \alpha_i v_i + \sum \beta_i v_i\right)$$
$$= \theta\left(\sum (\alpha_i + \beta_i) v_i\right)$$
$$= \sum (\alpha_i + \beta_i) w_i$$
$$= \sum \alpha_i w_i + \sum \beta_i w_i = \theta(v) + \theta(v')$$

Also $\theta(\alpha v) = \theta\left(\alpha \sum \alpha_i v_i\right) = \theta\left(\sum \alpha\alpha_i v_i\right) = \sum (\alpha\alpha_i) w_i$

$$= \alpha \sum \alpha_i w_i = \alpha\theta(v)$$

Thus θ is a homomorphism.

Now if $v \in$ Ker θ

then $\theta(v) = 0$

$\Rightarrow \theta\left(\sum \alpha_i v_i\right) = 0$

$\Rightarrow \sum \alpha_i w_i = 0$

$\Rightarrow \alpha_i = 0$ for all i $w_1, w_2, ..., w_n$ being LI

$\Rightarrow v = 0$

$\Rightarrow$ Ker $\theta = \{0\}$

$\Rightarrow$ θ is one–one.

That θ is onto is obvious. Hence θ is an isomorphism.

Corollary: Under an isomorphism, a basis is mapped onto a basis.

This follows by that first part of the theorem.

Example 4.53: 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.

NOTES

Solution: One can check that $V = \{f | f: \mathbf{R} \to \mathbf{R}, f \text{ cont.}\}$ is a vector space over **R**, under

$$(f + g)x = f(x) + g(x)$$
$$(\alpha f)x = \alpha(f(x))$$

Let $W = \{f \in V | f \text{ is a solution of given differential equation}\}$

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 the general solution is,

$$y = Ae^{-x} + be^{-2x} + Ce^{-3x}$$

If $S = \{e^{-x}, e^{-2x}, e^{-3x}\}$ then clearly S spans W

Let $$Ae^{-x} + Be^{-2x} + Ce^{-3x} = 0$$

Then $$-Ae^{-x} + (-2)\, Be^{-2x} + (-3C)\, e^{-3x} = 0$$
$$Ae^{-x} + (4B)\, e^{-2x} + (9C)\, e^{-3x} = 0 \quad \forall\, x$$

Put $x = 0$

$$\begin{bmatrix} 1 & 1 & 1 \\ -1 & -2 & -3 \\ 1 & 4 & 9 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0 \quad \Rightarrow M \begin{bmatrix} A \\ B \\ C \end{bmatrix} = 0$$

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 *LI* 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 $\Rightarrow \alpha_1 y_1 + \alpha_2 y_2 \in W$].

Example 4.54: If $S = \{v_1, v_2, ..., v_r\}$ is a *LI* subset of V and $v \in V$ be, such that, $v \notin L(S)$, then show that $S \cup \{v\}$ is a *LI* subset of V.

Solution: $S \cup \{v\} = \{v_1, v_2, ..., v_r, v\}$

Let $$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r + \alpha v = 0 \quad \alpha_i \in F,\ \alpha \in F$$

If $\alpha \neq 0$ then α^{-1} exists and we get

$$\alpha^{-1}(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r + \alpha v) = 0$$
$$\Rightarrow \quad v = (-\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + ... + (\alpha^{-1}\alpha_r)v_r$$
$$\Rightarrow \quad v \in L(S), \text{ a contradiction}$$

thus $$\alpha = 0$$
$$\Rightarrow \quad \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_r v_r = 0$$

$\Rightarrow$ $\alpha_i = 0$ for all i as $v_1, v_2,..., v_r$ are LI

$\Rightarrow$ $\alpha = \alpha_i = 0$ for all i

$\Rightarrow$ $v_1, v_2,..., v_r, v$ are LI

NOTES

Hence the result follows.

Theorem 4.34: Let W be a subspace of an FDVS V, then W is finite dimensional and dim $W \leq$ dim V. In fact, dim V = dim W *iff* $V = W$.

Proof: Let dim $V = n$, then n is the maximum number of LI elements in any subset of V. Since any subset of W will be a subset of V, n is the maximum number of LI elements in W.

Let $w_1, w_2,..., w_m$ be the maximum number of LI elements in W then $m \leq n$.

We show $\{w_1, w_2,..., w_m\}$ is a basis of W. These are already LI If $w \in W$ be any element then the set $\{w_1, w_2, ..., w_m, w\}$ is LD

$\Rightarrow \exists\ \alpha_1, \alpha_2,..., \alpha_m, \alpha$ in F (not all zero) such that,

$\alpha_1 w_1 + ... + \alpha_m w_m + \alpha w = 0$.

If $\alpha = 0$, we get $\alpha_i = 0$ for all i as $w_1,..., w_m$ are LI which is not true. Thus $\alpha \neq 0$ and so α^{-1} exists.

The above equation then gives us

$$w = (-\alpha^{-1}\alpha_1)w_1 + ... + (-\alpha^{-1}\ \alpha_m)\ w_m$$

Showing that $\{w_1, w_2,..., w_m\}$ spans W (and thus W is finite dimensional)

$\Rightarrow$ $\{w_1, w_2,..., w_m\}$ is a basis of W

$\Rightarrow$ dim $W = m \leq n =$ dim V

Finally, if dim V = dim $W = n$

and $\{w_1, w_2,..., w_n\}$ be a basis of W then as $\{w_1, w_2,..., w_n\}$ is LI in W it will be LI in V.

and as dim $V = n$, $\{w_1, w_2,..., w_n\}$ is a basis of V.

Now if $v \in V$ be any element then

$$v = \alpha_1 w_1 + \alpha_2 w_2 + ... + \alpha_n w_n \in W$$

$\Rightarrow$ $V \subseteq W \Rightarrow V = W$.

Conversely, of course, $V = W \Rightarrow$ dim V = dim W.

Notes:

(*i*) If W is a subspace of V where $W = (0)$ then dimension of W is taken to be zero.

(*ii*) **C** (**Q**) is not finite dimensional as if it is then its subspace **R**(**Q**) will also be finite dimensional, which is not true, as suppose dim **R**(**Q**) = n. Let $x_1, x_2,..., x_n$ be a basis of **R**(**Q**), then

$$\mathbf{R} = \{\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n \mid \alpha_i \in \mathbf{Q}\}$$

Since **Q** is a countable set, each α_i has countable choices. So **R** should be countable, which is not true. Hence dim **R**(**Q**) is not finite.

(*iii*) The result of theorem may not hold if V is not finite dimensional. Consider $V = F[x]$ and take $W = F[x^2]$, then W is a subspace of V, $W \neq V$ as $x \in V$, $x \notin W$. Here $S = \{1, x, x^2,..., x^n,...\}$ is a basis of V and

$T = \{1, x^2,..., x^{2n},...\}$ is a basis of W. The map $\theta : S \to T$, such that, $\theta(x^i) = x^{2i}$ is 1–1 onto and thus S & T have same cardinality $\Rightarrow \dim V = \dim W$.

NOTES

Theorem 4.35: Let W be a subspace of an FDVS V. Then

$$\dim \frac{V}{W} = \dim V - \dim W.$$

Proof: Let $\dim W = m$ and let $\{w_1, w_2, ..., w_m\}$ be a basis of W.

$w_1, w_2,..., w_m$ being LI in W will be LI in V and thus $\{w_1, w_2,..., w_m\}$ can be extended to form a basis of V.

Let $\{w_1, w_2,..., w_m, v_1, v_2,..., v_n\}$ be this extended basis of V.

then $\dim V = n + m$

Consider the set $S = \{W + v_1, W + v_2,..., W + v_n\}$, we show it forms a basis of $\frac{V}{W}$.

Let $\alpha_1(W + v_1) + ... + \alpha_n(W + v_n) = W, \quad \alpha_i \in F$

Then $W + (\alpha_1 v_1 + ... + \alpha_n v_n) = W$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n \in W$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n$ is a linear combination of $w_1,..., w_m$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = \beta_1 w_1 + ... + \beta_m w_m \quad \beta_j \in F$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n - \beta_1 w_1 - ..... - \beta_m w_m = 0$

$\Rightarrow \alpha_i = \beta_j = 0$ for all i, j.

$\Rightarrow \{W + v_1, W + v_2,....., W + v_n\}$ is LI

Again, for any $W + v \in \frac{V}{W}$, $v \in V$ means v is a linear combination of $w_1,..., w_m, v_1,..., v_n$.

i.e., $v = \alpha_1 w_1 + ... + \alpha_m w_m + \beta_1 v_1 + ... + \beta_n v_n \quad \alpha_i, \beta_j \in F$

giving
$$\begin{aligned} W + v &= W + (\alpha_1 w_1 + ... + \alpha_m w_m) + (\beta_1 v_1 + ... + \beta_n v_n) \\ &= W + (\beta_1 v_1 + ... + \beta_n v_n) \\ &= (W + \beta_1 v_1) + ... + (W + \beta_n v_n) \\ &= \beta_1(W + v_1) + \beta_2(W + v_2) + ... + \beta_n(W + v_n). \end{aligned}$$

Hence S spans $\frac{V}{W}$ and is therefore a basis.

$\therefore \quad \dim \frac{V}{W} = n$

Thus $\dim \frac{V}{W} = \dim V - \dim W.$

Note: Thus we notice that if V is a FDVS then so is $\frac{V}{W}$. Converse of this may not be true. Consider

$$V = F[x], \quad W = \{x^2 f(x) \mid f(x) \in V\}$$

Then W is a subspace of V and

$$\frac{V}{W} = \{W + a_0 + a_1 x \mid a_i \in F\} \text{ which}$$

is spanned by $\{W+1, W+x\}$ and thus $\frac{V}{W}$ is finite dimensional, whereas V is not.

NOTES

Theorem 4.36: If A and B are two subspaces of an FDVS V then

$$\dim (A + B) = \dim A + \dim B - \dim (A \cap B).$$

Proof: We have already proved that

$$\frac{A+B}{A} \cong \frac{B}{A \cap B}$$

$$\therefore \quad \dim \frac{A+B}{A} = \dim \frac{B}{A \cap B}$$

$$\Rightarrow \quad \dim (A+B) - \dim A = \dim B - \dim (A \cap B)$$

or that $\dim (A+B) = \dim A + \dim B - \dim (A \cap B)$.

Note: You should try to give an independent proof of the above theorem as an exercise.

Corollary: If $A \cap B = (0)$ then $\dim (A + B) = \dim A + \dim B$

i.e., $\dim (A \oplus B) = \dim A + \dim B$.

Example 4.55: Let W_1, W_2, W_3 be subspaces of an FDVS. Show that

$$\dim (W_1 + W_2 + W_3) \leq \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_1 \cap W_2) - \dim (W_1 \cap W_3) - \dim (W_2 \cap W_3) + \dim (W_1 \cap W_2 \cap W_3).$$

Solution: We have

$$\begin{aligned}\dim (W_1 + W_2 + W_3) &= \dim W_1 + \dim (W_2 + W_3) - \dim (W_1 \cap (W_2 + W_3)) \\ &= \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_2 \cap W_3) \\ &\quad - \dim (W_1 \cap (W_2 + W_3)) \\ &\leq \dim W_1 + \dim W_2 + \dim W_3 - \dim (W_2 \cap W_3) \\ &\quad - \dim (W_1 \cap W_2) - \dim (W_1 \cap W_3) \\ &\quad + \dim (W_1 \cap W_2 \cap W_3)\end{aligned}$$

as $(W_1 \cap W_2) + (W_1 \cap W_3) \subseteq W_1 \cap (W_2 + W_3)$.

Example 4.56: Let P_n be the vector space of all polynomials of degree $\leq n$ over **R**. Exhibit 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, $\alpha(P_2 + x^3) + \beta(P_2 + x^4) = \text{zero} = P_2$

$\Rightarrow \quad P_2 + \alpha x^3 + \beta x^4 = P_2$

$\Rightarrow \quad \alpha x^3 + \beta x^4 = a + bx + cx^2 \in P_2$

$\Rightarrow a = b = c = \alpha = \beta = 0$ as polynomial is zero, if each coefficient is zero.

Thus S is a basis of $\frac{P_4}{P_2}$.

Hence $\dim \frac{P_4}{P_2} = 2 = 5 - 3 = \dim P_4 - \dim P_2$.

NOTES

Theorem 4.37: Let W be a subspace of an FDVS V, then there exists a subspace W' of V such that $V = W \oplus W'$.

Proof: Let $\{w_1, w_2,..., w_m\}$ be a basis of W, then $w_1, w_2,..., w_m$ being *LI* in W will be *LI* in V. We extend these *LI* elements to form a basis of V, say $\{w_1,..., w_m, v_1,..., v_n\}$

Let $W' = L(\{v_1, v_2,..., v_n\})$, i.e., W' be the subspace spanned by $\{v_1, v_2,..., v_n\}$.

We show $\quad W \oplus W' = V$

Let $v \in V$ be any element, then

$$v = (\alpha_1 w_1 + ... + \alpha_m w_m) + (\beta_1 v_1 + ... + \beta_n v_n), \quad \alpha_i, \beta_j \in F$$

where the first bracket term belongs to W and the second to W'

$\therefore \quad v \in W + W'$ 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 $x \in W'$

$\Rightarrow x = a_1 w_1 + ... + a_m w_m \qquad a_i, b_j \in F$

$x = b_1 v_1 + ... + b_n v_n$

$\Rightarrow \quad a_1 w_1 + ... + a_m w_m + (-b_1) v_1 + ... + (-b_n) v_n = 0$

$\Rightarrow a_i = b_j = 0$ for all $i, j \qquad w_1,..., w_m, v_1,..., v_n$ being *LI*

Hence $\quad x = 0$

$\Rightarrow W \cap W' = (0)$

or that $\quad V = W \oplus W'$

Notes:

(*i*) W' is called complement of W. Thus we have proved that *every subspace of an* FDVS *has a complement.*

(*ii*) The above throrem can also be proved in any vector space (not essentially finite dimensional).

Corollary: If W' is any complement of W in V then $\dim W' = \dim V - \dim W$.

Since $V = W \oplus W' \Rightarrow \quad \dim V = \dim (W \oplus W') = \dim W + \dim W'$

$\Rightarrow \dim W' = \dim V - \dim W.$

Although every complement of a subspace has same dimension, it does not mean that a subspace has a unique complement.

Definition: Let $V(F)$ be a vector space. Subspaces $W_1, W_2,..., W_m$ of V are said to be independent if

$$w_1 + w_2 + ... + w_m = 0 \Rightarrow w_i = 0 \quad \forall i, \ w_i \in W_i$$

NOTES

Theorem 4.38: Let V be an FDVS Let $W_1, W_2,..., W_m$ be subspaces of V, where $W = W_1 + W_2 + ... + W_m$, then the following are equivalent:

(*i*) $W_1, W_2,..., W_m$ are independent

(*ii*) $W_j \cap (W_1 + W_2 + ... + W_{j-1}) = \{0\}, \quad \forall j, \ 2 \le j \le m$

(*iii*) If β_i is an ordered basis of W_i, $1 \le i \le m$, then $\beta = \{\beta_1, \beta_2,..., \beta_m\}$ is an ordered basis of W.

Proof: $(i) \Rightarrow (ii)$

Let $x \in W_j \cap (W_1 + W_2 + ... + W_{j-1})$ be any element

$\Rightarrow x \in W_j$ and $x \in W_1 + W_2 + ... + W_{j-1}$

$\Rightarrow x = w_j, \quad x = w_1 + w_2 + ... + w_{j-1} \quad w_i \in W_i$

$\Rightarrow \quad w_1 + w_2 + ... + w_{j-1} = w_i$

or that $w_1 + w_2 + ... + w_{j-1} + (-1)\, w_j + 0 + 0 \ ... + 0 = 0$

$\Rightarrow w_i = 0 \quad \forall i$ using (i)

$\Rightarrow x = 0 \Rightarrow$ result.

$(ii) \Rightarrow (iii)$

Let $\beta_i = \{x_{i_1},..., x_{i_{d_i}}\}$ be basis of W_i.

Let $\sum_{i=1}^{k} a_{i1}x_{i1} + a_{i2}x_{i2} + ... + a_{id_1}x_{id_i} = 0$

Then $\sum_{i=1}^{k} w_i = 0 \Rightarrow w_i = 0$ for all i (since, if j is the largest integer such that, $w_j \neq 0$, then $w_1 + ... + w_j = 0 \Rightarrow w_j \in W_j \cap (W_1 + ... + W_{j-1}) = \{0\}$ $\Rightarrow w_j = 0$, a contradiction).

$\therefore \ \beta = \{\beta_1,..., \beta_k\}$ is an independent set in W. Since β_i spans W_i for all i, β spans W.

$\therefore \ \beta$ is a basis of W.

$(iii) \Rightarrow (i)$

Let $\quad x_1 + ... + x_m = 0, \ x_i \in W_i$

Then $\quad \alpha_{1_1}x_{1_1} + ... + \alpha_{1d_1}x_{1_{d_1}} + ... + \alpha_{k_1}x_{k_1} + ... + x_{k_{d_k}} = 0$

$\Rightarrow$ each coefficient $\alpha_{ij} = 0$ as β is linearly independent

$\Rightarrow$ each $x_i = 0$

$\Rightarrow W_1,..., W_m$ are independent.

Example 4.57: Let V be a finite dimensional space and $W_1,..., W_m$ be subspaces of V such that

$V = W_1 + ... + W_m$ and dim V = dim W_1 + ... + dim W_m

Prove that $\quad V = W_1 \oplus ... \oplus W_m$.

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 $x = x_1 + ... + x_m, x_i \in W_i, x_i \in W_i \Rightarrow x_i$ is a linear combination of vectors in β_i.

$\Rightarrow$ x is a linear combination of vectors in $\beta = \{\beta_1, ..., \beta_m\}$

$\Rightarrow$ 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 $V < o(\beta_1) + ... + o(\beta_m) =$ dim $W_1 + ...$ + dim $W_k =$ dim V, a contradiction)

$\Rightarrow$ $W_1, ..., W_m$ are independent

$\Rightarrow$ $W_j \cap (W_1 + ... + W_{j-1}) = \{0\}$ for all j, $2 \le j \le m$

$\Rightarrow$ $V = W_1 \oplus W_2 + ... + \oplus W_m$.

4.10 VECTOR SPACE OF LINEAR TRANSFORMATION

To recall the definition, by a linear transformation, we mean a map $T: V \to W$, such that, $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ where $x, y \in V$, $\alpha, \beta \in F$ and V, W are vector spaces over the field F. You need to go through the definitions and results done earlier, especially on kernel and range of a linear transformation Also, we'll be dealing with vector spaces that are finite dimensional, unless mentioned otherwise.

Theorem 4.39: A linear transformation $T: V \to V$ is one-one iff T is onto.

Proof: Let $T: V \to V$ be one-one. Let dim $V = n$.

Let $\{v_1, v_2, ..., v_n\}$ be a basis of V, then $\{T(v_1), ..., T(v_n)\}$ will also be a basis of V as

$$\alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0$$

$\Rightarrow$ $T(\alpha_1 v_1 + ... + \alpha_n v_n) = T(0)$ (T a *lin*ear transformation)

$\Rightarrow$ $\alpha_1 v_1 + ... + \alpha_n v_n = 0$ (T is 1-1)

$\Rightarrow$ $\alpha_i = 0$ for all i

thus $T(v_1), ... T(v_n)$ are *LI* and as dim $V = n$ the result follows.

Let now $v \in V$ be any element

then $v = a_1 T(v_1) + a_2 T(v_2) + ... + a_n T(v_n)$ $a_i \in F$

$= T(a_1 v_1 + ... + a_n v_n)$

$= T(v')$ for some v'

Hence T is onto.

Conversely, let T be onto.

Here again we show that if $\{v_1, v_2, ... v_n\}$ is a basis of V then so also is $\{T(v_1), T(v_2), ..., T(v_n)\}$

For any $v \in V$, since T is onto, $\exists$ some $v' \in V$ such that,

$$T(v') = v$$

Again $v' \in V$ means $v' = \sum \alpha_i v_i$ $\alpha_i \in F$

$\therefore$ $v = T(v') = T(\sum \alpha_i v_i) = \sum \alpha_i T(v_i)$

$\Rightarrow$ $T(v_1), T(v_2), ..., T(v_n)$ span V

and as dim $V = n$, $\{T(v_1), ..., T(v_n)\}$ forms a basis of V.

Now if $v \in$ Ker T be any element

NOTES

NOTES

then $T(v) = 0$

$\Rightarrow T(\Sigma \alpha_i v_i) = 0$

$\Rightarrow \Sigma \alpha_i T(v_i) = 0$

$\Rightarrow \alpha_i = 0$ for all i as $T(v_1), ..., T(v_n)$ are LI

$\Rightarrow v = \Sigma \alpha_i v_i = 0$

$\Rightarrow$ Ker $T = \{0\} \Rightarrow T$ is 1-1.

Theorem 4.40: Let V and W be two vector spaces over F. Let $\{v_1, v_2, ..., v_n\}$ be a basis of V and $w_1, w_2, ..., w_n$ be any vectors in W (not essentially distinct). Then there exists a unique linear transformation.

$$T : V \to W, \text{ such that, } T(v_i) = w_i \quad i = 1, 2, ..., n.$$

Proof: Let $v \in V$ be any element, then $v = \sum_{i=1}^{n} \alpha_i v_i$, $\alpha_i \in F$ as $\{v_1, v_2, ..., v_n\}$ is a basis of V.

Define $T : V \to W$, such that,

$$T(v) = \Sigma \alpha_i w_i$$

Then T is a linear transformation (verify!).

Clearly here, $T(v_i) = T(ov_1 + ... + 1 \cdot v_i + ... + ov_n) = 1w_i$ for all i

To show uniqueness let T' be any other linear transformation from $V \to W$ such that

$$T'(v_i) = w_i$$

Let $v \in V$ be any element, then $v = \Sigma \alpha_i v_i$

$$T'(v) = T'(\Sigma \alpha_i v_i) = \Sigma \alpha_i T'(v_i) = \Sigma \alpha_i w_i = T(v)$$

Hence $T' = T$.

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 linear transformation

then we define Rank of T = dim Range $T = r(T)$

Nullity of T = dim Ker $T = v(T)$.

Theorem 4.41 (Sylvester's Law) : Let $T : V \to W$ be a linear transformation, then

$$\text{Rank } T + \text{Nullity } T = \dim V.$$

Proof: Let $\{x_1, x_2, ..., x_m\}$ be a basis of Ker T then $\{x_1, x_2, ..., x_m\}$ being LI in Ker T will be LI in V. Thus it can be extended to form a basis of V.

Let $\{x_1, x_2, ..., x_m, v_1, v_2, ..., v_n\}$ be the extended basis of V.

Then dim Ker T = nullity of $T = m$

dim $V = m + n$

We show $\{T(v_1), T(v_2), ..., T(v_n)\}$ is a basis of Range T

Now $\alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0$

$\Rightarrow T(\alpha_1 v_1 + ... + \alpha_n v_n) = 0$

$\Rightarrow \alpha_1 v_1 + \alpha_2 v_2 ... + \alpha_n v_n \in$ Ker T

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = \beta_1 x_1 + ... + \beta_m x_m$

Or $\alpha_1 v_1 + ... + \alpha_n v_n + (-\beta_1)x_1 + ... + (-\beta_m)x_m = 0$

$\Rightarrow \alpha_1 = \alpha_2 = ... = \beta_1 = ... = \beta_m = 0$

$\Rightarrow \alpha_i = 0$ for all i

i.e., $\{T(v_1), T(v_2), ..., T(v_n)\}$ is LI

Now if $T(v) \in$ Range T be any element then as $v \in V$

$$v = a_1x_1 + ... + a_mx_m + b_1v_1 + ... + b_nv_n \quad a_i, b_j \in F$$

$$\therefore \quad T(v) = a_1T(x_1) + ... + a_mT(x_m) + b_1T(v_1) + ... + b_nT(v_n)$$

$$= 0 + ... + 0 + b_1T(v_1) + ... + b_nT(v_n) \text{ [as } x_i \in \text{Ker } T\text{]}$$

or that $T(v)$ is a linear combination of $T(v_1), ..., T(v_n)$

which, therefore, form a basis of Range T.

$\therefore$ dim Range $T = n =$ rank T

which proves the theorem.

Theorem 4.42: If $T : V \to V$ be a linear transformation 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*)

$T(T(v)) = 0 \Rightarrow T(v) \in$ Ker T

Also $T(v) \in$ Range T (by definition)

$\Rightarrow T(v) = 0$

(*ii*) $\Rightarrow$ (*i*)

Let $x \in$ Range $T \cap$ Ker T

$\Rightarrow x \in$ Range T and $x \in$ Ker T

$\Rightarrow x = T(v)$ for some $v \in V$

And $T(x) = 0$

$x = T(v) \Rightarrow T(x) = T(T(v))$

$\Rightarrow 0 = T(T(v))$

$\Rightarrow T(v) = 0$ (given condition)

$\Rightarrow v = 0.$

Algebra of Linear Transformation: Rank Nullity Theorem and Change of Basis

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

$T + S : V \to W$, such that

$(T + S)v = T(v) + S(v), \quad v \in V$

Then $T + S$ is also a linear transformation from $V \to W$ as

$$(T + S)(\alpha x + \beta y) = T(\alpha x + \beta y) + S(\alpha x + \beta y)$$

$$= \alpha T(x) + \beta T(y) + \alpha S(x) + \beta S(y)$$

$$= \alpha(T + S)x + \beta(T + S)y$$

NOTES

NOTES

Again for $\alpha \in F$, we define the product of a linear transformation $T : V \to W$ with α, by $(\alpha T) : V \to W$ such that, $(\alpha T)v = \alpha(T(v))$.

It is easy to see that αT is a also a linear transformation 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.

$(T + S)v = T(v) + S(v) = S(v) + T(v) = (S + T)v$ for all $v \in V$

$\Rightarrow$ $T + S = S + T$ for all $S, T \in$ Hom (V, W)

The map $O : V \to W$, such that, $O(v) = 0$ is a linear transformation and

$(T + O)v = T(v) + O(v) = T(v) = (O + T)v$ for all v

Thus O is zero of Hom (V, W)

For any $T \in$ Hom (V, W), the map $(-T) : V \to W$, such that,

$(-T)v = -T(v)$

will be additive inverse of T.

Again, $[\alpha(T + S)]v = \alpha[(T + S)v] = \alpha[T(v) + S(v)] = \alpha T(v) + \alpha S(v)$

$= (\alpha T)v + (\alpha S)v = (\alpha T + \alpha S)v$ for all $v \in V$

$\Rightarrow$ $\alpha(T + S) = \alpha T + \alpha S$

$[(\alpha\beta)T]v = (\alpha\beta)T(v) = \alpha[\beta T(v)] = [\alpha(\beta T)]v$ for all v

$\Rightarrow$ $(\alpha\beta)T = \alpha(\beta T)$

$(1T)v = 1 \,.\, T(v) = T(v)$ 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 $T : V \to W$, $S : W \to Z$ be *lin*ear transformation

We define $ST : V \to Z$, such that,

$(ST)v = S(T(v))$

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 linear transformation $T : V \to V$ is called a *linear operator* on V, whereas a linear transformation $T : V \to F$ is called a *linear functional*. We use notation T^2 for $T.T$ and $T^n = T^{n-1}T$, etc.

Theorem 4.43: Let T, T_1, T_2 be linear operators on V, and let $I : V \to V$ be the identity map $I(v) = v$ for all v (which is clearly a linear transformation) 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*) $\alpha(T_1T_2) = (\alpha T_1)T_2 = T_1(\alpha T_2) \quad \alpha \in F$

(*iv*) $T_1(T_2T_3) = (T_1T_2)T_3$.

Proof: (*i*) Obvious.

(*ii*) $[T(T_1 + T_2)]x = T[(T_1 + T_2)x] = T[T_1(x) + T_2(x)]$

$= T(T_1(x)) + T(T_2(x)) = TT_1(x) + TT_2(x)$

$= (TT_1 + TT_2)x$

$\Rightarrow \quad T(T_1 + T_2) = TT_1 + TT_2$

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 definition.

See exercises for the generalised version of above theorem.

Theorem 4.44: 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 $\{v_1, v_2, ..., v_m\}$ and $\{w_1, w_2, ..., w_n\}$ be basis of V and W respectively.

Define mappings $T_{ij} : V \to W$, such that

$T_{ij}(v) = \alpha_i w_j \; 1 \le i \le m$

$1 \le j \le n$

where $v \in V$ is any element and therefore,

$v = \alpha_1 v_1 + \alpha_2 v_2 + ... \; \alpha_m v_m$ for some $\alpha_i \in F$

Note also that $T_{ij}(v_k) = 0$ if $k \neq i$

$= w_j$ if $k = i$

We show T_{ij} are linear transformation

Let $x, y \in V$ then $x = \sum_1^m \alpha_i v_i, \quad y = \sum_1^m \beta_i v_i \quad \alpha_i, \beta_i \in F$

Now $T_{ij}(x + y) = T_{ij}[(\alpha_1 v_1 + ... + \alpha_m v_m) + (\beta_1 v_1 + ... + \beta_m v_m)]$

$= T_{ij}[(\alpha_1 + \beta_1)v_1 + ... + (\alpha_m + \beta_m)v_m]$

$= T_{ij}(\gamma_1 v_1 + ... + \gamma_m v_m)$

$= \gamma_i w_j$

$= (\alpha_i + \beta_i)w_j = \alpha_i w_j + \beta_i w_j = T_{ij}(x) + T_{ij}(y)$

Also, $T_{ij}(\lambda x) = T_{ij}(\lambda(\alpha_1 v_1 + ... + \alpha_m v_m))$

$= T_{ij}(\lambda\alpha_1 v_1 + ... + \lambda\alpha_m v_m)$

$= (\lambda\alpha_i)w_j = \lambda(\alpha_i\, w_j) = \lambda T_{ij}\,(\Sigma\alpha_i v_i)$

$= \lambda T_{ij}(x)$

Hence $T_{ij} \in$ Hom (V, W). We claim $S = \{T_{ij} \mid 1 \le i \le m, 1 \le j \le n\}$ forms a basis of Hom (V, W)

NOTES

NOTES

Suppose

$\beta_{11}T_{11} + \beta_{12}T_{12} + ... + \beta_{1n}T_{1n} + \beta_{21}T_{21} + \beta_{22}T_{22} + ... + \beta_{2n}T_{2n} + ... + \beta_{m1}T_{m1} + \beta_{m2}T_{m2} + ... + \beta_{mn}T_{mn} = 0,\ \beta_{ij} \in F$

[where 0 is, of course, zero of Hom (V, W)]

By operating on v_1, we get

$\beta_{11}T_{11}(v_1) + \beta_{12}T_{12}(v_1) + ... + \beta_{1n}T_{1n}(v_1) + \beta_{21}T_{21}(v_1) + ... = 0$

$\Rightarrow \beta_{11}w_1 + \beta_{12}w_2 + ... + \beta_{1n}w_n + 0 + ... + 0 + ... = 0$

But $w_1, w_2 ..., w_n$ are LI

$\Rightarrow \beta_{11} = \beta_{12} = ... \beta_{1n} = 0$

Similarly, by operating on v_2 we will get $\beta_{21} = \beta_{22} = ... \beta_{2n} = 0$

Thus by operating on v_3, v_4 ... we find that all the coefficients are zero and hence S is LI. So, $o(S) = mn$.

Let Now $T \in$ Hom (V, W) be any element, then

$T : V \to W$ is a *lin*ear transformation

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 $w_1, w_2, ... w_n$

Let $T(v_1) = \alpha_{11}w_1 + \alpha_{12}w_2 + ... + \alpha_{1n}w_n$

Put $T_0 = \alpha_{11}T_{11} + \alpha_{12}T_{12} + ... + \alpha_{1n}T_{1n} + \alpha_{21}T_{21} + \alpha_{22}T_{22} + ... + a_{mn}T_{mn}$

(where α_{11}, α_{12} ... are, of course, the same as before)

Then $T_0(v_1) = \alpha_{11}T_{11}(v_1) + \alpha_{12}T_{12}(v_1) + ...$

$= \alpha_{11}w_1 + \alpha_{12}w_2 + \alpha_{2n}w_n + 0 + 0 + ... + 0$

$\Rightarrow T_0(v_1) = T(v_1)$

Similarly proceeding with $v_2, v_3, ... v_m$, we get

$T_0(v_2) = T(v_2)$

.....

$T_0(v_m) = T(v_m)$

Thus T_0 and T agree on all elements of the basis of V.

$\Rightarrow T_0$ and T agree on all elements of $V \Rightarrow T_0 = T$

But T_0 is a linear combination of members of S

$\Rightarrow T$ is a linear combination of members of S

$\Rightarrow S$ spansHom (V, W)

or that S forms a basis of Hom (V, W)

Hence dim Hom $(V, W) = mn$.

Corollary: Obviously dim Hom $(V, V) = m^2$ where dim $V = m$ and dim Hom $(V, F) = m \cdot 1 = m$ as dim $F(F) = 1$ as F is generated by 1 and thus $\{1\}$ is a basis of $F(F)$.

Example 4.58: Find the range, Rank, Ker and nullity of the linear transformation $T : \mathbf{R}^3 \to \mathbf{R}^3$, such that,

$T(x, y, z) = (x + z,\quad x + y + 2z,\quad 2x + y + 3z)$

Solution: Let $(x, y, z) \in$ Ker T be any element, then

$T(x, y, z) = (0, 0, 0)$

$\Rightarrow (x + z,\ x + y + 2z,\ 2x + y + 3z) = (0, 0, 0)$

$\Rightarrow \quad x + 0 + z = 0$

$x + y + 2z = 0$

$2x + y + 3z = 0$

Giving $x = -z,\ -z + y + 2z = 0$ i.e., $y = -z$

Again, from def. of T, we notice elements of the types $(x+z,\ x+y+2z,\ 2x + y + 3z)$ are in Range T

Now $(x + z, x + y + 2z, 2x + y + 3z) = (x + 0 + z, x + y + 2z, 2x + y + 3z)$

$= (x, x, 2x) + (0, y, y) + (z, 2z, 3z)$

$= x(1, 1, 2) + y(0, 1, 1) + z(1, 2, 3)$

Thus Range T is spanned by $\{(1, 1, 2), (0, 1, 1), (1, 2, 3)\}$

Since $(1, 1, 2) + (0, 1, 1) = (1, 2, 3)$ we find these vectors are LD So dim Range $T \leq 2$

Again as $(1, 1, 2)$ and $(0, 1, 1)$ are LI we find

dim Range $T = 2 =$ Rank T.

Example 4.59: 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 $T_1(V) =$ range T_1, is a subspace of W

Now $(\alpha T_1)v = \alpha(T_1(v)) \in T_1(V)$ for all $v \in V$

$\Rightarrow (\alpha T_1)V \subseteq T_1(V)$ ...(1)

Again as $\alpha \neq 0$, α^{-1} exists and thus

$(\alpha^{-1}T_1)\ V \subseteq T_1(V)$

$\alpha(\alpha^{-1}T_1)V \subseteq \alpha T_1(V)$

$\Rightarrow \quad T_1(V) \subseteq \alpha T_1(V)$

$\Rightarrow \quad T_1(V) = \alpha T_1(V)$ by (1)

$\Rightarrow \quad \dim T_1(V) = \dim \alpha T_1(V)$

Or $r(T_1) = r(\alpha T_1)$.

(*ii*) Since $(T_1 + T_2)x = T_1(x) + T_2(x)$ for all $x \in V$

$(T_1 + T_2)V \subseteq T_1(V) + T_2(V)$

$\Rightarrow \dim [(T_1 + T_2)V] \leq \dim [T_1(V) + T_2(V)]$

$\leq \dim T_1(V) + \dim T_2(V)$

$\Rightarrow \quad r(T_1 + T_2) \leq r(T_1) + r(T_2)$

Again $T_1 = (T_1 + T_2) - T_2 = (T_1 + T_2) + (-T_2)$

$\Rightarrow \quad r(T_1) = r[(T_1 + T_2) + (-T_2)]$

$\leq r(T_1 + T_2) + r(-T_2) = r(T_1 + T_2) + r(T_2)$

(using Equation (1) $\alpha = -1$)

$$\Rightarrow \quad r(T_1) - r(T_2) \leq r(T_1 + T_2)$$

Similarly $\quad r(T_2) - r(T_1) \leq r(T_1 + T_2)$

$$\Rightarrow \quad |r(T_1) - r(T_2)| \leq r(T_1 + T_2) \leq r(T_1) + r(T_2).$$

NOTES

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) linear transformation is also a linear transformation Let $T : V \to W$ be a 1-1 onto linear transformation and $T^{-1}: W \to V$ be its inverse.

We have to prove

$$T^{-1}(\alpha w_1 + \beta w_2) = \alpha T^{-1}(w_1) + \beta T^{-1}(w_2) \quad \alpha, \beta \in F, w_1, w_2 \in W$$

Since T is onto, for $w_1, w_2 \in W$, $\exists\ v_1, v_2 \in V$ such that $T(v_1) = w_1$, $T(v_2) = w_2$

$$\Leftrightarrow \quad v_1 = T^{-1}(w_1),\ v_2 = T^{-1}(w_2)$$

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 linear transformation $T : V \to W$ is called *non-singular* if Ker $T = \{0\}$, i.e., if T is 1-1.

Theorem 4.45: A linear transformation $T : V \to W$ is non-singular iff T carries each *LI* subset of V onto an *LI* subset of W.

Proof: Let T be non-singular and $\{v_1, v_2 ..., v_n\}$ be a *LI* subset of V. we show $\{T(v_1), T(v_2) ..., T(v_n)\}$ is an *LI* subset of W.

Now $\quad \alpha_1 T(v_1) + \alpha_2 T(v_2) + ... + \alpha_n T(v_n) = 0 \quad \alpha_i \in F$

$$\Rightarrow \quad T(\alpha_1 v_1 + ... + \alpha_n v_n) = 0$$

$$\Rightarrow \quad \alpha_1 v_1 + ... \ \alpha_n v_n \in \text{Ker } T = \{0\}$$

$$\Rightarrow \quad \alpha_1 v_1 + ... \ \alpha_n v_n = 0$$

$$\Rightarrow \quad \alpha_i = 0 \text{ for all } i \text{ as } v_1, v_2..., v_n \text{ are } LI$$

Conversely, let $v \in$ Ker T be any element

Then $\quad T(v) = 0$

$$\Rightarrow \quad \{T(v)\} \text{ is not } LI \text{ in } W$$

$$\Rightarrow \quad v \text{ is not } LI \text{ in } V. \text{ (by hypothesis)}$$

$$\Rightarrow \quad v = 0 \Rightarrow \text{Ker } T = \{0\}$$

$$\Rightarrow \quad T \text{ is non-singular.}$$

Theorem 4.46: Let $T : V \to W$ be a linear transformation where V and W are two FDVS with same dimension. Then the following are equivalent:

NOTES

(*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 $\{v_1, v_2,..., v_n\}$ is a basis of V then $\{T(v_1), T(v_2),..., T(v_n)\}$ is a basis of W.

Proof: (*i*) $\Rightarrow$ (*ii*) follows by definition.

(*ii*) $\Rightarrow$ (*iii*) T is non-singular

$\Rightarrow$ Ker $T = \{0\}$

$\Rightarrow$ dim Ker $T = 0$

Since dim Range T + dim Ker T = dim V, we get

dim Range T = dim V

$\Rightarrow$ dim Range T = dim W (given condition)

But Range T being a subspace of W, we find

Range $T = W$

(*iii*) $\Rightarrow$ (*i*) T onto means Range $T = W$

$\Rightarrow$ dim Range T = dim W = dim V

and as dim Range T + dim Ker T = dim V, we get

dim Ker $T = 0$

$\Rightarrow$ 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.

(*iv*) $\Rightarrow$ (*i*)

Let $\{T(v_1),..., T(v_n)\}$ be basis of W where $\{v_1,...v_n\}$ is basis of V. Any $w \in W$ can be put as

$w = \alpha_1 T(v_1) +...+ \alpha_n T(v_n)$

$= T(\alpha_1 v_1 +...+ \alpha_n v_n) = T(v)$ for some $v \in V$

$\therefore$ T is onto. Thus (*iii*) holds.

Hence (*i*) holds.

Example 4.60: 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 $(x_1, x_2, x_3) \in$ Ker T be any element

Then $T(x_1, x_2, x_3) = (0, 0, 0)$

$\Rightarrow (3x_1, x_1 - x_2, 2x_1 + x_2 + x_3) = (0, 0, 0)$

$\Rightarrow 3x_1 = 0, \; x_1 - x_2 = 0, \; 2x_1 + x_2 + x_3 = 0$

$\Rightarrow x_1 = x_2 = x_3 = 0$ or that Ker $T = \{(0, 0, 0)\}$

$\Rightarrow T$ is non-singular and thus invertible (refer Theorem 4.46)

NOTES

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

$$\begin{aligned} T(x_1, x_2, x_3) &= (z_1, z_2, z_3) \\ \Rightarrow \quad 2x_1 &= z_1 \\ x_1 - x_2 &= z_2 \\ 2x_1 + x_2 + x_3 &= z_3 \end{aligned}$$

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

$$T^{-1}(z_1, z_2, z_3) = \left(\frac{z_1}{3}, \frac{z_1}{3} - z_2, z_3 - z_1 + z_2\right)$$

Example 4.61: If $T : V \to V$ is a linear transformation, such that T is not onto, then show that there exists some $0 \neq v$ in V such that, $T(v) = 0$.

Solution: Since T is not onto, it is not 1-1 (theorem done)

Suppose $\exists$ no $0 \neq v \in V$ such that $T(v) = 0$

Then $T(v) = 0$ only when $v = 0$

$\Rightarrow$ Ker $T = \{0\} \Rightarrow T$ is 1-1, a contradiction.

Theorem 4.47: 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.

$$\begin{aligned} \text{Let} \quad ST(x) &= ST(y) \\ \text{Then} \quad S(T(x)) &= S(T(y)) \\ \Rightarrow \quad T(x) &= T(y) \text{ as } S \text{ is } 1-1 \\ \Rightarrow \quad x &= y \text{ as } T \text{ is } 1-1 \\ \Rightarrow \quad ST &\text{ is } 1-1. \end{aligned}$$

Again $ST : V \to U$, let $u \in$ U be any element then as S in onto, $\exists\, w \in W$ such that, $S(w) = u$ and as $T : V \to W$ is onto $\exists\, v \in V$, such that, $T(v) = w$

Now $T(v) = w \Rightarrow S(T(v)) = S(w) \Rightarrow ST(v) = u$

or that ST is onto.

Also $(ST)(T^{-1}S^{-1}) = S(T(T^{-1}S^{-1})) = S(TT^{-1})S^{-1} = S(IS^{-1}) = SS^{-1} = I$

Similarly $(T^{-1}S^{-1})(ST) = T^{-1}(S^{-1}(ST)) = T^{-1}(S^{-1}S)T = T^{-1}(IT) = T^{-1}T = I$

Showing that $(ST)^{-1} = T^{-1}S^{-1}$.

(*ii*) Let $v \in$ Ker T be any element

$$\begin{aligned} \text{Then} \quad T(v) &= 0 \\ \Rightarrow \quad S(T(v)) &= S(0) \\ \Rightarrow \quad ST(v) &= 0 \\ \Rightarrow \quad v &\in \text{Ker } ST \text{ and Ker } ST = (0) \text{ as } ST \text{ is 1-1} \\ \Rightarrow \quad v &= 0 \Rightarrow \text{Ker } T = (0) \Rightarrow T \text{ is 1-1.} \end{aligned}$$

(*iii*) Let $u \in U$ be any element. Since $ST : V \to U$ is onto, $\exists$ some $v \in V$ such that, $ST(v) = u$

i.e., $S(T(v)) = u$

Let $T(v) = w$ and $w \in W$ such that

$S(w) = u$

Then S is onto.

Example 4.62: Let V_1 and V_2 be vector spaces over F. Show that $V_1 \times V_2$ is FDVS if and only if V_1 and V_2 are FDVS

Solution: Let $V_1' = \{(v_1, 0) \mid v_1 \in V_1\}$

$V_2' = \{(0, v_2) \mid v_2 \in V_2\}$

then V_1' and V_2' are subspaces of $V_1 \times V_2$

Define $\theta_1 : V_1 \to V_1'$ such that,

$\theta_1(v_1) = (v_1, 0)$

Then θ_1 is an isomorphism

Similarly $\theta_2 : V_2 \to V_2'$ such that,

$\theta_2(v_2) = (0, v_2)$

will be an isomorphism.

So $V_1 \cong V_1', \quad V_2 \cong V_2'$

Suppose $V_1 \times V_2$ is FDVS, then V_1' and V_2' are FDVS (being subspaces of $V_1 \times V_2$)

$\Rightarrow$ V_1 and V_2 are FDVS

Conversely, if V_1 and V_2 are FDVS then $V_1 \times V_2$ is FDVS and dim $(V_1 \times V_2)$ = dim V_1 + dim V_2. (Note: If $\{e_1, e_2, ..., e_m\}$ and $\{f_1, f_2, ..., f_n\}$ are basis of V_1 and V_2 respectively, then $\{(e_1, 0), ..., (e_m, 0), (0, f_1), ..., (0, f_n)\}$ is a basis of $V_1 \times V_2$.)

4.10.1 Algebra of Linear Transformation

Let $U(F)$, $V(F)$ be vector spaces of dimension n and m respectively. Let $\beta = \{u_1, ..., u_n\}$, $\beta' = \{v_1, ..., v_m\}$ be their ordered basis respectively. Suppose $T : U \to V$ is a linear transformation. Since $T(u_1), ..., T(u_n) \in V$ and $\{v_1, ..., v_m\}$ spans V, each $T(u_i)$ is a linear combination of vectors $v_1, ..., v_m$.

Let $T(u_1) = \alpha_{11}v_1 + ... \alpha_{m1}v_m$

$T(u_2) = \alpha_{12}v_1 + ... + \alpha_{m2}v_m$

.....

$T(u_n) = \alpha_{1n}v_1 + ... + \alpha_{mn}v_m$

where each $\alpha_{ij} \in F$. Then the $m \times n$ matrix

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & ... & ... & \alpha_{1n} \\ : & : & ... & ... & : \\ : & : & ... & ... & : \\ : & : & ... & ... & : \\ \alpha_{m1} & \alpha_{m2} & ... & ... & \alpha_{mn} \end{bmatrix}$$

NOTES

NOTES

is called matrix of T with repsect 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 $M_{m\times n}(F)$ denote 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 4.48: Hom $(U, V) \cong M_{m\times n}(F)$.

Proof: Define θ : Hom $(U, V) \to M_{m\times n}(F)$, such that,

$$\theta(T) = [T]_{\beta, \beta'}$$

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 $\theta(S) = \theta(T)$, $S, T \in$ Hom (U, V)

Then $[S]_{\beta, \beta'} = [T]_{\beta, \beta'}$

$\Rightarrow$ $(a_{ij}) = (b_{ij})$

$\Rightarrow$ $a_{ij} = b_{ij}$ for all i, j

$\Rightarrow$ $S(u_j) = \sum_{i=1}^{m} a_{ij} v_i = \sum_{i=1}^{m} b_{ij} v_i = T(u_j)$ for all $j = 1, \ldots n$

$\Rightarrow$ $S = T \Rightarrow \theta$ is 1-1.

Let $A = (a_{ij})_{m\times n} \in M_{m\times n}(F)$. Then $\exists$ a linear transformation $T \in$ Hom (U, V) such that,

$$T(u_j) = \sum_{i=1}^{m} a_{ij} v_i \quad \text{for } j = 1, \ldots, n$$

$\therefore$ $A = [T]_{\beta, \beta'} = \theta(T) \Rightarrow \theta$ is onto.

Hence θ is an isomorphism and so Hom $(U, V) \cong M_{m\times n}(F)$.

Corollary: 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 $M_{m\times n}(F) = mn$

dim Hom $(U, V) = mn$.

Theorem 4.49: 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 $S(v_1) = a_{11}v_1 + \ldots a_{n1}v_1$

.....

$S(v_n) = a_{1n}v_1 + \ldots + a_{nn}v_n$

Where $a_{ij} \in F$

In general, $S(v_j) = \sum_{i=1}^{n} a_{ij} v_i$ for all $j = 1, ..., n$

$\therefore \quad [S]_\beta = (a_{ij})$

Similarly,

$$T(v_1) = b_{11}v_1 + ... + b_{n1}v_n$$

.....

$$T(v_n) = b_{1n}v_1 + ... + b_{nn}v_n \quad \text{where } b_{ij} \in F$$

In general $T(v_k) = \sum_{j=1}^{n} b_{jk} v_j$, for all $k = 1, ..., n$

$\therefore \quad [T]_\beta = (b_{jk})$

$$\therefore \quad ST(v_k) = S\left(\sum_{j=1}^{n} b_{jk} v_j\right) = \sum_{j=1}^{n} b_{jk} S(v_j) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} b_{jk}\right) v_i$$

$$[ST]_\beta = (c_{ik}), \text{ where } c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

Also, (i, k)th entry in $[S]_\beta [T]_\beta$

$$= \sum_{j=1}^{n} a_{ij} b_{jk} = c_{ik} = (i, k)\text{th entry in } [ST]_\beta$$

$\therefore \quad [ST]_\beta = [S]_\beta [T]_\beta$

Corollary: If S is an invertible linear transformation from $V(F)$ into $V(F)$, then so is $[S]_\beta$ with respect to any basis β of V and conversely.

Proof: Since S is invertaible, $\exists\ T : V \to V$ such that, $ST = I = TS$. Let β be an ordered basis of V. Then by above theorem,

$$[ST]_\beta = [I]_\beta = I, \text{ where } T = S^{-1}$$

$$\Rightarrow \quad [S]_\beta [T]_\beta = I$$

$$\Rightarrow \quad [S]_\beta [S^{-1}]_\beta = I$$

$$\Rightarrow \quad [S^{-1}]_\beta = [S]^{-1}_\beta \text{ for any basis } \beta \text{ of } V$$

Conversely, let $[S]_\beta$ be invertible. Then $\exists$ a matrix $A = (a_{ij})$ over F such that, $[S]_\beta A = I$

Let $T : V \to V$ be a linear transformation such that,

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i \quad \text{for all } j = 1, ... n$$

$$\therefore \quad [T]_\beta = A$$

$$\therefore \quad [S]_\beta [T]_\beta = I$$

$$\Rightarrow \quad [ST]_\beta = I$$

$$\Rightarrow \quad (ST)(v_j) = v_j \quad \text{for all } j = 1, ..., n$$

$$\Rightarrow \quad (ST)(x) = (ST)(\alpha_1 v_1 + ... + \alpha_n v_n)$$

$$= \alpha_1 v_1 + ... + \alpha_n v_n$$

$$= x \quad \text{for all } x \in V$$

$$\Rightarrow \quad ST = I \Rightarrow S \text{ is invertible.}$$

NOTES

NOTES

We now give a relation between matrices of a linear transformation with respect to two different basis of a vector space.

Theorem 4.50: 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 $x \in \text{Ker } S \Rightarrow S(x) = 0, x = \alpha_1 u_1 + ... + \alpha_n u_n, \quad \alpha_i \in F$

$\Rightarrow S(\alpha_1 u_1 + ... + \alpha_n u_n) = 0$

$\Rightarrow \alpha_1 S(u_1) + ... + \alpha_n S(u_n) = 0$

$\Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n = 0$

$\Rightarrow \alpha_i = 0$ for all i

$\Rightarrow x = 0$

$\Rightarrow$ Ker $S = \{0\}$

$\Rightarrow$ S is 1-1 and so onto.

$\therefore$ S is an isomorphism. Let $[T]_{\beta} = (a_{ij})$

Then $$T(u_j) = \sum_{i=1}^{n} a_{ij} u_i$$

$\therefore$ $$(STS^{-1})(v_j) = ST(u_j)$$

$$= S\left(\sum_{i=1}^{n} a_{ij} u_i\right) = \sum_{i=1}^{n} a_{ij} v_i$$

$\therefore$ $$[STS^{-1}]_{\beta'} = (a_{ij}) = [T]_{\beta}$$

$\Rightarrow$ $$[S]_{\beta'}[T]_{\beta'}[S^{-1}]_{\beta'} = [T]_{\beta}$$

$\Rightarrow$ $$[S]_{\beta'}[T]_{\beta'}[S]_{\beta}^{-1} = [T]_{\beta}$$

$\Rightarrow$ $$[T]_{\beta'} = [S]_{\beta'}^{-1}[T]_{\beta}[S]_{\beta'}$$

$$= P^{-1}[T]_{\beta} P, \text{ where } P = [S]_{\beta'}.$$

Example 4.63: Let T be a linear operator on $\mathbf{C}^2$ defined by $T(x_1, x_2) = (x_1, 0)$ Let $\beta = \{\in_1 = (1, 0), \in_2 = (0, 1)\}$, $\beta' = \{\alpha_1 = (1, i), \alpha_2 = (-i, 2)\}$ be ordered basis for $\mathbf{C}^2$. What is the matrix of T relative to the pair β, β'?

Solution: Now $$T(\in_1) = T(1, 0)$$

$$= (1, 0)$$

$$= a(1, i) + b(-i, 2)$$

$\Rightarrow$ $$a - bi = 1 \text{ where } a, b \in \mathbf{C}$$

$$ai + 2b = 0$$

$\Rightarrow$ $$a = 2, b = -i$$

$\Rightarrow$ $$T(\in_1) = 2\alpha_1 - i\alpha_2$$

Also $$T(\in_2) = T(0, 1) = (0, 0) = 0\alpha_1 + 0\alpha_2$$

$$\therefore \qquad [T]_{\beta\,\beta'} = \begin{bmatrix} 2 & 0 \\ -i & 0 \end{bmatrix}.$$

Example 4.64: 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.

NOTES

Solution: Let $V(F)$ be a vector space of dimension n. Let $\beta = \{v_1,..., v_n\}$ be an ordered basis of V. Let $A = (a_{ij})$. Then $\exists$ a linear transformation $T : V \to V$ such that

$$T(v_j) = \sum_{i=1}^{n} a_{ij} v_i$$

$$\therefore \qquad [T]_{\beta} = A.$$

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. So T is 1-1, onto.

Let $$\alpha_1 \begin{bmatrix} a_{11} \\ : \\ a_{n1} \end{bmatrix} + ... + \alpha_n \begin{bmatrix} a_{1n} \\ : \\ a_{nn} \end{bmatrix} = 0,\ \alpha_i \in F$$

$$\Rightarrow \qquad \begin{bmatrix} \alpha_1 a_{11} & \cdots & +\alpha_n a_{1n} \\ \cdots & \cdots & \cdots \\ \alpha_1 a_{n1} + & \cdots & +\alpha_n a_{nn} \end{bmatrix} = 0$$

$$\Rightarrow \qquad \alpha_1 a_{11} + ... + \alpha_n a_{1n} = 0$$

$$\cdots \qquad \cdots$$

$$\alpha_1 a_{n1} + ... + \alpha_n a_{nn} = 0$$

$$\Rightarrow \qquad \alpha_1 a_{11}\, v_1 + ... + \alpha_n a_{1n}\, v_1 = 0$$

$$\cdots \qquad \cdots$$

$$\alpha_1 a_{n1}\, v_n + ... + \alpha_n a_{nn}\, v_n = 0$$

$$\Rightarrow \qquad \alpha_1(a_{11}v_1 + ... + a_{n1}v_n) + ... + \alpha_n(a_{1n}v_1 + ... + \alpha_{nn}v_n) = 0$$

$$\Rightarrow \qquad \alpha_1 T(v_1) + ... + \alpha_n T(v_n) = 0$$

$$\Rightarrow \qquad T(\alpha_1 v_1 + ... + \alpha_n v_n) = 0$$

$$\Rightarrow \qquad \alpha_1 v_1 + ... + \alpha_n v_n = 0 \text{ as } T \text{ is 1-1}$$

$$\Rightarrow \qquad \alpha_i = 0 \text{ for all } i$$

$$\Rightarrow \qquad \text{columns of } A \text{ are linearly independent.}$$

Conversely, let columns of A be linearly independent over F.

Now $\quad x \in \text{Ker } T$

$$\Rightarrow \quad T(x) = 0,\ x \in V$$

$$\Rightarrow \quad T(\alpha_1 v_1 + ... + \alpha_n v_n, = 0$$

$$\Rightarrow \quad \alpha_1 T(v_1) + ... + \alpha_n T(v_n) = 0$$

$$\Rightarrow \quad \sum_{j=1}^{n} \alpha_j T(v_j) = 0 \ \Rightarrow \ \sum_{j=1}^{n} \alpha_j \left(\sum_{i=1}^{n} a_{ij} v_i \right) = 0$$

$$\Rightarrow \quad \sum_{i=1}^{n} \left(\sum_{j=1}^{n} (\alpha_j a_{ij}) \right) v_i = 0$$

NOTES

$$\Rightarrow \quad \sum_{j=1}^{n} \alpha_j a_{ij} = 0 \text{ for all } i = 1, ..., n$$

$$\Rightarrow \quad \alpha_1 \begin{bmatrix} a_{11} \\ : \\ a_{n1} \end{bmatrix} + ... + \alpha_n \begin{bmatrix} a_{1n} \\ : \\ a_{nn} \end{bmatrix} = 0$$

$\Rightarrow$ each $\alpha_i = 0$ as columns are linearly independent

$\Rightarrow$ $x = 0 \quad \Rightarrow$ Ker $T = \{0\}$

$\Rightarrow$ T is 1–1 and so onto

$\Rightarrow$ T is invertible.

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 How (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 4.51: *Let* $\{v_1, ..., v_n\}$ be a basis of V.

Define $\hat{v}_i : V \to F$ *such that,*

$\hat{v}_i (\alpha_1 v_1 + ... + \alpha_n v_n) = \alpha_i \quad i = 1, 2, ..., n$

Then $\hat{v}_i$ is a linear transformation for all $i = 1, ..., n$ and $\{\hat{v}_1, ..., \hat{v}_n\}$ is a basis of $\hat{V}$. Hence dim V = dim $\hat{V}$.

Proof: Let $v, v' \in V$

Suppose $v = \alpha_1 v_1 + ... + \alpha_n v_n$

$v' = \beta_1 v_1 + ... + \beta_n v_n, \quad \alpha_i, \beta_i \in F$

If $v = v'$, then $\alpha_j = \beta_j$ for all $j = 1, ..., n$

$\therefore \quad \hat{v}_i(v) = \alpha_i = \hat{v}_i (v')$

$\therefore$ $\hat{v}_i$ is well defined for all $i = 1, ..., n$

Also $\hat{v}_i(v + v') = \hat{v}_i(\overline{\alpha_1 + \beta_1} v_1 + ... + \overline{\alpha_n + \beta_n} v_n)$

$= \alpha_i + \beta_i$

$= \hat{v}_i(v) + \hat{v}_i(v')$

And $\hat{v}_i(\alpha v) = \hat{v}_i(\alpha\alpha_1 v_1 + ... + \alpha\alpha_n v_n)$

$= \alpha\alpha_i = \alpha \hat{v}_i(v)$

$\therefore$ $\hat{v}_i$ is a *linear transformation* for all $i = 1, ..., n$

By def., $\hat{v}_i(v_j) = (0v_1 + ... + 1v_j + ... + 0v_n) = 0$ if $j \neq i$

$= 1$ if $j = i$

$\therefore \quad \hat{v}_i(v_j) = \delta_{ij}$ for all $i, j = 1, ..., n$

Let $\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n = 0 \quad \alpha_i \in F$

Then $(\alpha_1 \hat{v}_1 + \ ... + \alpha_n \hat{v}_n)\ (v_j) = 0(v_j) = 0$

$\Rightarrow \quad \alpha_j \hat{v}_j(v_j) = 0$

$\Rightarrow \quad \alpha_j = 0 \quad$ for all $j = 1, ..., n$

$\therefore$ $\{\hat{v}_1, ..., \hat{v}_n\}$ is *LI* over *F*.

Let $f \in \hat{V}$. Let $f(v_i) = \alpha_i \quad i = 1, ..., n$

Then $(\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n)\ (v_i) = \alpha_i \hat{v}_i(v_i)$

$= \alpha_i \quad i = 1, ..., n$

$\therefore$ f and $\alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n$ agree on all bases elements of *V*.

So, $f = \alpha_1 \hat{v}_1 + ... + \alpha_n \hat{v}_n$

$\therefore$ $\{\hat{v}_1, ..., \hat{v}_n\}$ spans $\hat{V}$.

Hence, $\{\hat{v}_1, ..., \hat{v}_n\}$ is a basis of $\hat{V}$, called *dual basis* of $\{v_1, ..., v_n\}$ such that, $\hat{v}_i(v_j) = \delta_{ij}$.

Corollary: Let *V* be a finite dimensional vector space over *F*. Let $0 \neq v \in V$. Then $\exists f \in \hat{V}$ such that, $f(v) \neq 0$.

Proof: Since $v \neq 0$, $\{v\}$ is *LI* set. So, it can be extended to form a basis of *V*.

Let $\{v = v_1, v_2, ..., v_n\}$ be a basis of *V*.

Let $\{\hat{v}_1, ..., \hat{v}_n\}$ be corresponding dual basis. Then $\hat{v}_i(v_j) = \delta_{ij}$

$\therefore \quad \hat{v}_1(v_1) = 1$

Let $f = \hat{v}_1 \in \hat{V}$

Then $f(v) = f(v_1) = \hat{v}_1(v_1) = 1 \neq 0.$

Theorem 4.52: Let *V* be a finite dimensional vector space over *F*.

Define $\theta : V \to \hat{\hat{V}}$ such that,

$\theta(v) = T_v$ for all $v \in V$

where $T_v : \hat{V} \to F$ such that,

$T_v(f) = f(v)$ 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 $T_v(f + g) = (f + g)\ (v)$

$= f(v) + g(v)$

$= T_v(f) + T_v(g)$

Let $\alpha \in F$

Then $T_v(\alpha f) = (\alpha f)\ (v)$

$= \alpha f(v)$

$= \alpha T_v(f)$

$\therefore \quad T_v \in \hat{\hat{V}}$

NOTES

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 *linear transformation* as

$$\theta(v + v') = T_{v+v'} = T_v + T_{v'} = \theta(v) + \theta(v')$$

as $T_{v+v'}(f) = f(v + v')$

$= f(v) + f(v')$

$= T_v(f) + T_{v'}(f)$

$= (T_v + T_{v'})(f)$ for all $f \in \hat{V}$

$T_{v+v'} = T_v + T_{v'}$

Also $\theta(\alpha v) = T_{\alpha v} = \alpha T_v = \alpha\theta(v)$

As $T_{\alpha v}(f) = f(\alpha v)$

$= \alpha f(v)$

$= \alpha T_v(f)$ for all $f \in \hat{V}$

$\therefore \quad T_{\alpha v} = \alpha T_v$

Let $0 \neq v \in \text{Ker } \theta \Rightarrow \theta(v) = 0 \Rightarrow T_v = 0$

$\exists f \in \hat{V}$ such that, $f(v) \neq 0$

$\therefore \quad T_v(f) \neq 0$

a contradiction as $T_v = 0 \Rightarrow T_v(f) = 0$

$\therefore \quad \text{Ker } \theta = \{0\} \Rightarrow \theta$ is 1-1

$\therefore \quad V \cong \theta(V) \subseteq \hat{\hat{V}}$

$\Rightarrow \quad \dim \theta(V) = \dim V = \dim \hat{V} = \dim \hat{\hat{V}}$ (by Theorem 4.51)

$\therefore \quad \theta(V) = \hat{\hat{V}}$ as $\theta(V)$ is a subspace of $\hat{\hat{V}}$

$\therefore \theta$ is onto from V to $\hat{\hat{V}}$.

Thus θ is an isomorphism.

Corollary 1: Let V be a finite dimensional vector space over F. If L is a linear functional on $\hat{V}$, then $\exists$ a unique $v \in V$ such that, $L(f) = f(v)$ for all $f \in \hat{V}$.

Proof: L is a linear functional on $\hat{V}$

$\Rightarrow L \in \hat{\hat{V}} \Rightarrow \exists$ unique $v \in V$ such that,

$\theta(v) = L$ as θ is 1-1 onto

$\therefore \quad T_v = L$

$\Rightarrow L(f) = T_v(f) = f(v)$ for all $f \in \hat{V}$.

Corollary 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 $\{f_1, ..., f_n\}$ be a basis for $\hat{V}$.

By Theorem 4.51, $\exists$ a basis $\{L_1, ..., L_n\}$ for $\hat{\hat{V}}$ such that, $L_i(f_j) = \delta_{ij}$. $\exists$ unique $v_i \in V$ for each i

such that, $L_i = T_{v_i} = \theta(v_i)$

Since $\{L_1, L_2, ..., L_n\}$ is a basis for $\hat{V}$, $\{\theta^{-1} L_1, ..., \theta^{-1} L_n\} = \{v_1, ..., v_n\}$ is basis for V as θ is an isomorphism.

Also $\delta_{ij} = L_i(f_j) = T_{v_i}(f_j) = f_j(v_i)$

$\{f_1, ..., f_n\}$ is dual of basis $\{v_1, ..., v_n\}$ for V.

NOTES

Example 4.65: 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 such that, $L_i(p(x)) = p(t_i)$, $i = 1, 2, 3$. Show that $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$. Determine a basis for V such that, $\{L_1, L_2, L_3\}$ 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 $L_i(\alpha p(x)), \quad \alpha \in F$

$= L_i(q(x)), \; q(x) = \alpha p(x)$

$= q(t_i)$

$= \alpha p(t_i) = \alpha\, L_i(p(x)) \quad$ for all $i = 1, 2, 3$

$L_i \in \hat{V} \quad$ 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

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

$$\alpha_1 t_1 + \alpha_2 t_2 + \alpha_3 t_3 = 0$$

$$a_1 t_1^2 + \alpha_2 t_2^2 + \alpha_3 t_3^2 = 0$$

$$\begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0, \; A = \begin{bmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{bmatrix}$$

$$\det A = (t_1 - t_2)\,(t_2 - t_3)\,(t_3 - t_1)$$

$\neq 0$ as t_1, t_2, t_3 are distinct

Thus A^{-1} exists $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$

Hence $\{L_1, L_2, L_3\}$ is a *LI* set.

Since dim $V = 3$, $\{L_1, L_2, L_3\}$ is a basis of $\hat{V}$.

NOTES

Let $\{p_1(x), p_2(x), p_3(x)\}$ be a basis of V such that, $\{L_1, L_2, L_3\}$ is its dual basis.

Then $L_1(p_1) = 1,\ L_2(p_1) = 0,\ L_3(p_1) = 0$

$L_2(p_1) = 0 \quad \Rightarrow p_1(t_2) = 0$

$\Rightarrow t_2$ is a root of $p_1(x)$

$L_3(p_1) = 0 \quad \Rightarrow p_1(t_3) = 0$

$\Rightarrow t_3$ is a root of $p_1(x)$

Since $\deg p_1(x) \le 2,$

$p_1(x) = \alpha(x - t_2)\ (x - t_3), \quad \alpha =$ constant

$L_1\ (p_1) = 1 \quad \Rightarrow p_1(t_1) = 1$

$\Rightarrow \alpha(t_1 - t_2)\ (t_1 - t_3) = 1$

$$\Rightarrow \alpha = \frac{1}{(t_1 - t_2)\,(t_1 - t_3)}$$

$$\therefore \quad p_1(x) = \frac{(x - t_2)\,(x - t_3)}{(t_1 - t_2)\,(t_1 - t_3)}$$

Similarly, $$p_2(x) = \frac{(x - t_1)\,(x - t_3)}{(t_2 - t_1)\,(t_2 - t_3)},\ p_3(x) = \frac{(x - t_1)\,(x - t_2)}{(t_3 - t_1)\,(t_3 - t_2)}.$$

Example 4.66: 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

$$f_1(p) = \int_0^1 p(x)\,dx,\ f_2(p) = \int_0^1 p(x)\,dx,$$

$$f_3(p) = \int_0^{-1} p(x)\,dx$$

Show that $\{f_1, f_2, f_3\}$ is basis of $\hat{V}$. Determine a basis for V such that, $\{f_1, f_2, f_3\}$ is its dual basis.

Solution: It can be easily seen that $f_1, f_2, f_3 \in \hat{V}$.

Let $\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3 f_3 = 0, \quad \alpha_i \in \mathbf{R}$

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 $$A \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = 0,\ \det A \neq 0$$

$$\therefore \qquad A^{-1}A\begin{bmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{bmatrix} = 0 \Rightarrow \alpha_1 = \alpha_2 = \alpha_3 = 0$$

$\therefore \{f_1, f_2, f_3\}$ is a LI 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 such that, $\{f_1, f_2, f_3\}$ is its dual basis.

$$\therefore \qquad f_1(p_1) = 1, f_2(p_1) = 0, f_3(p_1) = 0$$

Let $\qquad p_1(x) = c_o + c_1x + c_2x^2$

$$f_2(p_1) = 0 \Rightarrow c_o x + c_1 \frac{x^2}{2} + c_2 \frac{x^3}{3}\Big|_0^2 = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 0 \text{ when } x = 2$$

$$f_3(p_1) = 0 \Rightarrow c_o x + c_1 \frac{x^2}{2} + c_2 \frac{x^3}{3}\Big|_0^{-1} = 0$$

$$\Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 0 \text{ when } x = -1$$

$$\therefore \qquad c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = \alpha x(x-2)(x+1)$$

$$f_1(p_1) = 1 \qquad \Rightarrow c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = 1 \text{ when } x = 1$$

$$\Rightarrow \alpha \cdot 1 (-1)(2) = 1 \Rightarrow \alpha = -\frac{1}{2}$$

$$c_o x + \frac{c_1}{2}x^2 + \frac{c_2}{3}x^3 = -\frac{1}{2}x(x-2)(x+1)$$

$$= -\frac{1}{2}x^3 + \frac{1}{2}x^2 + x$$

$$\therefore \qquad \frac{c_2}{3} = -\frac{1}{2}, \frac{c_1}{2} = \frac{1}{2}, \; c_o = 1$$

$$\therefore \qquad c_o = 1, c_1 = 1, c_2 = -\frac{3}{2}$$

$$\therefore \qquad p_1(x) = 1 + x - \frac{3}{2}x^2$$

Similarly, we can find $p_2(x), p_3(x)$.

Definition: Let W be a subset of V.

Define $\qquad A(W) = \{f \in \hat{V} \mid f(w) = 0 \quad \text{for all } w \in W\}$

Then $A(W)$ is a subspace of $\hat{V}$ as $\alpha, \beta \in F$,

$$f, g \in A(W) \Rightarrow \quad f(w) = 0 = g(w) \text{ for all } w \in W$$

$$\Rightarrow \alpha f(w) + \beta g(w) = 0 \quad \text{for all } w \in W$$

$$\Rightarrow (\alpha f + \beta g)(w) = 0 \quad \text{for all } w \in W$$

NOTES

$$\Rightarrow \qquad \alpha f + \beta g \in A(W)$$

$A(W)$ is called *annihilator* of W.

Example 4.67: Let U, W be sub-sets of V. If $U \subseteq W$, show that $A(U) \subseteq A(W)$.

NOTES

Solution: Let $f \in A(W)$ then, $f(w) = 0$ for all $w \in W$

$$\Rightarrow \quad f(u) = 0 \quad \text{for all } u \in U \text{ as } U \subseteq W$$
$$\Rightarrow \quad f \in A(U).$$

Theorem 4.53: Let V be a finite dimensional vector space and W, a subspace of V. Then $\dim A(W) = \dim V - \dim W$.

Proof: Let $\{w_1, ..., w_m\}$ be a basis of W.

It can be extended to form a basis of V.

Let $\{w_1, ..., w_m, v_{m+1}, ..., v_n\}$ be a basis of V.

Let $\{f_1, ..., f_m, f_{m+1}, ..., f_n\}$ be corresponding dual basis.

Then $f_i(w_j) = 0 \quad i = m+1, ..., n$

$$j = 1, ..., m$$

$\therefore \quad f_i \in A(W)$ for all $i = m+1, ..., n$

We show $\{f_{m+1}, ..., f_n\}$ is a basis of $A(W)$.

Let $\alpha_{m+1} f_{m+1} + ... + \alpha_n f_n = 0$

$\therefore \quad (\alpha_{m+1} f_{m+1} + ... + \alpha_n f_n)(v_k) = 0$ for all $k = m+1, .., n$

$\therefore \quad \alpha_k f_k (v_k) = 0$

$\therefore \quad \alpha_k = 0$ for all $k = m+1, ..., n$

So, $\{f_{m+1}, ..., f_n\}$ is a LI set.

Let $f \in A(W)$ then $f(w) = 0$ for all $w \in W$, $f \in \hat{V}$

$$f \in \hat{V} \Rightarrow f = \beta_1 f_1 + ... + \beta_m f_m + ... + \beta_n f_n$$
$$\Rightarrow 0 = f(w_j) = \beta_j f_j(w_j) = \beta_j \quad \text{for all } j = 1, ..., m$$
$$\Rightarrow f = \beta_{m+1} f_{m+1} ... + \beta_n f_n$$
$$\Rightarrow \{f_{m+1}, ..., f_n\} \text{ spans } A(W)$$

$\therefore \{f_{m+1}, ..., f_n\}$ is a basis of $A(W)$.

Hence $\dim A(W) = n - m = \dim V - \dim W$.

Corollary 1: $\dfrac{\hat{V}}{A(W)} \cong \hat{W}$

Proof: Since $\dim \dfrac{\hat{V}}{A(W)} = \dim \hat{V} - \dim A(W)$

$$= \dim V - \dim V + \dim W$$
$$= \dim W = \dim \hat{W}$$

Hence $\dfrac{\hat{V}}{A(W)} \cong \hat{W}$.

Corollary 2: If V is a finite dimensional vector space and W, a subspace of V, then

$$A(A(W)) \cong W.$$

Proof: Define $\theta : W \to A(A(W))$ such that,

$$\theta(w) = T_w$$

Where $T_w : \hat{W} \to F$ such that,

$$T_w(f) \to f(w)$$

$$T_w \in A(A(W)) \text{ as } T_w(f) = f(w) = 0 \quad \text{for all } f \in A(W)$$

Then as in Theorem 4.24, θ is well defined 1-1 linear transformation.

$$\therefore \quad W \cong \theta(W) \subseteq A(A(W))$$

Since $\dim A(A(W)) = \dim \hat{V} - \dim A(W)$

$$= \dim V - \dim A(W)$$

$$= \dim W$$

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 $f(x_1, x_2) = x_2$

In fact, $\{f\}$ 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 $\theta : W \to A(A(W))$ such that,

$$\theta(w) = T_w$$

is an isomorphism as basis of W is mapped to basis of $A(A(W))$.

Example 4.68: Let W_1, W_2 be subspaces of finite dimensional vector space V. Determine $A(W_1 + W_2)$.

Solution: $f \in A(W_1 + W_2)$

$$\Leftrightarrow \quad f(x) = 0 \quad \text{for all } x \in W_1 + W_2$$

$$\Leftrightarrow f(w_1) = 0 = f(w_2) \quad \text{for all } w_1 \in W_1, w_2 \in W_2$$

$$\Leftrightarrow \quad f \in A(W_1) \cap A(W_2)$$

$$\therefore \quad A(W_1 + W_2) = A(W_1) \cap A(W_2).$$

Example 4.69: 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 $\dim (A(W_1) \oplus A(W_2))$

NOTES

NOTES

$$= \dim A(W_1) + \dim A(W_2)$$
$$= \dim V - \dim W_1 + \dim V - \dim W_2$$
$$= 2 \dim V - (\dim W_1 + \dim W_2)$$
$$= 2 \dim V - \dim \hat{V} = \dim V = \dim \hat{V}$$

Since $A(W_1) \oplus A(W_2)$ is a subspace of $\hat{V}$

and $\dim \hat{V} = \dim (A(W_1) \oplus A(W_2))$,

$\hat{V} = A(W_1) \oplus A(W_2)$.

Theorem 4.54: If the system of homogeneous linear equations

$$a_{11}x_1 + \ldots + a_{1n}x_n = 0$$
$$\ldots \quad \ldots \quad \ldots$$
$$a_{m1}x_1 + \ldots + a_{mn}x_n = 0,$$

where $a_{ij} \in F$ is of rank r, then there are $n - r$ linearly independent solutions in $F^{(n)}$.

Proof: Let S be the set of solutions of the given system of equations

$S = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in F^n \mid \sum a_{ij}\, \alpha_j = 0, \quad i = 1, 2, \ldots, m\}$

Then S is a subspace of $F^n = V$

Let $\{v_1, v_2, \ldots, v_n\}$ be the standard basis of V

and $\{f_1, f_2, \ldots, f_n\}$ be its dual basis

Let U be the subspace of V as described above

Define $\theta : S \to A(U)$, such that,

$$\theta((\alpha_1, \alpha_2, \ldots, \alpha_n)) = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$$

Let $f = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$

Then $f(u_1) = (\alpha_1 f_1 + \ldots + \alpha_n f_n)\ (a_{11}v_1 + \ldots + a_{1n}v_n)$

$= \alpha_1 a_{11} + \ldots\ \alpha_n a_{1n}$

$= 0$ as $(\alpha_1, \ldots, \alpha_n) \in S$

Similarly $f(u_2) = \ldots = f(u_m) = 0$

So $f \in A(U)$

It can be easily shown that θ is a linear transformation.

If $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \text{Ker } \theta$ then $\sum_1^n \alpha_i f_i = 0$

$\Rightarrow \quad \alpha_i = 0 \quad \forall\ i$

$\Rightarrow \text{Ker } \theta = \{0\}$ or that θ is 1–1.

Let now $f \in A(U) \subseteq \hat{V}$

and suppose $f = \alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_n f_n$

Then $0 = f(u_1) = \alpha_1 a_{11} + \ldots + \alpha_n a_{1n}$

$\ldots \quad \ldots \quad \ldots$

$0 = f(u_m) = \alpha_1 a_{m1} + \ldots + \alpha_n a_{mn}$

$\therefore\ (\alpha_1, \alpha_2, \ldots, \alpha_n) \in S$

and $\theta((\alpha_1, \alpha_2, ..., \alpha_n)) = \alpha_1 f_1 + ... + \alpha_n f_n = f$

or that θ is onto.

Hence $S \cong A(U)$

$\Rightarrow \dim S = \dim A(U) = \dim V - \dim U$

$= n - r$

NOTES

Hence there are $n - r$ linearly independent solutions of the given system of equations.

Corollary: 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).

Example 4.70: Let m and n be positive integers. Let $f_1, ..., f_m$ be linear functionals on $F^{(n)}$. For α in $F^{(n)}$ define $T(\alpha) = (f_1(\alpha), ..., f_m(\alpha))$.

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 $f_1, ..., f_m$.

Solution: Since $f_1, ..., f_m$ are linear transformations, so is T. Let $\{e_1, ..., e_n\}$ be the standard basis of $F^{(n)}$.

Then $T(e_i) \in F^{(m)} \quad \forall\ i = 1, ..., n.$

So, $T(e_i) = (\beta_{i1}, ..., \beta_{im}) \quad \forall\ i = 1, ..., n.$

$\therefore \quad T(\alpha) = T(\alpha_1 e_1 + ... + \alpha_n e_n),\ \alpha = \alpha_1 e_1 + ... + \alpha_n e_n$

$= \alpha_1 T(e_1) + ... + \alpha_n T(e_n)$

$= \alpha_1(\beta_{11}, ..., \beta_{1m}) + ... + \alpha_n(\beta_{n1}, ..., \beta_{nm})$

$= (\alpha_1\beta_{11} + ... + \alpha_n\beta_{n1}, ..., \alpha_1\beta_{1m} + ... + \alpha_n\beta_{nm})$

For each $i (1 \leq i \leq m)$, $\exists$ a linear transformation

$f_i : F^{(n)} \to F$ such that,

$f_i(e_1) = \beta_{1i}, ..., f_i(e_n) = \beta_{ni}$

$\therefore \quad f_1(\alpha) = f_1(\alpha_1 e_1 + ... + \alpha_n e_n)$

$= \alpha_1\beta_{11} + ... + \alpha_n\beta_{n1}$

.....

$f_m(\alpha) = f_m(\alpha_1 e_1 + ... + \alpha_n e_n)$

$= \alpha_1\beta_{1m} + ... + \alpha_n\beta_{nm}$

So, $T(\alpha) = (f_1(\alpha), ..., f_m(\alpha)).$

Example 4.71: Let F be a subfield of complex numbers. We define n linear functionals on $F^{(n)}$ $(n \geq 2)$ by

$$f_k(x_1, ..., x_n) = \sum_{j=1}^{n} (k - j)x_j,\ 1 \leq k \leq m.$$

What is the dimension of the subspace annihilated by $f_1, ..., f_n$?

Solution: Now $f_1(x_1, ..., x_n) = ox_1 - x_2 - 2x_3 ... - (n - 1)\ x_n$

$f_2(x_1, ..., x_n) = x_1 + ox_2 - x_3 ... - (n - 2)\ x_n$

NOTES

$$f_3(x_1, ..., x_n) = 2x_1 + x_2 + ox_3 ... - (n-3)\, x_n$$

.....

$$f_n(x_1, ..., x_n) = (n-1)\, x_1 + (n-2)\, x_2 + (n-3)\, x_3 + ... + 1\, x_{n-1} + ox_n$$

Let W be the subspace of $F^{(n)}$ annihilated by $f_1, ..., f_n$.

Then $(x_1, ..., x_n) \in W$

$$\Rightarrow f_k(x_1, ..., x_n) = 0 \qquad \forall\ k = 1, 2, ..., n.$$

$$\begin{bmatrix} 0 & -1 & -2 & ... & ... & -(n-1) \\ 1 & 0 & -1 & ... & ... & -(n-2) \\ 2 & 1 & 0 & ... & ... & -(n-3) \\ ... & ... & ... & ... & ... & ... \\ n-1 & n-2 & n-3 & ... & ... & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = 0$$

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 $W = n - 2$.

Linear Transformation and Annihilator Subspace

Let V, W be vector spaces over F.

Let T be a linear transformation from V into W.

Define $T^t : \hat{W} \to \hat{V}$ such that,

$T^t(g) = gT$

Then T^t is a linear transformation called the *transpose* of T.

It can be easily shown that

(*i*) $(T_1 + T_2)^t = T_1^t + T_2^t$, where 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 linear transformations.

(*iii*) $(\alpha T)^t = \alpha T^t$, $\alpha \in F$, $T : V \to W$ is a linear trasnsformation

(*iv*) $I^t = I$, $I : V \to V$ is the identity map.

Theorem 4.55: 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

$\Leftrightarrow T^t(g) = 0$

$\Leftrightarrow gT = 0 \Leftrightarrow gTV = 0 \Leftrightarrow g(\text{Range } T) = 0$

$\Leftrightarrow g \in A(R_T)$

NOTES

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

$\Rightarrow f = T^t g, \quad g \in W$

$= gT$

$\Rightarrow f(n) = gT(n) = g(0) = 0 \quad \forall \ n \in N$

$\Rightarrow f \in A(N)$

$\Rightarrow$ 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, $A(N) =$ Range T^t

This proves (ii).

Lemma: Let $T : V \to W$ be a linear transformation. Let $\beta = \{v_1, ..., v_n\}$, $\beta' = \{w_1, ..., w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, ..., f_n\}$ 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 $$f = \sum_1^n c_i\, f_i, \ c_i \in F$$

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 4.56: *Let* $T : V \to W$ be a linear transformation. Let $\beta = \{v_1, ..., v_n\}$, $\beta' = \{w_1, ..., w_m\}$ be ordered basis of V, W respectively. Let $\hat{\beta} = \{f_1, ..., f_n\}$, $\hat{\beta}' = \{g_1, .., g_m\}$ be the dual basis of V, W respectively.

NOTES

Let $A = (a_{ij})$ be the matrix of T with respect to β, β' and $B = (b_{ij})$ be the matrix of T^t with respect to $\hat{\beta}'$ $\hat{\beta}$.

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 $T^t : \hat{W} \to \hat{V}$ such that,

$$T^t(g_j) = g_j T = f \text{ (say)}$$

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,

$$f = \sum_1^n f(v_j) f_i = \sum_1^n a_{ji} f_i$$

But
$$f = T^t g_j = \sum_1^n b_{ij} f_i$$

So,
$$\sum_1^n b_{ij} f_i = \sum_1^n a_{ji} f_i$$

$\Rightarrow$
$$\sum_1^n \left(b_{ij} - a_{ji} \right) f_i = 0$$

$\Rightarrow$ $b_{ij} = a_{ji} \ \forall \ i, j$. 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 $(a_{11}, ..., a_{1n}), ..., (a_{m1}, ..., a_{mn})$.

Similarly, *column rank* of A is defined as the dimension of the subspace of $F^{(m)}$ spanned by $(a_{11}, a_{21}, ..., a_{m1}), ..., (a_{1n}, ..., a_{mn})$.

Theorem 4.57: Let A be an $m \times n$ matrix over F. Then
Row rank of A = column rank of A.

Proof: Define $T : F^{(n)} \to F^{(m)}$ such that,

$$T((x_1, ..., x_n)) = (y_1, ..., y_m)$$

where
$$y_i = \sum_{j=1}^n a_{ij} x_j$$

Then T is a linear transformation.

Range $T = \{T(x_1, ..., x_n) \mid x_i \in F\}$
$= \{T(x_1\ (1, ..., 0) + ... + x_n(0, -0, 1)) \mid x_i \in F\}$
$= \{x_1 T(e_1) + ... + x_n\ T(e_n) \mid x_i \in F\}$

$e_i = n$th-tuple with ith co-ordinate 1 and zero elesewhere
$= \{$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

= Row rank of A (as Rank T^t = Rank T)

= Rank T.

Example 4.72: 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 such that, $T^t f = cf$.

Solution: Now $(T - cI)v = 0,\ v \neq 0$

$\Rightarrow v \in \text{Ker}\ (T - cI)$

$\Rightarrow \quad \text{Ker}\ (T - cI) \neq \{0\}$

$\Rightarrow \quad \dim \text{Ker}\ (T - cI) \geq 1$

$\Rightarrow \quad \text{nullity of}\ (T - cI) \geq 1$

$\Rightarrow \quad \text{rank of}\ (T - cI) < n$

$\Rightarrow \quad \text{rank of}\ (T - cI)^t < n$

$\Rightarrow \quad \text{nulity of}\ (T - cI)^t \geq 1$

$\Rightarrow \exists f \in \hat{V}$ such that $f \neq 0$ and $(T - cI)^t f = 0$

$\Rightarrow \quad T^t f = cf, f \neq 0.$

Example 4.73: Let A be $m \times n$ matrix with real entries. Prove that $A = 0 \Leftrightarrow Trace\ (A^t A) = 0$.

Solution: Let $A^t = B = (b_{ij})_{n \times m}$

$A = (a_{jk})_{m \times n}$

$A^t A = BA = C = (c_{ik}), \quad c_{ik} = \sum_{j=1}^{m} b_{ij}\, a_{jk}$

Trace $(A^t A) = 0$

$\Rightarrow \sum_{1}^{n} c_{ii} = 0$

$\Rightarrow c_{11} + \ldots + c_{nn} = 0$

$\Rightarrow \sum_{1}^{m} b_{ij} a_{ji} + \ldots + \sum_{1}^{m} b_{nj} a_{jn} = 0$

$\Rightarrow \sum (a_{ji})^2 + \ldots + \sum (a_{jn})^2 = 0$

$\Rightarrow a_{ji} = 0 \quad \forall\ i, j$

$\Rightarrow A = 0.$

Converse is obvious.

NOTES

4.11 ALGEBRA OF QUATERNION

In mathematics, a 'Quaternion Algebra' over a field F is a central simple algebra A over F that has dimension 4 over F. Every quaternion algebra becomes a matrix algebra by extending scalars (equivalently, tensoring with a field extension), i.e., for a suitable field extension K of F, $A \otimes_F K$ is isomorphic to the 2×2 matrix algebra over K.

The concept of a quaternion algebra we can said that as a simplification of **Hamilton's quaternions** to an arbitrary base field. The Hamilton quaternions are a quaternion algebra (in the above sense) over $F = \mathbb{R}$ (the real number field), and indeed the only one over $\mathbb{R}$ apart from the 2×2 real matrix algebra, up to isomorphism.

The algebra of Quaternions is a structure first studied by the Irish Mathematician William Rowan Hamilton which extends the two-dimensional complex numbers to four dimensions. Multiplication is non-commutative in quaternions, a feature which enables its representation of three-dimensional rotation. Hamilton's provocative discovery of quaternions founded the field of hypercomplex numbers. Suggestive methods like dot products and cross products implicit in quaternion products enabled algebraic description of geometry now widely applied in science and engineering.

Definition: A **Quaternion** corresponds to an ordered 4-tuple $q = (a,b,c,d)$, where $a,b,c,d \in \mathbb{R}$. A quaternion is denoted $q = a+bi+cj+dk$. The sum $bi+cj+dk$ is called the **vector part** of q, and a is the **real part**. Hamiltion coined the term vector in this context. Subsequent developments have extended the usage of the term vector to any element of a linear space. The vectors in $\mathbb{H}$ form a 3-dimensional subspace V.

The set of all quaternions is denoted by $\mathbb{H}$. It is straightforward to define component-wise addition and scalar multiplication on $\mathbb{H}$, making it a real vector space.

Multiplication follows the rules of the 'Quaternion Group' $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ that Hamilton carved into a stone of Broom Bridge, Dublin:

$$i^2 = j^2 = k^2 = ijk = -1$$

From the above equations alone, it is possible to derive rules for the pairwise multiplication of $\boldsymbol{i}$, $\boldsymbol{j}$, and $\boldsymbol{k}$:

$$\boldsymbol{ij = k,\ jk = i,\ ki = j} \quad \text{(Positive Cyclic Permutations)}$$

$$\boldsymbol{ij = -k,\ jk = -i,\ ki = -j} \quad \text{(Negative Cyclic Permutations).}$$

Using these, it is easy to define a general rule for multiplication of quaternions. Because quaternion multiplication is not commutative, $\mathbb{H}$ is not a field. However, every non-zero quaternion has a multiplicative inverse, so the quaternions are an example of a non-commutative division ring. It is important to note that the non-commutative nature of quaternion multiplication makes it impossible to define the quotient $\boldsymbol{p/q}$ of two quaternions $\boldsymbol{p}$ and $\boldsymbol{q}$ unambiguously, as the quantities $\boldsymbol{pq^{-1}}$ and $\boldsymbol{q^{-1}p}$ are generally different.

Like the more familiar complex numbers, the quaternions have a *conjugation*, often denoted by a superscript star: $\boldsymbol{q}^*$. The conjugate of the quaternion $q = a+bi+cj+dk$ is $\boldsymbol{q}^* = a-bi-cj-dk$. As is the case for the complex numbers, the product $\boldsymbol{qq}^*$ is always a positive real number equal to the sum of the squares of the quaternion's components. The norm of a quaternion is the square root of $\boldsymbol{qq}^*$.

If $\boldsymbol{pq}$ is the product of two quaternions, then $(\boldsymbol{pq})(\boldsymbol{pq})^* = (\boldsymbol{pp}^*)(\boldsymbol{qq}^*)$, implying that $\mathbb{H}$ forms a composition algebra.

The multiplicative inverse of a non-zero quaternion $\boldsymbol{q}$ is given by:

$$q^{-1} = \frac{q^*}{qq^*} \text{ where division is defined since } qq^* \neq 0.$$

Unlike in the complex case, the conjugate $\boldsymbol{q}^*$ of a quaternion $\boldsymbol{q}$ can be written as a polynomial in $\boldsymbol{q}$:

$$q^* = -\frac{1}{2}(q + iqi + jqj + kqk).$$

Structure

Quaternion algebra here means something more general than the algebra of Hamilton's quaternions. When the coefficient field F does not have characteristic 2, every quaternion algebra over F can be described as a 4-dimensional F-vector space with basis $\{1,i,j,k\}$ with the following multiplication rules:

$$i^2 = a$$
$$j^2 = b$$
$$ij = k$$
$$ji = -k$$

Where a and b are any given nonzero elements of F. From these rules we get:

$$k^2 = ijij = -iijj = -ab$$

The classical instances where $F = \mathbb{R}$ are Hamilton's quaternions ($a = b = -1$) and split-quaternions ($a = -1$, $b = +1$). In split-quaternions, $k^2 = +1$ and $jk = -i$, differing from Hamilton's equations.

The algebra defined in this way is denoted $(a,b)_F$ or simply (a,b). When F has characteristic 2, a different explicit description in terms of a basis of 4 elements is also possible, but in any event the definition of a quaternion algebra over F as a 4-dimensional central simple algebra over F applies uniformly in all characteristics.

A quaternion algebra $(a,b)_F$ is either a division algebra or isomorphic to the matrix algebra of 2×2 matrices over F; the latter case is termed split. The norm form is,

$$N(t + xi + yj + zk) = t^2 - ax^2 - by^2 + abz^2$$

Defines a structure of division algebra if and only if the norm is an anisotropic quadratic form, that is, zero only on the zero element. The conic $C(a,b)$ defined by

$$ax^2 + by^2 = z^2$$

has a point (x,y,z) with coordinates in F in the split case.

NOTES

Classification of Quaternion Algebra

It is a theorem of **Frobenius** that there are only two real quaternion algebras: 2×2 matrices over the reals and Hamilton's real quaternions.

In this way, over any local field F there are exactly two quaternion algebras: the 2×2 matrices over F and a division algebra. But the quaternion division algebra over a local field is usually not Hamilton's quaternions over the field. For example, over the p-adic numbers Hamilton's quaternions are a division algebra only when p is 2. For odd prime p, the p-adic Hamilton quaternions are isomorphic to the 2×2 matrices over the p-adics. To see the p-adic Hamilton quaternions are not a division algebra for odd prime p, observe that the congruence $x^2 + y^2 = -1 \bmod p$ is solvable and therefore by **Hensel's lemma** — here is where p being odd is needed — the equation

$$x^2 + y^2 = -1$$

is solvable in the p-adic numbers. Therefore the quaternion

$$xi + yj + k$$

has norm 0 and hence does not have a multiplicative inverse.

One way to classify the ***F*-algebra isomorphism classes** of all quaternion algebras for a given field, F is to use the one-to-one correspondence between isomorphism classes of quaternion algebras over F and isomorphism classes of their norm forms.

To every quaternion algebra A, one can associate a quadratic form N (called the norm form) on A such that

$$N(xy)=N(x)N(y)$$

for all x and y in A. It turns out that the possible norm forms for quaternion F-algebras are exactly the *Pfister 2-forms*.

Applications of Quaternion Algebras

- Quaternion algebras are applied in number theory, particularly to quadratic forms.
- They are concrete structures that generate the elements of order two in the **Brauer group** of F.
- For some fields, including algebraic number fields, every element of order 2 in its Brauer group is represented by a quaternion algebra.
- A theorem of **Alexander Merkurjev** implies that each element of order 2 in the Brauer group of any field is represented by a tensor product of quaternion algebras.
- In particular, over p-adic fields the construction of quaternion algebras can be viewed as the quadratic Hilbert symbol of local class field theory.
- This methods like dot products and cross products implicit in quaternion products enabled algebraic description of geometry now widely applied in science and engineering.

Check Your Progress

13. Define the linear combination.
14. When vector space V is said to be finite dimensional over F?
15. When vector space V is said to be linearly dependence?
16. What is basis of vector?
17. Define the product of two linear transform.
18. What do you understand by quaternion algebra?

4.12 ANSWERS TO 'CHECK YOUR PROGRESS'

1. Let V be a vector space over a field K, and let N be a subspace of V. We define an equivalence relation $\sim$ on V by stating that $x \sim y$ if $x - y \in N$. That is, x is related to y if one can be obtained from the other by adding an element of N. From this definition, one can deduce that any element of N is related to the zero vectors; more precisely, all the vectors in N get mapped into the equivalence class of the zero vector.
2. The elements of the field of fractions of the integral domain R have the form a/b with a and b in R and b 0. The field of fractions of the ring R is denoted by Quot(R) or Frac(R). This is referred as the quotient field, field of fractions or fraction field.
3. A ring R is called a Boolean ring if $x^2 = x$ for all $x \in R$.
4. A commutative division ring is known as a field. For example, set of rational numbers, set of real numbers and set of complex numbers under operation of addition and multiplication are field.
5. Existence of identity: Since $0 +_6 a = a = a +_6 0$ for all $a \in$ R, therefore $0 \in$ R is an additive identity.
6. Closure property: (i) We have $a +_5 b$ is a member of A for all $a, b \in$ A.

   $\therefore$ A is closed under the composition addition modulo 5.

   (ii) We have $a \times_5 b$ is a member of A for all $a, b \in$ A.

   $\therefore$ A is closed under the composition multiplication modulo 5.
7. Since the entries in the corresponding row and columns of both the table are identical, hence the compositions are commutative.
8. A non empty set R, together with two binary compositions + and . 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 $a, b \in R$

   (*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., $a + (-a) = (-a) + a = 0$

NOTES

(*v*) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$

(*vi*) $a \cdot (b + c) = a \cdot b + a \cdot c$

$(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$

NOTES

9. Let S be a non-empty subset of a ring (R, +, .) such that (S, +, .) itself is a ring. Then S is called a subring of R.
10. A subfield of a field *L* is a subset *K* of *L* that is a field with respect to the field operations inherited from L. Equally, a subfield is a subset that contains 1, and is closed under the operations of addition, subtraction, multiplication, and taking the inverse of a non-zero element of *K*.
11. Let $< V, + >$ be an abelian group and $< F, +, \cdot >$ be a field. Define a function $\times$ (called scalar multiplication) from $F \times V \to V$, such that, for all $\alpha \in F$, $v \in V$, $\alpha \cdot v \in V$. 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*) $1 \cdot x = x$, 1 being unity of *F*.

Also then, members of *F* are called scalars and those of *V* are called vectors

12. A vector with zero magnitude and any direction is called a zero vector or a null vector.
13. 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 $v_1, v_2, ..., v_n$ over *F*.
14. 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 are, $V = L(S)$. We use notation FDVS for a Finite Dimensional Vector Space.
15. Let $V(F)$ be a vector space. Elements $v_1, v_2, ..., v_n$ in *V* are said to be linearly dependent (over *F*) if $\exists$ scalars $\alpha_1, \alpha_2, ... \alpha_n \in F$, (not all zero) such that

$\alpha_1 v_1 + \alpha_2 v_2 + ... \alpha_n v_n = 0$

($v_1, v_2, ..., v_n$ are finite in number, not essentially distinct).

16. A FDVS *V* is said to have dimension *n* if *n* is the number of elements in any basis of *V*.
17. Product (composition) of two linear transformations

Let *V*, *W*, *Z* be three vector spaces over a field *F*

Let $T : V \to W$, $S : W \to Z$ be *lin*ear transformation

We define $ST : V \to Z$, such that,

$(ST)v = S(T(v))$

then *ST* is a linear transformation (verify), called product of *S* and *T*.

18. A 'Quaternion Algebra' over a field F is a central simple algebra A over F that has dimension 4 over F. Every quaternion algebra becomes a matrix algebra by extending scalars (equivalently, tensoring with a field extension), i.e., for a suitable field extension K of F, is isomorphic to the 2×2 matrix algebra over K.

NOTES

4.13 SUMMARY

- In abstract algebra, the field of fractions or field of quotients of an integral domain is the smallest field in which the integral domain can be embedded.
- The field of fractions of R is characterized by the universal property that if $f : R \to F$ is an injective ring homomorphism from R into a field F then there exists a unique ring homomorphism g : Quot(R) $\to F$ which extends f.
- If for some $a \in K$, a is not algebraic over F, then K is called transcendental extension of F.
- 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.
- A ring R is called a Boolean ring if $x^2 = x$ for all $x \in R$.
- Every non-zero elements of set of integers Z has no multiplicative inverse in Z. So set of integers is not a field.
- Existence of multiplicative inverse, i.e., for every non-zero $a \in$ F, there exists $\frac{1}{a} \in$ F such that, $a.\frac{1}{a} = \frac{1}{a}.a = 1$.
- Since all the entries in the composition table of addition are element of R, hence R is closed under addition modulo 6.
- We can easily observe from the table that the inverses of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively. Thus, the additive inverse exists.
- Since the entries in the corresponding row and columns of both the table are identical, hence the compositions are commutative.
- Since we say that + and . 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.
- 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.
- By Cauchy's theorem in groups, we know if p is any prime dividing $o(R)$ then $\exists\, x \in R$, s.t., $o(x) = p$. But order of each non zero element is 2 and thus 2 is the only prime dividing $o(R)$. Hence $o(R) = 2^n$.
- 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.

NOTES

- A non empty subset 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.
- 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.
- The characteristic of a ring with identity (unity) is zero or greater than zero according as the identity element of the ring regarded as a member of the additive group of the ring has the order zero or greater than zero.
- The order of each element of an integral domain (regarding elements as the members of additive group) is same.
- The characteristic of an integral domain R is 0 or $n > 0$ according as the order of any non-zero element regarding as a member of additive group of R is 0 or n.
- The ring of integers is a subring of the ring of rational numbers and ring of rational numbers is subring of ring of real numbers.
- Every ring R has $\{0\}$ and R as two subrings which are called improper subrings of R and all other subrings, if any is called proper subrings of R.
- The associativity and commutativity must hold in S as they hold in R because S is a subset of R. Also the distributive laws must hold in S as they hold in R. Thus, S is a subring of R.
- 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.
- The modulus or magnitude of a vector is the positive number measuring the length of the line representing it. It is also called the vector's absolute value. Modulus of a vector **a** is denoted by $|\ \mathbf{a}\ |$ or by the corresponding letter a in italics.
- 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 are, $V = L(S)$. We use notation FDVS for a Finite Dimensional Vector Space.
- Empty set φ is LI 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 LI We sometimes express it by saying that empty set is LI vacuously.
- $T : V \to W$, such that, $T(\alpha x + \beta y) = \alpha T(x) + \beta T(y)$ where $x, y \in V$, $\alpha, \beta \in F$ and V, W are vector spaces over the field F.
- A linear transformation $T : V \to V$ is called a linear operator on V, whereas a linear transformation $T : V \to F$ is called a linear functional. We use notation T^2 for $T.T$ and $T^n = T^{n-1}T$, etc.

- The algebra of Quaternions is a structure first studied by the Irish Mathematician William Rowan Hamilton which extends the two-dimensional complex numbers to four dimensions. Multiplication is non-commutative in quaternions, a feature which enables its representation of three-dimensional rotation.
- For some fields, including algebraic number fields, every element of order 2 in its Brauer group is represented by a quaternion algebra.

4.14 KEY TERMS

- **Quotient space:** In linear algebra, the quotient of a vector space V by a subspace N is a vector space obtained by 'Collapsing' N to zero. The space obtained is called a quotient space and is denoted V/N.
- **Fields:** A commutative division ring is known as a field. For example, Set of rational numbers, set of real numbers and set of complex numbers under operation of addition and multiplication are field.
- **Modulo:** The modulo operation finds the remainder after division of one number by another.
- **Subrings:** Let S be a non-empty subset of a ring (R, +, .), such that (S, +,.) itself is a ring. Then S is called a subring of R.
- **Vector spaces:** A vector space (also called a linear space) is a set of objects called vectors, which may be added together and multiplied 'Scaled' by numbers, called scalars.
- **Linear independence:** A set of vectors is said to be linearly dependent if at least one of the vectors in the set can be defined as a linear combination of the others; if no vector in the set can be written in this way, then the vectors are said to be linearly independent.
- **Basis of dimension:** A FDVS 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.
- **Quaternion algebra:** The concept of a quaternion algebra we can said that as a simplification of Hamilton's quaternions to an arbitrary base field.

4.15 SELF-ASSESSMENT QUESTIONS AND EXERCISES

Short-Answer Questions

1. What is quotient space?
2. Define the field.
3. State the commutative law.
4. Define the ring.

NOTES

5. Show that in a ring R, $a.0 = 0.a$ for all $a \in R$.
6. What is subring?
7. Generalise the vector space.
8. What is unit vector?
9. State the parallelogram law.
10. What do you understand by vector product?
11. How will you define the linear combination?
12. When is finite set $X = \{x_1, x_2, \ldots, x_n\}$ said to be LD?
13. Define the term basis of vector.
14. State the Sylvester's law.
15. What do you understand by algebra of linear transform?
16. What is linear algebra?
17. When W is a subspace of V?
18. Give the definition of quaternion algebra.

Long-Answer Questions

1. Elaborate on the quotient space with relevant examples.
2. Describe the fields with the help of theorems and examples.
3. Discuss about the rings and prove that a commutative ring R is an integral domain iff for all $a, b, c \in R$ $(a \neq 0)$ $ab = ac \Rightarrow b = c$.
4. Analyse the characteristics of a ring. Support your answer giving an example.
5. Discuss the subrings and subfield giving appropriate examples.
6. Explain in detail about the vector spaces with the help of examples and properties.
7. State and prove the theorems of linear combinations.
8. Explain linear dependence and linear independence.
9. Interpret the basis of vector space.
10. Analyse the algebra of linear transform giving examples.
11. Elaborate on the algebra of quaternion.

4.16 FURTHER READING

Hazarika, Padmalochan. 2003. *A Class Textbook of Business Mathematics*. New Delhi: S. Chand & Company Ltd.

Tremblay, Jean Paul and R. Manohar. 2004. *Discrete Mathematical Structures With Applications To Computer Science*. New York: McGraw-Hill Higher Education.

Ramaswamy, V. 2006. *Discrete Mathematical Structures with Applications to Combinatorics*. Hyderabad: Universities Press.

Kolman, Bernand, Roberty C. Busby and Sharn Cutter Ross. 2006. *Discrete Mathematical Structures*. London (UK): Pearson Education.

Liu, C. L. 1985. *Elements of Discrete Mathematics*, 2nd Edition. New York: McGraw-Hill Higher Education.

Arumugam, S. and Thangapandi Isaac. 2008. *Modern Algebra*. Chennai: Scitech Publications (India) Pvt. Ltd.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. New Delhi: Cambridge University Press.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

NOTES

UNIT 5 POSET, LATTICE AND BOOLEAN ALGEBRA

NOTES

Structure

5.0 INTRODUCTION

A partially ordered set (or poset) is a set taken together with a partial order on it. Properly, a partially ordered set is defined as an ordered pair, where is called the ground set of and is the partial order of. A totally ordered set is said to be complete if every non-empty subset that has an upper bound, has a least upper bound. A Hasse diagram is a graphical representation of the relation of elements of a partially ordered set (poset) with an implied upward orientation.

A lattice is a poset, a partially ordered set, in which every pair of elements has both a least upper bound and a greatest lower bound. In mathematics, a join-semi lattice (or upper semi lattice) is a partially ordered set that has a join (a least upper bound) for any non-empty finite subset. However complete lattice is a partially ordered set in which all subsets have both a supremum (join) and an infimum (meet). A sublattice is a subalgebra of the lattice considered as a universal algebra with two binary operations. A lattice L is said to be complemented if it is bounded and if every element in L has a complement.

It deals with variables that can have two discrete values, 0 (False) and 1 (True); and operations that have logical significance. The earliest method of manipulating symbolic logic was invented by George Boole and subsequently came to be known as Boolean algebra. A Boolean algebra is often represented by a tuple $(S, + \cdots 0,1)$, and a combination of some elements of S via the connectives + and and the complement is a Boolean expression. Switching system $(S, + \cdots 0,1)$ with $S = \{0,1\}$ is a Boolean algebra.

NOTES

In this unit, you will study about the partially ordered set and poset, partial ordering relation, Hasse diagrams, lattices and their types, Boolean algebra, Boolean functions, algebra of switching circuit.

5.1 OBJECTIVES

After going through this unit, you will be able to:

- Explain the partially ordered set and poset
- Describe the partial ordering relation
- Illustrate the Hasse diagrams
- Explain the different types of lattices
- Elaborate on the Boolean algebra and Boolean functions
- Analyse the algebra of switching circuit

5.2 PARTIAL ORDERING SET AND POSET

Definition: A partial order defines a notion of comparison. Two elements x and y may stand in any of four mutually exclusive relationships to each other: either $x < y$, or $x = y$, or $x > y$, or x and y are incomparable. A set with a partial order is called a partially ordered set (also called a poset). The term ordered set is sometimes also used, as long as it is clear from the context that no other kind of order is meant. In particular, totally ordered sets can also be referred to as 'Ordered Sets', especially in areas where these structures are more common than posets.

In mathematics and specifically in order theory, a partially ordered set or poset validates and generalizes the natural concept of an ordering, sequencing or arrangement of the elements of a set. Typically, a poset consists of a set together with a binary relation that specifies that for certain pairs of elements in the set one of the elements precedes the other. Such a relation is termed as partial order which states that every pair of elements may not be related. Though for some pairs, no element precedes the other in the poset. Thus, partial orders generalize the more familiar total orders, in which every pair is related. A finite poset can be visualized through its **Hasse diagram**, which depicts the ordering relation.

A relation R on a set A is said to be a partial order relation if R is reflexive, antisymmetric and transitive.

For example, Let S be non-empty. Define R as $\subseteq$ (contained in or equal to) $P(S)$. Clearly $(P(S), \subseteq$,is a partial order set. If

(*i*) $A \in P(S), A \subseteq A$

(*ii*) $A, B \in P(S), A \subseteq B$ and $B \subseteq A \Rightarrow A = B$

(*iii*) $A, B, C, \in P(S)$,

Whenever $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$. $\therefore \subseteq$ is a partial order relation on $P(S)$.

Let $\leq$ be a partial order on the set of integers and *a, b, c* be integers. Clearly,

(*i*) $a \leq a$; where $a \in Z$

(*ii*) If $a \leq b$ and $b \leq a$ then $a = b$,where $a, b \in Z$.

(*iii*) If $a \leq b$ and $b \leq c$ then $a \leq c$, where $a, b, c \in Z$.

$\therefore$ $(Z, \leq)$ is a partial order set (poset).

Comparable Integers: Two elements of a poset $(S, \leq)$ are said to be comparable if $a \leq b$ or $b \leq a$. Otherwise a and b are said to be incomparable.

For example, In the poset $(Z^+,1)$, the integers 2 and 8 are comparable whereas 3 and 5 are incomparable.

[a / b is read as a divides b and $a / b \Rightarrow b = k\,a$ for some $k \in Z$]

Chain: A poset (S, $\leq$) is called a chain if $\leq$ is total order relation. If every two elements of S are comparable then S is called a totally released set.

For example, The poset $(Z, \leq)$ is a chain, whereas the poset $(Z^+, 1)$ is not a chain.

5.2.1 Partial Ordering Relation

A binary relation R in a set P is called a partial order relation or a partial ordering in P if and only if R is reflexive, antisymmetric and transitive. It is denoted by the symbol $\leq$. If $\leq$ is a partial ordering on P, then the ordered pair $(P, \leq)$ is called a partially ordered set or a poset. If for any $x,y \in p$, if $x \leq y$ or $y \leq x$, then $(p, \leq)$ called a 'Totally Ordered Set'.

Example 5.1: Let R be the set of real numbers. The relation "less than or equal to" or "greater than or equal to" is a partial order on R.

Note: The symbol $\leq$ should not be confused with the standard "less than or equal to" relation on real numbers.

Example 5.2: Prove that "being a subset of is a partial order on the power set of a non-empty set of A".

Solution: Let $P(A) = 2^A = X$ be the power set of A, i.e., X is the set of all subsets of A. For any u,v,w in x, set $U \leq V \Leftrightarrow U \subseteq V$.

(*i*) **Reflexive:** Since $U \subseteq U$, $U \leq U$.

(*ii*) **Antisymmetric:** Suppose $U \leq V$ and $V \leq U$. Then $U \subseteq V$ and $V \subseteq U$. This implies that $U = V$.

(*iii*) **Transistive:** Suppose $U \leq V$ and $V \leq W$. Then $U \subseteq V$ and $V \subseteq W$. This implies that $U \leq W$.

Hence $U \leq W$.

Thus $(x, \leq)$ is a partial order.

Definition: A total order (or 'Totally Ordered Set', or 'Linearly Ordered Set') is a set plus a relation on the set (called a total order) that satisfies the conditions for a partial order plus an additional condition known as the comparability condition.

A relation <= is a total order on a set S ('<= totally orders S') if the following properties hold.

1. Reflexivity: a<=a for all a in S.

2. Antisymmetry: a<=b and b<=a implies a=b.

3. Transitivity: a<=b and b<=c implies a<=c.

4. Comparability (trichotomy law): For any a,b in S, either a<=b or b<=a.

NOTES

The first three are the axioms of a partial order, while addition of the **trichotomy law** defines a total order. Every finite totally ordered set is well ordered. Any two totally ordered sets with k elements (for k a non-negative integer) are order isomorphic, and therefore have the same order type (which is also an ordinal number).

Example 5.3: Let X be the set of positive integers. Prove that the relation 'Divides' and "intergral multiples of" are partial orderings on X.

Solution: If a and b are positive integers, then we say, 'a divides b' written a/b if and only if there is an integer c such that $ac = b$ (or b is an integral multiple of a). For any $a,b \in x$, set $a \leq b \Leftrightarrow a/b$ (=) $ac = b$.

(*i*) **Reflexive:** Since $a.1 = a$, a/a and hence $a \leq a$.

(*ii*) **Antisymmetric:** Suppose $a \leq b$ and $b \leq a$. Then there exist $c,d \in x$ such that $ac = b$ and $bd = a$. Since $a = bd = acd \Rightarrow cd = 1$, $c = 1$ and $d = 1$. Therefore $a = b$.

(*iii*) **Transitive:** Suppose for any $a,b,c \in x$, $a \leq b$ and $b \leq c$. Then there exist x, $y \in x$ such that $ax = b$ and $by = c$. Now $a\,xy = by = c$.

and since $xy \in X$, a/c. Therefore $a \leq c$. Thus $(X, \leq)$ is a partial order.

Example 5.4: Consider the set Z of integers. Define $a \leq b$ if there is a positive integer r such that $b = a^r$. Prove $(z, \leq)$ is a partial ordered set.

Solution: Let $a,b,c \in Z$.

(*i*) **Reflexive:** Since $a = a^1$, $a \leq a$.

(*ii*) **Antisymmetric:** Suppose $a \leq b$ and $b \leq a$. Then there exist positive integers r, s such that $b = a^r$ and $a = b^s$. Since $a = b^s = (a^r)^s = a^{rs}$ implies $rs = 1$. But $rs \in z \Rightarrow r = 1$ and $s = 1$. Hence, $a = b$.

(*iii*) **Transitive:** Suppose $a \leq b$ and $b \leq c$. Then there exist positive integers r,s such that $b = a^r$ and $c = b^s$. Now $c = b^s = (a^r)^s = a^{rs}$ and $rs \in Z$ implies that $a \leq c$. Thus $(Z, \leq)$ is a partially ordered set.

Example 5.5: If R is a partially ordered relation on a set x and $A \leq x$, show that $R \cap (A \times A)$ is a partial ordering relation on A.

Solution: Denote $R \cap (A \times A)$ by R^1.

(*i*) **Reflexive:** Let $x \in A$. Then $(x, x) \in A \times A$.

Since R is reflexive, $(x, x) \in R$. (Note that $x, x) \in R$ means xRx. Therefore $(x, x) \in R \cap (A \times A) = R^1$.

(*ii*) **Antisymmetric:** Suppose $(x, y) \in R^1$ and $(y, x) \in R^1$. This implies that $(x, y) \in R \cap (A \times A)$ and $(y, x) \in R \cap (A \times A)$. Since R is antisymmetric, $(x, y) \in R$ and $(y, x) \in R \Rightarrow x = y$.

(*iii*) **Transitive:** Suppose $(x, y) \in R^1 = R \cap (A \times A)$ and

$(y, z) \in R^1 = R \cap (A \times A)$. Such R is transitive.

$(x, y) \in R$ and $(y,z) \in R \Rightarrow (x, z) \in R$ clearly.

$(x, z) \in A \times A$ and hence $(x, z) \in R \cap (A \times A) = R^1$.
Thus $R^1 = R \cap (A \times A)$ is a partial ordering relation on A.

NOTES

5.2.2 Hasse Diagram of Partially Ordered Sets

The Hasse diagram of a poset P is a picture of P. So it is very useful in describing types of elements of P. Some times we define a partially ordered set by simply presenting its Hasse diagram.

Define a relation < on P by x < y (=) $x \leq y$ but $x \neq y$. Let $(p, \leq)$ be a partially ordered set. An element $y \in p$ is said to cover an element $x \in p$ if $x < y$ and if there does not exist an element $z \in p$ such that $x \leq z$ and $z \leq y$; that is

$$y \text{ cover } x \Leftrightarrow (x < y \text{ and } x \leq z \leq y \Rightarrow x = z \text{ or } z = y)$$

Here we say that y is an immediate predecessor of x or x is an immediate successor of y.

A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $(p, \leq)$.

Procedure

1. Represent each element of p by a small circle or a dot.
2. The circle for $x \in p$ is drawn below the circle for $y \in p$ if $x < y$, and a line is drawn between x and y if y covers x.
3. If $x < y$ but y does not cover x, then x and y are not connected directly by a single line. However, they are connected through one or more elements of p.

Notes:

1. The Hasse diagram of a part p need not be connected. Also, there can be no directed cycles in the diagram of p since the partial order relation is antisymmetric.
2. For a totally ordered set $(p, \leq)$, the Hasse diagram consists of circles one below the other.
3. It is possible to obtain the set of ordered pairs in $\leq$ from such a Hasse diagram.

Example 5.6: Let $p = \{\phi, (a), (a,b), (a,b,c)\}$ and the relation $\leq$ be such that $A \leq B$ if $A \subseteq B$, the inclusion relation on p. Draw Hasse diagram of $(p, \leq)$.

Solution: The Hasse diagram is drawn as follows:

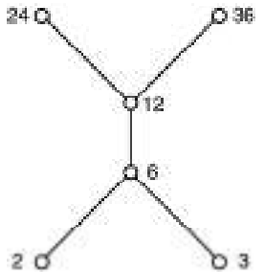
Example 5.7: Let $x = \{2,3,6,12,24,36\}$ and the relation $\leq$ be such that $x \leq y$ if x divides y. Draw the Hasse diagram of $(x, \leq)$.

Solution: Here,

$\leq$ = {(2,2), (2,6), (2,12), (2,24), (2,36), (3,3), (3,6),
(3,12), (3,24), (3,36), (6,6), (6,12), (6,24),
(6,36), (12,12), (12,24), (12,36), (24,24), (36,36)}

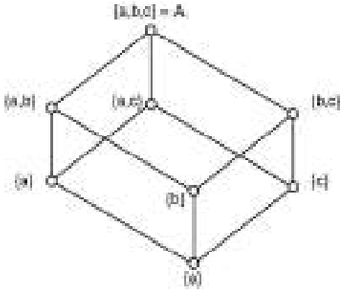
NOTES

So the corresponding Hasse diagram is as follows:

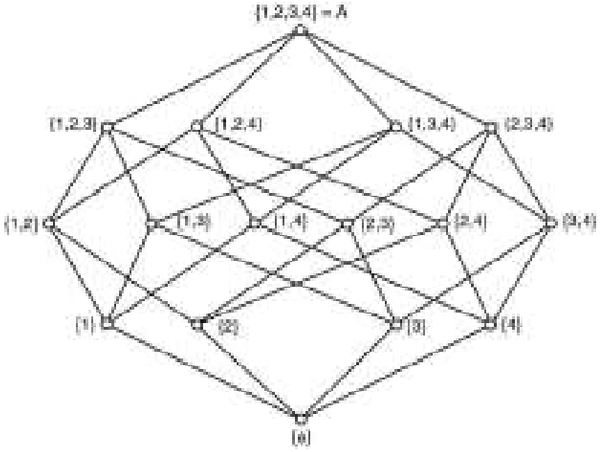


Example 5.8: Let $A = \{a,b,c\}$ and $p(A)$ be its power set. Let $\subseteq$ be the inclusion relation on $p(A)$. Draw Hasse diagram.

Solution: Here $p(A) = \{\phi,(a), (b), (c), (a,b), (a,c), (b,c), (a,b,c)\}$ and the corresponding Hasse diagram is:



Example 5.9: Let $A = \{1,2,3,4\}$ and $p(A)$ be its power set. Let $\subseteq$ be the inclusion relation on $p(A)$. Draw the Hasse diagram.



Solution: Let $(p, \leq)$ be a poset and let $A \subseteq P$. An element $x \in p$ is an *upper bound* for A if for all $a \in A$, $a \leq x$. Similarly, any element $x \in p$ is a lower bound for A if for all $a \in A$, $x \leq a$.

In other words, $x \in p$ is an upper bound of a and b if $a \leq x$ and $b \leq x$. Similarly, $x \in p$ is called a lower bound of a and b if $x \leq a$ and $x \leq b$.

LUB and GLB

An element $x \in p$ is a Least Upper Bound (LUB) for A, if x is an upper bound for A and $x \leq y$, where y is any upperbound for A. In otherwords $x \in p$ is LUB of a and b if $a \leq x$ and $b \leq x$ and if for $y \in p$, $a \leq y$, $b \leq y \Rightarrow x \leq y$.

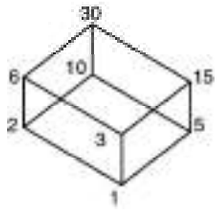
Similarly the Greatest Lower Bound (GLB) for A is an element $x \in p$ such that x is a lower bound and $y \leq x$ for all lower bounds for y. In otherwords $x \in p$ is GLB of a,b if $x \leq a, x \leq b$ and if $y \in p, y \leq a, y \leq b \Rightarrow y \leq x$.

Note: Some authors use the term supremum instead of LUB and infimum instead of GLB.

Example 5.10: Let $p = \{1, 2, 3,5,6,10,15,30\}$ and let $\leq$ be the relation "divides" on p. Then show that $(p, \leq)$ is a poset. Given the set of upper bounds of 2 and 3 is $\{x \in p : 2 \leq x,\ 3 \leq x\} = \{x \in p : 2/x, 3/x\} = \{6,30\}$. Draw the Hasse diagram.

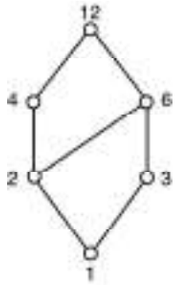
Solution: The least element of this set is 6. So LUB of 2 and 3 = 6. The set of lower bounds of 6 and 15 is $\{1, 3\}$. The greatest element of this set is 3. Hence, GLB of 6 and 15 = 3.

The Hasse diagram for this example is as follows:



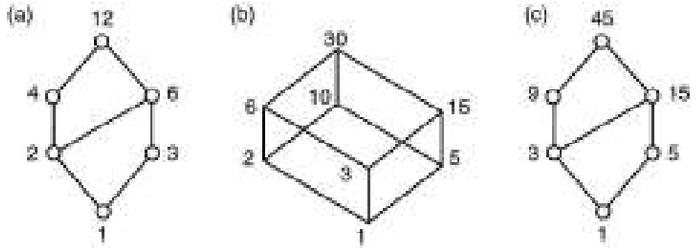
Example 5.11: Draw the Hasse diagram for $(N, \leq)$ where $A = \{1,2,3,4,12\}$ and $x \leq y$ if and only if x/y.

Solution: The Hasse diagram is drawn as follows:



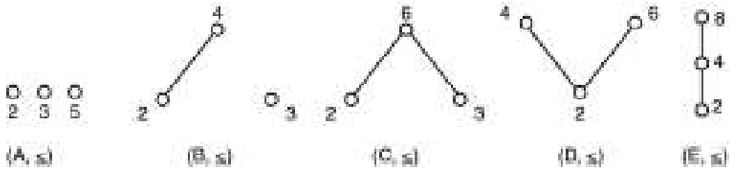
Example 5.12: Let A be the set of factors of a particular positive integer m and e, $\leq$ be the relation "divides", i.e., $\leq = \{(x, y) | x \in A$ and $y \in A$ and (x divides y)$\}$. Draw Hasse diagrams for (a) $m = 12$, (b) $m = 30$, (c) $m = 45$.

Solution: The Hasse diagram is drawn as follows:



Example 5.13: Show that there are only five distinct Hasse diagrams for partially ordered sets that contain three elements.

Solution: Let us assume that $a \leq b$ if a/b and consider the sets $A = \{2,3,5\}$, $B = \{2,3,4\}$, $C = \{2,3,6\}$, $D = \{2,4,6\}$, and $E = \{2,4,8\}$. Then its Hasse diagrams are as follows:



These are the only distinct Hasse diagrams for poset that contain three elements.

Greatest and Smallest Elements: An element $x \in p$ is called the greater element if for all $a \in p, a \leq x$. An element $x \in p$ is called the smallest element or least element if for all $a \in p, x \leq a$. The greatest element will be denoted by 1 and the smallest element by 0.

Theorem 5.1: If a poset $(p, \leq)$ has a least element, then this element is unique. Similarly, if a poset $(p, \leq)$ has the greatest element, then it is unique.

Proof: Suppose x_1 and x_2 are any two least elements. Since x_1 is a least element, $x_1 \leq x_2$ and x_2 is a least element, $x_2 \leq x_1$. However $\leq$ is antisymmetric we get $x_1 = x_2$. Thus, the least element, if it exists, is unique. Dually, the other result follows.

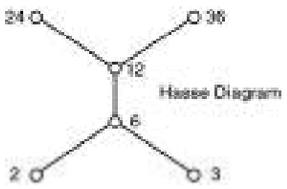
Example 5.14: Draw the Hasse diagram for $(X, \leq)$ where $X = \{2,3,6,12,24,36\}$ and $x \leq y$ if x/y. Find the following:

(*i*) The LUB and the GLB of $A = \{2,3,6\}$

(*ii*) The LUB and the GLB of $B = \{2,3\}$

(*iii*) The LUB and the GLB of $C = \{6,12\}$

Solution: The Hasse diagram is drawn as follows:



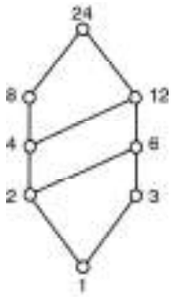
(*i*) LUB of $A = 6$; GLB of A does not exist

(*ii*) LUB of $B = 6$; but there is no GLB

(*iii*) LUB of $C = 12$; GLB of $C = 6$

NOTES

Example 5.15: From the Hasse diagram:



(*i*) Find all lower bounds 8 and 12

(*ii*) Find all upper bounds 8 and 12

(*iii*) Find the GLB of 8 and 12

(*iv*) Find the LUB of 8 and 12

Solution: The following are the upper and lower bounds:

(*i*) Lower bounds of 8 and 12 are 1,2,4.

(*ii*) Upper bound of 8 and 12 is 24.

(*iii*) GLB of 8 and 12 is 4.

(*iv*) LUB of 8 and 12 is 24.

5.3 HASSE DIAGRAMS

A **Hasse diagram** is a graphical representation of the relation of elements of a partially ordered set (poset) with an implied upward orientation. A point is drawn for each element of the partially ordered set (poset) and joined with the line segment according to the following rules:

- If $p < q$ in the poset, then the point corresponding to p appears lower in the drawing than the point corresponding to q.
- The two points p and q will be joined by line segment iff p is related to q.

To draw a Hasse diagram, provided set must be a poset. A poset or partially ordered set A is a pair, $(B, \leq)$ of a set B whose elements are called the vertices of A and obeys following rules:

Reflexivity $\rightarrow p \leq p \ \forall \ p \in B$

Anti-symmetric $\rightarrow p \leq q$ and $q \leq p$ iff $p = q$

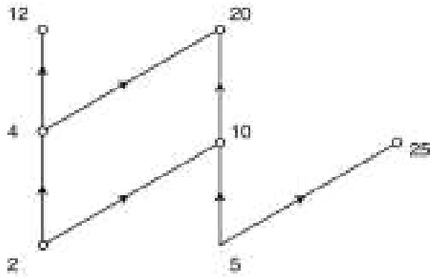
Transitivity $\rightarrow$ if $p \leq q$ and $q \leq r$ then $p \leq r$

We can represent the poset as a directed graph. Every poset consisting of a set and a relation can be represented as a graph. We have to do minor modification in this relational graph. Since partial ordering relation is reflexive and transitive the relational graph will consist of self loops and edges corresponding to the transitive relations.

NOTES

In the relational graph, the self loops and edges corresponding to the pairs (a, c) are removed whenever (a, b) and (b, c) are present. Finally, each edge is arranged so that its initial vertex is below its terminal vertex. All the arrows on the directed edges, are removed since all the edges point upward towards their terminal vertex.

Example 5.16: Draw the Hasse diagram representing the partial ordering $\{(a, b) / a /b\}$ on $\{2, 4, 5, 10, 12, 20, 25\}$.



Solution: Here the relation set = {(2, 4), (2, 12), (4, 12), (5, 10), (5, 20), (5, 25), (10, 20)}

Maximal and Minimal Elements: An element a of a poset $(S, \leq)$ is called maximal element if there is no $b \in S$ such that $a < b$. Similarly an element a of a poset $(S, \leq)$ is called minimal if there is no $b \in S$ such that $b < a$.

Note: In the Hasse diagram, it is easy to spot the maximal and minimal element, because they are the 'top' and 'bottom' elements in that diagram.

Upper and Lower Bound: An element υ of a poset $(s, \leq)$ is called an upper bound of S if $a \leq \upsilon \ \forall \ a \in S$. Similarly an element l of a poset $(S, \leq)$ is called an lower bound of S if $l \leq a \ \forall \ a \in S$.

The element x is called the least upper bound of the set S if (i) x is an upper bound of S and (ii) x $\leq$ z whenever z is an upper bound of S. Similarly, the element y is called the greatest lower bound of S if

(i) y is a lower bound of S and

(ii) $z \leq y$, whenever z is a lower bound of S.

Example 5.17: Find the greatest lower bound and the least upper bound of the sets $\{3, 9, 12\}$ and $\{1, 2, 4, 5, 10\}$ if they exist in the poset $(z_+, 1)$.

Solution: An integer is a lower bound of $\{3, 9, 12\}$ if 3, 9 and 12 are divisible by this integer. Such integers are 1 and 3 only. Clearly 3 is the greatest lower bound of $\{3, 9, 12\}$.

Similarly the greatest lower bound for $\{1, 2, 4, 5, 10\}$ is 1.

An integer is an upper bound for $\{3, 9, 12\}$ if it is divisible by 3, 9 and 12.

The integers with this properly are those divisible by the lcm of 3, 9 and12, which is 36. Hence 36 is the least upper bound for the set $\{3, 9, 12\}$.

Similarly 20 is the least upper bound for the set $\{1, 2, 4, 5, 10\}$.

Lattice: A poset in which every pair of elements has both a least upper bound and a greatest lower bound is called a lattice.

Example:

(*i*) The poset ($\{1, 2, 4, 8\}$,1) is a lattice.

(*ii*) The poset ($P(S), \subseteq$) is a lattice.

Here $A \cup B$ = Least upper bound of A and B and $A \cap B$ = Greatest lower bound of A and B, for any $A \subseteq S, B \subseteq S$.

NOTES

5.3.1 Duality

In the mathematical field of order theory, every partially ordered set P gives rise to a dual (or opposite) partially ordered set which is often denoted by P^{op} or P^{d}. This dual order P^{op} is defined to be the same set, but with the **inverse order**, i.e. , $x \leq y$ holds in P^{op} if and only if $y \leq x$ holds in P. It is easy to state that this construction, which can be depicted by flipping the **Hasse diagram** for P upside down, will indeed yield a partially ordered set. In a broader sense, two partially ordered sets are also said to be duals if they are dually isomorphic, i.e. , if one poset is *order isomorphic* to the dual of the other. The importance of this simple definition stems from the fact that every definition and theorem of order theory can readily be transferred to the dual order. Formally, this is captured by the Duality Principle for ordered sets:

- If a given statement is valid for all partially ordered sets, then its dual statement, obtained by inverting the direction of all order relations and by dualizing all order theoretic definitions involved, is also valid for all partially ordered sets.
- If a statement or definition is equivalent to its dual then it is said to be self-dual. Note that the consideration of dual orders is so fundamental that it often occurs implicitly when writing ≥ for the dual order of ≤ without giving any prior definition of this 'New' symbol.

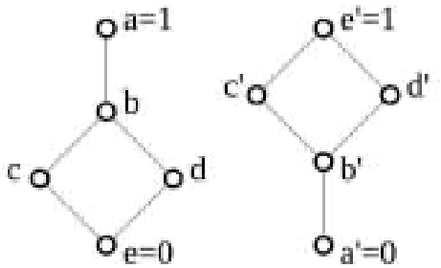


Fig. 5.1 *Bounded Distributive Lattice, and it's Dual*

Naturally, there are a great number of examples for concepts that are dual:

- Greatest elements and least elements
- Maximal elements and minimal elements
- Least upper bounds (suprema, $\vee$) and greatest lower bounds (infima, $\wedge$)
- Upper sets and lower sets
- Ideals and filters
- Closure operators and kernel operators.

NOTES

Examples of notions which are self-dual include:

- Being a (complete) lattice
- Monotonicity of functions
- Distributivity of lattices, i.e., the lattices for which $\forall\, x,y,z: x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ holds are exactly those for which the dual statement $\forall\, x,y,z: x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ holds
- Being a Boolean algebra
- Being an order isomorphism.

Since partial orders are antisymmetric, the only ones that are self-dual are the equivalence relations.

Product of Poset

In order of increasing strength, i.e., decreasing sets of pairs, three of the possible partial orders on the Cartesian product of two partially ordered sets are (Refer Figure 5.2):

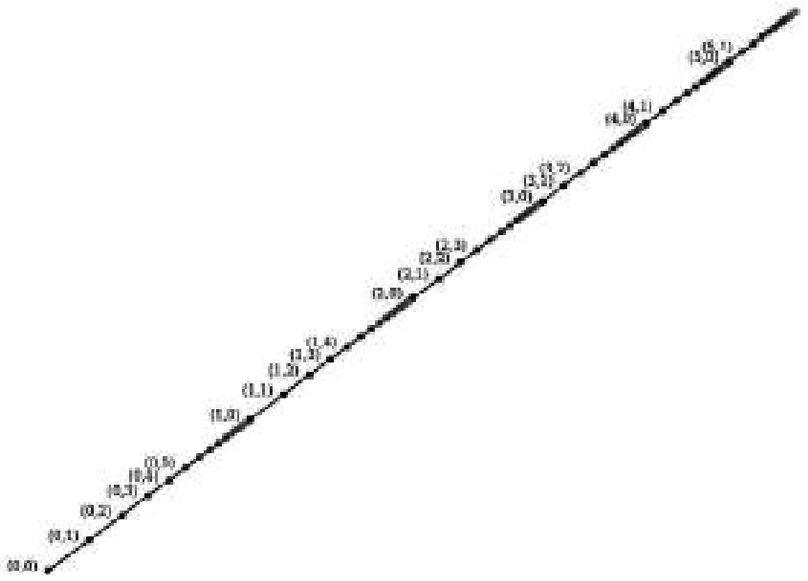


Fig. 5.2 (a) *Lexicographic Order on $\mathbb{N} \times \mathbb{N}$*

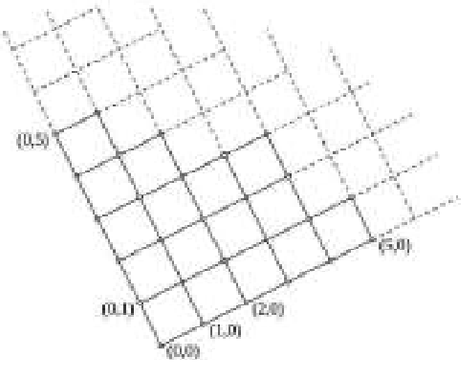


Fig. 5.2 (b) *Product Order on $\mathbb{N} \times \mathbb{N}$*

In Figure 5.2 the (c) show that reflexive closure of strict direct product order on elements covered by (3, 3) and covering (3, 3) are highlighted in green and red, respectively.

NOTES

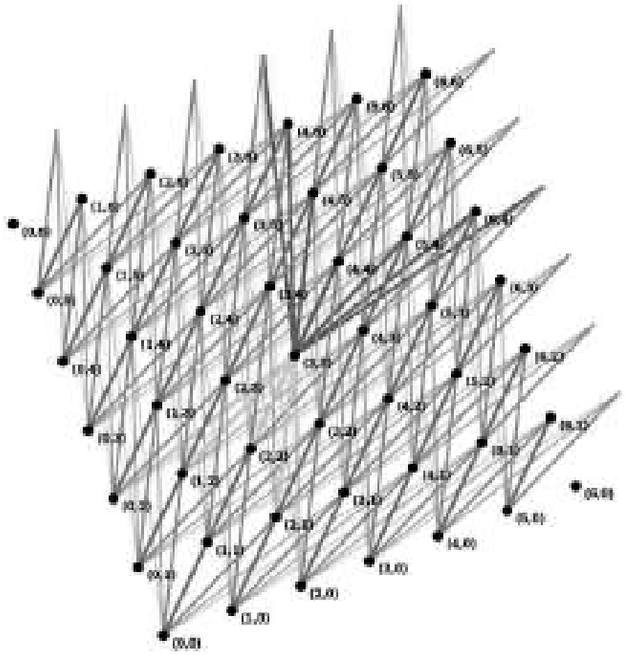


Fig. 5.2 (c) *Reflexive Closure of Strict Direct Product Order*

- The lexicographical order: $(a, b) \leq (c, d)$ if $a < c$ or ($a = c$ and $b \leq d$);
- The product order: $(a, b) \leq (c, d)$ if $a \leq c$ and $b \leq d$;
- The reflexive closure of the direct product of the corresponding strict orders: $(a, b) \leq (c, d)$ if ($a < c$ and $b < d$) or ($a = c$ and $b = d$).

All three can similarly be defined for the Cartesian product of more than two sets.

Applied to *ordered vector spaces* over the same field, the result is in each case also an ordered vector space.

Sums of Partially Ordered Sets

Another way to combine two (disjoint) posets is the ordinal sum (or linear sum), $\boldsymbol{Z = X \oplus Y}$, defined on the union of the underlying sets $\boldsymbol{X}$ and $\boldsymbol{Y}$ by the order $a \leq_{\boldsymbol{Z}} b$ if and only if:

- $a, b \in$ X with $a \leq_X b$, or
- $a, b \in Y$ with $a \leq_Y b$, or
- $a \in X$ and $b \in Y$.

If two posets are well-ordered, then so is their ordinal sum.

Series-parallel partial orders are formed from the ordinal sum operation (in this way called series composition) and another operation called parallel composition. Parallel composition is the disjoint union of *two partially ordered sets*, with no order relation between elements of one set and elements of the other set.

NOTES

Totally Ordered Set

A totally ordered set is a set plus a relation on the set (called a total order) that satisfies the conditions for a partial order plus an additional conditional known as the comparability condition.

Check Your Progress

1. What do you understand by partially ordered set and poset?
2. Define the comparable integer.
3. State the totally ordered set.
4. What is Hasse diagram of poset?
5. Write a short note on greatest and smallest elements.
6. What do you understand by Hasse diagram?
7. When element x is called LUB?

5.4 LATTICES

A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a Greatest Lower Bound (GLB) and a Least Upper Bound (LUB).

The Greatest Lower Bound (GLB) of a subset $\{a, b\} \subseteq L$ will be denoted by $a \wedge b$ and the Least Upper Bound (LUB) by $a \vee b$. So GLB $\{a, b\} = a \wedge b$, called the meet of a and b and LUB $\{a, b\} = a \vee b$, called the join of a and b.

Note that $\wedge$ and $\vee$ are binary operations and we denote the lattice by $(\wedge, \vee)$. From the definition of $\wedge$ and $\vee$, the following is denoted:

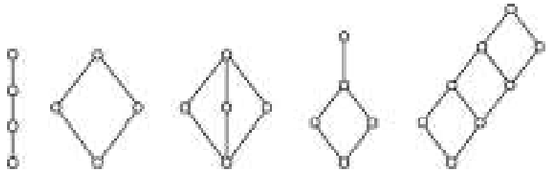
(*i*) $a \leq a \vee b$; $b \leq a \vee b$ (i.e., $a \vee b$ is an UB of a and b).

(*ii*) $a \wedge b \leq a$; $a \wedge b \leq b$ (i.e., $a \wedge b$ is a LB of a and b).

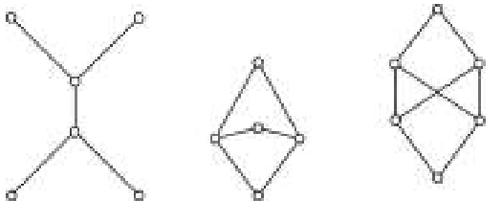
(*iii*) If $a \leq c$ and $b \leq c$ then $a \vee b \leq c$ (i.e., $a \vee b$ is the LUB of a and b).

(*iv*) If $c \leq a$ and $c \leq b$ then $c \leq a \wedge b$. (i.e., $a \wedge b$ is the GLB of a and b).

For example, the following are Lattices:



For example, the following are Posets but not Lattices:



NOTES

For example, let A be any set and $L = P(A)$ be its power set. The poset $(L, \subseteq)$ is a lattice in which for any $x, y, \in L$, $x \wedge y = x \cap y$ and $x \vee y = x \cup y$.

Similarly let I be the set of positive integers. For any $x, y \in I$, $x \leq y$ if x/y. Define $x \vee y = \text{LCM}(x, y)$ and $x \wedge y = \text{GCD} \in (x, y)$. Then $(I, \wedge, \vee)$ is a lattice.

Theorem 5.2: Let $(L, \leq)$ be a lattice in which $\wedge$ and $\vee$ denote the operations of meet and join respectively. For any $a, b, c \in L$, we have

(*i*) $a \wedge a = a$; $a \vee a = a$ (Idempotent)

(*ii*) $a \wedge b = b \wedge a$; $a \vee b = b \vee a$ (Commutative)

(*iii*) $(a \wedge b) \wedge c = a \wedge (b \cap c)$; $(a \vee b) \vee c = a \vee (b \vee c)$ (Associative)

(*iv*) $a \wedge (a \vee b) = a$; $a \vee (a \wedge b) = a$ (Absorption)

Proof: Following are the proof of above mentioned statements:

(*i*) Since $a \leq a$, we know that a is a lower bound of $\{a, a\} = \{a\}$. If b is also a lower bound and if $a \leq b$ then we have $b \leq a$ and $a \leq b$. By antisymmetry, $a = b$. So a is the GLB of $\{a\}$. Therefore, $a \wedge a = a$. **Dually**, $a \vee a = a$ follows.

(*ii*) Let $x = a \wedge b = \text{GLB}\ \{a, b\}$. Since $\{a, b\} = \{b, a\}$, GLB $\{b, a\} = x$. So $b \wedge a = x$. Hence $x = a \wedge b = b \wedge a$. **Dually**, $a \vee b = b \vee a$ follows.

(*iii*) Let $x = a \wedge (b \wedge c)$ and $y = (a \wedge b) \wedge c$.

Now $x = a \wedge (b \wedge c) \Rightarrow x \leq a,\ x \leq b \wedge c$

$\Rightarrow x \leq a, x \leq b, x \leq c$

$\Rightarrow x \leq a \wedge b, x \leq c$

$\Rightarrow x \leq (a \wedge b) \wedge c = y.$

Similarly, $y \leq x$ follows. By antisymmetry, $x = y$ and hence, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

Dually, $a \vee (b \vee c) = (a \vee b) \vee c$ follows.

(*iv*) By definition, for any $a \in L$, $a \leq a$ and $a \leq a \vee b$

Therefore, $a \leq a \wedge (a \vee b)$. But $a \wedge (a \vee b) \leq a$. Hence $a \wedge (a \vee b) = a$. Dually, $a \vee (a \wedge b) = a$ follows.

Theorem 5.3: Let $(L, \leq)$ be a lattice in which $\wedge$ and $\vee$ denote the operations of meet and join, respectively. For any $a, b \in L$,

$a \leq b \quad \Leftrightarrow a \wedge b = a$

$\Leftrightarrow a \vee b = b$

Proof: Assume that $a \leq a$. Since $a \leq b$, it follows that $a \leq a \wedge b$. But by definition of $\wedge$, $a \wedge b \leq a$. Therefore $a \wedge b = a$. Conversely, suppose $a \wedge b = a$. Then $a \leq b$. Hence $a \leq b \Leftrightarrow a \wedge b = a$. Similarly $a \leq b \Leftrightarrow a \vee b = b$ follows.

Isotonicity Law

Theorem 5.4: Let $(L, \leq)$ be a lattice in which $\wedge$ and $\vee$ denote the operations of meet and join, respectively. For any $a, b, c, \in L$,

$$b \leq c \Rightarrow \begin{cases} a \wedge b \leq a \wedge c \\ a \vee b \leq a \vee c \end{cases}$$

NOTES

Proof: Assume that $b \leq c$. Since $a \wedge b \leq b$, by transitivity, $a \wedge b \leq c$. Since $a \wedge b \leq a$, it follows that,

$$a \wedge b \leq a \wedge c$$

Now, $b \leq c$ and $c \leq a \vee c$ implies $b \leq a \vee c$. But $a \leq a \vee c$. Hence $a \vee b \leq a \vee c$.

Note: For any $a, b, c \in L$, by Isotonicity law,

$a \leq b \wedge a \leq c \Rightarrow a \leq b \vee c$

$a \leq b \wedge a \leq c \Rightarrow a \leq b \vee c$

$c \leq b \wedge a \leq a \Rightarrow b \wedge c \leq a$

$c \leq b \wedge a \leq a \Rightarrow b \vee c \leq a.$

Distributive Inequality

Theorem 5.5: Let $(L, \leq)$ be a lattice. For any $a, b, c, \in L$, the following inequalities are hold.

(*i*) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

(*ii*) $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$

Since $a \leq a \vee b$ and $a \leq a \vee c$, we have,

$$a \leq (a \vee b) \wedge (a \vee c) \quad \text{... (5.1)}$$

Since $b \wedge c \leq b \leq a \vee b$ and $b \wedge c \leq c \leq a \vee c$,

$$b \wedge c \leq (a \vee b) \wedge (a \vee c) \quad \text{... (5.2)}$$

From Equations (5.1) and (5.2) we have,

$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

Similarly, Case (ii) follows.

Modular Inequality

Theorem 5.6: Let $(L, \leq)$ be a lattice. For any $a, b, c \in L$,

$$a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$$

Proof: Suppose $a \leq c$. Then $a \vee c = c$.

By distributive inequality, $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

Since $a \vee c = c$,

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c.$$

Conversely, let us assume that $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Since,

$$\begin{aligned} a &\leq a \vee (b \wedge c) \\ &\leq (a \vee b) \wedge c \\ &\leq c \end{aligned}$$

We get $a \leq c$. Hence proved.

Idempotence is the property of certain operations in *mathematics* and *computer science* that they can be applied multiple times without changing the result beyond the initial application.

Idempotent Law states that combining a quantity with itself either by logical addition or logical multiplication will result in a logical sum or product, i.e., the equivalent of the quantity.

$$A + A = A$$

$$A \times A = A$$

Example 5.18: Prove that in a lattice $(L, \leq)$, for any $a, b, c \in L$, if $a \leq b \leq c \Rightarrow a \vee b = bc$, and $(a \wedge b) \vee (b \wedge c) = b = (a \vee b) \wedge (a \vee c)$.

Solution: Since $a \leq b$ and $a \leq c$, $a \leq b \wedge c$. Again $b \leq b$ and $b \leq c$ implies $b \leq b \wedge c$.

Now $a \leq b \wedge c$ and $b \leq b \wedge c \Rightarrow a \vee b \leq b \wedge c$ ... (1)

Again, $b \wedge c \leq b \leq a \vee b$ ... (2)

From Equations (1) and (2), $a \vee b = b \wedge c$.

Hence, $a \wedge b \leq b$ and $b \wedge c \leq b$, we get $(a \wedge b) \vee (b \wedge c) \leq b$. Since $b \leq c$ and $b \leq b$ implies $b \leq b \wedge c$. Again this implies $b \leq (b \wedge c) \vee (a \wedge b)$. Hence, $(a \wedge b) \vee (b \wedge c) = b$. Similarly, $(a \vee b) \wedge (a \vee c) = b$ follows.

Example 5.19: Prove that in a lattice $(L, \leq)$, for any $a, b, c, d, \in L$, if $a \leq b$ and $c \leq d$ then $a \wedge c \leq b \wedge d$.

Solution: Since $a \wedge c \leq a \leq b$ and $a \wedge c \leq c \leq d$, $a \wedge c \leq b \wedge d$.

Distributive Lattice

A Lattice $(L, \leq)$ is said to be distributive lattice if for any $a, b, c, \in L$,

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Theorem 5.7: Let $a, b, c \in L$, where $(L, \leq)$ is a distributive lattice. Then $a \vee b = a \vee c$ and $a \wedge b = a \wedge c \Rightarrow b = c$.

Proof: We know that,

$b = b \vee (b \wedge a)$ (Absorption)

$= b \vee (a \wedge b)$ (Commutative)

$= b \vee (a \wedge c)$ $(\because a \wedge b = a \wedge c)$

$= (b \vee a) \wedge (b \vee c)$ (Distributive)

$= (a \vee b) \wedge (c \vee b)$ (Commutative)

$= (a \vee c) \wedge (c \vee b)$ $(\because a \vee b = a \vee c)$

$= (c \vee a) \wedge (c \vee b)$ (Commutative)

$= c \vee (a \wedge b)$ (Distributive)

$= c \vee (a \wedge c)$ $(\because a \wedge b = a \wedge c)$

$= c \vee (c \wedge a)$ (Commutative)

$= c$ (Absorption)

Hence proved.

Modular Lattice: A Lattice $(L, \leq)$ is said to be modular lattice

if $a \leq c \Rightarrow a \vee (b \wedge c) = (a \vee b) \wedge c$.

NOTES

Bounded Lattice: A Lattice $(L, \leq)$ which has both, a least element denoted by 0, and the greatest element denoted by 1 is called a bounded lattice.

Note: If $L = \{a_1, a_2, ..., a_n\}$ with $\bigwedge_{i=1}^{n} a_i = 0$ and $\bigvee_{i=1}^{n} a_i = 1$. It satisfies $a \vee 0 = a$, $a \vee 1 = 1$, $a \wedge 1 = a$ and $a \wedge 0 = 0$.

Complement of an Element: In a bounded Lattices $(L, \leq)$, an element $b \in L$ is called a complement of an element $a \in L$ if $a \wedge b = 0$ and $a \vee b = 1$, we denote b by a.

Complement Lattice: A Lattice $(L, \leq)$ is said to be complemented lattice if every element of L has at least one complement.

Example 5.20: Show that De Morgan's laws hold in a complemented distributive lattice.

Solution: To process that $(a \wedge b)' = a' \vee b'$ and $(a \vee b)' = (a' \wedge b')$, consider

$$\begin{aligned}
(a \wedge b)' \wedge (a' \vee b') &= \big((a \wedge b) \wedge a'\big) \vee \big((a \wedge b) \wedge b'\big) && \text{(Distributive)} \\
&= \big((b \wedge a) \wedge a'\big) \vee \big((a \wedge b \wedge \wedge b'\big) && \text{(Commutative)} \\
&= \big(b \wedge (a \wedge a')\big) \vee \big(a \wedge (b \wedge b')\big) && \text{(Associative)} \\
&= (b \wedge 0) \vee (a \wedge 0) \\
&= 0 \vee 0 = 0
\end{aligned}$$

Again,

$$\begin{aligned}
(a \wedge b)' \wedge (a' \vee b') &= \big(a \vee (a' \vee b') \wedge \big(b \vee (a' \vee b')\big) && \text{(Distributive)} \\
&= \big(a \vee (a' \vee b')\big) \wedge \big(b \vee (b' \vee a')\big) && \text{(Commutative)} \\
&= \big((a \vee a') \vee b'\big) \wedge \big((b \vee b') \vee a'\big) && \text{(Associative)} \\
&= (1 \vee b') \wedge (1 \vee a') \\
&= 1 \wedge 1 = 1
\end{aligned}$$

Hence, $a' \vee b'$ is the complement of $(a \wedge b)$. So $a' \vee b' = (a \wedge b)'$. Similarly, $(a \vee b)' = a' \wedge b'$ follows.

Example 5.21: Show that in a complemented lattice $(L, \leq)$,

$$a \leq b \Leftrightarrow a' \vee b = 1 \Leftrightarrow a \wedge b' = 0 \Leftrightarrow b' \leq a'$$

Solution: Consider $a \leq b \Leftrightarrow a \wedge b = a$

$$\begin{aligned}
&\Leftrightarrow a' \vee a = a' \vee (a \wedge b) = 1 \\
&\Leftrightarrow (a' \vee a) \wedge (a' \vee b) = 1 \\
&\Leftrightarrow 1 \wedge (a' \vee b) = 1 \\
&\Leftrightarrow a' \vee b = 1
\end{aligned}$$

Again, $a \leq b \Leftrightarrow a \vee b = b$

$$\begin{aligned}
&\Leftrightarrow b \wedge b' = (a \vee b) \wedge b' = 0 \\
&\Leftrightarrow (a \wedge b') \vee (b \wedge b') = 1 \\
&\Leftrightarrow (a \wedge b') \vee 0 = 0 \\
&\Leftrightarrow a \wedge b' = 0.
\end{aligned}$$

To prove the last one,

$$\begin{aligned}
a \leq b &\Leftrightarrow a \vee b = b \\
&\Leftrightarrow (a \vee b') = b' \\
&\Leftrightarrow a' \wedge b' = b' \\
&\Leftrightarrow a' \wedge a' = b' \quad \text{(Commutative)} \\
&\Leftrightarrow b' \leq a'.
\end{aligned}$$

NOTES

Example 5.22: Consider the lattice $L = \{1, 2, 3, 4, 6, 12\}$, the divisions of 12 ordered by divisibility. Find the following:

(*i*) The lower bound and upper bound of L

(ii) The complement of 4.

(*iii*) Is L a complemented lattice?

Solution: The solution is obtained as follows:

(*i*) The lower bound of L is 1and the upper bound is 12.

(*ii*) Since $4 \wedge 3 = \gcd(4,3) = 1$ and

$4 \vee 3 = \text{lcm}(4,3) = 12$, then the complement of 4 is 3.

(*iii*) Since $6 \wedge x = \gcd(6, x)$

$\neq 1$ for $x \neq 1$ and $6 \vee 1 = \text{lcm}(6,1)$

$\neq 12$, 6 has no complement and hence L is not a complemented lattice.

Sublattice

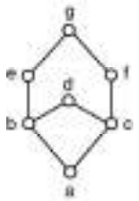
Let M be a non-empty subset of a Lattice $(L, \leq)$. We say that M is a sublattice of L if M itself is a lattice with respect to the operations of L.

Note: So M is a sublattice of L if and only if M is closed under the operations $\wedge$ and $\vee$ of L.

Complete Lattice

A partially ordered set is called a complete lattice if every subset has a least upper bound and greatest lower bound.

Example 5.23: Consider the following lattice L.



Determine whether each of the following is a sublattice of L.

$$M = \{a, b, c, g\}$$

$$N = \{a, b, f, g\}$$

$$O = \{b, d, e, g\}$$

$$P = \{a, d, e, g\}$$

Solution: Since $b \vee c = d$, and $d \notin M$, M is not a sublattice. Since $d \wedge e = b$ and $b \notin p$, p is not a sublattice. But N and O are sublattices.

Example 5.24: Suppose M is a sublattice of a distributive lattice L. Show that M is a distributive lattice.

Solution: For a distributive lattice L, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a, b, c \in L$. Since M is closed, each element of M is also in L, the distributive laws hold for all elements in M. Hence M is a distributive lattice.

NOTES

Example 5.25: Prove that in a distributive lattice $(L, \leq)$, if an element has a complement then this complement is unique.

Solution: Suppose for any $a \in L$ has two complements say b and c in L. Then $a \vee b = 1$; $a \wedge b = 0$ and $v\ a \vee c = 1$; $a \wedge c = 0$.

Consider $b = b \wedge 1 = b \wedge (a \vee c)$

$= (b \wedge a) \vee (b \wedge c)$ (Distributive)

$= 0 \vee (b \wedge c) = (a \wedge c) \vee (b \wedge c)$

$= (a \vee b) \wedge c$ (Distributive)

$= 1 \wedge c = c$

Semilattice

In mathematics, a *join-semilattice* (or upper *semilattice*) is a **partially ordered set** that has a join (a least upper bound) for any non-empty finite subset. Dually, a meet-semilattice (or lower semilattice) is a partially ordered set which has a meet (or greatest lower bound) for any non-empty finite subset. Every join-semilattice is a meet-semilattice in the inverse order and vice versa.

Semilattices can also be defined algebraically: join and meet are associative, commutative, idempotent binary operations, and any such operation induces a partial order (and the respective inverse order) such that the result of the operation for any two elements is the least upper bound (or greatest lower bound) of the elements with respect to this partial order. A lattice is a partially ordered set that is both a meet- and join-semilattice with respect to the same partial order. Algebraically, a lattice is a set with two associative, commutative idempotent binary operations linked by corresponding *absorption laws*.

Definition 1: An order theoretic meet-semilattice $\langle S, \leq \rangle$ gives rise to a binary operation $\wedge$ such that $\langle S, \wedge \rangle$ is an algebraic meet-semilattice. Conversely, the meet-semilattice $\langle S, \wedge \rangle$ gives rise to a binary relation $\leq$ that partially orders S in the following way: for all elements x and y in S, $x \leq y$ if and only if $x = x \wedge y$.

Definition 2: The relation $\leq$ introduced in this way defines a partial ordering from which the binary operation $\wedge$ may be recovered. Conversely, the order induced by the algebraically defined semilattice $\langle S, \wedge \rangle$ coincides with that induced by $\leq$.

Hence the two definitions may be used interchangeably, depending on which one is more convenient for a particular purpose. A similar conclusion holds for join-semilattices and the dual ordering $\geq$.

A meet-semilattice is an algebraic structure $\langle S, \wedge \rangle$ consisting of a set S with a binary operation $\wedge$, called meet, such that for all members x, y, and z of S, the following identities hold:

Associativity: $x \wedge (y \wedge z) = (x \wedge y) \wedge z$

Commutativity: $x \wedge y = y \wedge x$

Idempotency: $x \wedge x = x$

A meet-semilattice $\langle S, \wedge \rangle$ is bounded if S includes an identity element 1 such that $x \wedge 1 = x$ for all x in S.

If the symbol $\vee$, called join, replaces $\wedge$ in the definition just given, the structure is called a join-semilattice. One can be ambivalent about the particular choice of symbol for the operation, and speak simply of semilattices. A semilattice is a commutative, idempotent semigroup; i.e., a commutative band. A bounded semilattice is an idempotent commutative monoid.

A partial order is induced on a meet-semilattice by setting $x \leq y$ whenever $x \wedge y = x$. For a join-semilattice, the order is induced by setting $x \leq y$ whenever $x \vee y = y$. In a bounded meet-semilattice, the identity 1 is the greatest element of S. Similarly, an identity element in a join semilattice is a least element.

Convex Sublattice

Let $\mathcal{L} = (\boldsymbol{L}, \cap, \cup)$ be a lattice and $S \subseteq L$. S is convex if for $a, b \in S$ and $c \in L$ $a \leq c \leq b \Rightarrow c \in S$.

If furthermore S induces a sublattice S of $\mathcal{L}$, then S is a convex sublattice of $\mathcal{L}$.

5.5 BOOLEAN ALGEBRA

Boolean algebra is named after George Boole, who used it to study human logical reasoning. For example, any event can be true or false. Similarly, connectives can be of any of the following three basic forms:

1. a OR b
2. a AND b
3. NOT a

Boolean algebra consists of a set of elements B, with two binary operations {+} and {.} and a unary operation {′}, such that the following axioms hold:

- The set B contains at least two distinct elements x and y.
- **Closure**: For every x, y in B,
  - x + y
  - x . y
- **Commutative laws**: For every x, y in B,
  - x + y = y + x
  - x . y = y . x
- **Associative laws**: For every x, y, z in B,
  - (x + y) + z = x + (y + z) = x + y + z
  - (x . y) . z = x .(y . z) = x . y . z
- **Identities** (0 and 1):
  - 0 + x = x + 0 = x for every x in *B*
  - 1 . x = x . 1 = x for every x in B
- **Distributive laws**: For every x, y, z in B,
  - x . (y + z) = (x . y) + (x . z)
  - x + (y . z) = (x + y) . (x + z)

NOTES

- **Complement**: For every x in B, there exists an element x′ in B such that,
  - o $x + x' = 1$
  - o $x \cdot x' = 0$

Duality Principle: Every valid Boolean expression (equality) remains valid if the operators and identity elements are interchanged.

+ ↔ .
1 ↔ 0

For example, given the expression,

$$a + (b \cdot c) = (a + b). (a + c)$$

Its dual expression is:

$$a. (b + c) = (a. b) + (a. c)$$

The advantage of this theorem is that if you prove one theorem, the other follows automatically.

For example, if $(x + y + z)' = x'. y.' z'$ is valid, then its dual is also valid:

$$(x. y. z)' = x' + y' + z'$$

Apart from the axioms/postulates, there are other useful theorems. These entire theorems are useful for reducing the expression.

1. **Idempotency**
   (a) $x + x = x$ (b) $x \cdot x = x$
   Proof of (a):

$$\begin{aligned} x + x &= (x + x).1 \text{ (Identity)} \\ &= (x + x). (x + x') \text{ (Complement)} \\ &= x + x. x' \text{ (Distributive)} \\ &= x + 0 \text{ (Complement)} \\ &= x \text{ (Identity)} \end{aligned}$$

2. **Null elements** for **'+'** and **'.'** operators
   (a) $x + 1 = 1$ (b) $x \cdot 0 = 0$
3. **Involution**

$$(x')' = x$$

4. **Absorption**
   (a) $x + x \cdot y = x$ (b) $x \cdot (x + y) = x$
5. **Absorption (variant)**
   (a) $x + x' \cdot y = x + y$ (b) $x \cdot (x' + y) = x. y$
6. **De Morgan**
   (a) $(x + y)' = x' \cdot y'$ (b) $(x \cdot y)' = x' + y'$
7. **Consensus**
   (a) $x. y + x' \cdot z + y. z = x \cdot y + x' \cdot z$
   (b) $(x + y) \cdot (x' + z) \cdot (y + z) = (x + y) \cdot (x' + z)$

The set B = {0, 1} and the logical operations OR, AND and NOT satisfy all the axioms of Boolean algebra.

A **Boolean expression** is an algebraic statement containing Boolean variables and operators. Theorems can be proved using the truth table method. They can also be proved by an algebraic manipulation using axioms/postulates or other basic theorems.

NOTES

5.5.1 Applications of Boolean Algebra

- In particular, by taking the variables to represent values of on and off (or 0 and 1), Boolean algebra is used to design and analyze digital switching circuitry, such as that found in personal computers, pocket calculators, cd players, cellular telephones, and a host of other electronic products.
- Boolean algebra has a variety of uses in the real world. It is used in light switches. This basic is significant especially in a large lighting system where the lighting system is interconnected in such a way that it can be controlled using one or more switches.
- Boolean algebra is commonly used in industries that produce computers, its implementation is realized by the integrated circuits that are in container form, consisting of a large number of logic gates. The communication between the gates is made possible by the use of an external connection of pins that are related to the input and output lines of the individual gate.
- The commonly used is the printed circuit board because they have metallic strips. The gate networks can be applied in the internal connections after programming has been done to improve the workability of the integrated circuits. This makes it ready to be incorporated into the systems. Once embedded into the computer systems, the computer will be able to carry out arithmetic and logical operations. Algebra enables the machine to determine the value of an output signal (1 or 0) or to save a value into the storage unit.
- Boolean algebra has been used to come up with an analysis of flight accidents. The events that lead to failures in complex systems are incorporated with probabilistic and logical tools. It is based upon the breaks down and groups the causal agents of the accident using the fault tree method. The faulty tree is used purposely for maintenance tests, risk analysis, and probability maintenance. To identify the cause of a problem, the faulty tree uses a deductive process to show the relationship between the events that added up to the cause of the accident.
- Applied Boolean algebra are search engines. Search engines, such as Google and duckduckgo use Boolean algebra to enable the users to get data whenever they request or search. The concept of Boolean search has been implemented by the use of logical AND, OR, and NOT. The Boolean search considers each webpage on the Internet as an element of a set.
- Today, Boolean algebra is of significance to the theory of probability, geometry of sets, and information theory. Furthermore, it constitutes the basis for the design of circuits used in electronic digital computers.
- Switching theory used a two-valued Boolean algebra (sometimes called Switching algebra) as a notation to represent the operation of such logic

NOTES

networks. The two algebraic values are most often represented as "0" and "1," although "T" and "F" are sometimes used to emphasize the relation to propositional logic.

- One example of a Boolean ring is the power set of any set X, where the addition in the ring is symmetric difference, and the multiplication is intersection. As another example, we can also consider the set of all finite or cofinite subsets of X, again with symmetric difference and intersection as operations.
- A set of rules or Laws of Boolean Algebra expressions have been invented to help reduce the number of logic gates needed to perform a particular logic operation resulting in a list of functions or theorems known commonly as the Laws of Boolean Algebra.
- Logical OR represents the addition of the binary bits whereas Logical AND represents the product of all the bits. Now, since this Boolean algebra is based on logical operations and keeps switching between the two values of 0 and 1 based on the operation, it is also known as logical algebra or switching algebra.
- A Boolean algebra can be seen as a generalization of a power set algebra or a field of sets, or its elements.
- A ring R is Boolean if all its elements are idempotent, i.e., $x^2 = x$ for all $x \in R$. A simple example of a Boolean ring is Z^2. Products of Boolean rings are also Boolean, so we may construct a large class of such rings.

5.6 BOOLEAN FUNCTIONS

A **Boolean function** is an expression formed with binary variables, the two binary operators OR and AND, the unary operator NOT, and the equal and parenthesis signs. Its result is also a binary value. The general usage is '**.**' for AND, '**+**' for OR and '**′**' for NOT.

Precedence of Operators

To lessen the brackets used in writing Boolean expressions, operator precedence can be used. Precedence (highest to lowest): $' \rightarrow . \rightarrow +$

For example,

$$a .b + c = (a. b) + c$$

$$b' + c = (b') + c$$

$$a + b' . c = a + ((b'). c)$$

In order to avoid confusion, use brackets to overwrite precedence.

Truth Table

A truth table is a table, which consists of every possible combination of inputs and its corresponding outputs.

INPUTS	OUTPUTS
...	...
...	...

NOTES

For basic logic gates, the truth table is already being discussed. Now, for the complex digital systems, it is very important to derive the truth table.

A truth table describes the behaviour of a system that is to be designed. This is the starting point for any digital system design. A designer must formulate the truth table first. It is the responsibility of the designer to decide the number of output bits to represent the behaviour of the system.

For example, if you have to design a 2-bit multiplier, which multiplies two inputs A and B, each of the two bits, then it should be noted that the output must be at least of 4 bits since the maximum result that you can have from this multiplication is 1001(9) corresponding to the maximum value of both the inputs, i.e., 11(3). The block diagram and the truth table are shown as follows:

Fig. 5.3 *2-Bit Multiplier Block Diagram*

In the truth table formation, inputs are taken as A_1A_0 for A input and B_1B_0 for B input. Output resulting from multiplication is to be represented as $P_3P_2P_1P_0$, where P_3 is the MSB and P_0 is the LSB bit. If A = 10, i.e., 2 and B = 11, i.e., 3, then the result of multiplication will be 0110, i.e., 6. So, the bits at the output will be $P_3 = 0$, $P_2 = 1$, $P_1 = 1$, $P_0 = 0$. The complete truth table for the multiplier will be as shown in Table 5.1.

Table 5.1 *Truth Table for 2-Bit Multiplier*

A_1	B_0	B_1	B_0	P_3	P_2	P_1	P_0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	0	0	0	0	0
0	1	0	1	0	0	0	1
0	1	1	0	0	0	1	0
0	1	1	1	0	0	1	1
1	0	0	0	0	0	0	0
1	0	0	1	0	0	1	0
1	0	1	0	0	1	0	0
1	0	1	1	0	1	1	0
1	1	0	0	0	0	0	0
1	1	0	1	0	0	1	1
1	1	1	0	0	1	1	0
1	1	1	1	1	0	0	1

After the truth table, you have to write the Boolean expression for the output bit and then realize the reduced expression using logic gates.

Whenever a Boolean expression for any output signal is to be written from the truth table, only those input combinations for which the output is high is to be written. As an example, let us write the **Boolean expression** for Table 5.2.

NOTES

Table 5.2 *Truth Table*

x	y	z	F_1	F_2	F_3	F_4
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	1	1
1	0	0	0	1	1	1
1	0	1	0	1	1	1
1	1	0	1	1	0	0
1	1	1	0	1	0	0

The Boolean expression for the output F_1 will be $F_1 = x.\ y.\ z'$. This is in the Sum-of-Products form, which will be discussed later.

As can be seen from Table 5.2, output F_1 is 1 only when input xyz is 110. This is represented as $x.\ y.\ z'$. Similarly, you can write the output expression for the rest of the output signals.

$$F_2 = x'.\ y'.\ z + x\ .y'.\ z' + x.\ y'.\ z + x.\ y.\ z' + x.\ y.\ z$$

F_2 can be reduced using Boolean algebra and can be written as follows:

$$\begin{aligned} F_2 &= x'.\ y'.\ z + x\ .y'.\ (z' + z) + x.\ y.\ (z' + z) \\ &= x'.\ y'.\ z + x\ .y' + x.\ y \\ &= x'.\ y'.\ z + x\ .(y' + y) \\ &= x'.\ y'.\ z + x \\ &= (x' + x).\ (y'.\ z + x) \text{ (Using } \textbf{Absorption Rule)} \\ &= \textbf{1. (}y'.\ z + x) \\ &= (y'.\ z + x) \end{aligned}$$

Similarly, it can be shown that $F_3 = F_4 = x.\ y' + x'.\ z$

Complement of Functions

For a function F, the **complement** of this function F′ is obtained by interchanging 1 with 0 and vice versa in the function's output values. As an example, take the following function F_1 and its complement, F_1':

Table 5.3 *Truth Table of Function and its Complement*

x	y	z	F_1	F_1'
0	0	0	0	1
0	0	1	0	1
0	1	0	0	1
0	1	1	0	1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	0
1	1	1	0	1

The same can also be verified using the Boolean algebra technique. In Table 5.3, if $F_1 = xyz'$, then its complement will be:

$$\begin{aligned} F_1' &= (x.\ y.\ z')'. \\ &= x' + y' + (z')' \text{ (Using De Morgan's theorem)} \\ &= x' + y' + z \end{aligned}$$

NOTES

This is the same as that obtained from the truth table by algebraic manipulation, which is given as follows:

$$F_1' = x'.y'.z' + x'.y'.z + x'.y.z' + x'.y.z + x.y'.z' + x.y'.z + x.y.z$$
$$= x'.y'.(z' + z) + x'.y.(z' + z) + x.y'.(z' + z) + x.y.z$$
$$= x'.y' + x'.y + x.y' + x.y.z$$
$$= x'.(y' + y) + x.(y' + y.z)$$
$$= x' + x.(y' + y.z)$$
$$= x' + x(y' + y).\ (y' + z)$$
$$= x' + x.\ (y' + z)$$
$$= (x' + x).(x' + y' + z\ )$$
$$= (x' + y' + z)$$

The following are some more general forms of **De-Morgan's theorems** used for obtaining complement functions:

$$(A + B + C + ... + Z)' = A'.\ B'.C' \ldots .\ Z'$$
$$(A.\ B.\ C... .Z)' = A' + B' + C' + \ldots + Z'$$

Standard Forms

Certain types of Boolean expressions lead to gating networks, which are desirable from the implementation point of view. The following are two standard forms for writing a Boolean expression:

- Sum-Of-Product (SOP)
- Product-Of-Sum (POS)

Before using SOP and POS forms, you must know the following terms:

- **Literal:** A variable on its own or in its complemented form is known as a literal.

  Examples: x, x′, y, y′

- **Product Term**: It is a single literal or a logical product (AND) of several literals.

  Examples: x, x.y.z′, A′.B, A.B

- **Sum Term**: It is a single literal or a logical sum (OR) of several literals.

  Examples: x, x +y + z′, A′+B, A+B

- **Sum-Of-Products (SOP) Expression**: It is a product term or a logical sum (OR) of several product terms.

  Examples: x, x + y. z′, x .y′ + x′. y. z , A.B+A′.B′

- **Product-Of-Sum (POS) Expression**: It is a sum term or a logical product (AND) of several sum terms.

  Examples: x, x.(y + z′), (x +y′).(x′ + y+ z), (A+B).(A′+B′)

Every Boolean expression can either be expressed as a Sum-Of-Product or Product-Of-Sum expression. For example,

NOTES

SOP: $x'.y + x.y' + x.y.z$

POS: $(x + y').(x' + y).(x' + z')$

Both: $x' + y + z$ or $x.y.z'$

Neither: $x.(w' + y.z)$ or $z' + w.x'.y + v.(x.z + w')$

Minterm and Maxterm

Consider two binary variables x, y. Each variable may appear as itself or in the complemented form as literals (i.e., x, x′ and y, y′). For two variables, there are four possible combinations with the AND operator, namely:

$$x'.y', x'.y, x.y' \text{ and } x.y$$

These product terms are called **Minterms**. In other words, A **Minterm** of n variables is the product of *n* literals from the different variables. In general, *n* variables can give 2^n Minterms.

Similarly, a **Maxterm** of n variables is the sum of n literals from the different variables.

Examples: x′+y′, x′+y, x+y′, x+y

In general, n variables can give 2^n Maxterms.

The Minterms and Maxterms of 2 variables are denoted by m_0 to m_3 and M_0 to M_3, respectively. In Table 5.4, all the Minterms and Maxterms are written.

Table 5.4 *Minterms and Maxterms*

Minterms				Maxterms	
x	**y**	**Term**	**Notation**	**Term**	**Notation**
0	0	x' .y'	m_0	x + y	M_0
0	1	x' .y	m_1	x + y'	M_1
1	0	x .y'	m_2	x' + y	M_2
1	1	x .y	m_3	x' + y'	M_3

If you examine carefully, each Minterm is the complement of the corresponding Maxterm. For example, $m_2 = x.y'$ and $m_2' = (x.y')' = x' + (y')' = x'+y = M_2$. In other words, **Maxterm is the sum of terms of the corresponding Minterm with its literal complemented.**

Canonical Form: Sum of Minterms

Canonical form is a unique way of representing Boolean expressions. Any Boolean expression can be written in the form of the sum of Minterm. A Σ symbol is used for showing the sum of Minterms. For example,

NOTES

Table 5.5 *Sum of Minterms*

x	y	x	F_1	F_2	F_3
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	0	0	0
0	1	1	0	0	1
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	0	1	0

Sum-of-Minterms by gathering/summing the Minterms of the function (where result is a 1) can be obtained as follows:

$$F_1 = x.y.z' = \Sigma m\ (6)$$

$$F_2 = x'.y'.z + x.y'.z' + x.y'.z + x.y.z' + x.y.z = \Sigma m(1,4,5,6,7)$$

$$F_3 = x'.y'.z + x'.y.z + x.y'.z' + x.y'.z = \Sigma m(1,3,4,5)$$

Canonical Form: Product of Maxterms

Maxterms are sum terms. For Boolean functions, the Maxterms of a function are the terms for which the result is 0. Boolean functions can be expressed as Products-of-Maxterms. For Table 5.5, each output F_1, F_2 and F_3 can be represented in Product-of-Maxterm. A Π symbol is used to represent Product-of-Maxterms.

$$F_1 = (x + y + z).(x + y + z').(x + y' + z).(x + y' + z').(x' + y + z).(x' + y + z').(x' + y' + z')$$

$$= \Pi M(0,1,2,3,4,5,7)$$

$$F_2 = (x + y + z).(x + y' + z).(x + y' + z')$$

$$= \Pi M(0,2,3)$$

$$F_3 = (x + y + z).(x + y' + z).(x' + y' + z).(x' + y' + z')$$

$$= \Pi M(0,2,6,7)$$

Conversion of Canonical Forms

Sum-of-Minterms $\Rightarrow$ Product-of-Maxterms

- Rewrite Minterm shorthand using Maxterm shorthand.
- Replace Minterm indices with indices not already used.

For example, $F_1(x,y,z) = \sum m(6) = \prod M(0,1,2,3,4,5,7)$.

Product-of-Maxterms $\Rightarrow$ Sum-of-Minterms

- Rewrite Maxterm shorthand using Minterm shorthand.
- Replace Maxterm indices with indices not already used.

For example, $F_2(x,y,z) = \prod M(0,2,3) = \sum m(1,4,5,6,7)$.

Sometimes, you are given the reduced expression for any Boolean expression. In this case, you need to find Minterms or Maxterms present in the expression. To convert from a general expression to a Minterm or Maxterm expression, you can use either the truth table or the algebraic manipulation.

NOTES

For example, suppose you wish to find all the Minterm expansions of F = AB′ + A′C.

The truth table for the expression is represented as shown in Table 5.6:

Table 5.6

A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

From the Table 5.6, $F = A'.B'.C + A'.B.C + A.B'.C' + A.B'.C$

$= \Sigma m\,(1, 3, 4, 5)$

Using Algebraic Manipulation

Use X + X′ = 1 to introduce the missing variables in each term; this introduction will not change the overall expression value. Therefore, for the Boolean expression F = AB′ + A′C, the missing variable in the first term is C and in the second term is B. So, the missing variable can be introduced as follows:

$= A.B'.(C + C') + A'.C.(B + B')$

$= A.B'.C + A.B'.C' + A'.B.C + A'.B'.C$

$= m_5 + m_4 + m_3 + m_1$

$= \sum m\,(1, 3, 4, 5)$

Similarly, you can find all the Maxterms for reduced expressions**.** Find the Maxterms expansion of F = (A + B′) (A′ + C)

Using Algebraic Expression: In this case, XX′ = 0 is used to introduce missing variables in each term.

Therefore, **F = (A + B′+ CC′). (A′ + C + BB′)**

Assuming that (A + B′) = X and C.C′ = YZ, you can use the expression rule

= X+YZ =(X+Y)(X+Z)

$F = (A + B'+C)(A+B'+C')(A'+B+C)(A'+B'+C)$

$= \prod(2, 3, 4, 6)$

Using the Truth Table:

A	B	C	F
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

$F(A,B,C) = \prod(2, 3, 4, 6)$

NOTES

Boolean Algebra as Lattices

Let B be a non-empty set with two binary operations + (or $\vee$) and, (or $\wedge$), a unary operation, and two distinct elements 0 and 1. Then B is called a Boolean algebra if the following axioms hold wher a,b, c are any elements in B.

(i) $a + b = b + a$; $a \cdot b = b \cdot a$ (commutative laws)

(ii) $a + (b \cdot c) = (a + b) \cdot (a + c)$; $a.(b + c) = (a \cdot b)(a \cdot c)$ (Distributie laws)

(iii) $a + 0 = a$; $a \cdot 1 = a$ (Identity laws)

(iv) $a + a' = 1$; $a \cdot a' = 0$ (Complement laws)

Boolean algebra is a lattice which contains a least element and a greatest element and which is both complemented and distributive.

We denote the Boolean algebra B by (B, +, ., 1, 0, 1). Here we call 0 as the zero element, 1 as the unit element, and a′ is complement of a, + and . are called sum and product.

Let B = {0,1}, the set of binary digits with the binary operations of + and . and the unary operation defined by

+	1	0
1	1	1
0	1	0

·	1	0
1	1	0
0	1	0

′	1	0
	0	1

Then B is a Boolean algebra.

Atom

A non-zero element ‘a’ in a Boolean algebra (B, +, .,′) is called an atom if for every $x \in B$, $x \wedge a = a$ or $x \wedge a = 0$.

Note: Here the condition $x \wedge a = a$ means that x is a successor of a and $x \wedge a = 0$ is true only when x and a are ‘not connected’. So in any Boolean algebra, the immediate successors of the 0-element are called atoms.

Let A be any non-empty set and P(A) the power set of A. In Boolean algebra $(p(A), \cup, \cap, ')$ over $\subseteq$, the singleton sets are the atoms since each element p(A) can be described completely and uniquely as the union of singleton sets.

Let B = {1,2, 3, 5, 6, 10, 15, 30} and let the relation $\leq$ be divides. The operation $\wedge$ is GCD and $\vee$ is LCM. The 0-element is 1. Then the set of atoms of the Boolean algebra is {2,3,5}.

Notes:

1. Let (B, +, . ,′) be any finite Boolean algebra and let A be the set of all atoms. Then (B, +,., ′) is isomorphic to $(p(A), \cup, \cap, ')$.
2. Every finite Boolean algebra (B,+,.,′) has 2^n elements for some position integer n.
3. All Boolean algebra of order 2^n are isomorphic to each other. Finite Boolean algebras are *n*-tuples of 0′s and 1′s.

The simplest nontrivial Boolean algebra is the Boolean algebra B = {0, 1}, the set of binary digits with the binary operations of + and . and the unary operation ′ given by,

+	1	0
1	1	1
0	1	0

·	1	0
1	1	0
0	1	0

′	1
1	0
0	1

NOTES

If we form $B^2 = B \times B$, we obtain the set $B^2=\{(0,0), (0,1), (1, 0), (1, 1)\}$. Define +, . and ′ by

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

$(0, 1).(1,1) = (0.1, 1.1) = (0, 1)$ and

$(0,1)′ = (0′, 1′) = (1, 0).$

The B^2 is a Boolean algebra.

Note: Here B^2 is a Boolean algebra of order 4 under component wise operations. Since all Boolean algebra of order 4 are isomorphic to each other, this is a simple way of describing all Boolean algebras of order 4. In general, any Boolean algebra of order 2^n are isomorphic to B^n.

Example 5.26: Find the atoms of the Boolean algebra (i) B^2 (ii) B^4 (iii) B^n for $n \geq 1$.

Solution:

(i) (0, 1) and (1, 0)

(ii) (1,0,0,0), (0,1,0,0), (0,0,1,0) and (0,0,0,1)

(iii) The *n*-tuples with exactly one 1.

5.7 BOOLEAN EXPRESSION

It is possible to implement any Boolean expression using NAND gates. The following procedure is to be followed:

- Obtain Sum-Of-Products of Boolean expression: e.g., $F_3 = xy′+x′z$
- Use De Morgan theorem to obtain expression using 2-level NAND gates.

e.g., $F_3 = xy′+x′z$

$= \{(xy′+x′z)′\}′$ Involution

$= ((xy′)′. (x′z)′)′$ De-Morgan theorem

Implement this modified expression using NAND gate.

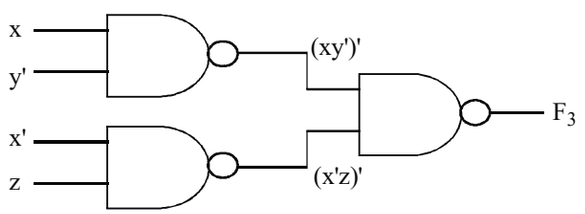


Fig. 5.4 *Implementation Using NAND Gate*

It is also possible to implement any Boolean expression using NOR gates. The following procedure is to be followed:

(i) Obtain Product-Of-Sums Boolean expression: e.g., $F_6 = (x+y′).(x′+z)$

(ii) Use De-Morgan theorem to obtain expression using 2-level NOR gates

e.g., $F_6 = (x+y').(x'+z)$

$= ((x+y').(x'+z))''$ Involution

$= ((x+y')'+(x'+z)')'$ De-Morgan theorem

Implement this modified expression using NOR gate.

NOTES

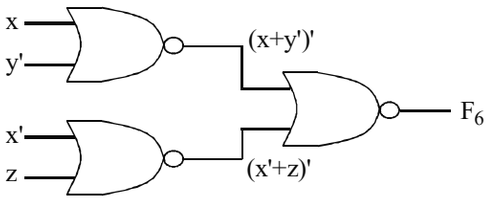
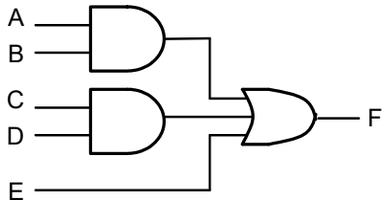


Fig. 5.5 *Implementation Using NOR Gate*

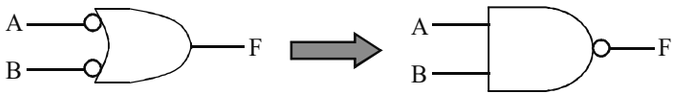
Implementation of SOP Expressions

Sum-Of-Products (SOP) expressions can be implemented using either (1) 2-level AND-OR logic circuits or (2) 2-level NAND logic circuits.

(1) 2-level AND-OR logic circuit: F = AB + CD + E



It can be proved that the OR gate with all its input complemented is equivalent to the AND gate with bubble at the output, i.e., NAND gate.

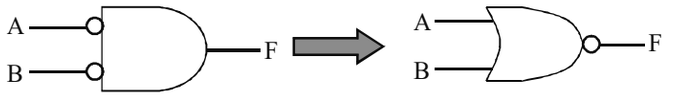


Proof: With OR gate

$F = A' + B'$

$= (A.B)'$ De-Morgan theorem

Similarly, it can be proved that the AND gate with all its input complemented is equivalent to the OR gate with bubble at the output, i.e., NOR gate.



Proof: With AND gate

$F = A'. B'$

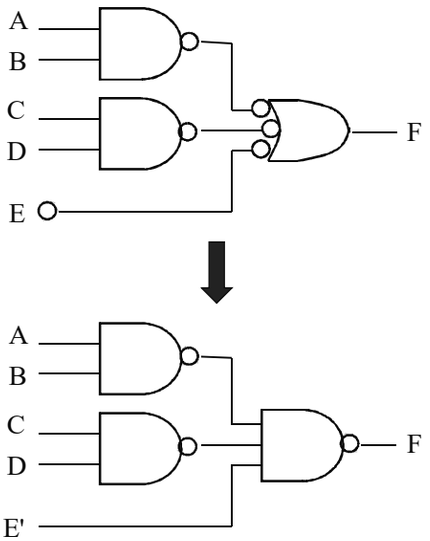
$= (A+B)'$ De-Morgan theorem

So using the transformation method discussed, you can realize any SOP realization of AND-OR with only NAND. This is known as NAND-NAND circuit transformation. The following steps are involved:

NOTES

(i) Add double bubbles in the path between the AND gate outputs and the OR gate inputs.

(ii) Change OR with inverted inputs to NAND and bubbles at inputs to their complements.

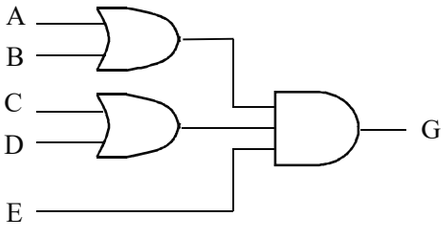


Implementation of POS Expressions

Product-of-Sums expressions can be implemented using:

- 2-level OR-AND logic circuits
- 2-level NOR logic circuits

(1) OR-AND logic circuit: G = (A+B). (C+D).E

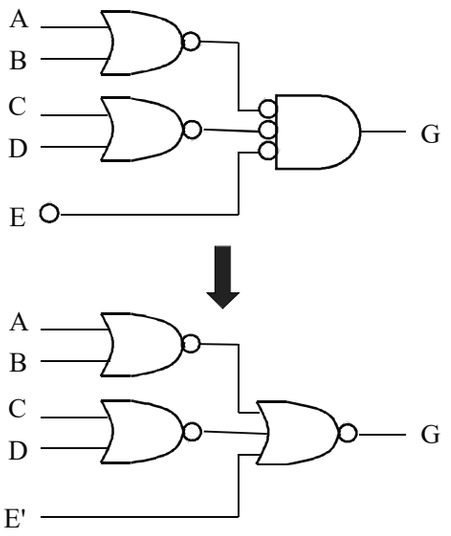


(2) NOR-NOR-based realization:

Using the transformation method discussed, you can realize any POS realization of OR-AND with only NOR. This is known as NOR-NOR circuit transformation. The following steps are involved:

(i) Add double bubbles in the path between OR gate outputs and AND gate inputs.

(ii) Changed AND-with-inverted-inputs to NOR and bubbles at inputs to their complements.



5.8 ALGEBRA OF SWITCHING CIRCUIT

Boolean algebra is used to simplify the practical use of logic circuits. The function of logic circuit is translated into symbolic form. Some rules of algebra are used for the resulting equation which is able to lessen the number of arithmetic operations and the simplified equation is translated again into the form of logic circuit. This equivalent function is achieved with the help of components. Various rules are presented to reduce the Boolean expressions into the simplest way. The identities and properties are used to review the many identities. For example, 'A' can be proved symbolically in two terms, such as A+1 = 1 and 1A=A to achieve the final result and the logical circuit is designed in the following way (Refer Figure 5.6).

A + AB = A

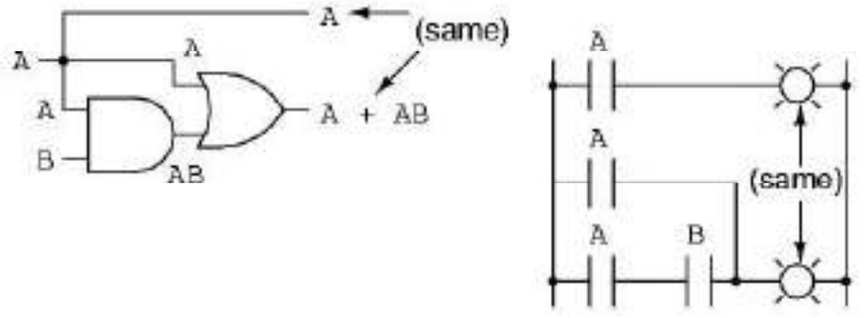
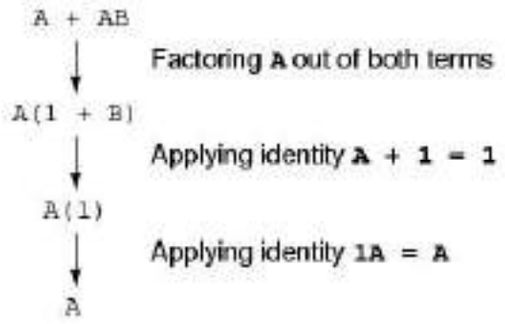


Fig. 5.6 *Logical Circuit for Expression A + AB =A*

Let take an expression as A+AB and factoring A out of both terms. Applying identity A+1 = 1 and in the next step, applying identity 1A=A that returns value A. It can be proved in the following way:

NOTES



The rule A+1 = 1 is used to reduce (B+1) term to 1. If rule A+1=1 is expressed by using alphabet A then it is not necessary that it only applies to expression containing A. The Boolean expression ABC+1 reduces to 1 with the help of A+1=1 identity. The term A in identity's standard form is used to represent ABC in the expression. The following Figure 5.7 shows the arrangement of logical circuit for the expression $\mathbf{A + \bar{A}B = A + B}$.

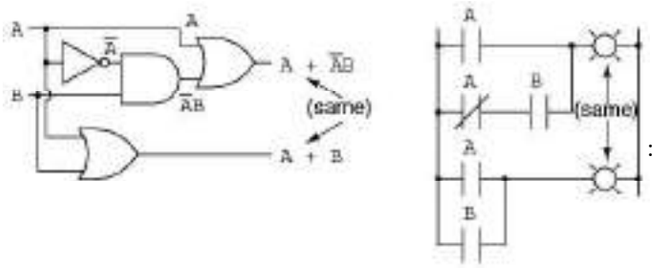
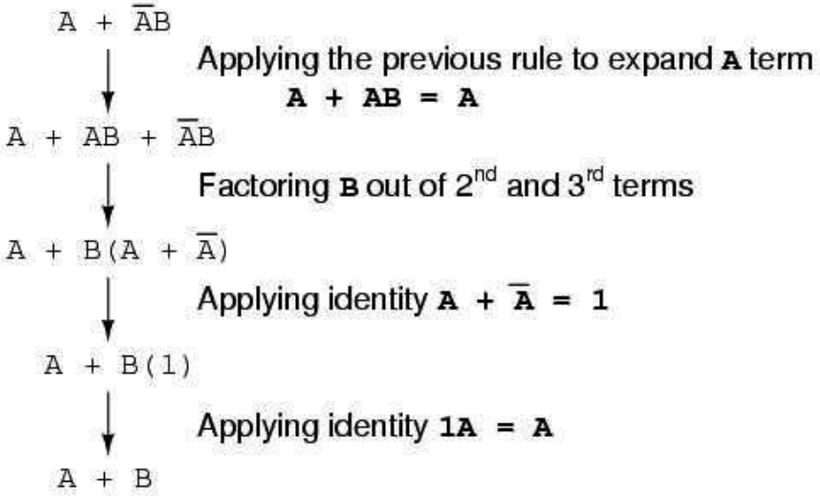


Fig. 5.7 *Logical Circuit for Expression*

The expression can be explained in the following way:



The expression (A+AB=A) is used with the rule to simplify 'A' term and then change 'A' into the expression 'A+AB'. Other rule is involved to simplify the product-of-sum expression and the logical circuit is designed for the expression (A+B) (A+C) = A + BC (Refer Figure 5.8).

$$\mathbf{(A + B)\,(A + C) = A + BC}$$

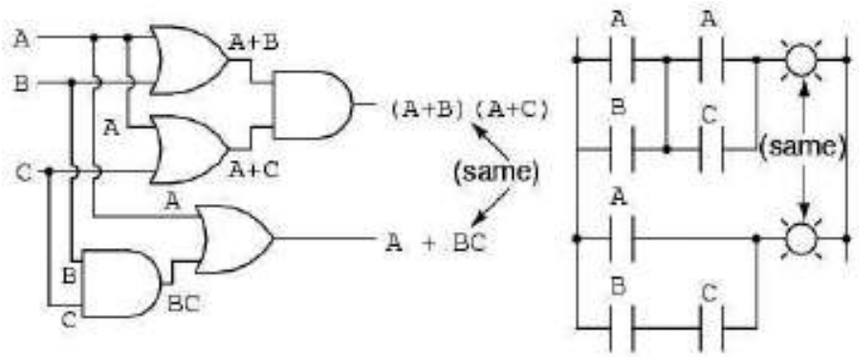


Fig. 5.8 *Logical Circuit for Expression*

This expression can be simplified in the following way:

(A + B) (A + C)

Distributing terms

AA + AC + AB + BC

Applying identity **AA = A**

A + AC + AB + BC

Applying rule **A + AB = A** to the A + AC term

A + AB + BC

Applying rule **A + AB = A** to the A + AB term

A + BC

Basically, the three useful Boolean rules are implied to simplify the Boolean expression in the following way:

$A + AB = A$

$A + \overline{A}B = A + B$

$(A + B)(A + C) = A + BC$

Check Your Progress

8. Define the lattice.
9. State the isotonicity law.
10. When lattice is said to be distributive lattice?
11. What is complement element?
12. Define sublattice.
13. What do you understand by Boolean algebra?
14. State the duality principle.
15. Define the Boolean function.
16. Is Boolean algebra used to logic circuit and why?

NOTES

5.9 ANSWERS TO 'CHECK YOUR PROGRESS'

1. In mathematics and specifically in order theory, a partially ordered set or poset validates and generalizes the natural concept of an ordering, sequencing or arrangement of the elements of a set. Typically, a poset consists of a set together with a binary relation that specifies that for certain pairs of elements in the set one of the elements precedes the other.
2. Two elements of a poset $(S, \leq)$ are said to be comparable if $a \leq b$ or $b \leq a$. Otherwise a and b are said to be incomparable.
3. A binary relation R in a set P is called a partial order relation or a partial ordering in P if and only if R is reflexive, antisymmetric and transitive. It is denoted by the symbol $\leq$. If $\leq$ is a partial ordering on P, then the ordered pair $(P, \leq)$ is called a partially ordered set or a poset. If for any $x,y \in p$, if $x \leq y$ or $y \leq x$, then $(p, \leq)$ called a 'Totally Ordered Set'.
4. The Hasse diagram of a poset P is a picture of P. So it is very useful in describing types of elements of P. Some times we define a partially ordered set by simply presenting its Hasse diagram.
5. An element $x \in p$ is called the greater element if for all $a \in p, a \leq x$. An element $x \in p$ is called the smallest element or least element if for all $a \in p, x \leq a$. The greatest element will be denoted by 1 and the smallest element by 0.
6. A Hasse diagram is a graphical representation of the relation of elements of a partially ordered set (poset) with an implied upward orientation. A point is drawn for each element of the partially ordered set (poset) and joined with the line segment according to the following rules:
   - If p<q in the poset, then the point corresponding to p appears lower in the drawing than the point corresponding to q.
   - The two points p and q will be joined by line segment iff p is related to q.
7. The element x is called the least upper bound of the set S if (i) x is an upper bound of S and (ii) x ≤ z whenever z is an upper bound of S. Similarly, the element y is called the greatest lower bound of S if

   (i) y is a lower bound of S and

   (ii) $z \leq y$, whenever z is a lower bound of S.
8. A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements a, $b \in L$ has a Greatest Lower Bound (GLB) and a Least Upper Bound (LUB).
9. Let $(L, \leq)$ be a lattice in which $\wedge$ and $\vee$ denote the operations of meet and join, respectively.
10. A Lattice $(L, \leq)$ is said to be distributive lattice if for any $a, b, c, \in L$,

    $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

    $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
11. In a bounded Lattices $(L, \leq)$, an element $b \in L$ is called a complement of an element $a \in L$ if $a \wedge b = 0$ and $a \vee b = 1$, we denote b by a.

NOTES

12. Let M be a non-empty subset of a Lattice $(L, \leq)$. We say that M is a sublattice of L if M itself is a lattice with respect to the operations of L.
13. Boolean algebra is named after George Boole, who used it to study human logical reasoning.
14. Every valid Boolean expression (equality) remains valid if the operators and identity elements are interchanged.
15. A Boolean function is an expression formed with binary variables, the two binary operators OR and AND, the unary operator NOT, and the equal and parenthesis signs. Its result is also a binary value. The general usage is '.' for AND, '+' for OR and ''' for NOT.
16. Boolean algebra is used to simplify the practical use of logic circuits. The function of logic circuit is translated into symbolic form. Some rules of algebra are used for the resulting equation which is able to lessen the number of arithmetic operations and the simplified equation is translated again into the form of logic circuit. This equivalent function is achieved with the help of components. Various rules are presented to reduce the Boolean expressions into the simplest way. The identities and properties are used to review the many identities.

5.10 SUMMARY

- A finite poset can be visualized through its Hasse diagram, which depicts the ordering relation.
- A poset (S, $\leq$) is called a chain if $\leq$ is total order relation. If every two elements of S are comparable then S is called a totally released set.
- The Hasse diagram of a poset P is a picture of P. So it is very useful in describing types of elements of P. Some times we define a partially ordered set by simply presenting its Hasse diagram.
- Define a relation $<$ on P by $x < y$ (=) $x \leq y$ but $x \neq y$. Let $(p, \leq)$ be a partially ordered set. An element $y \in p$ is said to cover an element $x \in$ p if $x < y$ and if there does not exist an element $z \in p$ such that $x \leq z$ and $z \leq y$;
- A partial ordering $\leq$ on a set P can be represented by means of a diagram known as a Hasse diagram or a partially ordered set diagram of $(p, \leq)$.
- The Hasse diagram of a part p need not be connected. Also, there can be no directed cycles in the diagram of p since the partial order relation is antisymmetric.
- An element $x \in p$ is a Least Upper Bound (LUB) for A, if x is an upper bound for A and $x \leq y$, where y is any upperbound for A. In otherwords $x \in p$ is LUB of a and b if $a \leq x$ and $b \leq x$ and if for $y \in p$, $a \leq y$, $b \leq y \Rightarrow x \leq y$.
- Every poset consisting of a set and a relation can be represented as a graph. We have to do minor modification in this relational graph. Since partial ordering relation is reflexive and transitive the relational graph will consist of self loops and edges corresponding to the transitive relations.

NOTES

- An element a of a poset $(S, \leq)$ is called maximal element if there is no $b \in S$ such that $a < b$. Similarly an element a of a poset $(S, \leq)$ is called minimal if there is no $b \in S$ such that $b < a$.
- The Greatest Lower Bound (GLB) of a subset $\{a, b\} \subseteq L$ will be denoted by $a \wedge b$ and the Least Upper Bound (LUB) by $a \vee b$. So GLB $\{a, b\} = a \wedge b$, called the meet of a and b and LUB $\{a, b\} = a \vee b$, called the join of a and b.
- Let $(L, \leq)$ be a lattice in which $\wedge$ and $\vee$ denote the operations of meet and join respectively.
- A Lattice $(L, \leq)$ which has both, a least element denoted by 0, and the greatest element denoted by 1 is called a bounded lattice.
- A Lattice $(L, \leq)$ is said to be complemented lattice if every element of L has at least one complement.
- Let M be a non-empty subset of a Lattice $(L, \leq)$. We say that M is a sublattice of L if M itself is a lattice with respect to the operations of L.
- Boolean algebra is named after George Boole, who used it to study human logical reasoning.
- A Boolean expression is an algebraic statement containing Boolean variables and operators. Theorems can be proved using the truth table method.
- A truth table is a table, which consists of every possible combination of inputs and its corresponding outputs.
- A truth table describes the behaviour of a system that is to be designed. This is the starting point for any digital system design. A designer must formulate the truth table first. It is the responsibility of the designer to decide the number of output bits to represent the behaviour of the system.
- For a function F, the complement of this function F′ is obtained by interchanging 1 with 0 and vice versa in the function's output values.
- Let B be a non-empty set with two binary operations + (or $\vee$) and, (or $\wedge$), a unary operation, and two distinct elements 0 and 1. Then B is called a Boolean algebra if the following axioms hold wher a,b, c are any elements in B.
- The rule A+1 = 1 is used to reduce (B+1) term to 1. If rule A+1=1 is expressed by using alphabet A then it is not necessary that it only applies to expression containing A.
- The expression (A+AB=A) is used with the rule to simplify 'A' term and then change 'A' into the expression 'A+AB'. Other rule is involved to simplify the product-of-sum expression and the logical circuit is designed for the expression (A+B) (A+C) = A + BC

5.11 KEY TERMS

- **Totally ordered set:** A total order (or 'Totally Ordered Set', or 'Linearly Ordered Set') is a set plus a relation on the set (called a total order) that satisfies the conditions for a partial order plus an additional condition known as the comparability condition.

NOTES

- **Hasse diagram:** A Hasse diagram is a graphical representation of the relation of elements of a partially ordered set (poset) with an implied upward orientation. A point is drawn for each element of the partially ordered set (poset) and joined with the line segment.
- **Lattice:** A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a Greatest Lower Bound (GLB) and a Least Upper Bound (LUB).
- **Boolean algebra:** Boolean algebra is named after George Boole, who used it to study human logical reasoning. For example, any event can be true or false.
- **Boolean function:** A Boolean function is an expression formed with binary variables, the two binary operators OR and AND, the unary operator NOT, and the equal and parenthesis signs. Its result is also a binary value. The general usage is '.' for AND, '+' for OR and ''' for NOT.

5.12 SELF-ASSESSMENT QUESTIONS AND EXERCISES

Short-Answer Questions

1. State the partial ordering set or poset.
2. Give the concept of totally ordered set.
3. What do you understand by Hasse diagram?
4. Define the maximal and minimal elements.
5. State the product of poset.
6. Define the term lattice.
7. When lattice $(L, \leq)$ is said to be complement lattice?
8. Generalised the Boolean algebra.
9. State the Boolean function.
10. What is truth table?
11. What do you understand by Boolean expression?
12. Give the uses of Boolean algebra in logic circuit.

Long-Answer Questions

1. Explain the partial ordering set or poset and totally ordered set with appropriate examples.
2. Illustrate the Hasse diagram with the help of examples.
3. Discuss in detail about the various type of lattice with relevant examples.
4. Discuss in detail about the Boolean algebra and their applications.
5. Elaborate on the Boolean function and Boolean expression giving examples.
6. Analyse the algebra of switching circuit.

NOTES

5.13 FURTHER READING

Hazarika, Padmalochan. 2003. *A Class Textbook of Business Mathematics*. New Delhi: S. Chand & Company Ltd.

Tremblay, Jean Paul and R. Manohar. 2004. *Discrete Mathematical Structures With Applications To Computer Science*. New York: McGraw-Hill Higher Education.

Ramaswamy, V. 2006. *Discrete Mathematical Structures with Applications to Combinatorics*. Hyderabad: Universities Press.

Kolman, Bernand, Roberty C. Busby and Sharn Cutter Ross. 2006. *Discrete Mathematical Structures*. London (UK): Pearson Education.

Liu, C. L. 1985. *Elements of Discrete Mathematics*, 2nd Edition. New York: McGraw-Hill Higher Education.

Arumugam, S. and Thangapandi Isaac. 2008. *Modern Algebra*. Chennai: Scitech Publications (India) Pvt. Ltd.

Bhattacharya, P. B., S. K. Jain and S. R. Nagpaul. 1997. *Basic Abstract Algebra*, 2nd Edition. New Delhi: Cambridge University Press.

Datta, K. B. 2002. *Matrix and Linear Algebra*. New Delhi: Prentice Hall of India Pvt. Ltd.

NOTES

NOTES