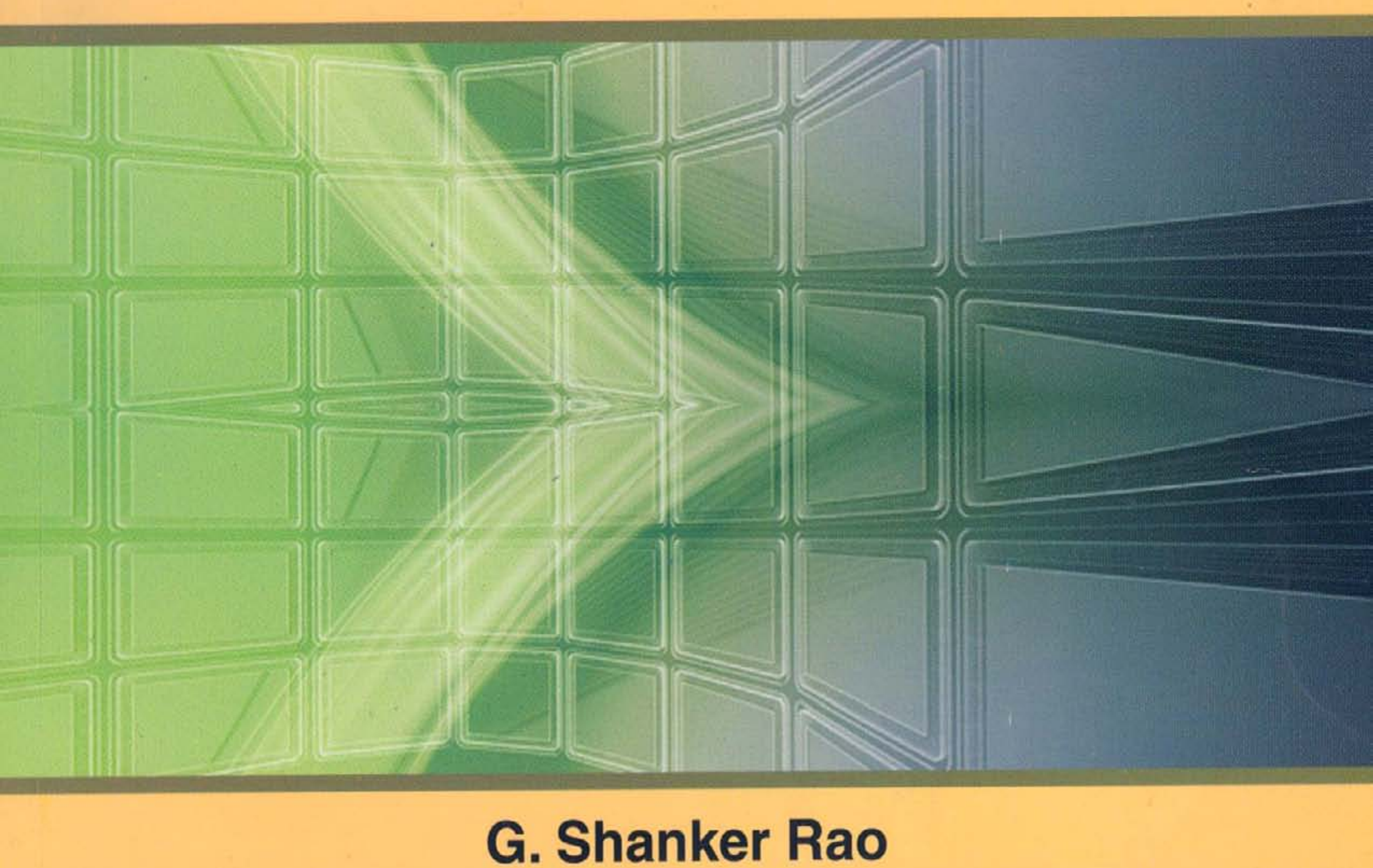
NEW AGE

SECOND EDITION

Discrete Mathematical Structures



G. Shanker Rao

NEW AGE INTERNATIONAL PUBLISHERS

Discrete Mathematical Structures

This page intentionally left blank

Discrete Mathematical Structures

(SECOND EDITION)

G. Shanker Rao
Member of
Staff University College of Engineering
Osmania University, Hyderabad, (A.P.)
Formerly HOD, Mathematics
Govt. Girraj P.G. College, Nizamabad

PUBLISHING FOR ONE WORLD
NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS
New Delhi • Bangalore • Chennai • Cochin • Guwahati • Hyderabad
Jalandhar • Kolkata • Lucknow • Mumbai • Ranchi
Visit us at **www.newagepublishers.com**

Published by New Age International (P) Ltd., Publishers

ISBN (13) : 978-81-224-2884-1

PUBLISHING FOR ONE WORLD

NEW AGE INTERNATIONAL (P) LIMITED, PUBLISHERS
4835/24, Ansari Road, Daryaganj, New Delhi - 110002
Visit us at **www.newagepublishers.com**

To

my wife,

Usha Rani

This page intentionally left blank

Preface to the Second Edition

This edition is a revision of 2002 edition of the book. Considerable attention has been given to improve the first edition. As far as possible efforts were made to keep the book free from typographic and other errors. Most of the changes were made at the suggestions of the individuals who have used the first edition of the book and who were kind enough to send their comments. Enhancements to the material devoted to mathematical logic methods of proof, combinations and graph theory are designed to help the readers master the subject.

I am thankful to the chief editor and the editors of New Age International (P) Limited, Publishers for the interest and cooperation during the production of the second edition of the book.

The author would like to express his appreciation to Sri Saumya Gupta, Managing Director, New Age International (P) Limited, for his encouragement.

Any suggestions for future improvements of this book will be gratefully received

G. Shanker Rao

This page intentionally left blank

Preface to the First Edition

This book explains some of the fundamental concepts in discrete structures. It can be used by the students in mathematics and computer science as an introduction to the fundamental ideas of discrete mathematics. The topics mathematical logic, sets, relations, function, Boolean algebra, logic gates, combinations, algebraic structures, graph theory and finite state machines have been discussed in this book. Throughout I have made an extensive use of worked examples to develop the general ideas.

Chapter 1 deals with mathematical logic. Propositions, logical equivalence, tautologies, fallacies, quantifiers, and methods of proof were briefly discussed in this chapter.

Chapter 2 is devoted to set theory.

Chapter 3 deals with relations. Reflexive, symmetric and transitive relations, have been discussed.

Chapter 4 deals with functions and recurrence relations.

Chapter 5 covers Boolean algebra. Lattices, Boolean functions, karnaugh maps, canonical forms have been discussed in this chapter.

Chapter 6 covers logic gates.

Chapter 7 deals with Elementary combinatorics. Permutation combinations and Binomial theorem have been discussed in this chapter.

Chapter 8 deals with graph theory. Isomorphism, colouring of graphs, trees, spanning trees have been explored in this chapter.

Chapter 9 covers Algebraic Structures. Groups, rings and fields, their properties have been briefly discussed in this chapter.

Chapter 10 explains finite state machines.

I am much indebted to Sri Siva Kumar, Manager, New Age International (P) Limited, Publishers Hyderabad Branch, whose suggestions and criticism helped me in writing the book. I am thankful to Sri Arvind Mishra of New Age International (P) Limited, Publishers.

G. SHANKER RAO

This page intentionally left blank

Contents

Preface to the Second Edition *vii*
Preface to the First Edition *ix*

1. Mathematical Logic **1–43**

1.1 Introduction *1*
1.2 Statements *1*
1.3 Laws of Formal Logic *1*
1.4 Connectives and Compound Statements *2*
1.5 Proposition *4*
1.6 Solved Examples *4*
Exercise 1.1 *6*
1.7 Conditional Statements 9
1.8 Well Formed Formulas *11*
1.9 Tautology *12*
1.10 Contradiction *12*
1.11 Contingency *12*
1.12 Logical Equivalence *12*
1.13 Solved Examples *12*
1.14 Laws of Logic *14*
1.15 The Duality Principle *15*
1.16 Solved Examples *15*
1.17 Logical Implication *17*
1.18 Other Connectives *18*
1.19 Normal Forms *20*
Exercise 1.2 *22*
1.20 Solved Examples *25*
Exercise 1.3 *26*

1.21 Quantifiers *28*
1.22 Methods of Proof *31*
Exercise 1.4 *42*

2. Set Theory **44–68**

2.1 Introduction *44*
2.2 Sets and Operations on Sets *44*
2.3 Subsets *45*
2.4 Null Set *46*
2.5 Singleton *46*
2.6 Finite Set *47*
2.7 Infinite Set *47*
2.8 Universal Set *47*
2.9 The Power Set *47*
2.10 Disjoints Sets *47*
2.11 Properties of Set Containment *48*
2.12 Operations on Sets: Union of Sets *48*
2.13 Properties of Union Operation *48*
2.14 Intersection of Sets *51*
2.15 Properties of Intersection Operation *51*
2.16 Distributive Laws *53*
2.17 Complement of a Set *54*
2.18 Properties of Complementation *54*
2.19 Properties of Difference *56*
2.20 Symmetric Difference *57*
2.21 Properties of Symmetric Difference *57*
2.22 Venn Diagrams *58*
2.23 Principle of Duality *59*
2.24 Solved Examples *59*
Exercise 2.1 *59*
2.25 Sets of Numbers *62*
2.26 Cardinality *63*
2.27 Cartesian Product of Sets *65*
Exercise 2.2 *67*

3. Relations **69–89**

3.1 Concept of Relation *69*
3.2 Properties of Relations *70*

3.3 Miscellaneous Examples *71*
3.4 Irreflexive Relation *72*
3.5 Asymmetric Relation *72*
3.6 Compatible Relation *72*
3.7 Universal Relation *72*
3.8 Complementary Relation *73*
3.9 Relation-Related Sets *73*
3.10 Equivalence Classes *73*
3.11 Relations on Coordinate Diagrams *75*
3.12 Tabular Form of a Relation *75*
3.13 Transitive Extension *77*
3.14 Transitive Closure *77*
3.15 Matrix Representation of Relations *79*
3.16 Relations and Digraphs *80*
3.17 Composition of Relations *84*
Exercise 3.1 85

4. Functions and Recurrence Relations 90–117

4.1 Introduction *90*
4.2 Definition *90*
4.3 One-to-One Mapping *91*
4.4 Onto-Mapping (Surjection) *92*
4.5 Bijection (One-to-One, Onto) *92*
4.6 Identity Mapping *92*
4.7 Composition of Function *92*
4.8 Associativity of Mappings *93*
4.9 Constant Function *93*
4.10 Inverse Mapping *93*
4.11 Characteristic Function of a Set *96*
4.12 Solved Examples *96*
Exercise 4.1 98
4.13 Recursion and Recurrence Relations *100*
Exercise 4.2 107
4.14 Recurrence Relations and Solutions of Recurrence Relations *107*
4.15 Generating Functions *108*
4.16 Solution of Non-Homogeneous Linear Recurrence Relations *113*
Exercise 4.3 116

5. Boolean Algebra 118–162

5.1 Introduction *118*
5.2 Partial Ordering *118*
5.3 Totally Ordered Set *118*
5.4 Dual Order *119*
5.5 Hasse Diagram *119*
5.6 Lexicographic Ordering *121*
5.7 Cover of an Element *122*
5.8 Least and Greatest Elements *122*
5.9 Minimal and Maximal Elements (Members) *123*
5.10 Upper and Lower Bounds *124*
5.11 Well-Order Set *127*
5.12 Binary and n-Ary Operations *127*
5.13 Choice Functions *127*
5.14 Axiom of Choice *128*
5.15 Well-Ordering Theorem *128*
5.16 Lattices *128*
5.17 Some Properties of Lattices *129*
5.18 Lattice as an Algebraic System *130*
5.19 Bounded Lattices *130*
5.20 Sub Lattices, Direct Products *132*
Exercise 5.1 135
5.21 Boolean Algebra *137*
5.22 Sub-Boolean Algebra *141*
5.23 Direct Products *142*
5.24 Homomorphism *142*
5.25 Atoms of Boolean Algebra *142*
5.26 Boolean Expressions and Minimization of Boolean Functions *143*
5.27 Minimization of Boolean Expressions *148*
Exercise 5.2 161

6. Logic Gates 163–183

6.1 Introduction *163*
6.2 Gates and Boolean Algebra *165*
6.3 Applications *173*
6.4 Special Sequences *179*
Exercise 6.1 180

7. Elementary Combinatorics 184–217

7.1 Introduction *184*
7.2 Basics of Counting *184*
Exercise 7.1 186
7.3 Permutations and Combinations *187*
7.4 Solved Examples *189*
7.5 Permutations with Like Elements *190*
7.6 Circular Permutations *191*
Exercise 7.2 193
7.7 Combinations *195*
7.8 Power Set *196*
7.9 Basic Identities *198*
7.10 Partition and Cross Partitions *200*
7.11 Permutations and Combinations with Unlimited Repetitions *202*
Exercise 7.3 204
7.12 The Pigeon-hole Principle *206*
Exercise 7.4 208
7.13 Binomial Theorem *208*
7.14 Solved Examples *213*
7.15 Multinomial Theorem *215*
Exercise 7.5 216

8. Graph Theory 218–346

8.1 Introduction *218*
8.2 Basic Definitions *218*
8.3 Incidence and Degree *221*
8.4 Order of a Graph *225*
8.5 Size of a Graph *225*
8.6 Solved Examples *228*
Exercise 8.1 233
8.7 Edges in Series *237*
8.8 Adjacency *237*
8.9 Matrix Representation of Graphs *238*
8.10 Linked Representation (or Adjacency Structure) *240*
8.11 The Cycle Matrix *241*
8.12 Path Matrix *242*
Exercise 8.2 243
8.13 Walks, Paths and Circuits *249*
8.14 Subgraphs *252*

8.15 Removal of Vertices and Edges from a Graph *253*
8.16 Addition of a Vertex *254*
8.17 Operations on Graphs *254*
8.18 Complement of a Graph *257*
8.19 Connected Graph *258*
8.20 Partitions *259*
8.21 Cycle Graph *262*
8.22 Path Graph *262*
8.23 Wheel Graph *262*
8.24 Bipartite Graph *263*
8.25 Solved Examples *264*
8.26 Isomorphism *265*
8.27 Solved Examples *266*
Exercise 8.3 271
8.28 Forest *274*
8.29 Cut Vertex *275*
8.30 Cut Edge (Bridge) *275*
8.31 Cut Set *275*
8.32 Separable and Non-Separable Graphs *276*
8.33 Labeled and Weighted Graphs *276*
8.34 Connectivity *277*
Exercise 8.4 280
8.35 Trees and Some Properties of Trees *280*
8.36 Distance *282*
8.37 Spanning Tree *285*
8.38 Rooted Tree *292*
8.39 Expression Trees *294*
8.40 Binary Tree *294*
8.41 Solved Examples *297*
8.42 Complete Binary Tree *298*
8.43 Height Balanced Binary Tree *298*
8.44 B-Tree *299*
8.45 Distance Between Spanning Trees of a Graph *299*
8.46 Chord of a Graph *300*
8.47 Rank and Nullity *300*
Exercise 8.5 300
8.48 Planar Graphs *303*
8.49 Homeomorphic Graphs *309*
8.50 Dual of a Graph *310*

8.51 Solved Examples *312*

Exercise 8.6 313

8.52 Eulers Graphs *314*

Exercise 8.7 318

8.53 Hamiltonian Graphs *319*

Exercise 8.8 325

8.54 Graph Colouring *327*

Exercise 8.9 336

8.55 Digraphs *338*

8.56 Relations and Digraphs *340*

8.57 Arborescence *342*

8.58 Warshall's Algorithm *343*

Exercise 8.10 345

9. Algebraic Structures 347–403

9.1 Introduction *347*

9.2 Binary Operation *347*

9.3 General Properties *347*

Exercise 9.1 349

9.4 n-Ary Operation *350*

9.5 Algebraic Structures (Algebraic Systems) *350*

9.6 Semi-group *351*

9.7 Homomorphism of Semi-groups *351*

9.8 Isomorphism of Semi-groups *352*

9.9 Monoid *352*

9.10 Monoid Homomorphism *353*

9.11 Groups *353*

9.12 Solved Examples *354*

9.13 Addition Modulo m *358*

9.14 Multiplication Modulo P *359*

9.15 Additive Group of Integers Modulo m *360*

9.16 Congruences *360*

Exercise 9.2 361

9.17 Elementary Properties of Groups *362*

9.18 Alternative Postulates for a Group *365*

9.19 Order of an Element *366*

9.20 Sub-group *368*

9.21 Centre of a Group *370*

9.22 Cosets *370*

9.23 Index of a Sub-group *373*

Exercise 9.3 374

9.24 Isomorphism *375*

9.25 Properties of Isomorphism *376*

9.26 Cyclic Groups *377*

Exercise 9.4 379

9.27 Normal Sub-groups *380*

9.28 Permutation Groups *382*

9.29 Cyclic Permutation *385*

9.30 Group Homomorphism *389*

9.31 Kernel of a Homomorphism *390*

9.32 Solved Examples *392*

Exercise 9.5 394

9.33 Algebraic System with Two Binary Operations *395*

9.34 Special Types of Rings *396*

9.35 Properties of Rings *397*

9.36 Sub-Rings *399*

9.37 Coefficients and Exponents *399*

Exercise 9.6 402

10. Finite State Machines 404–434

10.1 Introduction *404*

10.2 Transition Table *405*

10.3 Transition Diagram (State Diagram) *406*

10.4 Finite State Machine (Alternative Definition) *407*

10.5 Equivalence of Finite State Machines *410*

10.6 Covering *411*

10.7 Finite State Homomorphism *414*

Exercise 10.1 416

10.8 Formal Language, Grammar *419*

10.9 Finite Automata *423*

Exercise 10.2 428

10.10 Non-Deterministic Finite Automation (NDFA) *429*

10.11 Finite Automata with Outputs *433*

Bibliography 435

Index 436–440

1

Mathematical Logic

1.1 INTRODUCTION

In this chapter we shall study mathematical logic, which is concerned with all kinds of reasoning. Mathematical logic has two aspects. On one hand it is analytical theory of art of reasoning whose goal is to systematize and codify principles of valid reasoning. It may be used to judge the correctness of statements which make up the chain. In this aspect logic may be called ‘classical’ mathematical logic. The other aspect of Mathematical logic is inter-related with problems relating the foundation of Mathematics. G. Frege (1884–1925) developed the idea, regarding a mathematical theory as applied system of logic.

Principles of logic are valuable to problem analysis, programming and logic design.

1.2 STATEMENTS

A statement is a declarative sentence which is either true or false but not both. The truth or falsity of a statement is called its truth value. The truth values ‘True’ and ‘False’ of a statement are denoted by T and F respectively. They are also denoted by 1 and 0.

Example 1: Bangalore is in India.

Example 2: $3 + 7 = 9$.

Example 3: Roses are red.

Statements are usually denoted by the letters p, q, r, ... The capital letters A, B, C, ..., P, Q, ... with the exception of T and F are also used.

1.3 LAWS OF FORMAL LOGIC

Now we state two famous laws of Formal Logic.

1.3.1 Law of Contradiction

According to the law of Contradiction the same predicate cannot be both affirmed and denied precisely of the same subject; i.e., for every proposition p it is not the same that p is both true and false.

1.3.2 Law of Excluded Middle

If p is a statement (proposition), then either p is true or p is false, and there cannot be middle ground.

1.4 CONNECTIVES AND COMPOUND STATEMENTS

Statements can be connected by words like ‘not’, ‘and’, etc.

These words are known as logical connectives. The statements which do not contain any of the connectives are called atomic statements or simple statements.

The common connectives used are: negation (~) [or (¬)], and (∧) or (∨), if ... then (→), if and only if (↔), equivalence (≡) or (⇔). We will use these connectives along with symbols to combine various simple statements.

1.4.1 Compound Statement

A statement that is formed from atomic (Primary) statements through the use of sentential connectives is called a compound statement.

1.4.2 Truth Table

The table showing the Truth values of a statement formula is called ‘Truth Table’.

1.4.3 Conjunction

A compound statement obtained by combining two simple statements say p and q, by using the connective “and” is called conjunction, i.e., the conjunction of two statements p and q is the statement $p \wedge q$. It is read as “p and q”.

The statement $p \wedge q$ has the truth value T, whenever both p and q have the truth value T, otherwise $p \wedge q$ has the truth value F. The above property can also be written in the form of the table below, which we regard as defining $p \wedge q$:

Table 1.1 *Truth table for conjunction*

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

Example 1: Form the conjunction of

p: Delhi is in India.

q: 5 + 7 = 12.

Solution: $p \wedge q$ is the statement:

“Delhi is in India and 5 + 7 = 12”

Example 2: From the conjunction of

p: It is raining.

q: The sun is shining.

Solution: $p \wedge q$. It is raining and the sun is shining.

Example 3: Construct a Truth Table for the conjunction of "$n > 3$" and "$n < 10$" when $n \in N$.

Solution: When $n > 3$ and $n < 10$ are true, the conjunctive statement "$n > 3$ and $n < 10$" is true. The Truth Table is given below:

Table 1.2

$n > 3$	$n < 10$	$n > 3$ and $n < 10$
T	T	T
T	F	F
F	T	F
F	F	F

1.4.4 Disjunction

Any two simple statements can be combined by the connective "or" to form a statement called the disjunction of the statements; i.e., if p and q are simple statements, the sentence "p or q" is the disjunction of p and q.

The disjunction of p and q is denoted symbolically by $p \vee q$

$p \vee q$ is read as " p or q"

If p is 'True' or q is 'True' or both p and q are 'True', then $p \vee q$ is true, otherwise $p \vee q$ is false. The truth table of $p \vee q$ is given below:

Table 1.3 *Truth table of* $p \vee q$

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

Example 1: Let p: $5 + 2 = 7$, q: $9 + 2 = 10$ then

$$p \vee q: 5 + 2 = 7 \text{ or } 9 + 2 = 10$$

Example 2: Let p: Roses are red

q: Violets are blue, then,

$p \vee q$: Roses are red or violets are blue.

1.4.5 Negation

Let p be any simple statement, then the negation of p is formed by writing "it is false that" before p. The negation of p is also obtained by writing "p is false".

The negation is p is denoted by $\sim p$.

If the statement p is true, then "$\sim p$ is false" and if p is false then $\sim p$ is true. The Truth Table for negation is given below:

Table 1.4

p	$\sim p$
T	F
F	T

Example 1: Let p: Tajmahal is in New York.

Then the negation of p is

$\sim p$: it is false that Tajmahal is in New York.

Example 2: Form the negation of the statement

p: It is cold

Solution: $\sim p$: It is not cold.

Example 3: Form the negation of the statement

p: $n > 12$

Solution: $\sim p$: $n > 12$ is false.

1.5 PROPOSITION

If $p, q, r, s, ...$ are Simple Statements then the Compound Statement $P(p, q, r, s, ...)$ is called a Proposition. The statement $p, q, r, ...$ are called the Sub-statements or Variables of P.

The truth value of proposition P depends on the truth values of the variables, $p, q, r, ...$ If the truth values of the variables are known to us, then we can find the truth value of the proposition P. A truth table is a simple way to show this relationship.

Example: Find the truth table of the Proposition $\sim p \wedge q$

Solution: The truth table of $\sim p \wedge q$ is:

Table 1.5 *Truth table* $\sim p \wedge q$

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

1.6 SOLVED EXAMPLES

Example 1: Let p be "it is cold" and q be "it is raining". Give a simple verbal sentence which describes each of the following:

(*i*) $\sim p$ (*ii*) $\sim p \wedge \sim q$

Solution:

(*i*) $\sim p$: It is not cold

(*ii*) $\sim p \wedge \sim q$: It is not cold and it is not raining.

Example 2: Let p be "He is tall" and let q be "He is Handsome". Write each of the following statements in symbolic form using p and q.

(*i*) He is tall and handsome.

(*ii*) He is neither tall nor handsome.

Solution: (*i*) $p \wedge q$ (*ii*) $\sim p \wedge \sim q$

Example 3: Write the disjunction of:

Roses are red. Violets are blue.

Solution: Let p: Roses are red

q: Violets are blue then the disjunction of p and q is $p \vee q$: Roses are red or violets are blue.

Example 4: Determine the truth value of each of the following statements (Propositions):

(*i*) 3 + 5 = 8 or 2 +1 = 9

(*ii*) 4 +3 = 7 and 5 + 2 = 7

(*iii*) Agra is in England or 1 + 9 = 8

Solution: (*i*) Let p: 3 + 5 = 8, q: 2 + 1 = 9

p is true, q is false

hence $p \vee q$ is true

i.e., Truth Value of $p \vee q$ is T

(*ii*) Let p: 4 + 3 = 7, q: 5 + 2 = 7

p is true and q is true $\Rightarrow$ $p \wedge q$ is true (T)

(*iii*) Let p: Agra is in England

q: 1 + 9 = 8

p is false; q is false $\Rightarrow$ $p \vee q$ is false.

Example 5: Construct a truth table for $p \wedge \sim p$.

Solution: The truth table for $p \wedge \sim p$ is given below:

Table 1.6

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

Example 6: Construct the truth table for $p \vee \sim p$

Solution:

Table 1.7

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

Example 7: Find the truth table for $p \wedge (q \vee r)$

Solution:

Table 1.8

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

Example 8: Find the truth table for $\sim(\sim p)$ (Double negation)

Solution:

Table 1.9

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

EXERCISE 1.1

1. Determine the truth value of each of the following:

(*a*) 4 + 2 = 6 and 2 + 2 = 4

(*b*) 5 + 4 = 9 and 3 + 3 = 5

(*c*) 6 + 4 = 10 and 1 + 1 = 3

(*d*) Charminar is in Hyderabad or 7 + 1 = 6

(*e*) It is not true that Delhi is in Russia

(*f*) It is false that 3 + 3 = 6 and 2 + 2 = 8

2. Construct truth tables for the following:

(*a*) $\sim(p \vee q)$

(*b*) $\sim(p \vee \sim q)$

(*c*) $(p \wedge q) \vee (p \wedge q)$

(*d*) $(p \vee q) \vee \sim p$

(*e*) $\sim(\sim p \vee \sim q)$

(*f*) $p \wedge (q \wedge p)$

(*g*) $p \vee \sim(p \wedge q)$

3. Write the negation of each statement

(*a*) Violets are blue (*b*) Delhi is in America

(*c*) 3 + 3 = 7

4. Let *p* be “Mark is rich” and *q* be “Mark is happy”

Write each of the following in symbolic form.

(*a*) Mark is poor but happy

(*b*) Mark is neither rich nor happy

(*c*) Mark is either rich or happy

(*d*) Mark is either poor or else; he is both rich and happy

5. Let *p* be “It is cold” and let *q* be “It is raining”

Give a simple verbal sentence which describes each of the following statements:

(*a*) $\sim p$ (*b*) $p \wedge q$

(*c*) $p \vee q$ (*d*) $\sim p \wedge \sim q$

6. Write the symbols for connectives in the following sentences:

(*a*) Either *p* or not *p* (*b*) *p* and not *q*

(*c*) not *p* or not *q* (*d*) not *p* and *q*

7. Write the conjunction of:

(*a*) It is raining; It is snowing (*b*) 4 + 7 = 11; 2 × 4 = 7

8. Let *p* be “He is tall” and *q* be “He is handsome”

Write each of the following statements in symbolic form using *p* and *q*

(*a*) He is tall and handsome

(*b*) He is tall but not handsome

(*c*) He is neither tall nor handsome

Answers:

2. (*a*)

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

(*b*)

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

(*c*)

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

(*d*)

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

(*e*)

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

(*f*)

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

(*g*)

p	q	$p \wedge q$	$\sim(p \wedge q)$	$p \wedge \sim(p \wedge q)$
T	T	T	F	T
T	F	F	T	T
F	T	F	T	F
F	F	F	T	T

3. (*a*) Violets are not blue

(*b*) Delhi is not in America

(or It is not the case that Delhi is in America)

(*c*) 3 + 3 = 7
(or It is not the case that 3 + 3 = 7)

4. (*a*) $\sim p \wedge q$ (*b*) $\sim p \wedge \sim q$ (*c*) $p \vee \sim q$ (*d*) $\sim p \vee (p \wedge \sim q)$

5. (*a*) It is not cold (*b*) It is cold and raining
(*c*) It is cold or it is raining (*d*) It is not cold and it is not raining.

6. (*a*) $p \vee \sim p$ (*b*) $p \wedge \sim q$ (*c*) $\sim p \vee \sim q$ (*d*) $\sim p \wedge q$

7. (*a*) It is raining and it is snowing
(*b*) 4 + 7 = 11 and 2 × 4 = 7

8. (*a*) $p \wedge q$ (*b*) $\sim p \wedge \sim q$ (*c*) $\sim p \wedge \sim q$

1.7 CONDITIONAL STATEMENTS

1.7.1 Conditional $p \rightarrow q$

If p and q are any two statements then the statement $p \rightarrow q$ which is read as "if p then q" is called a Conditional statement.

The symbol → is used to denote connective "If ... then"

The conditional $p \rightarrow q$ can also be read:

(*a*) p only if q (*b*) p implies q (*c*) p is sufficient for q (*d*) q if p

The conditional $p \rightarrow q$ has two simple statements p and q connected by "if ... then"

The statement p is called the antecedent and the statement q is called the consequent (or conclusion). If p is true and q is false, then conditional $p \rightarrow q$ is false. In other cases $p \rightarrow q$ is true.

The truth values of $p \rightarrow q$ are given in Table 1.10.

Table 1.10 *Truth table for* $p \rightarrow q$

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

Example 1: If Delhi is in India, then 3 + 3 = 6

Example 2: Let p: He is a graduate
q: He is a lawyer then,
$p \rightarrow q$: If he is a graduate, then he is a lawyer.

1.7.2 Biconditional

A statement of the form "p if and only if q" is called a Biconditional statement. It is denoted by $p \rightleftarrows q$ (or by $p \leftrightarrow q$).

A Biconditional statement contains the connective "if and only if " and has two conditions. If p and q have the same truth value, then $p \leftrightarrow q$ is true. The truth values $p \leftrightarrow q$ are given in Table 1.11.

Table 1.11 *Truth table for* $p \leftrightarrow q$

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

Example 1: Bangalore is in India, if and only if 4 + 4 = 8.

Example 2: 3 + 3 = 6 if and only if 4 + 3 =7.

1.7.3 Converse, Inverse and Contrapositive Propositions

If $p \rightarrow q$, is a conditional statement, then

(*a*) $q \rightarrow p$ is called its converse

(*b*) $\sim p \rightarrow \sim q$ is called its inverse

(*c*) $\sim q \rightarrow \sim p$ is called its contrapositive.

The truth values of these propositions are given in Tables 1.12, 1.13 and 1.14, respectively.

Table 1.12 *Truth table for the converse of* $p \rightarrow q$

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

Table 1.13 *Truth table for the inverse of* $p \rightarrow q$

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

Table 1.14 *Truth table for contraposition*

p	q	$\sim q$	$\sim p$	$\sim q \to \sim p$
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

Example: Write the contrapositive of the implication

"if it is raining, then I get wet"

Solution: let p: It is raining

q: I get wet

then the contrapositive is

$\sim q \to \sim p$: If I do not get wet, then it is not raining.

1.8 WELL FORMED FORMULAS

Statement formulas contain one or more simple statements and some connectives. If p and q are any two statements, then

$$p \vee q, (p \wedge q) \vee (\sim p), (\sim p) \wedge q$$

are some statement formulas derived from the statement variables p and q where p and q called the components of the statement formulas. A statement formula has no truth value. It is only when the statement variables in a statement formula are replaced by definite statements that we get a statement, which has a truth value that depends upon the truth values of the statements used in replacing the variables. A statement formula is a string consisting of variables, parentheses and connective symbols. A statement formula is called a well formed (w f f) if it can be generated by the following rules:

1. A statement variable p standing alone is a well formed formula.
2. If p is a wellformed formula, then $\sim p$ is a well formed formula.
3. If p and q are wellformed formulas, then $(p \wedge q)$, $(p \vee q)$, $(p \to q)$ and $(p \leftrightarrow q)$ are well formed formulas.
4. A string of symbols is a well formed formula if and only if it is obtained by finitely many applications of the rules 1, 2 and 3.

According to the above recursive definition of a well formed formula $\sim(p \vee q)$, $(\sim p \wedge q)$, $(p \to (p \vee q))$ are well formed formulas.

A statement formula is not a statement and has no truth values. But if we substitute definite statements in place of variables in given formula we get a statement. The truth value of this resulting statement depends upon the truth values of the statements substituted for the variables, which appears as one of the entries in the final column of the truth table constructed. Therefore the truth table of a well formed formula is the summary of truth values of the resulting statements for all possible assignments of values to the variables appearing in the formula. The final column entries of the truth table of a well formed formula gives the truth values of the formula.

1.9 TAUTOLOGY

A statement formula that is true for all possible values of its propositional variables is called a Tautology.

Example 1: $(p \vee q) \leftrightarrow (q \vee p)$ is a tautology.

Example 2: $p \vee \sim p$ is a tautology.

1.10 CONTRADICTION

A statement formula that is always false is called a contradiction (or absurdity).

Example: $p \wedge \sim p$ is an absurdity.

1.11 CONTINGENCY

A statement formula that can either be true or false depending upon the truth values of its propositional variables is called a contingency.

Example: $(p \to q) \wedge (p \wedge q)$ is a contingency.

1.12 LOGICAL EQUIVALENCE

Two propositions P and Q are said to be logically equivalent or simply equivalent if $P \to Q$ is a tautology.

Example: $\sim(p \wedge q)$ and $\sim p \vee \sim q$ are logically equivalent.

Two formulas may be equivalent, even if they do not contain the same variables. Two statement formulas P and Q are equivalent if $P \rightleftarrows Q$ is a tautology and conversely, if $P \rightleftarrows Q$ is a tautology then P and Q are equivalent. If "P is equivalent Q" then we can represent the equivalence by writing "$P \Leftrightarrow Q$" which can also be written as $P \Leftrightarrow Q$. The symbol "$\Leftrightarrow$" is not a connective. We usually drop the quotation marks.

1.13 SOLVED EXAMPLES

Example 1: The converse of a statement is given. Write the inverse and the contrapositive statements "if I come early, then I can get the car".

Solution: Inverse: "If I cannot get the car, then I shall not come early"

Contrapositive: If I do not come early, then I cannot get the car.

Example 2: The inverse of a statement is given. Write the converse and contrapositive of the statement. "If a man is not a fisherman, then he is not a swimmer".

Solution: Converse: "If he is a swimmer, then the man is a fisherman".

Contrapositive: "If he is not a swimmer, then the man is not a fisherman".

Example 3: Determine a truth table of $\sim p \to (q \to p)$

Solution:

Table 1.15

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

Example 4: Show that $p \wedge \sim p$ is a contradiction.
Solution: The truth table for $p \wedge \sim p$ is given below:

Table 1.16

p	$\sim p$	$p \wedge \sim p$
T	F	F
T	F	F

$p \wedge \sim p$ is always false, hence $p \wedge \sim p$ is a contradiction.

Example 5: Show that $p \vee \sim p$ is a tautology.
Solution: We construct the truth table for $(p \vee \sim p)$

Table 1.17

p	$\sim p$	$(p \vee \sim p)$
T	F	T
T	T	T

$p \vee \sim p$ is always true.

Hence $p \vee \sim p$ is a tautology.

Example 6: Show that $(p \wedge q) \rightarrow p$ is tautology.
Solution: Let us construct the truth table for the statement $(p \wedge q) \rightarrow p$

Table 1.18

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

In Table 1.18, we notice that the column (4) has all its entries as T. Hence $(p \wedge q) \to p$ is a tautology.

Example 7: Show that $\sim(p \to q) \equiv (p \wedge \sim q)$

Solution: Let us construct the truth table for the given propositions:

Table 1.19

p	q	$p \to q$	$\sim(p \to q)$	$\sim q$	$p \wedge \sim q$
T	T	T	F	F	F
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	F	T	F

From the truth table it is clear that the truth values of $\sim(p \to q)$ and $p \wedge \sim q$ are identical.

Hence $\sim(p \to q) \equiv p \wedge \sim q$.

1.14 LAWS OF LOGIC

1. Idempotent Laws:

(*a*) $p \vee p \equiv p$ (*b*) $p \wedge p \equiv p$

2. Commutative Laws:

(*a*) $p \vee p \equiv q \vee p$ (*b*) $p \wedge q \equiv q \wedge p$

3. Associative Laws:

(*a*) $(p \vee q) \vee r \equiv p \vee (q \vee r)$ (*b*) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

4. Distributive Laws:

(*a*) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(*b*) $p \wedge (q \vee r) \equiv (p \vee q) \vee (p \wedge r)$

5. Identity Laws:

(*a*) (*i*) $p \vee f \equiv p$ (*ii*) $p \vee t \equiv t$

(*b*) (*i*) $p \wedge f \equiv f$ (*ii*) $p \wedge t \equiv p$

6. Complement Laws:

(*a*) (*i*) $p \wedge \sim p \equiv t$ (*ii*) $p \wedge \sim p \equiv f$

(*b*) (*i*) $\sim\sim p \equiv p$ (*ii*) $\sim t \equiv f, \sim f \equiv t$

7. De Morgan's Laws:

(*a*) $\sim(p \vee q) \equiv \sim p \wedge \sim q$ (*b*) $\sim(p \wedge q) \equiv \sim p \vee \sim q$

where t and f are used to denote the variables which are restricted to the truth values true and false respectively.

1.15 THE DUALITY PRINCIPLE

The Principle of duality states that any established result involving statement formulas and connectives $\vee$ and $\wedge$ gives a corresponding dual result by replacing $\wedge$ by $\vee$ and $\vee$ by $\wedge$. If the formula contains special variables t and f, the corresponding dual is obtained by replacing t by f and f by t. The connectives $\wedge$ and $\vee$ are called duals of each other.

Definition 1.1: Two statement formulas P and P^* are said to be duals of each other if either one can be obtained from the other by replacing $\wedge$ and $\vee$ and $\vee$ by $\wedge$.

Example: Write the duals of

(*a*) $(p \wedge q) \vee r$ (*b*) $(p \wedge q) \vee r$ (*c*) $\sim(p \wedge q)$

Solution: The duals are

(*a*) $(p \vee q) \wedge r$ (*b*) $(p \vee q) \wedge r$ (*c*) $\sim(p \vee q)$

1.16 SOLVED EXAMPLES

Example 1: Simplify the following statements:

(*a*) $\sim(p \vee \sim q)$ (*b*) $\sim(\sim p \wedge q)$ (*c*) $\sim(\sim p \vee \sim q)$ (*d*) $(p \vee q) \wedge \sim p$

Solution:

(*a*) $\sim(p \vee \sim q) = \sim p \wedge \sim\sim q$ (De Morgan's law)

$= \sim p \wedge q$

(*b*) $\sim(\sim p \wedge q) = \sim\sim p \vee \sim q$ (De Morgan's law)

$= p \vee \sim q$

(*c*) $\sim(\sim p \wedge \sim q) = \sim\sim p \vee \sim q$

$= p \vee \sim q$

(*d*) $(p \vee q) \wedge \sim p = \sim p \wedge (p \vee q)$

$= (\sim p \wedge p) \vee (\sim p \wedge q)$

$= f \vee (\sim p \wedge q)$

$= \sim p \wedge q$

Example 2: Show that

$$(\sim p \wedge (\sim q \wedge r) \vee (q \wedge r) \vee (p \wedge r) \Leftrightarrow r$$

where $\Leftrightarrow$ is the symbol for equivalence

Solution: $\sim p \wedge (\sim q \wedge r) \vee (q \wedge r) \vee (p \wedge r)$

$\Leftrightarrow (\sim p \wedge (\sim q \wedge r) \vee [(q \vee p) \wedge r]$

$\Leftrightarrow [(\sim p \wedge \sim q) \wedge r] \vee [(q \vee p) \wedge r]$

$\Leftrightarrow [(\sim p \wedge \sim q) \vee [(q \vee p)] \wedge r$

$\Leftrightarrow [(\sim p \vee \sim q) \vee (p \vee q)] \wedge r$

$\Leftrightarrow t \wedge r$ (t denotes tautology)

$\Leftrightarrow r$

Example 3: Simplify

(*i*) $p \vee (p \wedge q)$ (*ii*) $(p \vee q) \wedge (\sim p \wedge q)$

Solution: (*i*) $p \vee (p \wedge q) = (p \vee t) \wedge (p \vee q)$

$= p \wedge (t \vee q)$ (t: tautology)

$= p \wedge t$

$= p$

(*ii*) $(p \vee q) \wedge (\sim p \wedge q)$

$= (\sim p \wedge \sim q) \vee (\sim p \wedge q)$

$= \sim p \wedge (\sim q \vee q)$

$= \sim p \wedge t$ (t: tautology)

$= \sim p$

Example 4: Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

Solution: Let us construct the truth table:

Table 1.20

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

All the entries in the last column of the truth table are True (T). Hence given proposition is a tautology.

Example 5: Show that

$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

Solution: We construct the truth table for given propositions:

Table 1.21

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

From the truth table it is clear that the truth values of $\sim(p \rightarrow q)$ and $p \wedge \sim q$ are identical. Hence

$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

Example 6: Show that

$$\sim(p \leftrightarrow q) \equiv \sim p \leftrightarrow q \equiv p \leftrightarrow \sim q$$

Solution: We prove the equivalence by means of a truth table.

Table 1.22

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

The truth values of columns (4), (6) and (8) are alike; which proves the equivalence of the formulas $\sim(p \leftrightarrow q)$, $\sim p \leftrightarrow q$, and $p \leftrightarrow \sim q$.

Example 7: There are two restaurants next to each other. One has a sign that says "Good food is not cheap", and the other has the sign that says "cheap food is not good".

Are the signs saying the same thing?

If so verify.

Solution: Let p: food is good
q: food is cheap

Then we have, $\sim p$: food is not good
$\sim q$: food is not cheap

Therefore, the given statements are

$p \rightarrow \sim q$: Good food is not cheap

$q \rightarrow \sim p$: Cheap food is not good

The truth table for the statements is given below:

Table 1.23

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

From the table, it is clear that both the signs say the same thing.

1.17 LOGICAL IMPLICATION

We state the following theorem:

Theorem 1.1: Let $P(p_1, p_2, ...)$ and $Q(p_1, p_2,...)$ be two propositions. Then the following conditions are equivalent:

1. $\sim P(p_1, p_2, ...) \vee Q(p_1, p_2, ...)$ is a Tautology.
2. $P(p_1, p_2, ...) \wedge Q(p_1, p_2, ...)$ is a Contradiction.
3. $P(p_1, p_2, ...) \rightarrow Q(p_1, p_2, ...)$ is a Tautology.

Definition 1.2: A proposition $P\,(p_1, p_2, ...)$ is said to logically imply a proposition $Q\,(p_1, p_2, ...)$ if one of the conditions in Theorem 1.1 holds.

If $P\,(p_1,\ p_2,\ ...)$ logically implies $Q\,(p_1,\ p_2,\ ...)$ then we symbolically denote it by writing $P\,(p_1, p_2, ...) \Rightarrow Q\,(p_1, p_2, ...)$

Example 1: $(p \wedge q) \wedge \sim(p \vee q)$ is a contradiction.

Hence $p \wedge q \Rightarrow p \vee q$

Example 2: $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is a tautology.

Hence $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$

Theorem 1.2: The relation in propositions defined by

$$P\,(p_1, p_2, ...) \Rightarrow Q\,(p_1, p_2, ...)$$

is reflexive, anti-symmetric and transitive.

Note: The symbols $\rightarrow, \Rightarrow$ are not the same $\Rightarrow$ is not a connective nor $P \Rightarrow Q$ is a statement formula (proposition). $P \Rightarrow Q$ defines a relation in composite propositions $P \rightarrow Q$. The symbol $\rightarrow$ is a connective and note that $P \rightarrow Q$ is just a proposition.

1.18 OTHER CONNECTIVES

We now introduce the connectives NAND, NOR which have useful applications in the design of Computers.

The word NAND is a combination of "NOT" and "AND" where "NOT" stands for negation and "AND" for the conjunction. It is denoted by the symbol $\uparrow$.

If P and Q are two formulas then $P \uparrow Q \leftrightarrow \sim(P \wedge Q)$

The connective $\uparrow$ has the following equivalence:

$$P \uparrow P \leftrightarrow \sim(P \wedge P) \leftrightarrow \sim P \vee \sim P \Leftrightarrow \sim P$$

$$(P \uparrow Q) \uparrow (P \uparrow Q) \leftrightarrow \sim (P \uparrow Q) \leftrightarrow P \wedge Q$$

$$(P \uparrow P) \uparrow (Q \uparrow Q) \leftrightarrow \sim P \uparrow \sim Q \Leftrightarrow \sim (\sim P \wedge \sim Q) \leftrightarrow P \vee Q$$

The connective NAND is commutative but not associative:

i.e., $P \uparrow Q \leftrightarrow Q \uparrow P$ but $P \uparrow (Q \uparrow R) \leftrightarrow \sim P \vee (Q \wedge R)$ and

$(P \uparrow Q) \uparrow R \leftrightarrow \sim (P \wedge Q) \sim R$. Therefore the connective $\uparrow$ is not associative.

The connective NOR is a combination of "NOT" and "OR", where NOT stands for negation and "OR" stands for the disjunction.

The connective NOR is denoted by the symbol $\downarrow$.

The connective $\downarrow$ has the following equivalence:

$$P \downarrow P \leftrightarrow \sim (P \vee P) \leftrightarrow \sim P \wedge \sim P \Leftrightarrow \sim P$$

$$(P \downarrow P) \downarrow (P \downarrow Q) \leftrightarrow \sim (P \downarrow Q) \leftrightarrow P \vee Q$$

$$(P \downarrow P) \downarrow (Q \downarrow Q) \leftrightarrow \sim P \uparrow \sim Q \leftrightarrow P \wedge Q$$

The connective $\downarrow$ is commutative, but not associative, i.e.

$$P \downarrow Q \Leftrightarrow Q \downarrow P \text{ but } (P \downarrow Q) \downarrow Q \leftrightarrow (P \vee Q) \wedge \sim R$$

$$P \downarrow (Q \downarrow R) \leftrightarrow \sim P \wedge (Q \vee R)$$

Therefore the connective $\downarrow$ is not associative.

The connectives $\wedge, \vee, \sim$ can be expressed in terms of the connective $\downarrow$ as follows:

(*i*) $\sim p \equiv p \downarrow p$ (*ii*) $\sim q \equiv q \downarrow q$

(*iii*) $p \wedge q \equiv (p \downarrow p) \downarrow (q \downarrow q)$ (*iv*) $p \vee q \equiv (p \downarrow q) \downarrow (p \downarrow q)$

Let us verify the above by means of the following truth tables:

Table 1.24

p	q	$\sim p$	$P \downarrow p$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	T

From the above truth table it is clear that $\sim p \equiv p \downarrow p$

Similarly, $\sim q \equiv q \downarrow q$

Now consider the table

Table 1.25

p	q	$p \wedge q$	$p \downarrow p$	$q \downarrow q$	$(p \downarrow p) \downarrow (q \downarrow q)$
(1)	(2)	(3)	(4)	(5)	(6)
T	T	T	F	F	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	F	T	T	F

The identical truth values of columns (3) and (6) reveal that

$$p \wedge q \equiv (p \downarrow p) \downarrow (q \downarrow q)$$

In order to verify (*iv*) we construct the truth table

Table 1.26

p (1)	q (2)	$p \vee q$ (3)	$p \downarrow q$ (4)	$(p \downarrow q) \downarrow (p \downarrow q)$ (5)
T	T	T	F	T
T	F	T	F	T
F	T	T	F	T
F	F	F	T	F

The truth values of columns (3) and (5) are alike, which proves the equivalence

$$p \vee q \equiv (p \downarrow q) \downarrow (p \downarrow q)$$

1.19 NORMAL FORMS

Definition 1.3: If a given statement formula A ($p_1, p_2, \ldots p_n$) involves n atomic variables, we have 2^n possible combinations of truth values of statements replacing the variables.

The formula A is a tautology if A has the truth value T for all possible assignments of the truth values to the variables p_1, p_2, ... p_n and A is called a contradiction if A has the truth value F for all possible assignments of the truth values of the n variables. A is said to be satisfiable if A has the truth value T for atleast one combination of truth values assigned to $p_1, p_2, \ldots p_n$.

The problem of determining whether a given statement formula is a Tautology, or a Contradiction is called a decision problem.

The construction of truth table involves a finite number of steps, but the construction may not be practical. We therefore reduce the given statement formula to normal form and find whether a given statement formula is a Tautology or Contradiction or atleast satisfiable.

A formula, which is a product (conjunction) of the variables and their negations is called an Elementary product.

If p and q are atomic values then p, $\sim p$, $\sim p \wedge q$, $p \wedge \sim p$ are some examples of Elementary products.

The sum of (disjunction) of variables and their negations in a formula is called Elementary sum.

If p and q are any two atomic variables p, $\sim p \vee q$, $p \vee \sim p$ and $\sim q \vee p \vee \sim p$ are some examples of Elementary sums.

1.19.1 Disjunctive Normal Form

Definition 1.4: Let A denote a given formula. Another formula B which is equivalent to A is called a Disjunctive normal form of A if B is a sum of elementary products.

A disjunctive normal form of a given formula is constructed as follows:

(*i*) Replace '→', '↔' by using the logical connectives $\wedge$, $\vee$ and ~.

(*ii*) Use De Morgan's laws to eliminate ~ before sums or products.

(*iii*) Apply distributive laws repeatedly and eliminate product of variables to obtain the required normal form.

Example 1: Obtain disjunctive normal form of $p \wedge (p \rightarrow q)$

Solution: $p \wedge (p \to q) \equiv p \wedge (\sim p \vee q) \equiv (p \wedge \sim p) \vee (p \wedge q)$

Example 2: Obtain disjunctive normal form of

$$p \vee (\sim p \to (q \vee (q \to \sim r)))$$

Solution:

$$\begin{aligned} & p \vee (\sim p \to (q \vee (q \to \sim r))) \\ \equiv\ & p \vee (\sim p \to \mathrm{q} \vee (\sim q \vee \sim r))) \\ \equiv\ & p \vee (p \vee (q \vee (\sim q \vee \sim r))) \\ \equiv\ & p \vee p \vee q \vee \sim q \vee \sim r \\ \equiv\ & p \vee q \vee \sim q \vee \sim r \end{aligned}$$

Therefore, the disjunctive normal form of

$$p \vee (\sim p \to (q \vee (\sim q \to \sim r))) \text{ is } p \vee q \vee \sim q \sim r$$

1.19.2 Conjunctive Normal Form

Let A denote a given formula, another formula B which is equivalent to A is called conjunctive normal formula if B is a product of an elementary sum.

Example: Obtain conjunctive normal of

$$p \wedge (p \to q)$$

Solution: $p \wedge (p \to q) \equiv p \wedge (\sim p \vee q)$

Hence $p \wedge (\sim p \vee q)$ is the conjunctive normal form of $p \wedge (p \to q)$

1.19.3 Principal Disjunctive Normal Form

Let p and q be the two statement variables. Then $p \wedge q$, $p \wedge \sim q$, $\sim p \wedge q$, and $\sim p \wedge \sim q$ are called minterms of p and q. They are called Boolean Conjunctives of p and q. Each minterm has the truth value T for exactly one combination of truth values of the variables p and q. There are 2^2 possible minterms for the two variables p and q. Note that none of the minterms should contain both a variable and its negation. The number of minterms in n variables is 2^n.

We now introduce one more normal form called the principal normal form in the next definition.

Definition 1.5: If A is a given formula, then an equivalent formula B, consisting of disjunctives of minterms only is called the Principal disjunctive normal form of the formula A.

The principle disjunctive normal formula of A is also called the sum-of-products canonical form of A.

Example: Obtain the principal disjunctive normal form of $(\sim p \vee \sim q) \to (\sim p \wedge r)$

Solution: $(\sim p \vee \sim q) \to (\sim p \wedge r)$

$$\begin{aligned} & \Leftrightarrow \sim(\sim p \vee \sim q) \vee (\sim p \wedge r) \\ & \Leftrightarrow \sim (\sim(p \wedge q)) \vee (\sim p \wedge r) \\ & \Leftrightarrow (p \wedge q) \vee (\sim p \wedge r) \\ & \Leftrightarrow (p \wedge q \wedge (r \vee \sim r)) \vee (\sim p \wedge r \wedge (q \vee \sim q)) \\ & \Leftrightarrow (p \wedge q \wedge r) \vee (p \wedge q \wedge \sim r) \vee (\sim p \wedge r \wedge q) \vee (\sim p \wedge r \wedge \sim q) \end{aligned}$$

The principal disjunctive normal form of the given formula is

$$(p \wedge q \wedge r) \vee (p \wedge q \wedge \sim r) \vee (\sim p \wedge q \wedge r) \vee (\sim p \wedge \sim q \wedge r)$$

1.19.4 Principal Conjunctive Normal Form

The dual of a minterm is called a Maxterm. For a given number of variables the maxterm consists of disjunctions in which each variable or its negation, but not both, appears only once. Each of the maxterm has the truth value *F* for exactly one combination of the truth values of the variables. Now we define the principal conjunctive normal form.

Definition 1.6: If *A* is a given formula, then an equivalent formula *B* is called principle conjunctive normal form of *A* if *B* is a product of maxterms.

The principal conjunctive normal form of *A* is also called the Product-of-sums canonical form.

Example: Obtain the principal conjunctive normal form of

$$(p \wedge q) \vee (\sim p \wedge r)$$

Solution: $(p \wedge q) \vee (\sim p \wedge r)$

$$\Leftrightarrow ((p \wedge q) \vee \sim p) \vee ((p \wedge q) \vee r)$$

$$\Leftrightarrow (p \vee \sim p) \wedge (q \vee \sim p) \wedge (p \vee r) \wedge (q \vee r)$$

$$\Leftrightarrow (q \vee \sim p \vee (r \wedge \sim r)) \wedge (p \vee r \vee (q \wedge \sim q)) \wedge (q \vee r \vee (p \wedge \sim p))$$

$$\Leftrightarrow (q \vee \sim p \vee r) \wedge (q \vee \sim p \vee \sim r) \wedge (p \vee r \vee q)$$

$$\wedge (p \vee r \vee \sim q) \wedge (q \vee r \vee p) \wedge (q \vee r \vee \sim p)$$

$$\Leftrightarrow (\sim p \vee q \vee r) \wedge (\sim p \vee q \vee \sim r) \wedge (p \vee q \vee r) \wedge (p \vee \sim q \vee r)$$

EXERCISE 1.2

1. The following statement is of the form $p \vee q$. Write out the contradictory statement in the form $\sim p \wedge \sim q$:

"Either he is a fool or he has some evil design."

2. Let *p*: A triangle is equilateral

q: It is equiangular

then write $p \to q$ the conditional $p \to q$

3. The converse of a statement is given. Write the inverse and contrapositive statements.

"If he is considerate of others, then a man is a gentleman."

4. The converse of a statement is: If a steel rod or stretcher, then it has been heated:

Write inverse and contrapositive statements.

5. The contrapositive of a statement is given as

"If $x < 2$, then $x + 4 < 6$"

Write the converse and inverse.

6. Let p: It is cold and q: It is raining. Give a simple verbal sentence which describes each of the following statements:

(a) $p \wedge \sim(q)$ (b) $q \to p$ (c) $p \leftrightarrow \sim q$

7. Write an equivalent formula for $p \wedge (q \leftrightarrow r) \vee (r \leftrightarrow p)$ which does not contain biconditional.

8. Show that

(a) $\sim (p \wedge q) \to (\sim p \vee) (\sim p \vee q) \Leftrightarrow \sim p \vee q$

(b) $(p \vee q) \wedge (\sim p \wedge (\sim p \wedge q)) \Leftrightarrow (\sim p \wedge q)$

(c) $p \to q \Leftrightarrow \sim p \vee q$

9. By means of a truth table prove that

$$p \wedge q \equiv (p \downarrow q) \downarrow (q \downarrow p) \equiv \sim p \downarrow \sim q$$

10. Show that $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

11. Show that $(p \wedge q) \wedge \sim (p \vee q)$ is a contradiction.

12. Show that $\sim (p \vee q) \leftrightarrow (\sim p \wedge \sim q)$ is a tautology.

13. By means of a truth table prove that

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

(b) $p \to (q \vee r) \equiv (p \to q) \vee (p \to r)$

14. Let p be "He is rich" and let q be "He is honest". Write each of the following statements in symbolic forms using p and q:

(a) To be poor is to be honest.

(b) It is necessary to be poor in order to be honest.

(c) He is poor only if he is dishonest.

(d) If he is poor if he is dishonest.

15. Prove that

(a) $p \to q \equiv \sim p \to \sim q$ (b) $p \to q \equiv \sim p \vee q$

16. Write the contradiction of each of the following disjunction statements:

(1) $x = 2$ or $x = 4$ (2) $x > 3$ or $x < 3$

17. Show that $p \leftrightarrow \sim q$ does not logically imply that $p \to q$

18. Prove the following:

(a) $p \vee \sim(p \wedge q)$ is a Tautology.

(b) $(p \wedge q) \wedge \sim (p \vee q)$ is a Contradiction.

(c) $(p \wedge q) \to (p \vee q)$ is a Tautology.

19. Show that $p \wedge q$ logically implies $p \leftrightarrow q$.

20. Decide whether each of the following is true or false:

(a) $p \Rightarrow p \wedge q$ (b) $p \Rightarrow p \vee q$ (c) $p \wedge q \Rightarrow p$

(d) $p \vee q \Rightarrow p$ (e) $q \Rightarrow p \to q$

21. Write the disjunction, the conjunction, and two implications involving the two statements. I like cats. I like dogs.

22. If

A: The Eiffel Tower is in Australia
B: Australia is below the Equator
C: The Eiffel Tower is in Paris
D: Paris is in France
E: France is in Australia

Prove the following:

(1) The argument (A $\wedge$ B) $\rightarrow$ is valid

(2) (C $\wedge$ D) $\rightarrow$ is invalid

(3) (A $\vee$ E) $\rightarrow$ is invalid

23. Simplify the following compound propositions

(*a*) $(p \vee q) \wedge \sim[(\sim p \vee q]$

(*b*) $\sim[\sim\{(p \vee q) \wedge r\} \vee \sim q]$

24. Show that $[(r \rightarrow s) \wedge \{(r \rightarrow s) \rightarrow (t \rightarrow u)\}] \rightarrow [\sim t \vee u]$ is a tautology

Answers:

1. Either the man is born free or he is nowhere in chains.

2. If a triangle is equilateral, then it is equiangular.

3. Inverse: If a man is not a gentleman, then he is not considerate of others.

Contrapositive: If he is not considerate of others, then the man is not a gentleman.

4. Inverse: If a steel rod is not heated, then it does not stretch.

Contrapositive: If a steel rod does not stretch, then it has not been heated.

5. Converse: If $x > 2$, then $x + 4 > 6$

Inverse: If $x + 4 > 6$, then $x > 2$

6. $p \rightarrow \sim q$: It is cold, then it is not raining.

$q \leftrightarrow p$: It is raining if and only if it is raining.

$p \leftrightarrow \sim q$: It is cold if and only is it is not raining.

7. $p \wedge (q \rightarrow r) \wedge (r \rightarrow q) \vee (r \rightarrow p) \wedge (p \rightarrow r)$

14. (*a*) $\sim p \leftrightarrow \sim q$ (*b*) $q \rightarrow \sim p$

(*c*) $\sim p \rightarrow \sim q$ (*d*) $\sim p \wedge q$

16. (1) $x \neq 2$ and $x > \neq 4$ (2) $x > 3$ and $x = 3$

20. (*a*) False (*b*) True (*c*) True (*d*) False (*e*) True

21. (1) I like cats or I like dogs.

(2) I like cats and I like dogs.

(3) If I like cats then I like dogs.

(4) I like cats if I like dogs.

23. (*a*) $p \wedge (\sim q)$ (*b*) $q \wedge r$

1.20 SOLVED EXAMPLES

Example 1: Show that

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

Solution: Consider L.H.S.

$$(p \wedge (\sim p \vee q)) \vee (q \wedge \sim (p \wedge q)$$

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

$$\equiv f \vee (p \wedge q) \vee (q \wedge \sim p) \vee (q \wedge \sim p) \vee (q \wedge \sim q) \qquad (\because p \wedge \sim p = f)$$

$$\equiv (p \wedge q) \vee (q \wedge \sim p) \vee f$$

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

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

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

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

$$\equiv q \wedge t \qquad (\because p \vee \sim p = t)$$

$$\equiv q$$

$$\equiv \text{R.H.S.}$$

Hence $(p \wedge (\sim p \vee q)) \vee (q \wedge \sim (p \wedge q) \equiv q$

Example 2: Obtain the disjunctive normal form of

(*a*) $p \vee (\sim p \to (q \vee (q \to \sim r)))$

Solution:

(*a*) $p \vee (\sim p \to (q \vee (q \to \sim r)))$

$$\equiv p \vee (\sim p \to q \vee (\sim q \vee \sim r))$$

$$\equiv p \vee (p \vee q \vee (\sim q \vee \sim r))$$

$$\equiv p \vee p \vee q \vee \sim q \vee \sim r$$

$$\equiv p \vee q \vee \sim q \vee \sim r$$

Example 3: Show that

$((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee q$ is a tautology.

Solution: Consider

$$((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee q$$

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

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

$$\equiv (f \vee (\sim q \wedge \sim p) \vee (p \wedge \sim q) \vee \sim q) \vee q$$

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

$$\equiv (\sim q \wedge \sim p) \vee (p \wedge \sim q) \vee t \qquad (\text{Since } \sim q \vee q \equiv t)$$

$$\equiv t$$

Hence $((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee q$ is a tautology.

Example 4: Obtain the principal disjunctive normal form of $\sim p \vee q$

Solution: $\sim p \vee q \equiv (\sim p \wedge (q \vee \sim q)) \vee (q \wedge (p \vee \sim p))$

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

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

Hence $(\sim p \wedge q) \wedge (\sim p \wedge \sim q) \wedge (p \wedge q)$ is the required principal disjunctive normal form.

Example 5: Prove the following logical equivalencies:

(i) $[(p \vee q) \wedge (p \vee \sim q)] \vee q \Leftrightarrow p \vee q$

(ii) $p \vee [p \wedge (p \vee q)] \Leftrightarrow p$

(iii) $[p \vee q \vee (\sim p \wedge \sim q \wedge r)] \Leftrightarrow p \vee q \vee r$

(iv) $[(\sim p \vee q) \wedge (p \wedge (p \wedge q))] \Leftrightarrow p \wedge q$

Solution:

(i) $(p \vee q) \wedge (p \vee \sim q) \Leftrightarrow p \vee (q \wedge \sim q)$ (by distributive law)

$\Leftrightarrow p \vee f$ (*f*: fallacy)

$\Leftrightarrow p$ (by using identity law)

(ii) $p \vee [p \wedge (p \vee q)] \Leftrightarrow p \vee q$

$\Leftrightarrow p$ (by an idempotent law)

(iii) $[p \vee q \vee (\sim p \wedge \sim q \wedge r)] \Leftrightarrow (p \vee q) \vee [(\sim (p \vee q) \wedge r)]$

$\Leftrightarrow [(p \vee q) \vee \sim (p \vee q)] \wedge [(p \vee q) \vee r]$

$\Leftrightarrow t \wedge (p \vee q \vee r)$ (*t*: tautology)

$\Leftrightarrow p \vee q \vee r$

(iv) $(\sim p \vee q) \wedge [p \wedge (p \wedge q)] \Leftrightarrow (\sim p \vee q) \wedge (p \wedge q)$

$\Leftrightarrow [\sim p \wedge (p \wedge q)] \vee [q \wedge (p \wedge q)]$

$\Leftrightarrow [(\sim p \wedge p) \wedge q] \vee [q \wedge (p \wedge q)]$

$\Leftrightarrow [(f \wedge q) \vee (q \wedge (p \wedge q))]$ (*f*: fallacy)

$\Leftrightarrow f \vee (p \wedge q)$

$\Leftrightarrow p \wedge q$

EXERCISE 1.3

1. Construct truth tables for the following:

(a) $\sim(\sim p \wedge \sim q)$

(b) $p \wedge (p \vee q)$

(c) $(q \wedge (p \to q)) \to p$

2. Prove $(p \to q) \Leftrightarrow (\sim p \vee q)$

3. Show that $p \to (q \to r) \Leftrightarrow (\sim q \vee r) \Leftrightarrow (p \wedge q) \to r$

4. Show that $((p \vee q) \wedge \sim (\sim p \wedge (\sim q \vee \sim r))) \vee (\sim p \wedge \sim q) \vee (\sim p \wedge \sim r)$ is a tautology.

5. Write the duals of

(*a*) $(p \vee q) \wedge r$

(*b*) $(p \wedge q) \vee t$

(*c*) $\sim(p \vee q) \wedge (p \vee \sim (q \wedge \sim s))$

6. Show that $(p \vee q) \wedge (\sim p \wedge (\sim p \wedge q)) \Leftrightarrow \sim p \wedge q$

7. Prove the following implication:

(*a*) $(p \wedge q) \Rightarrow (p \rightarrow q)$

(*b*) $(p \rightarrow (q \rightarrow r) \Rightarrow (p \rightarrow q) \rightarrow (p \rightarrow r))$

8. Write an equivalence formula for $p \wedge (q \leftrightarrow r) \vee (r \leftrightarrow p)$ which does not contain biconditional.

9. Obtain disjunctive normal forms of

(*a*) $p \wedge (p \rightarrow q)$

(*b*) $\sim(p \vee q) \leftrightarrow (p \wedge q)$

10. Obtain the principal disjunctive normal forms of

(*i*) $\sim p \vee q$

(*ii*) $(p \wedge q) \vee (\sim p \wedge r) \vee (q \wedge r)$

(*iii*) $p \rightarrow ((p \rightarrow q) \wedge \sim(\sim q \vee \sim p))$

11. Obtain the principal conjunctive normal forms of

(*i*) $(\sim p \rightarrow r) \wedge (q \leftrightarrow p)$

(*ii*) $(q \rightarrow p) \wedge (\sim p \wedge q)$

(*iii*) $q \wedge (p \vee \sim q)$.

12. Show that $(P \rightarrow Q) \wedge (R \rightarrow Q)$ and $(P \vee R) \rightarrow Q$ are equivalent. ***(MCA, Oct., 2001, MKU)***

13. Define Tautology and contradiction. Find which of the following is a tautology and which is a contradiction:

$(P \wedge Q) \wedge \rceil (P \vee Q), P \vee \rceil (P \wedge Q)$ ***(MCA, Oct., 2001, MKU)***

14. Show that if $p \rightarrow q, q \rightarrow r, \rceil (p \wedge r)$ and $(p \vee r)$ then r. ***(MCA, Oct., 2001, MKU)***

15. Construct a truth table for the formula

$(P \wedge Q) \vee (\rceil P \wedge Q) \vee (P \wedge \rceil Q) \vee (\rceil P \wedge \rceil Q)$ ***(MCA, May 2001, MKU)***

16. (*a*) Construct the truth table for the following compound statements and which of them are tautologies:

(*i*) $(q \wedge r) \rightarrow (p \wedge \rceil r)$

(*ii*) $p \rightarrow q \rightleftarrows (\rceil p \vee q)$

write an equivalent formula for

$P \wedge (Q \rightleftarrows R) \vee (R \rightleftarrows P)$

which contains neither the biconditional nor the conditional

(*b*) Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises

$P \vee Q, Q \rightarrow R, P \rightarrow M$ and $\rceil M$. ***(MCA, May 2001, MKU)***

17. For any propositions p, q prove the following:

(a) $\sim (p \downarrow q) \Leftrightarrow (\sim p \uparrow \sim q)$

(b) $\sim (p \uparrow q) \rightleftarrows (\sim p \downarrow \sim q)$

18. For any proposition p, q, r prove the following:

(a) $p \uparrow (q \uparrow r) \rightleftarrows \sim p \vee (q \wedge r)$

(b) $p \downarrow (q \downarrow r) \rightleftarrows \sim p \wedge (q \vee r)$.

1.21 QUANTIFIERS

In this section we introduce, two logical notions called quantifiers. So far we have discussed the propositions in which each statement has been about a particular object. In this section we shall see how to write propositions that are about whole classes of objects.

In grammar a predicate is the word in a sentence which expresses what is said of the object. It is a part of a declarative sentence describing the properties of an object or relation among objects (The word 'Predicate' and property will be used to mean the same thing) for example 'is a cricket player', 'is a teacher' 'is short' are predicates. In logic the word predicate has a broader role than in grammar. The basis for this is the observation that a predicate is supplemented by, including a variable x as a place holder, for the intended subject, the result behaves as 'a statement function', in the sense that for each value of x a statement results. Consider the statement

$$p : x \text{ is an even number}$$

The truth value of p depends on the value of x. p is true when $x = 4$, and false when $x = 11$. The statement p is not a proposition. In this section we extend the system of logic to include such statements.

In grammar 'Rajan loves' is not a predicate. If 'x' is introduced as a place holder for the object, then we get the result as

'Rajan loves x'.

which is a statement function. Thus we can define, a predicate $p(x)$ as an expression having the quality that on an assignment of values to the variable x, from an appropriate domain, a statement results.

Definition 1.7: Let P (x) be a statement involving variable x and a set D. We call P a propositional function if for each x in D, P (x) is a proposition. The set D is called the domain of discourse (or universe of discourse) of P. It is the set of all possible values which can be assigned to variables in statements involving predicates.

For example the domain of discourse for P (x): "x is a cricket player" can be taken as the set of all human beings and the statement.

$$x^2 - 3x - 7 = 0$$

is a propositional function. The domain of discourse is the set of real numbers.

1.21.1 Universal Quantifier

Consider the proposition

'All odd prime numbers are greater than 2'. The word 'all' in this proposition is a logical quantifier. The proposition can be translated as follows:

"For every x, if x is an odd prime then x is greater than 2"

Similarly, the proposition:

'Every rational number is a real number' may be translated as.

For every x, if x is a rational and number, then x is a real number.

The phrase 'for every x' is called a universal quantifier. In symbols it is denoted by $\forall x$.

The phrases 'for every x', 'for all x' and 'for each x', have the same meaning and we can symbolize each by $\forall x$.

If $P(x)$ denotes a predicate (propositional function), then the universal quantification for $P(x)$, is the statement.

"For all values of x, $P(x)$ is true"

Example 1: Let $A = \{x : x$ is a natural number less than $9\}$

Here $P(x)$ is the sentence "x is a natural number less than 9"

The common property is "is a natural number less than 9"

$P(1)$ is true, therefore, $1 \in A$

$P(12)$ is not true, therefore $12 \notin A$

Example 2: Let $P(x)$: $x + 5 < 9$, then for all $x \geq 0$, $P(x)$ is a false statement because $P(5)$ is not true.

1.21.2 Existential Quantifier

In some situations we only require that there be at least one value for each the predicate is true. This can be done by prefixing $P(x)$ with the phrase "there exists an x'". The phrase "there exists an x'" is called an existential quantifier. The existential quantification for a predicate is the statement "There exists a value of x" for which $P(x)$.

The symbol $\exists$, is used to denote the logical quantifier 'there exists' the phrases 'There exists an x', 'There is a x', for some x' and 'for at least one x' have the same meaning.

The existential quantifier for $P(x)$ is denoted by $\exists\ x\ P(x)$.

Example 1: The proposition:

There is a dog without a tail can be written as

($\exists$ a dog) (the dog without tail)

Example 2: The proposition:

There is an integer between 2 and 8 inclusive may be written as

($\exists$ an integer) (the integer is between 2 and 8)

The propositions which include quantifiers may be negated as follows:

Example 3: Negate the proposition

All integers are greater than 8.

Solution: We can write the given proposition as

($\forall$ integers x) $(x > 8)$

The negation is

($\exists$ an integer x) ($x \leq 8$)

i.e., the negated proposition is: There is an integer less than or equal to 8.

In the negation a proposition 'for all' becomes 'there is' and 'there is' becomes 'for all' i.e., the symbol $\forall$ becomes $\exists$ and $\exists$ becomes $\forall$.

Example 4: The negated proposition of

($\exists$ an integer x) ($0 \leq x \leq 8$) is

($\forall$ integers x) ($x < 0$ or $x > 8$)

The following table gives us the equivalences involving quantifiers.

Table 1.27 *Equivalences involving quantifiers*

I_1^1	Distributivity of $\exists$ over $\vee$ $\exists\, x\,(P(x) \vee Q(x)) \equiv \exists\, x\, P(x) \vee \exists\, x\, Q(x)$ $\exists\, x\,(P \vee Q(x)) \equiv P \vee (\exists\, x\, Q(x))$
I_2^1	Distributivity of $\forall$ over $\wedge$ $\forall\, x\,(P(x) \wedge Q(x)) \equiv \forall\, x\, P(x) \wedge \forall\, x\, Q(x)$ $\forall\, x\,(P \wedge Q(x)) \equiv P \wedge (\forall\, x\, Q(x))$
I_3^1	$\rceil(\exists\, x\, P(x)) \equiv \forall\, x \rceil(P(x))$
I_4^1	$\rceil(\forall\, x\, P(x)) \equiv \exists\, x \rceil(P(x))$
I_5^1	$\exists\, x\,(P \wedge Q(x)) \equiv P \wedge (\exists\, x\, Q(x))$
I_6^1	$\forall\, x\,(P \vee Q(x)) \equiv P \vee (\forall\, x\, Q(x))$
I_7^1	$\forall\, x\, P(x) \Rightarrow \exists\, x\, P(x)$
I_8^1	$\forall\, x\, P(x) \vee \forall\, x\, Q(x) \Rightarrow \vee\,(P(x) \vee Q(x))$
I_9^1	$\exists\, x\,(P(x) \wedge Q(x)) \Rightarrow \exists\, x\, P(x) \wedge \exists\, x\, Q(x)$

Rules of inference for addition and deletion of quantifiers are given by the following table:

Table 1.28 *Rules of inference for addition and deletion of quantifiers*

R_1	Universal instantiation. $\dfrac{\forall\, x\, P(x)}{\therefore P(k)}$ k is some element of the universe.
R_2	Existential instantiation $\dfrac{\exists\, x\, P(x)}{\therefore P(k)}$ k is some element for which $P(k)$ is true.

Contd.

R_3 Universal generalization

$$\frac{P(x)}{\forall x\ P(x)}$$

R_4 Existential generalization

$$\frac{P(k)}{\therefore \exists\ x\ P(x)}$$

k is some element on the universe.

1.22 METHODS OF PROOF

In this section, we discuss different types of Proof: Direct Proof, Indirect Proof, Proof by counter example and proof by cases.

1.22.1 Direct Proof

We assume that P is true, and from the available information the conclusion q is shown to be true by valid reference. In this methods of proof we construct a chain of statements P, P_1, P_2, P_3, ..., P_n, ... , q where P is either a hypothesis of the theorem or an axiom and each of the implications $p \Rightarrow p_1,\ p_1 \Rightarrow p_2, ...,\ p_n \Rightarrow q$ is either an axiom or is implied by the implication preceding it.

Example 1: If x is an even integer then x^2 is an even integer.

Solution: Direct Proof

Let p: x is an even integer

q: x^2 is an even integer.

Consider, the hypothesis p. If x is an even integer they by the definition of an even integer.

$x = 2m$ for some integer m.

Hence $$x^2 = (2m)^2 \Rightarrow x^2 = 4m^2$$

$x^2 = 4m^2$ is clearly divisible by 2. Therefore x^2 is an even integer. Thus $p \to q$.

Example 2: If a and b are odd integer, then $a + b$ is an even integer.

Solution: (Direct Proof) An odd integer is of the form $2k + 1$, where k is some integer given that a and b are even integers, therefore $a = 2m_1 + 1$, $b = 2m_2 + 1$ for some integers m_1 and m_2.

Then
$$\begin{aligned} a + b &= (2m_1 + 1) + (2m_2 + 1) \\ &= 2m_1 + 1 + 2m_2 + 1 \\ &= 2m_1 + 2m_2 + 2 \\ &= 2\ (m_1 + m_2 + 1) \end{aligned}$$

But $m_1 + m_2 + 1$ is an integer, therefore $a + b$ is an even integer.

Example 3: If a is number such that $a^2 - 7a + 12 = 0$, then show that $a = 3$, $a = 4$ by direct proof.

Solution: $a^2 - 7a + 12 = 0$ using the rules of algebra, we can write

$$a^2 - 7a + 12 = (a - 3)\ (a - 4) = 0$$

i.e., product of the two numbers $(a - 3)$ and $(a - 4)$ is zero. Therefore, $a - 3 = 0$ or $a - 4 = 0$

$$a - 3 = 0 \Rightarrow a = 3,\ a - 4 = 0 \Rightarrow a = 4$$

Hence $$a = 3 \text{ or } a = 4$$

Example 4: Prove that if $|x| > |y|$ then $x^2 > y^2$, by direct method.

Solution: Since $|x| > |y|$ then $|x|^2 > |y|^2$

Now $|x|^2 = x^2$ and $|y|^2 = y^2$, hence $x^2 > y^2$

1.22.2 Method of Contraposition

Indirect Proof: This method of proof is very useful and is powerful at all levels of the subject mathematics. Indirect method follows from the Tautology $(p \to q) \leftrightarrow ((\sim q) \to (\sim p))$. This states that the implication $p \Rightarrow q$ is equivalent to $\sim q \Rightarrow \sim p$. To prove $p \Rightarrow q$ indirectly, we assume that q is false and then show that p is false.

Example 1: For any integer $n > 2$, prove that n Prime $\Rightarrow$ n odd.

Solution: Let p: n Prime

q: n odd

then $\sim q$: n even

$\sim p$: n not prime

If n is an even number greater than 2, then $n = 2m$ for some integer $m > 1$. Thus n is divisible by 2 and $n \neq 2$, therefore n cannot be prime thus we have $\sim q \Rightarrow \sim p$ i.e., if n is any number bigger than 2, then n cannot be prime.

Example 2: Prove: If α^2 is an even integer, then α is an even integer.

Solution: Let p: α^2 is an even integer

q: α is an even integer

let $\sim q$ be true then, α is not an even integers therefore α must be odd. α is of the form $\alpha = 2m + 1$ for some integer m.

$$\alpha = 2m + 1$$

$$\Rightarrow \quad \alpha^2 = (2n + 1)^2$$
$$= 4n^2 + 4n + 1$$
$$= 2\,(2m^2 + 2m) + 1$$

α^2 is of the form $\alpha^2 = 2n + 1$ where $n = (2m^2 + 2m)$

i.e., α^2 is odd

Thus, we have $\sim q \Rightarrow \sim p$

Hence by contraposition α is even.

1.22.3 Proof by Contradiction

In this method of proof, we assume the opposite of what we are trying to prove and get a logical contradiction. Hence our assumption must have been false. Therefore what we were originally required to prove must be true. To prove $p \to q$ is true, in this the proof can be constructed as follows:

(*i*) Assume $p \wedge (\sim q)$ is true.

(*ii*) On the basis of the assumption find some conclusion that is false.

(*iii*) Then the contradiction discovered in step (*ii*) leads us to the conclusion that $p \wedge (\sim q)$ is false which powers that $p \to q$ is true.

Example 1: Suppose that the integers 1, 2, 3, ..., 10 are randomly positioned around a circular wheel. Show that the sum of some set of 3 consecutively positioned numbers is at least 15.

Solution: (Proof by Contradiction)

Let a_r respect the integer at position *r* on the wheel. Then we are to prove

$$\left.\begin{aligned} & a_1 + a_2 + a_3 \geq 15 \\ \text{or}\quad & a_2 + a_3 + a_4 \geq 15 \\ & \vdots \\ \text{or}\quad & a_{10} + a_1 + a_2 \geq 15 \end{aligned}\right\} \qquad \text{... (1)}$$

where $a_1 + a_2 + ... + a_{10} = 1 + 2 + 3 + ... + 10$

Let us assume that, the above conclusion is false. Then we must have

$$\begin{aligned} & a_1 + a_2 + a_3 < 15 \\ & a_2 + a_3 + a_4 < 15 \\ & \vdots \\ & a_{10} + a_1 + a_2 < 15 \end{aligned}$$

We can write the above the inequalities as

$$\begin{aligned} & a_1 + a_2 + a_3 \leq 14 \\ & a_2 + a_3 + a_4 \leq 14 \\ & \vdots \\ & a_{10} + a_1 + a_2 \leq 14 \end{aligned}$$

Taking the sum: we get

$$3(a_1 + a_2 + ... + a_{10}) \leq 10 \times 14$$

i.e., $$3(1 + 2 + ... + 10) \leq 140$$

or $$3 \cdot \frac{10 \cdot (10+1)}{2} \leq 140$$

or $$3 \times 5 \times 11 \leq 140$$

or $$165 \leq 140$$

a contradiction

Hence the given proposition i.e. (1) is true

Example 2: Show that $\sqrt{2}$ is not a rational number.

Solution: Let us assume that $\sqrt{2}$ is rational. Then we can find integers such that

$$\sqrt{2} = \frac{p}{q}$$

where p and q have no common factor. After canceling the common factors squaring on both sides, we get

$$2 = \frac{p^2}{q^2}$$

$$\Rightarrow p^2 = 2q^2$$

$$\Rightarrow p^2 \text{ is even}$$

$$\Rightarrow p \text{ is even}$$

$$\Rightarrow p = 2m \text{ for some integer } m.$$

$$\Rightarrow (2m)^2 = 2q^2$$

$$\Rightarrow 4m^2 = 2q^2$$

$$\Rightarrow q^2 = 2m^2$$

$$\Rightarrow q \text{ is even}$$

Hence p and q have common factor of 2, which is a contradiction to the statement that a and b have no common factors.

Hence our assumption that $\sqrt{2}$ is rational leads to a contradiction. Thus $\sqrt{2}$ is irrational.

1.22.4 Proof by Counter Example

To show that $\forall x, P(x)$ it is sufficient to give specific example k, in the universe such that $P(k)$ is false, where the object k is called a counter example to the assertion $\forall x, P(x)$.

Example: Prove or disprove the statement:

If x and y are real number

$$(x^2 = y^2) \Leftrightarrow (x = y)$$

-3, 3 are real number and $(-3)^2 = 3^2$ but $-3 \neq 3$

Hence the result is false and implication is false.

1.22.5 Proof by Cases

To prove $p \to q$ by cases, we take p to be in the form $p_1 \vee p_2 \vee ... \vee p_n$ by proving separately, each of the following $p_1 \to q$, $p_2 \to q$, ..., $p_n \to q$ we can establish $(p_1 \vee p_2 \vee ... \vee p_n) \to q$.

In this section, we discuss rules of inference. Which are criteria for determining the validity of an argument. The rules of inference will be given in terms of statement formulas. Before discussing the rules of inference, we define consistency, which is an extremely important notion in mathematical logic.

Definition 1.8: A collection of statements is consistent if the statements can all be true simultaneously.

A set of formulas $H_1, H_2, H_3, ..., H_n$ is said to be consistent if their conjunction $H_1 \wedge H_2 \wedge ... \wedge H_n$ has the truth value T for some assignment of the truth values to the atomic variables appearing in $H_1, H_2, ..., H_n$. And a set of formulae $H_1, H_2, ..., H_n$ is inconsistent if their conjunction $H_1 \wedge H_2 \wedge ... \wedge H_n$ implies a contradiction, that is $H_1 \wedge H_2 \wedge ... \wedge H_n \Rightarrow S \wedge \urcorner S$ (a contradiction) where is S is any formula.

We use the notion of inconsistency in a method of proof called proof by contradiction (or indirect proof) we now begin our discussion by stating the following two rules of inference.

Rule P: A premise may be introduced at any point in the derivation.

Rule T: A formula S may be introduced in a derivation if S is tautologically implied by any one or more of true preceding formulas in the derivation.

1.22.6 Rules of Inference

The following tables give us the rules of inference:

Table 1.29

Implications:

I_1 $P \wedge Q \Rightarrow P$ (Simplification)

I_2 $P \wedge Q \Rightarrow Q$ (Simplification)

I_3 $P \Rightarrow P \vee Q$ (Addition)

I_4 $Q \Rightarrow P \vee Q$ (Addition)

I_5 $\urcorner P \Rightarrow P \rightarrow Q$

I_6 $Q \Rightarrow P \rightarrow Q$

I_7 $\urcorner(P \rightarrow Q) \Rightarrow P$

I_8 $\urcorner(P \rightarrow Q) \Rightarrow \urcorner Q$

I_9 $P, Q \Rightarrow P \wedge Q$

I_{10} $\urcorner P, P \vee Q \Rightarrow Q$ (Disjunctive syllogism)

I_{11} $P, P \rightarrow Q \Rightarrow Q$ (Modus Ponens)

I_{12} $\urcorner Q, P \rightarrow Q \Rightarrow \urcorner P$ (Modus Tollens)

I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ (Hypothetical syllogism)

I_{14} $P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$ (Dilemma)

Equivalences:

E_1 $\urcorner\urcorner P \Leftrightarrow P$ (Double negation)

E_2 $P \wedge Q \Leftrightarrow Q \wedge P$ (Commutative law)

E_3 $P \vee Q \Leftrightarrow Q \vee P$ (Commutative law)

E_4 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ (Associative law)

Contd.

E_5 $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ (Associative law)

E_6 $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (Distributive law)

E_7 $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee Q)$ (Distributive law)

E_8 $\urcorner (P \wedge Q) \Leftrightarrow \urcorner P \vee \urcorner Q$ (De Morgan's law)

E_9 $\urcorner (P \vee Q) \Leftrightarrow \urcorner P \wedge \urcorner Q$ (De Morgan's law)

E_{10} $P \vee P \Leftrightarrow P$

E_{11} $P \wedge P \Leftrightarrow P$

E_{12} $R \vee (P \wedge \urcorner P) \Leftrightarrow R$

E_{13} $R \wedge (P \vee \urcorner P) \Leftrightarrow R$

E_{14} $R \vee (P \vee \urcorner P) \Leftrightarrow T$

E_{15} $R \wedge (P \wedge \urcorner P) \Leftrightarrow F$

E_{16} $P \rightarrow Q \Leftrightarrow \urcorner P \vee Q$

E_{17} $\urcorner (P \rightarrow Q) \Leftrightarrow P \wedge \urcorner Q$

E_{18} $P \rightarrow Q \Leftrightarrow \urcorner Q \rightarrow \urcorner P$

E_{19} $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$

E_{20} $\urcorner (P \rightleftarrows Q) \Leftrightarrow P \rightleftarrows \urcorner Q$

E_{21} $P \rightleftarrows Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

E_{22} $(P \rightleftarrows Q) \Leftrightarrow (P \wedge Q) \vee (\urcorner P \wedge \urcorner Q)$

The rules 'Modus Ponens' and 'Hypothetical Syllogism' are known as the fundamental rules of inference.

De Morgan's laws and the law of contraposition are the other fundamental rules, from which other rules follow. Modus Ponens is also called the rule of detachment. It can be stated as follows:

Whenever the statements p and $(p \rightarrow q)$ are accepted as true, then we must accept the statement q as true.

The tabular form of the rule is given below

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline \therefore q \end{array}$$

In the above tabular presentation p and $(p \rightarrow q)$, which are above the horizontal line are the Premises (Hypotheses). The assertion q which below the Horizontal line is the conclusion.

The rule of Hypothetical Syllogism is also known as the transitive rule. It can be stated as follows:

If two implications $(p \to q)$ and $(q \to r)$ are true, then the implication $(p \to r)$ is true.

The tabular form of the rule is given below:

$$\begin{array}{r} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

The transitive rule can be extended to a larger number of implications as follows:

$$\begin{array}{r} p \to q \\ q \to r \\ r \to s \\ \hline \therefore p \to s \end{array}$$

$$\begin{array}{r} p_1 \to p_2 \\ p_2 \to p_3 \\ p_3 \to p_4 \\ \vdots \\ p_{n-1} \to p_n \\ \hline \therefore p_1 \to p_n \end{array}$$

Most of the arguments are based on the two fundamental rules of inference. In an argument premises are always taken to be true. Whereas the conclusion may or may not be true. The conclusion is true only when the argument is true. To list the validity of an argument we can also employ the laws of logic, logical equivalences and tautologies

Modus Tollens is a rule of denying. It can be stated as follows:

If $p \to q$ is true and q is false, then p is false.

The tabular form of the rule is gives below:

$$\begin{array}{r} p \to q \\ \sim q \\ \hline \therefore \sim p \end{array}$$

Rule of Disjunctive Syllogism, States that if $p \vee q$ is true and p is false, then q is true.

In tabular form, the rule can be written as follows:

$$\begin{array}{r} p \vee q \\ \sim q \\ \hline \therefore \sim q \end{array}$$

1.22.7 Fallacies

Faulty inferences are know as fallacies. There are three forms of fallacies:

1. The fallacy of affirming the consequent
2. The fallacy of denying the antecedent
3. The non Sequitur fallacy

The fallacy of affirming the consequent has the following tabular form:

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore p \end{array} \qquad \text{(fallacy)}$$

The fallacy of denying antecedent is presented in the following form:

$$\begin{array}{l} p \to q \\ \quad \sim p \\ \hline \therefore \sim q \end{array} \qquad \text{(fallacy)}$$

Fallacies of assuming converse and all logical errors are Special Cases of the non Sequitur fallacy. It can be presented as follows.

$$\begin{array}{l} p \\ \hline \therefore q \end{array}$$

Example 1: Prove that the following arguments are valid

(*a*)
$$\begin{array}{l} p \to r \\ q \to r \\ \hline \therefore (p \vee q) \to r \end{array}$$

(*b*)
$$\begin{array}{l} p \to r \\ \sim p \to q \\ q \to s \\ \hline \therefore \sim r \to s \end{array}$$

Solution (*a*) Consider

$(p \to r) \wedge (q \to r)$

We have

$$(p \to r) \wedge (q \to r) \Leftrightarrow (\sim p \vee r) \wedge (\sim q \vee r)$$

$$\Leftrightarrow (r\ u \sim p) \wedge (r \vee q) \qquad \text{(commutative law)}$$

$$\Leftrightarrow r \vee (\sim p \wedge \sim q) \qquad \text{(distributive law)}$$

$$\Leftrightarrow r \vee \sim (p \vee q) \qquad \text{(De Morgan's law)}$$

$$\Leftrightarrow \sim (p \vee q) \vee r \qquad \text{(commutative law)}$$

$$\Leftrightarrow (p \vee q) \rightarrow r$$

$(p \rightarrow r) \wedge (q \rightarrow r)$ and $(p \vee q) \rightarrow r$ are logically equivalence. Hence the given argument is valid

(b) we have

$$(p \rightarrow r) \wedge (\sim p \rightarrow q) \wedge (q \rightarrow s) \Rightarrow (p \rightarrow r) \wedge (\sim p \rightarrow s) \qquad \text{(by rule of Syllogism)}$$

$$\Leftrightarrow (\sim r \rightarrow \sim p) \wedge (\sim p \rightarrow s) \qquad \text{(by the rule of contrapositive)}$$

$$\Rightarrow \sim r \rightarrow s \qquad \text{(by rule of Syllogism)}$$

$(p \rightarrow r) \wedge (\sim p \rightarrow q) \wedge (q \rightarrow s)$ and $\sim r \rightarrow s$ are logically equivalent. Hence, the given argument is valid

***Example 2*:** Prove that the argument given below is a valid argument

$$\begin{array}{l} p \rightarrow (q \rightarrow r) \\ \sim q \rightarrow \sim p \\ \underline{\quad p \qquad\qquad} \\ \therefore r \end{array}$$

Solution: Consider $[p \rightarrow (q \rightarrow r)] \wedge (\sim q \rightarrow \sim p) \wedge p$

We have

$$[p \rightarrow (q \rightarrow r)] \wedge (\sim q \rightarrow \sim p) \wedge p$$

$$\Leftrightarrow [(p \rightarrow (q \rightarrow r)) \wedge p] \wedge (\sim q \rightarrow \sim p)$$

$$\Rightarrow (q \rightarrow r) \wedge (\sim q \rightarrow \sim p) \qquad \text{(by the rule of Modus Ponens)}$$

$$\Leftrightarrow (q \rightarrow r) \wedge (\sim \sim p \rightarrow \sim \sim q) \qquad \text{(by contraposition)}$$

$$\Leftrightarrow (q \rightarrow r) \wedge (p \rightarrow q)$$

$$\Leftrightarrow p \rightarrow r \qquad \text{(by the rule of Syllogism)}$$

$$\Leftrightarrow r \qquad \text{(since } p \text{ is true)}$$

$[p \rightarrow (q \rightarrow r) \wedge [\sim q \rightarrow \sim p) \wedge p$ and r are logically equivalent. Therefore the given argument is valid

Example 3: Text the validity of the argument:

If I drive to work, then I will arrive tired

$$\begin{array}{l} \underline{\quad \text{I am not tired} \quad} \\ \therefore \text{I do not drive to work} \end{array}$$

Solution:

Let p: I drive to work

q: I arrive tired

The argument has the following Symolic form

$$\begin{array}{c} p \rightarrow q \\ \underline{\sim q} \\ \therefore \sim p \end{array}$$

By the rule of Modus Tollens, the argument is valid

Example 4: Text the validity of the argument

If a person is poor, he is unhappy

$$\begin{array}{c} \underline{\text{If a person is unhappy, he dies young}} \\ \therefore \text{Poor person die young} \end{array}$$

Solution:

Let p: a person is poor

q: a person is unhappy

r: a person dies young

Then the argument takes the following form:

$$\begin{array}{l} p \rightarrow q \\ \underline{q \rightarrow r} \\ \therefore p \rightarrow r \end{array}$$

by the law of hypothetical; Syllogism, (i.e., transitive rule) the argument is valid

Example 5: Prove $\rceil Q,\ P \rightarrow Q \Rightarrow \rceil P$

Solution: A formal proof is as follows:

1. $P \rightarrow Q$	P
2. $\rceil Q \rightarrow \rceil P$	T, (1) and E_{18}
3. $\rceil Q$	P
4. $\rceil P$	T, (2), (3) and I_{11}

Example 6: Show that $\rceil P$ follows, logically from $\rceil(P \wedge \rceil Q),\ \rceil Q \vee P,\ \rceil R$.

Solution: A formal proof is as follows:

1. $\rceil(P \wedge \rceil Q)$	P
2. $\rceil P \vee Q$	$\because\ \rceil(P \wedge Q) \Leftrightarrow \rceil P \vee \rceil Q$
3. $P \rightarrow Q$	$\because\ P \rightarrow Q \Leftrightarrow \rceil P \vee Q$
4. $\rceil Q \vee R$	P

5.	$Q \to R$	
6.	$P \to R$	(3), (5)
7.	$\rceil R$	P
8.	$\rceil P$	$\rceil Q, P \to Q \Rightarrow \rceil P$

We now introduce another rule of inference called rule CP or rule of conditional proof.

Rule *CP:* If we can derive *S* from *R* and a set of premises, then we can derive $R \to S$ from the set of premises alone.

The above rule is also called deduction theorem.

Example 7: Show that $R \to S$ can be derived from the premises $P \to (P \to S)$, $\rceil R \vee P$, and Q.

Solution: We include *R* as an additional premise and show *S*, so that $R \to S$ can be derived.

1.	$\rceil R \vee S$	P
2.	R	P (assumed premises)
3.	P	T, (1), (2) and I_{10}
4.	$P \to (Q \to S)$	P
5.	$Q \to S$	T, (3), (4) and I_{11}
6.	Q	P
7.	S	T, (5), (6) and I_{11}
8.	$R \to S$	$C\,P$

We shall now give an example to prove inconsistency in the given set of formula.

Example 8: Show that $(R \to \rceil Q)$, $R \vee S$, $S \to \rceil Q$, $P \to Q \Leftrightarrow \rceil P$ are inconsistent.

Solution: A formal proof is:

1.	P	(assumed)
2.	$P \to Q$	Rule P
3.	Q	(1) and (2)
4.	$S \to \rceil Q$	P
5.	$Q \to \rceil S$	$P \to Q \rightleftarrows \rceil Q \to \rceil P$
6.	7S	(3), (5)
7.	$R \vee S$	P
8.	$\rceil R \to S$	$P \to Q \rightleftarrows \rceil P \vee \rceil Q$
9.	$\rceil S \to R$	$P \to Q \rightleftarrows \rceil Q \to \rceil P$
10.	R	(6), (9)
11.	$R \to \rceil Q$	P
12.	$\rceil Q$	(10), (11)
13.	$Q \wedge \rceil Q$	(3), (12)

Inconsistent

EXERCISE 1.4

1. If a real number x is such that $|x| > 5$, then $x^2 > 25$ (give the proof by cases).
2. Prove the statement by contradiction: “In a room of 15 people, 2 or more people have their birthday in the same month.
3. Prove deductively that all right angles are equal.
4. Prove by using direct method: If an integer a is such that $a - 2$, is divisible by 3, then $a^2 - 1$ is divisible by 3.
5. Prove by using contrapositive method: If x^2 is an odd integer, then x is an odd integer.
6. Prove by using direct method:

   (*i*) Sum of two even integers is an even integer.

   (*ii*) The sum of an even integer and an odd integer is an odd integer.

   (*iii*) The product of an even integer and an odd integer is an even integer.
7. Disprove the proposition (by counter example) for every integer x there is an integer y where $y^2 = x$.
8. Prove that $\sqrt{5}$ is not a rational number (prove by contradiction).
9. Prove that if $x^2 - 4 = 0$, then $n \neq 0$ by the method of contradiction.
10. Prove by direct method:

    If x and y are rational numbers then $n + y$ is rational.
11. Find a counter example:

    If $a > b$ then $a^2 > b^2$
12. Give a direct proof that if a and b are odd integers then $a + b$ is even.
13. Prove using contrapositive that if $x^2 - 4 < 0$, then $-2 < x < 2$.
14. Rewrite the following propositions using the symbols $\forall$ and $\exists$.

    (*a*) There is a cat without a tail.

    (*b*) There is an integer between 2 and 15 inclusive.

    (*c*) All odd prime numbers are bigger than 2.

    (*d*) All elephants have trunks.

    (*e*) All cats like cream.

    (*f*) All students are clever.

    (*g*) Every clever student is successful.

    (*h*) There are some successful students who are not clever.
15. Negate the following propositions:

    (*a*) $(\forall\ a > 0)\ (\exists\ b > 0)\ a + b$ is prime.

    (*b*) ($\forall$ integers m) ($\exists$ an integer n) $(m^2 = n)$.

    (*c*) All good students study hard.

    (*d*) All fish swim.

    (*e*) ($\exists$ an integer x) $(5 \leq x < 25)$.

(*f*) There is a triangle whose sum of angles $\neq 180^\circ$.

(*g*) If the teacher is absent, then some students do not complete their home work.

(*h*) All the students completed their home work and the teacher is present.

16. Prove that the following argument is valid. If a baby is hungry, then the baby cries. If the baby is not mad, then he does not cry. If a baby is mad, then he has a red face. Therefore if a baby is hungry, then he has a red face.

17. Suppose that the 10 integers 1, 2, …, 10 are randomly positioned around a circular wheel. Show that the sum of some set of 3 consecutively positioned numbers is at least 17.

18. Compute the truth value of the statement

$(p \to q) \leftrightarrow (\sim q \to \sim p)$ (***MCA, 2000, VTU***)

Answer: T

19. Determine whether each of the following statements are a tautology, a contingency or an absurdity

(*a*) $p \to (q \to p)$

(*b*) $(p \wedge q) \to p$

(*c*) $(p \wedge (p \to q)) \to q$

(*d*) $(q \wedge (\sim p)) \leftrightarrow r$ (***B.E, Mar. 2001, VTU***)

20. Show that $(P \vee Q) \rceil (\rceil P \wedge (\rceil Q \vee \rceil R))) \vee (\rceil P \wedge \rceil Q) \vee (\rceil P \wedge \rceil R)$ is a tautology (***B.E., Feb. 2002, VTU***)

21. Let k be an integer. If k^2 is odd then show that k is an odd integer

(***B.E Mar. 2001, VTU***)

22. Explain the differences between tautology and contingency

Answer:

19. (a) Tautology (b) Tautology (c) Tautology (d) Contingency

2

Set Theory

2.1 INTRODUCTION

The notion of a set is elementary to all of Mathematics and every branch of mathematics can be considered as a study of sets of objects of one kind or another. Cantor was the founder of the theory of sets. The word set is a primitive term and is regarded as one of the basic undefined ideas of mathematics. But we must have an Intuitive idea of what we mean by a set. Let us now consider the idea of a set.

2.2 SETS AND OPERATIONS ON SETS

2.2.1 Set

Definition 2.1:

A set is collection of well defined objects.

In the above definition the words set and collection for all practical purposes are Synonymous. We have really used the word set to define itself.

2.2.2 Notation

Each of the objects in the set is called a member of an element of the set. The objects themselves can be almost anything. Books, cities, numbers, animals, flowers, etc.

Elements of a set are usually denoted by lower-case letters. While sets are denoted by capital letters of English larguage.

The symbol $\in$ indicates the membership in a set.

If "a is an element of the set A", then we write $a \in A$.

The symbol $\in$ is read "is a member of " or "is an element of ".

The symbol $\notin$ is used to indicate that an object is not in the given set.

The symbol $\notin$ is read "is not a member of " or "is not an element of ".

If x is not an element of the set A then we write $x \notin A$.

2.2.3 Specifying Sets

There are five different ways of specifying sets:

(*i*) One method of specifying a set is to list all the members of the set between a pair of braces. Thus $\{1, 2, 3\}$ represents a set. This method is called "The listing method".

Example 1:

(*i*) {3, 6, 9, 12, 15}

(*ii*) {a, b, c, d}

This method of listing the elements of the set is also known as 'Tabulation'. In this method the order in which the elements are listed is immaterial, and is used for small sets.

(*ii*) Another method of defining particular sets is by a description of some attribute or characteristic of the elements of the set. This method is more general and involves a description of the set property.

$$A = \{x \mid x \text{ has the property } P\}$$

Designates "the set A of all objects 'x' such that x has the property P". This notation is called Set-Builder notation. The vertical bar | is read as "such that".

Example 2:

(*i*) $A = \{x \mid x$ is a positive Integer greater then 100}.

This is read as "the set of all x is a positive Integer less than 25".

(*ii*) $B = \{x \mid x$ is a complex number}.

Note: Repetition of objects is not allowed in a set, and a set is collection of objects without ordering.

(*iii*) We can describe a set by its characteristic function.

$$\mu A(x) = \begin{cases} 1 & \text{if} \quad x \in A \\ 0 & \text{if} \quad x \notin A \end{cases}$$

(*iv*) In another method we describe the set by a recursive formula:

Example 3: Let $x_0 = 2,\ x_1 = 1$ and $x_{i+1} = x_i + x_{i-1};\ i \geq 1$ and $A = \{x_i : i \geq 0\}$.

(*v*) We can also describe a set by an operation on some other sets.

2.3 SUBSETS

Definition 2.2: A set A is a subset of the set B if and only if every element of A is also an element of B. We also say that A is contained in B, and use the notation $A \subseteq B$.

Symbolically: If $x \in A \Rightarrow x \in B$, then $A \subseteq B$.

If $A \subseteq B$, it is possible that $A = B$, to emphasize this fact we write $A \subseteq B$.

If A is contained in B, then we may also state that B contains A and write $B \supseteq A$.

2.3.1 Proper Subset

Definition 2.3: A set A is called proper subset of the set B. If (*i*) A is subset of B and (*ii*) B is not a subset A

i.e., A is said to be a proper subset of B if every element of A belongs to the set B, but there is atleast one element of B, which is not in A. If A is a proper subset of B, then we denote it by $A \subset B$.

Note: Every set is a subset to itself.

2.3.2 Equal Sets

If A and B are sets such that every element of A is an element of B and every element of B is an element of, A then A and B are equal (Identical). We write "$A = B$", and it is read as A and B are identical.

2.3.3 Super Set

If A is subset of B, then B is called a superset of A.

Example:

(*i*) If $A = A\{0, 2, 9\}$, $B = \{0, 2, 7, 9, 11\}$ then $A \subset B$ (A is a proper subset of B).

(*ii*) If $A = \{a, a, b\}$, $B = \{a, b\}$, then A and B denoted the same set, i.e., $A = B$.

(*iii*) If $A = \{1, 2, 4\}$, $B = \{2, 4, 6, 8\}$ A is proper subset of B and B is a superset of A.

2.4 NULL SET

Definition 2.4: The set with no elements is called an empty set or null set. A Null set is designated by the symbol ϕ.

The null set is a subset of every set, i.e., If A is any set then $\phi \subset A$.

Example:

(*i*) The set of real roots of the polynomial $x^2 + 9 = 0$.

(*ii*) $\{x \mid 5x = 5x + 2\}$.

2.5 SINGLETON

Definition 2.5: A set having only one element is called a singleton.

Example: (*i*) $A = \{8\}$, (*ii*) $\{\phi\}$

Theorem 2.1: Two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

Proof: If $A = B$, every member of A is a member of B and every member of B is a member of A.

Hence $A \subseteq B$ and $B \subseteq A$

Conversely let us suppose that $A \neq B$, then there is either an element of A that is not in B or there is an element of B that is not in A. But $A \subseteq B$, therefore every element of A is in B and $B \subseteq A$, therefore every element of B is in A. Therefore, our assumption that $A \neq B$ leads to a contradiction, hence $A = B$.

Theorem 2.2: If ϕ and ϕ' are empty sets, then $\phi = \phi'$.

Proof: Suppose $\phi \neq \phi'$. Then one of the following statements must be true:

1. There is an element $x \in \phi$ such that $x \notin \phi'$
2. There is an element $x \in \phi'$ such that $x \notin \phi$.

But both these statements are false, since neither ϕ nor ϕ' has any elements. If follows that $\phi = \phi'$.

2.6 FINITE SET

Definition 2.6: A set is said to be finite, if it has finite number of elements.

Example:

(*i*) {1, 2, 3, 5}

(*ii*) The letters of the English alphabet.

2.7 INFINITE SET

Definition 2.7: A set is infinite, if it is not finite.

Example:

(*i*) The set of all real numbers.

(*ii*) The points on a line.

2.8 UNIVERSAL SET

Definition 2.8: In many discussions all the sets are considered to be subsets of one particular set. This set is called the universal set for that discussion.

The Universal set is often designated by the script letter U (or by X).

Universal set in not unique, and it may change from one discussion to another.

Example: If $A = \{0, 2, 7\}$, $B = \{3, 5, 6\}$, $C = \{1, 8, 9, 10\}$ then the universal set can be taken as the set.

$$U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

2.9 THE POWER SET

Definition 2.9: The set of all subsets of a set A is called the power set of A.

The power set of A is denoted by P (A).

Hence $$P(A) = \{x | x \subseteq A\}$$

The power set of A is also denoted sometimes by 2A

If A has n elements in it, then P (A) has 2^n elements:

Example 1: If $A = \{a, b\}$ then

$$P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$$

Example 2**:** The empty set ϕ, has only subset, therefore $P(\phi) = \{\phi\}$.

Note: A set is never equal to its power set. In the programming language Pascal, the notion power set is used to define data type in the language.

2.10 DISJOINTS SETS

Definition 2.10: Two sets are said to be disjoint if they have no element in common.

Example: The sets, $A = \{0, 4, 7, 9\}$ and $B = \{3, 6, 10\}$ are disjoint.

2.11 PROPERTIES OF SET CONTAINMENT

2.11.1

If A is any set then $A \subseteq A$

Proof: If $x \in A$, then $x \in A$ (by the repetition of the statement)

Hence $A \subseteq A$

2.11.2

If $A \subseteq B,$ and $B \subseteq C$ then $A \subseteq C$ where A, B and C are sets

Proof: Let $x \in A$. Then

$$\begin{aligned} x \in A &\Rightarrow x \in B \, (A \subseteq B) \\ &\Rightarrow x \in C \, (A \subseteq C) \end{aligned}$$

if $x \in A$ then $x \in C$, therefore $A \subseteq C$.

2.12 OPERATIONS ON SETS: UNION OF SETS

Definition 2.11: The union of two sets A and B is the set whose elements are all of the elements in A or in B or in both.

The union of sets A and B denoted by $A \cup B$ is read as "A union B".

Symbolically: $A \cup B = \{x | x \in A \text{ or } x \in B\}$

Example:

(*i*) If $A = \{5, 7, 8\}$, $B = \{2, 7, 9, 10, 11\}$ then, $A \cup B = \{2, 5, 7, 8, 9, 10, 11\}$

(*ii*) If $A = \{x | x \in Z, \text{ and } x \geq 3\}$ and $B = \{x | x \in Z, \text{ and } x \geq 8\}$

then $A \cup B = \{x | x \in Z,\ x \geq 3\}$

Where Z denoted the set of integers.

Union of More than Two Sets

Definition 2.12: If $A_1, A_2, A_3, ..., A_n$ denote, sets then the union of these sets denoted by $\bigcup_{i=1}^{n} A_i$ is defined as $\bigcup_{i=1}^{n} A_i = \{x | x \in A_i$ for at least one set $A_i\}$.

2.13 PROPERTIES OF UNION OPERATION

2.13.1

If A and B are two sets then:

(*i*) $A \subseteq (A \cup B)$

(*ii*) $B \subseteq (A \cup B)$

(*iii*) $A \cup U = U$ where U is the universal set.

Proof:

(*i*) Let $x \in A$. Then

$$x \in A \;\Rightarrow\; x \in A \text{ or } x \in B$$
$$\Rightarrow\; x \in (A \cup B)$$

Thus $A \subseteq A \cup B$

(*ii*) Let $x \in B$

Then $x \in B \;\Rightarrow\; x \in A$ or $x \in B$
$$\Rightarrow\; x \in (A \cup B)$$

Hence $B \subseteq A \cup B$

2.13.2

If A is any set then (*i*) $A \cup \phi = A$ (*ii*) $A \cup A = A$

Proof:

(*i*) Clearly $A \subseteq (A \cup \phi)$ … (1)

Conversely, let $x \in A \cup \phi$

$$x \in A \cup \phi \;\Rightarrow\; x \in A \text{ or } x \in \phi$$
$$\Rightarrow\; x \in A$$

Thus $A \cup \phi \subset A$ … (2)

from (1) and (2), we have

$$A \cup \phi = A$$

(*ii*) Clearly $A \subseteq A \cup A$ … (1)

Now let $x \in A \cup A$

$$x \in A \cup A \;\Rightarrow\; x \in A \text{ or } x \in A$$
$$\Rightarrow\; x \in A$$

Thus $A \cup A \subseteq A$ … (2)

Combining (1) and (2), we get

$$A \cup A = A$$

(*iii*) In order to prove that $A \cup U = U$ we have to prove that $(A \cup U) \subseteq U$ and $U \subseteq (A \cup U)$

Every set is a subset of the universal set.

i.e., $(A \cup U) \subseteq U$ … (1)

also $U \subseteq (A \cup U)$ … (2)

Combining (1) and (2), we get

$$A \cup U = U.$$

2.13.3

Union of sets is commutative, i.e., If A and B are any sets, then $A \cup B = B \cup A$

Proof: Let $x \in A \cup B$, then

$$\begin{aligned} x \in A \cup B &\Rightarrow x \in A \text{ or } x \in B &&\dots(1)\\ &\Rightarrow x \in B \text{ or } x \in A \\ &\Rightarrow x \in (B \cup A) \end{aligned}$$

Hence $(A \cup B) \subseteq (B \cup A)$ ... (1)

Conversely, let $x \in (B \cup A)$, then

$$\begin{aligned} x \in (B \cup A) &\Rightarrow x \in B \text{ or } x \in A \\ &\Rightarrow x \in A \text{ or } x \in B \\ &\Rightarrow x \in (A \cup B) \end{aligned}$$

Thus $(B \cup A) \subseteq (A \cup B)$ … (2)

From (1) and (2) we have

$$A \cup B = B \cup A.$$

2.13.4 Associative Law for Addition

Union of sets is Associative, i.e., If A, B and C are any three sets, then $(A \cup B) \cup C = A \cup (B \cup C)$

Proof: Let $x \in (A \cup B) \cup C$ then

$$\begin{aligned} x \in (A \cup B) \cup C &\Rightarrow x \in (A \cup B) \text{ or } x \in C &&\dots(1)\\ &\Rightarrow (x \in A \text{ or } x \in B) \text{ or } x \in C \\ &\Rightarrow x \in A \text{ or } (x \in B \text{ or } x \in C) \\ &\Rightarrow x \in A \text{ or } x \in (B \cup C) \\ &\Rightarrow x \in A \cup (B \cup C) \end{aligned}$$

Hence $(A \cup B) \cup C \subseteq A \cup (B \cup C)$

conversely, let $x \in A \cup (B \cup C)$

$$\begin{aligned} x \in (A \cup B) \cup C &\Rightarrow x \in A \text{ or } x \in (B \cup C) &&\dots(1)\\ &\Rightarrow x \in A \text{ or } (x \in B \text{ or } x \in C) \\ &\Rightarrow (x \in A \text{ or } x \in B) \text{ or } x \in C \\ &\Rightarrow x \in A \cup B \text{ or } x \in C \\ &\Rightarrow x \in (A \cup B) \cup C \end{aligned}$$

Thus $A \cup (B \cup C) \subseteq (A \cup B) \cup C$ … (2)

Hence from (1) and (2), we have

$$(A \cup B) \cup C = A \cup (B \cup C)$$

2.14 INTERSECTION OF SETS

Definition 2.13: The intersection of two sets A and B is the set whose elements are all of the elements common to both A and B.

The intersection of the sets of "A" and "B" is denoted by $A \cap B$ and is read as "A intersection B" ***symbolically***: $A \cap B = \{x | x \in A \text{ and } x \in B\}$

Intersection of More than Two Sets

Definition 2.14: If $A_1, A_2, A_3, \ldots A_n$ denote sets, then the intersection of these sets denoted by

$\bigcap_{i=1}^{n} A_i$ is defined as follows

$$\bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ for every } i \ (i = 1, 2, \ldots, n)\}$$

$$= \{x \mid x \text{ belongs to all sets } A_i\}$$

Example: (*i*) $A = \{1, 2, 3, 8\}$, $B = \{5, 8, 9\}$ than $A \cap B = \{8\}$.

(*ii*) If $A = \{a, b, c, d\}$, $B = \{b, d, e, f, g\}$ then $A \cap B = \{b, d\}$.

2.15 PROPERTIES OF INTERSECTION OPERATION

2.15.1

If A and B are any two sets then

(*i*) $A \cap B \subseteq A$ (*ii*) $A \cap B \subseteq B$

Proof:

(*i*) Let x be an element of the set $A \cap B$, then

$$x \in A \cap B \Rightarrow x \in A \text{ and } x \in B$$
$$\Rightarrow x \in A$$

Hence $A \cap B \subseteq A$

(*ii*) Let x be a number of the set $A \cap B$, then

$$x \in A \cap B \Rightarrow x \in A \text{ and } x \in B$$

Hence $\Rightarrow A \cap B \subseteq B$

2.15.2

If A is any set then

(*i*) $A \cap \phi = \phi$, (*ii*) $A \cap A = A$, (*iii*) $A \cap U = A$, where U is the universal set.

Proof:

(*i*) ϕ is a subset of every set, therefore

$$\phi \subseteq A \cap \phi \qquad \text{... (1)}$$

and $$A \cap \phi \subseteq \phi$$

from (1) and (2) we have $$A \cap \phi = \phi \qquad \text{... (2)}$$

(*ii*) Clearly $A \cap A \subseteq A$ … (1)

Let *x* be a member of *A*, then

$$x \in A \Rightarrow x \in A \text{ and } x \in A \text{ (by the repetition of the statement)}$$
$$\Rightarrow x \in A \cap A$$

Thus $$A \subseteq A \cap A \qquad \text{… (2)}$$

Combining (1) and (2), we get

$$A \cap A = A$$

(*iii*) Clearly $A \cap U \subseteq A$

Let *x* be any member of *A*, then

$$x \in A \Rightarrow x \in U \qquad (\therefore A \subseteq U)$$
$$\Rightarrow x \in A \text{ and } x \in U$$
$$\Rightarrow x \in A \cap U$$

Hence $$A \subseteq A \cap U \qquad \text{… (2)}$$

Combining (1) and (2), we get

$$A \cap U = A$$

2.15.3 Commutative Law

Intersection of sets is commutative, i.e., if *A* and *B* are any two sets, then $A \cap B = B \cap A$

Proof: Let $x \in A \cap B$, then

$$x \in A \cap B \Rightarrow x \in A \text{ and } x \in B$$
$$\Rightarrow x \in B \text{ and } x \in A$$
$$\Rightarrow x \in B \cap A$$

Thus $$A \cap B \subseteq B \cap A \qquad \text{… (1)}$$

Conversely, Let $x \in B \cap A$, then

$$x \in B \cap A \Rightarrow x \in B \text{ and } x \in A$$
$$\Rightarrow x \in A \text{ and } x \in B$$
$$\Rightarrow x \in A \cap B$$

Hence $$B \cap A \subseteq A \subseteq B \qquad \text{… (2)}$$

Combining (1) and (2) $A \cap B = B \cap A$

2.15.4 Associative Law for Intersection

Intersection of sets is associative, i.e., if A, B and C are any three sets, then $(A \cap B) \cap C = A \cap (B \cap C)$

Proof: Let $x \in (A \cap B) \cap C$, then

$$\begin{aligned} x \in (A \cap B) \cap C &\Rightarrow x \in (A \cap B) \text{ and } x \in C \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ and } x \in C \\ &\Rightarrow x \in A \text{ and } (x \in B \text{ and } x \in C) \\ &\Rightarrow x \in A \text{ and } x \in B \cap C \\ &\Rightarrow x \in A \cap (B \cap C) \end{aligned}$$

Hence $$(A \cap B) \cap \subseteq A \cap (B \cap C)$$

Conversely, Let $x \in A \cap (B \cap C)$, then

$$\begin{aligned} x \in A \cap (B \cap C) &\Rightarrow x \in A \text{ and } (x \in B \cap C) \\ &\Rightarrow x \in A \text{ and } (x \in B \text{ and } x \in C) \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ and } x \in C \\ &\Rightarrow x \in (A \cap B) \text{ and } x \in C \\ &\Rightarrow x \in (A \cap B) \in C \end{aligned}$$

Thus $$A \cap (B \cap C) \subseteq (A \cap B) \cap C \qquad \ldots (2)$$

Combining (1) and (2), we get

$$(A \cap B) \cap C = A \cap (B \cap C)$$

2.16 DISTRIBUTIVE LAWS

2.16.1

Intersection of sets is distributive over the union of sets, i.e., if A, B and C are any three sets, then

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

Proof: Let $x \in A \cap (B \cup C)$, Then

$$\begin{aligned} x \in A \cap (B \cup C) &\Rightarrow x \in A \text{ and } x \in (B \cup C), \\ &\Rightarrow x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\Rightarrow x \in (A \cap B) \text{ or } x \in (A \cap C) \\ &\Rightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

Thus $$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) \qquad \ldots (1)$$

conversely let $x \in (A \cap B) \cup (A \cap C)$, then

$$\begin{aligned} x \in (A \cap B) \cup (A \cap C) &\Rightarrow x \in (A \cap B) \text{ or } x \in (A \cap C) \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \end{aligned}$$

$$\Rightarrow x \in A \text{ and } (x \in B \text{ or } x \in C)$$

$$\Rightarrow x \in A \text{ and } x \in (B \cup C)$$

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

Hence $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ … (2)

From (1) and (2), we have

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

2.16.2

Union of sets is distributive over the intersection, i.e., if A, B and C are any three sets, then

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

2.17 COMPLEMENT OF A SET

2.17.1 Relative Complement (or Difference of Sets)

Definition 2.15: If A and B are subsets of the universal set U, then the relative complement of B in A is the set of all elements in A which are not in A. It is denoted by $A - B$ thus:

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

Example: Let $A = \{a, b, c\}$ and $B = \{b, c, d, e, f, g\}$, then $A - B = \{a\}$.

2.17.2 Complement of Set

Definition 2.16: If U is a universal set containing the set A, then $U - A$ is called the complement of A. It is denoted by A' or by $\bar{A}$.

Thus $\bar{A} = A' = \{x : x \notin A\}$

2.18 PROPERTIES OF COMPLEMENTATION

If A and B are two subsets of universal set U, then

(1) $\bar{U} = \phi$ (5) $\overline{(\bar{A})} = A$

(2) $\overline{(\phi)} = U$ (6) $A \subseteq B \Rightarrow \bar{B} \subseteq \bar{A}$

(3) $A \cup \bar{A} = \cup$ (7) $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$ (De Morgan's laws)

(4) $A \cap \bar{A} = \phi$ (8) $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$ (De Morgan's laws)

Proof: (1) Clearly $\phi \subseteq \bar{U}$

Conversely $x \in \bar{U} \Rightarrow x \notin U$

$$\Rightarrow x \in \phi$$

Hence $\bar{U} \subseteq \phi$

Now $\phi \subseteq \bar{U}$ and $\bar{U} \subseteq \phi$

$$\Rightarrow \bar{U} = \phi$$

Proof: (2) Let $x \in \bar{\phi}$, then

$$x \in \bar{\phi} \Rightarrow x \notin \phi$$
$$\Rightarrow x \in U$$

Thus $\bar{\phi} \subseteq U$

Conversely let $x \in U$, then

$$x \in U \Rightarrow x \notin \phi$$
$$\Rightarrow x \in \bar{\phi}$$

Hence $U \subseteq \bar{\phi}$

Therefore $\bar{\phi} \subseteq U$ and $U \subseteq \bar{\phi} \Rightarrow \bar{\phi} = U$

The properties (3) and (4) are very simple and follow immediately from the definition of complement, we prove the remainig.

Proof: (5) If $x \in \overline{\left(\bar{A}\right)}$ then $x \notin A$

Hence $x \in \overline{\left(\bar{A}\right)} \Rightarrow x \notin \bar{A}$

$$\Rightarrow x \in A$$

Thus $\overline{\left(\bar{A}\right)} \subseteq A$ … (1)

Conversely, let $x \in A$, then

$$x \in A \Rightarrow x \notin \bar{A}$$
$$\Rightarrow x \in \overline{\left(\bar{A}\right)} \quad \ldots (2)$$

Hence $A \subseteq \overline{\left(\bar{A}\right)}$

Therefore from (1) and (2)

$$\overline{\left(\bar{A}\right)} = A$$

Proof: (6) We have $A \subseteq B$

Let $x \in \bar{B}$, then

$$x \in \bar{B} \Rightarrow x \notin B$$
$$\Rightarrow x \notin A \quad (\therefore A \subseteq B)$$
$$\Rightarrow x \in \bar{A}$$

Hence $\bar{B} \subseteq \bar{A}$

Proof: (7) Let $x \in \overline{(A \cap B)}$; then

$$x \in \overline{(A \cap B)} \Rightarrow x \notin (A \cap B)$$

$$\Rightarrow x \notin A \text{ or } x \notin B$$

$$\Rightarrow x \in \overline{A} \text{ or } x \in \overline{B}$$

$$\Rightarrow x \in \overline{A} \cup \overline{B}$$

Hence $\overline{(A \cap B)} \subseteq \overline{A} \cup \overline{B}$ … (1)

Conversely, let $x \in \overline{A} \cup \overline{B}$, then

$$x \in \left(\overline{A} \cup \overline{B}\right) \Rightarrow x \in \overline{A} \text{ or } x \in \overline{B}$$

$$\Rightarrow x \notin A \text{ or } x \notin B$$

$$\Rightarrow x \notin (A \cap B)$$

$$\Rightarrow x \in \overline{(A \cap B)}$$

Thus $\overline{A} \cup \overline{B} \subseteq \overline{(A \cap B)}$ … (2)

From (1) and (2), we have

$$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$$

Proof: (8) Let $x \in \overline{(A \cup B)}$, then

$$x \in \overline{(A \cup B)} \Rightarrow x \notin A \cup B$$

$$\Rightarrow x \notin A \text{ and } x \notin B$$

$$\Rightarrow x \in \overline{A} \text{ and } x \in \overline{B}$$

$$\Rightarrow x \in \overline{A} \cap \overline{B}$$

Hence $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$ … (1)

Conversely, let $x \in A \cap B$, then

$$x \in \overline{A} \cap \overline{B} \Rightarrow x \in \overline{A} \text{ and } x \in \overline{B}$$

$$\Rightarrow x \notin A \text{ and } x \notin B$$

$$\Rightarrow x \notin (A \cup B)$$

$$\Rightarrow x \in \overline{(A \cup B)}$$

Thus $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$ … (2)

Combining (1) and (2), we have $\left(\overline{A \cup B}\right) = \overline{A} \cap \overline{B}$

The above properties of union and intersection of sets are called set Identities.

2.19 PROPERTIES OF DIFFERENCE

If A and B are two subsets of a universal set, then

1. $A - B = A \cap \overline{B}$
2. $\overline{A} = U - A$
3. $A - A = \phi$
4. $A - \phi = A$

5. $A - B = B - A$, if and only if $A = B$

6. $A - B = A$ if and only if $A \cap B = \phi$

7. $A - B = \phi$ if and only if $A \subseteq B$

Proof: (1) Let $x \in A - B$, then

$$\begin{aligned} x \in A - B &\Rightarrow x \in A \text{ and } x \notin B \\ &\Rightarrow x \in A \text{ and } x \in \overline{B} \\ &\Rightarrow x \in A \cap \overline{B} \end{aligned}$$

Hence $$A - B \subseteq A \cap \overline{B} \qquad \ldots (1)$$

Conversely let $x \in A \cap B$, then

$$\begin{aligned} x \in A \cap B &\Rightarrow x \in A \text{ and } x \in \overline{B} \\ &\Rightarrow x \in A \text{ and } x \notin B \\ &\Rightarrow x \in A - B \end{aligned}$$

Therefore $$A \cap \overline{B} \subseteq A - B \qquad \ldots (2)$$

From (1) and (2), we have $A - B = A \cap \overline{B}$

2.20 SYMMETRIC DIFFERENCE

Definition 2.17: The symmetric difference of two sets *A* and *B* is the relative complement of $A \cap B$ with respect to $A \cup B$. It is denoted by $A \Delta B$ (or by $A \oplus B$)

Symbolically: $A \Delta B = \{x | x \in A \cup B \text{ and } x \notin A \cap B\}$

Example: Let $A = \{1, 2, 3, 4, 5, 6, 7\}$ $B = \{3, 4, p, q, r, s\}$

Then, we have $A \cup B = \{1, 2, 3, 4, 5, 6, 7, p, q, r, s\}$ and $A \cap B = \{3, 4\}$

We get $A \Delta B = \{1, 2, 5, 6, 7, p, q, r, s\}$

Note: We can also find the symmetric difference by using the identity.

$$A \Delta B = (A - B) \cup (B - A)$$

In the above example, we have $A - B = \{1, 2, 5, 6, 7\}$;
and $B - A = \{p, q, r, s\}$

Hence $A \Delta B = (A - B) \cup (B - A) = \{1, 2, 5, 6, 7, p, q, r, s\}$

2.21 PROPERTIES OF SYMMETRIC DIFFERENCE

If *A* and *B* are any two sets, then

1. $A \Delta A = \phi$

2. $A \Delta B = B \Delta A$

3. $A \Delta \phi = A$

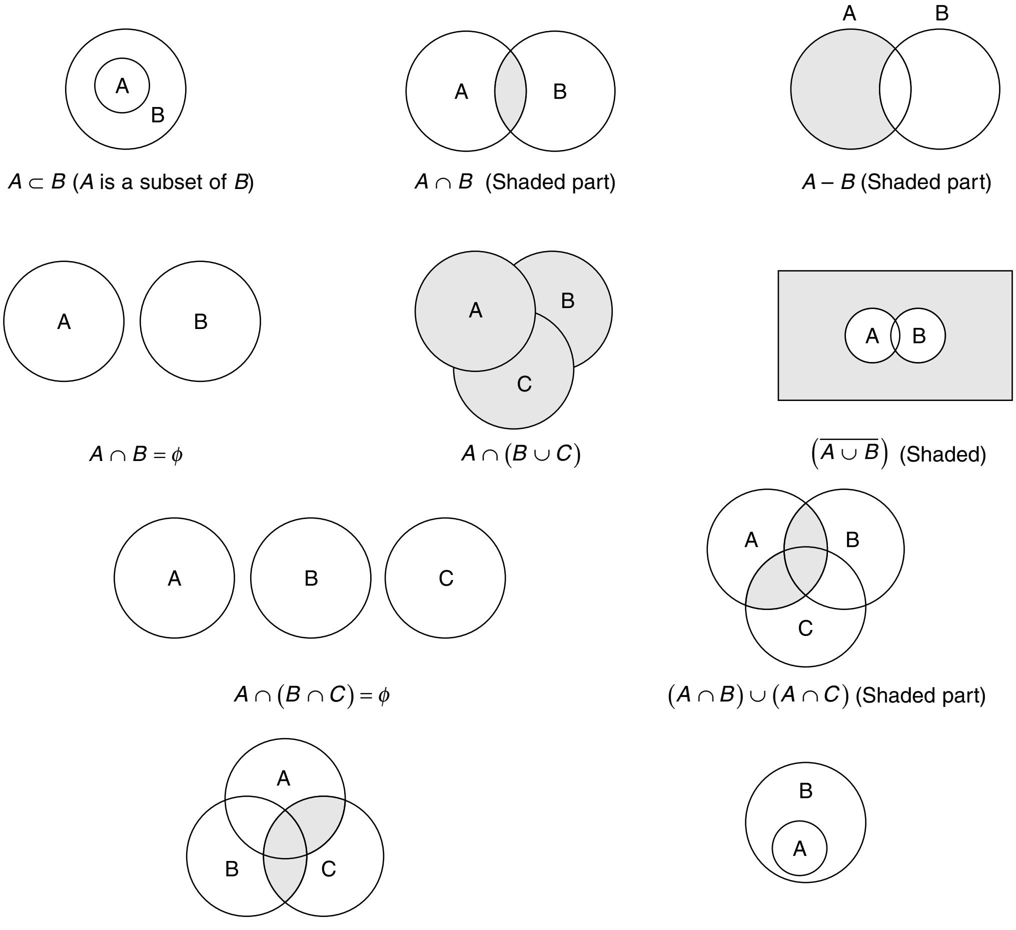
4. $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

5. $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

2.22 VENN DIAGRAMS

Set operation can be illustrated by Venn diagrams. A venn diagram is a useful device to our consideration of relationships that may exist between the subsets of a given universe. The universal set U is represented by the set of points inside and on the boundary of a single closed curve (usually a rectangle). If A is a subset of U is then represented by the points inside and on the boundary of another simple closed curve (usually a circle) inside the rectangle. Several venn diagrams, together with their interpretations are shown below (usually the label U is ommitted).

Using venn diagram, we can produce a geometrical interpretation for any expression involving sets and set operations. However, it should be noted that, venn diagrams do not prove the truth of a relationship between sets, they only illustrate plausibility.



$A \subset B$ (A is a subset of B)

$A \cap B$ (Shaded part)

$A - B$ (Shaded part)

$A \cap B = \phi$

$A \cap (B \cup C)$

$(\overline{A \cup B})$ (Shaded)

$A \cap (B \cap C) = \phi$

$(A \cap B) \cup (A \cap C)$ (Shaded part)

$(A \cup B) \cap C$ (Shaded)

$A \cap B = A$ if $A \subseteq B$

Fig. 2.1 Venn Diagrams

2.23 PRINCIPLE OF DUALITY

The principle of duality states that any established result involving sets and complements and operations of union and intersection gives a corresponding dual result by replacing U by ϕ and $\cup$ by $\cap$, and vice versa.

Example: Consider $A \cup \overline{A} = U$

Applying the principle of dualilty, we get $A \cap \overline{A} = \phi$

2.24 SOLVED EXAMPLES

Example 1: Prove that $A \cap (B - C) \subset A - (B \cap C)$

Solution: Let $x \in A \cap (B - C)$, then

$$\begin{aligned} x \in A \cap (B - C) &\Rightarrow x \in A \text{ and } x \in (B - C) \\ &\Rightarrow x \in A \text{ and } (x \in B, \text{ and } x \notin C) \\ &\Rightarrow x \in A \text{ and } x \notin (B \cap C) \\ &\Rightarrow x \in A - (B \cap C) \end{aligned}$$

Hence $$A \cap (B - C) \subset A - (B \cap C)$$

Example 2: Show that $\left[A \cap \left(B \cup \overline{A}\right)\right] \cup B = B$

Solution:

$$\begin{aligned} \left[A \cap \left(B \cup \overline{A}\right)\right] \cup B &= \left((A \cap B) \cup \left(A \cap \overline{A}\right)\right) \cup B \\ &= ((A \cap B) \cup \phi) \cup B \\ &= (A \cap B) \cup B = B \end{aligned}$$

Example 3: Give that ϕ is an empty set, find $P(\phi)$, $P(P(\phi))$, $P\left(P\left(P(\phi)\right)\right)$

Solution:

$$\begin{aligned} P(\phi) &= \{\phi\} \\ P\left(P(\phi)\right) &= \{\phi, (\phi)\} \\ P\left(P\left(P(\phi)\right)\right) &= \{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\} \end{aligned}$$

EXERCISE 2.1

I(***a***) Illustrate the following identities by means of venn diagrams:

1. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
2. $A \cap U = A$
3. $A \cup U = U$
4. $A \cup B = \overline{(A \cup B)} \cup (A \cap B)$

5. $\overline{(A \cup B)} = A \cap B$

6. $(A \cup B) \cap B = A \cap \overline{B}$

7. $\overline{A} \cup (A \cap B) = \overline{A} \cup B$

8. $A \cap (A \cup B) = A$

(*b*) 1. $A \subseteq B \Leftrightarrow A \cup B = B$ ***(MCA, OSM, 1999)***

2. If A and B and subsets of universal set, then $A \subset B$; if and only if $\overline{B} \subseteq \overline{A}$

(MCA, OSM, 1996)

3. Use Venn diagram to show that

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ***(MCA, OSM, 1998)***

4. Prove that $A - (A \cap B) = (A - B)$ ***(MCA, OSM, 1998)***

5. If A_0 and A_k are sets of real numbers defined as

$A_0 = \{a / a \leq 1\}$

$A_k = \{a / a \leq 1 + 1/k ;\ k = 1, 2, \overline{\ldots}\}$

$\prod\limits_{k=1}^{\infty} = A_0$ ***(MCA, OSM, 1999)***

$k = 1$

6. Show that $P(A) \cup P(B) \subseteq P(A \cup B)$ where $P(X)$ is the power set of set X

(MCA, OSM, 1998)

7. Let A be a set with k elements and $P(A)$ its power set show that the cardinclity of $P(A)$ is 2^k.

II

1. $A = \{1, 2\}$, $B = \{1, 2, 4, 5\}$ and $C = \{5, 7, 9, 10\}$ find

(*a*) $A \cup B$ (*b*) $A \cap B$ (*c*) $(A \cup B) \cup C$

(*d*) $(A \cap B) \cap C$ (*e*) $(A \cup B) \cap C$ (*f*) $(A \cap B) \cup C$

2. If $A = \{a, b, c, d\}$, $B = \{c, d, e\}$ and $C = \{e, f, g, h\}$ state the elements of the sets.

(*a*) $A \cup C$ (*b*) $B \cap A$

(*c*) $B \cap (A \cup C)$ (*d*) $(B \cap A) \cup (B \cap C)$

3. If $U = \{x \in Z \mid -5 < x < 5\}$ and $A = (x \in Z \mid -2 < x < 3)$ state the elements of the sets.

$\overline{A}, \overline{A} \cap \overline{A}, A \cap U, A \cup U$ {Z is the set of integers}

4. If $U = \{1, 2, 3, 4, \ldots 10\}$, $A = \{x \in U \mid x \text{ is a prime}\}$, $B = \{x \in U \mid x$ is odd} Show that $A \cap B = (A \cup B)$

5. $U = \{a, b, c, d, e, f, g\}$, $A = \{a, b, c, d\}$, $B = \{a, b, c, d, e, f\}$ and $C = \{a, b, g\}$ find $\overline{A}, \overline{B}, \overline{C}$,

$A - B, B - C$, $A \cap B(A \cup B)$ and $B \cap C$.

6. If $A = \{a, b, c, e, f, \}$, $B = \{b, e, f, r, s\}$ and $C = \{a, t, u, v\}$ find $A \cap B$, $A \cap C$ and $B \cap C$.

7. If $A = \{x \mid x$ is an integer and $x \le 4\}$ and $U = Z$, then write A.

8. If $U = \{a, b, c, d, e, f, g, h\}$, $A = \{a, c, f, g\}$, $B = \{a, e\}$, $C = \{b, h\}$ compute

   (a) $A - B$ (b) A (c) B (d) $A \cup B$

9. List all the subsets of (a) $A = \{a, b, c\}$, (b) $\{a, b, c, d\}$.

10. If $A_1 = \{1, 5\}$, $A_2 = \{1, 2, 4, 6\}$, $A_3 = \{3, 4, 7\}$, $B = \{2, 4\}$ and $I = \{1, 2, 3\}$

    Verify the Identies.

    (a) $B \cup \left(\bigcap_{i=1}^{3} A_i\right) = \bigcap_{i=1}^{3} (B \cup A_i)$ (b) $B \cup \left(\bigcup_{i=1}^{3} A_i\right) = \bigcup_{i=1}^{3} (B \cap A_i)$

11. If $A_1 = \{\{1, 2\}, \{3\}\}$, $A_2 = \{\{1\}, \{2, 3\}\}$, and $A_3 = \{1, 2, 3\}$ these show that A_1, A_2, A_3 are mutually disjoint.

12. If A and B are two given sets then, prove that $A \cap (B - A) = \phi$

13. If $A = \{1, 3, 5, 7, 8, 9\}$ and $B = \{3, 5, 8\}$ then verify:

    $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$

14. If $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 4, 5\}$and $C = \{1, 3, 4, 5, 6, 7\}$ verify

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

15. If $A \oplus$ denotes the symmetric difference of two sets A and B, then find $A \oplus B$ for the following:

    (a) $A = \{a, b\}$, $B = \{a, c\}$ (b) $A = \{a, b\}$, $B = \{b, c\}$

16. If $A = (1, 3, 5, 7, 9\}$ and $B = \{3, 5, 8\}$ then find $A \Delta B$ (symmetric difference of the sets A and B).

17. Prove (or disprove) by Venn diagram or otherwise that

    $(A \cup B) \cap (B \cup \overline{C}) \subset (A \cap \overline{B})$ (***MCA, OSM, 1997***)

18. A and B are two independent events. The Probability that both A and B occur is 1/12. The Probability that neither A nor B occures is 1/2. Find the values of $P(A)$ and $P(B)$.

19. A and B are two events such that $P(A) = 0.3$, $P(B) = 0.4$ and $P\,\overline{(AB)} = 0.5$ find $P\left(B \mid \left(A \cup \overline{B}\right)\right)$.

20. A die of 6 faces is thrown 4 times. What is the probability that the minimul value is not less than 2 and the maximum value is not grater than 5

21. Define a partition of a set.

22. Define a power set. Illustrate with an example.

Answers:

II 1. (a) $\{1, 2, 4, 5\}$; (b) $\{1, 2\}$; (c) $\{1, 2, 4, 5, 7, 9, 10\}$; (d) ϕ; (e) $\{5\}$; (f) $\{1, 2, 5, 7, 9, 10\}$

2. (a) $\{a, b, c, d, e, f, g, h\}$, ($b$) $\{c, d\}$, (c) $\{c, d, e\}$, (d) $\{c, d, e\}$

3. $\overline{A} = \{x \in Z \mid -5 < x < -2 \cup 3 < x < 5\}$

   $\overline{A} \cap \overline{A} = U$

   $A \cap U = A,\ A \cup U = U$

5. $\bar{A} = \{e, f, g\}, \bar{B} = \{b, g\}, \bar{C} = \{c, d, e, f\}$,
   $A - B = \{b\}, B - C = \{c, d, e, f\}$
   $A \cap B = \{a, c, d\}$
   $A \cup B = \{a, b, c, d, e, f\}$
   $B \cap C = \{a, b\}$
6. $A \cap B = \{b, e, f\}, A \cap C = \{a\}, B \cap C = \phi$
7. $\bar{A} = \{x | x \in Z, x > 4\}$
8. (*a*) $A - B = \{c, f, g\}$
   (*b*) $\bar{A} = \{b, d, e\}$
   (*c*) $\bar{B} = \{b, c, d, f, g\}$
   (*d*) $\{a, c, e, f, g\}$
9. (*a*) $P(A) = \{\{f\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}$
   (*b*) $\{f, \{a\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, b, d\}, \{a, c, d\}$ $\{b, c, d\}\{a, b, c, d\}\}$
15. (*a*) $\{b, c\}$, (*b*) $\{a, c\}$
16. $A \Delta B = \{1, 7, 8, 9\}$
18. $\frac{1}{4}, \frac{1}{3}$
19. $\frac{1}{4}$
20. $\frac{16}{81}$

2.25 SETS OF NUMBERS

We now introduce here several sets and their notations that will be used throughout this book.

(*a*) $Z^+ = \{x \mid x \text{ is a positive integer}\} = \{1, 2, 3,4...\}$

(*b*) $N = \{x \mid x \text{ is a positive integer and zero}\} = \{0, 1, 2, 3, 4...\}$

Note: 1, 2, 3, 4 … are natural numbers.

(*c*) The rational integers are the members of the set *Z*, where

$$Z = \{... -3, -2, -1, 0, 1, 2, 3, 4 ...\}$$

(*d*) The rational numbers are the members of the set.

$$Q = \{p/q \mid p \in Z, q \in Z, \text{ and } q \neq 0\}$$

(*e*) The irrational numbers are the members of the set of all real numbers that cannot be expressed as the quotient *p*/*q* of two integers.

Example: $\sqrt{2}, \sqrt{3}, \pi,$ ..., etc., are all irrational.

(*f*) The real numbers are the members of the set formed by the union of the sets of rational and irrational numbers it is denoted by *R*.

$$\therefore\ R = \{x \mid x \text{ is a real number}\}$$

2.26 CARDINALITY

2.26.1 Finite Set

Definition 2.18: A set *A* is called a finite set if it has *n* distinct members (elements) where $n \in N$ (refer 1.5).

2.26.2 Cardinality of a Set

Definition 2.19: If *A* is finite set with *n* distinct elements, then *n* is called the cardinality of *A*. The cardinality of *A* is denoted by $|A|$ [or by $n(A)$].

Example: Let $A = \{a, b, c, d\}$, then *A* is a finite set and $|A| = 4$

2.26.3 Cardinality of Union of Two Sets

Number of elements in $A \cup B$: (Cardinality of union) If *A* and *B* are any two finite sets then, the numbers of elements in $A \cup B$, denoted by $|A \cup B|$ is given by $|A \cup B| = |A| + |B| - |A \cap B|$

Note: The number of elements in $A \cap B$, is also denoted by $n(A \cup B)$.

2.26.4 Cardinality of Union of Three Sets

Number of elements in $A \cup B \cup C$: If *A*, *B* and *C* are any three finite sets, then

$$|A \cup B \cup C| = |A| + |B| + |C| - |B \cap C| - |C \cap A| - |A \cap B| + |A \cap B \cap C|$$

Example 1: If $n(A) = 2$, $n(B) = 3$, $n(A \cap B) = 1$, find $n(A \cup B)$

Solution: Given $|A| = 2$, $|B| = 3$, $|A \cap B| = 1$

Using the formula $|A \cup B| = |A| + |B| - |A \cap B|$

We get $|A \cup B| = 2 + 3 - 1 = 4$

Example 2: Verify:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

Where $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 3, 4, 6\}$, $C = \{3, 4, 6, 8\}$

Solution: We have $A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 8\}$

$$A \cap B \cap C = \{3, 4\}$$

$$A \cap B = \{2, 3, 4\},\ B \cap C = \{3, 4, 6\}$$

$$C \cap A = \{3, 4\}$$

$$|A|+|B|+|C|-|A\cap B|-|B\cap C|-|C\cap A|+|A\cap B\cap C|$$
$$=5+4+4-3-3-2+2$$
$$=7=|A\cap B\cap C|$$

Example 3: Out of 30 students in a dormitory, 15 take an art course, 8 take a biology course and 6 take a chemistry course. It is known that 3 students take all the three courses. Show that 7 or more students take none of the courses.

Solution: Let A be the set of students taking an art course
B be the set of students taking a biology course
C be the set of students taking a chemistry course

Then we have

$$|A|=15, |B|=8, |C|=6, |A\cap B\cap C|=3$$

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|B\cap C|-|C\cap A|+|A\cap B\cap C|$$
$$=15+8+6-|A\cap B|-|B\cap C|-|C\cap A|+3$$
$$=3\ 2-|A\cap B|-|B\cap C|-|C\cap A| \quad \text{... (1)}$$

But $|A\cap B|\geq|A\cap B\cap C|, |B\cap C|\geq|A\cap B\cap C|, |C\cap A|\geq|A\cap B\cap C|$

Therefore, $|A\cap B|+|B\cap C|+|C\cap A|\geq 3\,|A\cap B\cap C|$

From (1), we have

$$|A\cup B\cup C|\geq 32-3\,|A\cap B\cap C|=32-3\times 3$$

Hence $|A\cup B\cup C|\geq 23$

The number of students taking atleast one course ≥ 23. The students taking none of the courses $\geq 30-23=7$.

Hence, seven or more students take none of the courses.

2.26.5 Comparable Sets

Definition 2.20: Two sets A and B are said to be comparable if $A\subset B$ or $B\subset A$

2.26.6 Sets Not Comparable

Definition 2.21: Two sets A and B are said to be not comparable if $A\not\subset B$ and $B\not\subset A$.

Example 1: Let $A=\{1, 2, 3\}$ and $B=\{1, 2, 3, 4, 6\}$ then A is comparable to B, since A is a subset of B.

Example 2: If $A=\{a, c\}, B=\{b, c, d, e, f\}$ then $A\not\subset B$ and $B\not\subset A$. Therefore the sets A and B are not comparable.

2.26.7 Multiset

Definition 2.22: A collection of objects that are not necessarily distinct is called a multiset.

Example: $\{a, a, b, b\ c, c\}$

2.26.8 Multiplicity

Definition 2.23: Let S be a multiset and $x \in S$. The multiplicity of x is defined to be the numbers of times the element x appears in the multiset S.

Example 1: Let $S = \{a, a, b, b, b, d, d, d, e\}$

Then Multiplicity of a is 2

Multiplicity of b is 3

Multiplicity of d is 3

Multiplicity of e is 1

If A and B are multisets then $A \cup B$ and $A \cap B$ are also multisets. The multiplicity of an element $x \in A \cup B$ is equal to the maximum of the multiplicity of x in A and B.

The multiplicity of $x \in A \cap B$ is equal to the minimum of the multiplicities of x in A and in B.

Example 2: Let $A = \{a, a, a, b, b, c, c, d, d\}$

and $B = \{a, a, b, b, c, d\}$

Then $A \cup B = \left\{a, a, a, b, b, c, c, d, d\right\}$

$A \cap B = \{a, a, b, c, d\}$

2.27 CARTESIAN PRODUCT OF SETS

2.27.1 Ordered Pair

Definition 2.24: If $a \in B$, and $b \in B$ then the ordered pair is the set $\{\{a\}, \{a, b,\}\}$ consisting of the pair $\{a, b\}$ and the singleton $\{a\}$. It is represented by (a, b).

In the ordered pair (a, b), the element is a called the first element and the element b is called the second element.

Example: If $P\,(x, y)$ is a point in the plane, then the coordinates of P from an pair. The first member x, is called the x-coordinate of P and y is called y-coordinate of P.

Note: If (a, b) and (a', b') are two ordered pairs such that $(a, b) = (a', b')$ then $a = a'$ and $b = b'$.

2.27.2 Cartesian Product

Definition 2.25: If A and B are two non-empty sets, then the cartesian product of A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

The cartesian product of the sets A and B is denoted by $A \times B$.

Using set notation we can write $A \times B$ as

$$A \times B = \{(a, b) \mid a \in A, \text{ and } b \in B\}$$

Example: If $A = (0, 1, 2)$, $B = \{3, 5\}$, then

$$A \times B = \{(0, 3), (0, 5), (1, 3), (1, 5), (2, 3), (2, 5)\}$$

Note: If A and B are both the set of real numbers then $A \times B$ is the cartesian plane. The cartesian product of sets can also be represented by tree diagrams.

2.27.3

If A, B, C are sets then

(*i*) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

(*ii*) $A \times (B \cap C) = (A \times B) \cap (A \times C)$ ***(V.T.U., B.E., 2000)***

Proof: (*i*) $A \times (B \cup C)$

$$= \{(x, y) : x \in A,\ y \in B \cup C\}$$
$$= \{(x, y) : x \in A \text{ and } y \in B \text{ or } y \in C\}$$
$$= \{(x, y) : x \in A,\ y \in B \text{ or } x \in A,\ y \in C\}$$
$$= \{(x, y) : (x, y) \in A \times B \text{ or } (x, y) \in A \times C\}$$
$$= (A \times B) \cup (A \times C)$$

(*ii*) $A \times (B \cap C)$

$$= \{(x, y): x \in A,\ y \in B \cap C\}$$
$$= \{(x, y): x \in A \text{ and } y \in B \text{ and } y \in C\}$$
$$= \{(x, y): x \in A,\ y \in B \text{ and } x \in A,\ y \in C\}$$
$$= \{(x, y): (x, y) \in A \times B \text{ and } (x, y) \in A \times C\}$$
$$= (A \times B) \cap (A \times C)$$

2.27.4

If A, B, and C are non-empty sets then

$$A \subseteq B \Rightarrow A \times C \subseteq B \times C$$

Proof: Let (a, b) be any element $A \times C$, then

$$\Rightarrow a \in B \text{ and } b \in C \qquad (\because A \subseteq B)$$
$$\Rightarrow (a, b) \in B \times C$$

Hence $A \times C \subseteq B \times C$

2.27.5 Cartesian Product of *n* Sets

Let $A_1, A_2, A_3, ..., A_n$ denote n sets where $n \geq 2$, then the Cartesian product $A_1 \times A_2 \times ... A_n$ is the set of all n-tuples of the form $(a_1, a_2, a_3, ..., a_n)$ where $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$, $a_n \in A_n$.

From the definition we have

$$A_1 \times A_2 \times A_3 \times ... A_n = \{(a_1, a_2, a_3, ..., a_n): a_i \in A_i,\ 1 \leq i \leq n\}$$

EXERCISE 2.2

1. Let $A = \{1, 2, 4\}$, $B = \{0, 2\}$ find $A \times B$.

2. Prove that $A \times B = \phi$ if $A = \phi$, $B = \phi$.

3. Prove that $A \times B = B \times A$ if and only of $A = B$.

4. If $A = \{a, b\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$

Find

(1) $A \times (B \cup C)$, $(A \times B) \cup (A \times C)$ and show that

$A \times (B \cup C) = (A \times B) \cup (A \times C)$

(2) Find $A \times (B \cap C)$ and show that

$A \times (B \cap C) = (A \times B) \cap (A \times C)$

5. If A, B and C are sets then

6. Prove that

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

(*ii*) Show that $\overline{A} - \overline{B} = B - A$

7. If A, B and C are any sets

Show that $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

8. If A is a proper subset of B, then show that $A \cup (B - A) = B$

9. Prove (or disprove) by Venn diagram or otherwise that

$(A \cup B) \cap \left(B \cup \overline{C}\right) \subset \left(A \cap \overline{B}\right)$ ***(OU, MCA, 1997)***

10. Define the following:

(*i*) Power set

(*ii*) Partition of a set give examples

11. Prove the following and represent by Venn diagram:

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

(*ii*) $A - (B \cup C) = (A - B) \cap (A - C)$ ***(OU, MCA, 1991)***

12. Show by an example that

(*i*) $A \times B \neq B \times A$

(*ii*) $(A \times B) \times C = A \times (B \times C)$ ***(OU, MCA, 1994)***

13. Write the sets

(*i*) $\phi \cup \{\phi\}$

(*ii*) $\{\phi\} \cup \{\phi\}$ and

(*iii*) $\{\phi, \{\phi\}\} - \phi$ ***(OU, MCA, 1995)***

14. Show that $A \subseteq B$ implies that $A \cup (B - A) = 0$ ***(OU, MCA, 1995)***

15. Show that $A - B \subseteq C$ if and only if $A - C \subseteq B$ ***(OU, MCA, 1995)***

16. If A and B subsets of the Universal set U, then show that

$\overline{A} \oplus \overline{B} = A \oplus B$ ***(OU, MCA, 1995)***

17. For the sets S, T and V prove that

$(S \cap T) \times V = (S \times V) \cap (T \times V)$ ***(OU, MCA, 1995, 96)***

18. Use Venn diagrams to show that

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ***(OU, MCA, 1998)***

19. Show that $P(A) \cup P(B) \subseteq P(A \cup B)$ where $P(X)$ is the powerset of X. ***(OU, MCA, 1998)***

20. Let A, B, C be subsets of U prove or disprove

$(A \cup B) \cap \left(B \cup \overline{C}\right) \subset A \cap B$ ***(OU, MCA, 1998)***

21. (*a*) Show that $A \subseteq B \Leftrightarrow A \cup B = B$

(*b*) $A \cap \overline{A} = \phi$; $A + \phi = A$ ***(OU, MCA, 1999)***

22. 35 children of a class draw a map. 26 children use red colour and some children use yellow colour. If 19 use both the colours. Find the number of children who used the yellow colour.

(Ans: 28)

23. In a class of 42 students each play atleast one of three games—hockey, cricket, and football. It is found that the play cricket, 20 play hockey and 24 play football, 3 play both cricket and football, 2 play both hockey and football and none play all the three games. Find the number of students who play cricket but not hockey. ***(Ans: 31)***

24. Use Venn diagram to show that the following argument is valid:

P_1: All dictionaries are useful

P_2: Many owns only romance novels

P_3: No violance novel is useful

P_4: Many does not own a dictionary.

25. In a survey of 500 people 285 are interested in football game, 195 are interested in hockey game, 115 are interested in basketball game, 45 in football and basketball, 70 in football and hockey and 50 in hockey and basketball games; and 50 are not interested in any of these three games.

(*i*) How many people are interested in all the three of the games?

(*ii*) How many people are interested in exactly one of the games? ***(VTU, BE, Aug. 2000)***

26. If there are 200 faculty members that speak French, 50 that speak Russian, 100 that speak Spanish, 20 that speak French and Russian, 60 that speak French and Spanish, 35 that speak Russian and Spanish, while only 10 that speak French, Russian and Spanish. Determine how many speak either French or Russian or Spanish? ***(VTU, MCD, Sep. 1999)***

27. If A_k are sets such that $A_0 = \{a/a \leq 1\}$ and $A_k = \{a/a \leq 1 + 1/k\}$, prove that $\underset{k=1}{\overset{\infty}{\pi}} A_k = A_0$.

3

Relations

3.1 CONCEPT OF RELATION

This chapter deals primarily with the concept of a Relation.

A relation may involve equality or inequality. The mathematical concept of a relation deals with the way the variables are related or paired. A relation may signify a family tie between such as “is the son of” “is the brother of”, “ is the sister of”. In mathematics the expressions like, “is less than”, “is greater than”, “is perpendicular to”, “is parallel to” are relations. In this chapter, we shall only consider relations called binary relations. The ‘equivalence relation’ in sets is also discussed.

Definition 3.1: Let A and B be non-empty sets, then any subset of R of the cartesian product $A \times B$ is called a relation from A to B.

Example 1: Let $A = \{3, 6, 9\}$, $B = \{4, 8, 12\}$

Then $R = \{(3, 4), (3, 8), (4, 12)\}$ is a relation from A to B.

Example 2: Let $A = \{1, 2, 3\}$, $B = \{a, b\}$

Then $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

If $R = \{(1, a), (3, b)\}$, then $R \subseteq A \times B$ and R is a relation from A to B.

Example 3: Let A denote the set of real numbers define

$R = \{(a, b)\colon 4a^2 + 25b^2 \leq 100\}$ clearly R is a relation on A.

If $(a, b) \in R$, we often write aRb and state “a is related to b”.

If $R \subseteq A \times A$, then R is a relation from A to A, and R is called a relation in A.

If R is a relation from A to B, then the set of all first elements of the ordered pairs (a, b), which belong to R is called the domain of R. The range of R is the set of all second coordinates of the ordered pairs (a, b) which belong to R. From the definition it is clear that relation R is also a set and many operations can be applied to relation R to obtain a new relation.

If R_1 and R_2 are two relations with the same domain D and same range then we can define the relation $R_1 \cup R_2$ and $R_1 \cap R_2$ with the same domain D and same range R.

Null set $\varnothing$ is a subset of every set. Therefore for any specified non-empty domain, and range, $\varnothing$ is a relation, called null relation or empty relation.

3.2 PROPERTIES OF RELATIONS

3.2.1 Reflexive Relation

Definition 3.2: Let *R* be a relation defined in a set *A*; then *R* is reflexive if *aRa* holds for all $a \in A$, i.e., if $(a, a) \in R$ for all $a \in A$.

Example 1: Let $A = \{a, b, c\}$ and $R = \{(a, a), (b, b), (c, c)\}$ then *R* is a reflexive relation in *A*.

Example 2: 'Equality' is a reflexive relation, since an element equals itself.

3.2.2 Symmetric Relation

Definition 3.3: A relation *R* defined in set *A* is said to be 'symmetric' if *bRa* holds whenever *aRb* holds for $b \in A$, i.e., *R* is symmetric in *A* if

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

Example: Let *R* be relation 'is perpendicular to' in the set of all straight lines, then *R* is a symmetric relation.

3.2.3 Transitive Relation

Definition 3.4: A relation *R* in set *A* is said to be transitive if

$$(a, b) \in R \ (b, c) \in R \Rightarrow (a, c) \in R$$

i.e., if *aRb* and $bRc \Rightarrow aRc,\ a, b, c \in A.$

Example 1: Let *A* denote the set of straight lines in a plane and *R* be a relation in *A* defined by 'is parallel to' then *R* is a transitive relation in *A*.

Example 2: Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$ then *R* is transitive.

3.2.4 Equivalence Relation

Definition 3.5: A relation *R* in a set *A* is said to be an equivalence relation in *A*, if *R* is reflexive, symmetric and transitive.

Example: (*i*) Let *A* be the set of all triangle in a plane and let *R* be a relation in *A* defined by 'is congruent to', then *R* is reflexive, symmetric and transitive.

$\therefore$ *R* is an Equivalence relation in *A*.

(*ii*) Let $A = \{a, b, c\}$, and $R = \{(a, a), (a, b), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$ then *R* is an equivalence relation in *A*.

3.2.5 Anti-symmetric Relation

Definition 3.6: Let *R* be a relation in a set *A*, then *R* is called anti-symmetric.

$$(a, b) \in R,\ (b, a) \in R \Rightarrow a = b \ \forall \ a, b \in R$$

i.e., *aRb* and $bRb \Rightarrow a = b$

Example: Let *N* denote the set of Natural Numbers *R* be a relation in *N*, defined by '*a* is a divisor' of *b*, i.e., *aRb* if a divides *b* then *R* is anti-symmetric since *a* divides *b* and *b* divides $a \Rightarrow a = b$.

3.2.6 The Inverse of a Relation

Let R be a relation from A to B. Then the relation $R^{-1} = \{(b, a): (a, b) \in R\}$ from B to A is called the inverse of R.

Example: Let $A = \{1, 2, 3\}$, $B = \{4, 5\}$ and $R = \{(1, 4), (2, 5), (3, 5)\}$ be a relation from A to B. then $R^{-1} = \{(4, 1), (5, 2), (5, 3)\}$

3.3 MISCELLANEOUS EXAMPLES

Example 1: If a relation R is transitive then prove that its inverse relation R^{-1} is also transitive.

Solution: Let (a, b) and $(b, c) \in R^{-1}$ then $(b, a) \in R$ and $(c, b) \in R$ is transitive, therefore R

$$(c, b) \in R \text{ and } (b, a) \in R \Rightarrow (c, a) \in R$$

$$\Rightarrow (a, c) \in R^{-1}$$

i.e., $(a, b) \in R^{-1}$ and $(b, c) \in R^{-1} \Rightarrow (a, c) \in R^{-1}$

Hence R^{-1} is transitive.

Example 2: $A = \{2, 3\}$, $B = \{3, 4, 5, 6\}$ and R is a relation from A to B defined as follows:

$(a, b) \in R$ if "a divides b" write the solution set of R.

Solution: 2 divides 4 and 2 divides 6

$$\Rightarrow (2, 4) \in R \text{ and } (2, 6) \in R$$

3 divides 3, 3 divides 6

$$\Rightarrow (3, 3) \in R \text{ and } (3, 6) \in R$$

4 divides 4 $\Rightarrow (4, 4) \in R$

Thus $R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$

Example 3: Let A be the set of triangles in the Euclidean plane, and R is the relation in A defined by "a is similar to b" then show that R is an equivalence relation in A.

Solution: Every triangle is similar to itself: the relation R is reflexive. If "a is similar to b" then "b is similar to a", i.e. $(a, b) \Rightarrow (b, a) \in R$

Hence R is symmetirc.

Clearly, if "a is similar to b", "b is similar to c" then "a is similar to c".

Therefore, the relation R is transitive. R is reflexive, symmetric and transitive. Thus R is an equivalence relation.

Example 4: X is a family of sets and R is relation in X defined by "x is subset of y" show that R is anti-symmetric and transitive.

Solution: Let $(A, B) \in R$ and $(B, A) \in R$ then $A \subset B$ and $B \subset A \Rightarrow A = B$.

Thus R is anti-symmetric also $A \subset B$, $B \subset C \Rightarrow A \subset C$. Therefore R is transitive.

Example 5: Show that the relation "Equality" defined in any set A, is an Equivalence relation.

Solution: (*i*) $a = a$ for every $a \in A$

Thus R is reflexive

$a = b$ implies $b = a$ for all $a, b \in A$

$\therefore$ R is symmetric

and (*ii*) $a = b$, $b = c$ implies $a = c$

for all $a, b, c \in A$

$\therefore$ R is transitive.

Thus R is an equivalence relation in A.

Example 6: Let Z denote the set of integers and the relation R in Z be defined by "aRb" iff $a - b$ is an even integer". Then show that R is an equivalence relation.

1. R is reflexive; since
   $\varnothing = a - a$ is even, hence aRa for every $a \in Z$.
2. R is symmetric:
   If $a - b$ is even then $b - a = -(a - b)$ is also even hence $aRb \Rightarrow bRa$
3. R is transitive: for if aRb and bRc then both $a - b$ and $b - c$ are even.
   Consequently, $a - c = (a - b) + (b - c)$ is also even.
   $\therefore$ aRb and $bRc \Rightarrow aRc$

Thus, R is an equivalence relation.

3.4 IRREFLEXIVE RELATION

Definition 3.7: A relation R on a set A is irreflexive if $a \not R a$ for every $a \in A$

Example: Let $A = \{1, 2, 3\}$ and

$$R = \{(1, 2), (2, 3), (3, 1), (2, 1)\}$$

Then the relation R is irreflexive on A.

3.5 ASYMMETRIC RELATION

Definition 3.8: A relation R defined on a set A is asymmetric if whenever aRb, then $b \not R a$.

Example: Let $A = \{a, b, c\}$ and $R = \{(a, b), (b, c)\}$ be a relation on A. Clearly R is a symmetric.

3.6 COMPATIBLE RELATION

Definition 3.9: A relation R in A is said to be a compatible relation if it is reflexive and symmetric.

If R is an equivalence relation on A, then R is compatible relation on A.

3.7 UNIVERSAL RELATION

Definition 3.10: A relation R in a set A is said to be universal relation if

$$R = A \times A.$$

Example 1: Let $A = \{a, b\}$, then

$R = \{(a, a), (a, b), (b, a), (b, b)\}$ is a universal relation on set A.

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

$$R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$$

is a universal relation on A.

3.8 COMPLEMENTARY RELATION

Definition 3.11: Let R be a relation from A to B, then the complement of R denoted by R' and is expressed in terms of R as follows;

$$aRb \text{ if } a \not R b$$

Example: Let $A = \{1, 2, 3\}$ and

$$R = \{(1, 1), (1, 2), (1, 3), (2, 2), (3, 3)\}$$

Then $$R' = \{(2, 1), (2, 3), (3, 1), (3, 2)\}$$

3.9 RELATION-RELATED SETS

Definition 3.12: Let A and B denote two non-empty sets and R be a relation from A to B. We can define various sets related to the relation R:

3.9.1 *R*-relative Set of an Element

Let $x \in A$, then the R-relative set of x is defined to be the set of all elements y in B with the property that x is related to y, where R is relation from A to B. It is denoted by $R(x)$ or by $[x]R$. Thus in symbols we can write:

$$R(x) = [x]R = \{y \in B/xRy\}$$

Example: Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$ and $R = \{(1, a), (2, b), (3, c), (3, d)\}$

Then $R(3) = \{c, d\}$.

3.9.2 *R*-relative Set of a Subset

Definition 3.13: Let $A_1 \subseteq A$, then the R-relative set of A_1 is said to be the set of all elements y in such that x is R-related to y for some $x \in A_1$. It is denoted by

$R(A_1)$. Thus in symbols:

$$R(A_1) = \{\, y \in B \mid xRy \text{ for some } x \text{ in } A_1\}$$

Example: Let $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$ and $R = \{(1, a), (2, b), (2, d), (3, c), (4, d), (5, c), (5, d)\}$

If $A_1 = \{2, 5\}$ then $R(A_1) = \{b, c, d\}$

3.10 EQUIVALENCE CLASSES

Let $A = \{1, 2, 3, 4\}$ and

$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1)\}$ be a relation defined on A.

Clearly R is reflexive, symmetric and transitive. Therefore R is an Equivalence relation on A.

Consider $[1]_R$, $[2]_R$, and $[4]_R$

We have $[1]_R = \{1, 2\}$, $[2]_R = \{1, 2\}$,

$[3]_R = \{3\}$ and $[4]_R = \{4\}$

Observe that

$$[1]_R = [2]_R$$

$$[1]_R \cap [3]_R = [1]_R \cap [4]_R = [2]_R \cap [3]_R = [2]_R \cap [4]_R = \varnothing$$

and $$[1]_R \cup [2]_R \cup [3]_R \cup [4]_R = A$$

Thus, the relation R is such that it gives rise to subset $[x]_R$ of A for which either $[x]_R = [y]_R$ or $[x]_R \cap [y]_R = \varnothing \ \forall\ x, y \in A$

Thus, the relation R on A, induces a partition in A.

Theorem 3.1: Every equivalence relation on a set generates a unique partition of the set. The blocks of this partition correspond to the R-equivalence classes.

Proof: Let R be an equivalence defined on a set A. For any $x \in A$ the $[x]_R \subseteq A$ be given by

$$[x]_R = \{y \mid y \in A \text{ and } x R y\}$$

The relation R is an equivalence relation

$\Rightarrow$ R is reflexive

$\Rightarrow$ $x R x$ is true

$\Rightarrow$ $x \in [y]_R$

Let $y \in A$ such that xRy, then $y \in [y]_R$

R is symmetric, therefore $xRy \Rightarrow yR x$

$$x \in [y]_R$$

Let $z \in [y]_R$ then

$$xR\, y,\ xR\, z \Rightarrow yR\, z$$

$$\Rightarrow [y]_R \subseteq [x]_R$$

by symmetry, $$[x]_R \subseteq [y]_R$$

$\therefore$ $$[x]_R \subseteq [y]_R \text{ and } [y]_R \subseteq [x]_R \Rightarrow [x]_R \subseteq [y]_R$$

If xRy, then it is shown that $[x]_R = [y]_R$. If $x \not R y$, then we must show that $[x]_R$ and $[y]_R$ are disjoint. To prove that, let us assume that, there is atleast one element

say $$z \in [x]_R \cap [y]_R$$

now, $xR\, z$ and $yR\, y$

$\Rightarrow$ $xR\, z$ and $yR\, y$

$\Rightarrow$ $xR\, y$ [by Transitivity]

which is a contradiction

Hence $$xR\, y \Rightarrow [x]_R \cap [y]_R = \varnothing$$

From the above it is clear that each element of A generates an R-equivalence class which is non-empty. The R-equivalence classes generated by any two elements are either equal or disjoint, and the union of R-equivalence classes generated by the element of A is the set A. Hence the R-equivalence classes generated by the elements of A defines a partition of A.

Note: The family of equivalence classes generated by the elements of A is denoted by A/R and is called quotient set of A and R. Each element of A/R is a set.

Example: Let Z be the set of integers and let R be the relation called "congruent modulo 5" defined by

$$R = \{(x,\ y) \mid x \in Z,\ y \in Z \text{ and } (x - y) \text{ is divisible by } 5\}$$

Determine the equivalence classes generated by the element of Z.

Solution: The equivalence classes are

$[0]_R = \{ \ldots \ldots -10, -5, 0, 5, 10, 15, \ldots\}$

$[1]_R = \{ \ldots \ldots -9, -4, 1, 6, 11, 16, \ldots\}$

$[2]_R = \{ \ldots \ldots -8, -3, 2, 7, 12, 17, \ldots\}$

$[3]_R = \{ \ldots \ldots -7, -2, 3, 8, 13, 18, \ldots\}$

$[4]_R = \{ \ldots \ldots -6, -1, 4, 9, 14, 19, \ldots\}$

$\therefore \quad Z/R = \{[0]_R, [1]_R, [2]_R, [3]_R, [4]_R\}$

3.11 RELATIONS ON COORDINATE DIAGRAMS

If A and B are two subsets of the set of real numbers and R is relation from A to B; then the relation R can be displayed on a coordinate diagram of $A \times B$ in which the ordered pairs of R are represented by points in a cartesian plane.

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

$R = \{(1, 3), (1, 5), (2, 3) (3, 3), (3, 5), (4, 5)\}$

Sketch R on the coordinate diagram of $A \times B$

Solution: The sketch of R on the coordinate diagram of $A \times B$ is a follows.

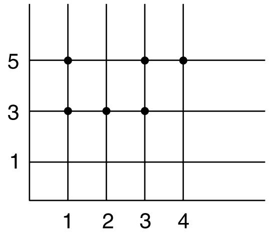


Fig. 3.1

3.12 TABULAR FORM OF A RELATION

A relation (Binary relation) on a set A can be represented in the tabular form. The tabular form of a relation is useful in determining whether the binary relation is a reflexive relation.

For example: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (1, 2), (2, 2), (1, 4), (2, 4), (3, 2), (4, 3)\}$ be a relation on A

The tabular form of the relation R is given below:

	1	2	3	4
1	✓	✓		✓
2		✓		✓
3		✓		
4			✓	

Fig. 3.2

The check marks in the cells represent the elements (the ordered pairs) of R. If the cells in the main diagonal of table contain check marks then R is reflexive. For example: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$

The tabular form of R is:

	1	2	3	4
1	✓			✓
2		✓		✓
3			✓	
4				✓

Fig. 3.3

The cells in the main diagonal of the table contain check marks. Thus R is a reflexive relation in A.

If the relation R is a symmetrical relation in a set A, then the check marks will be symmetrical with respect to the main diagonal in the table. For example, consider the relation

$R = \{(1, 2), (1, 4), (2, 1), (2, 3), (3, 2), (3, 4), (4, 1), (4, 3), (4, 4)\}$

Defined on the set $A = \{1, 2, 3, 4\}$

The table given below represents R:

	1	2	3	4
1		✓		✓
2	✓		✓	
3		✓		✓
4	✓		✓	✓

Fig. 3.4

The check marks are in cells that are symmetric with respect to the main diagonal. Therefore R is symmetric.

3.13 TRANSITIVE EXTENSION

Definition 3.14: Let R be a relation on the set A. Another relation R_1 defined on A is called the transitive extension of R if R_1 contains R and

$(a, b) \in R,\ (b, c) \in R \Rightarrow\ (a, c) \in R_1$

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

$R = \{(1, 2), (2, 3), (3, 2), (2, 4)\}$ and

$R_1 = \{(1, 2), (1, 3), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$

Clearly R_1 contains R and $(a, b) \in R, (b, c) \in R \Rightarrow\ (a, c) \in R_1$

	1	2	3	4
1		✓		
2			✓	✓
3		✓		
4				

(*a*) Relation *R*

	1	2	3	4
1		✓	✓	
2		✓	✓	✓
3		✓	✓	✓
4				

(*b*) Relation R_1

Fig. 3.5

R is shown in Fig. 3.5 (*a*) and R_1 is shown in Fig. 3.5 (*b*). Note that the ordered pairs in R_1 which are not in R are marked with heavy check marks.

3.14 TRANSITIVE CLOSURE

Definition 3.15: Let R be a relation on the set A. R_1 denote the transitive extension of R, R_2 denote the transitive extension of R_1 and in general R_{i+1} denote the transitive extension of R_i, then the transitive closure of R is defined as the set union of R, R_1, R_2, … R_i, R_{i+1}…. It is denoted by R^+. Thus

$$R^+ = R \cup R_1 \cup R_2 \cup \ldots \cup R_i \cup R_{i+1} \cup \ldots.$$

R^+ is the smallest transitive relation containing R.

Example: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4), (2, 1)\}$

Then $R^+ = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4)\}$ is the transitive closure of R.

Theorem 3.2: Let R be a relation from A to B and let A_1 and A_2 be two subsets of A, then

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

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

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

Proof: (*i*) Let $y \in R(A_1)$

$$y \in R(A_1) \Rightarrow xR\,y \text{ for some } x \in A_1$$

$$\Rightarrow x \in A_2 \qquad [\text{Since } A_1 \subseteq A_2]$$

$$\therefore \qquad R(A_1) \subseteq R(A_2)$$

(*ii*) Let $y \in R(A_1 \cup A_2)$ then xRy for some x in $A_1 \cup A_2$ now $x \in A_1 \cup A_2 \Rightarrow x \in A_1$ or $x \in A_2$

If $x \in A_1$, then $xRy \Rightarrow y \in R(A_1)$ by the same argument; if $x \in A_2$ then $y \in R(A_2)$ in either case $y \in R(A_1) \cup R(A_2)$

$$\therefore R(A_1 \cup A_2) \subseteq R(A_1) \cup R(A_2)$$

Conversely,

$$A_1 \subseteq A_1 \cup A_2 \Rightarrow R(A_1) \subseteq R(A_1 \cup A_2) \text{ [by } (i)]$$

similarly $A_2 \subseteq A_1 \cup A_2 \Rightarrow R(A_2) \subseteq R(A_1 \cup A_2)$

therefore $R(A_1) \cup R(A_2) \subseteq R(A_1 \cup A_2)$

Thus (*ii*) is true.

(*iii*) Let $y \in R(A_1 \cap A_2)$ then xRy for some x in $A_1 \cap A_2$ now $x \in A_1 \cap A_2 \Rightarrow x \in A_2$ and $x \in A_2$

$$\Rightarrow y \in R(A_1) \text{ and } y \in R(A_2)$$

$$\Rightarrow y \in R(A_1) \cap (A_2)$$

Thus $R(A_1 \cap A_2) \subseteq R(A_1) \cap R(A_2)$

Example 1: Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d, e, f\}$ consider the relation

$$R = \{(1, a), (1, c), (2, d), (2, e), (2, f), (3, b)\}$$

Let $A_1 = \{1, 3\}$ and $A_2 = \{2, 3\}$ then we have

$$R(A_1) = \{a, b, c\}$$

and $R(A_2) = \{b, d, e, f\}$

Hence $R(A_1) \cup R(A_2) = \{a, b, c, d, e, f\}$

and $R(A_1) \cap R(A_2) = \{b\}$

now $R(A_1 \cup A_2) = R(A) = \{a, b, c, d, e, f\}$

$$R(A_1) \cup R(A_2)$$

also $R(A_1 \cap A_2) = R\{3\} = \{b\}$

$\Rightarrow R(A_1 \cap A_2) \subseteq R(A_1) \cap R(A_2)$ holds.

Example 2: Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d, e, f\}$ consider the relation

$$R = \{(1, a), (1, c), (1, e), (2, b), (2, d), (2, f), (3, c), (3, d), (4, a), (4, f)\}$$

Let $A_1 = \{1, 4\}$ $A_2 = \{1, 3, 4\}$ then $A_1 \subset A_2$

and $R(A_1) = \{a, c, e, f\}$

$$R(A_2) = \{a, c, d, e, f\}$$

Clearly $\qquad R(A_1) \subseteq R(A_2)$

Thus $A_1 \subseteq A_2 \Rightarrow R(A_1) \subseteq R(A_2)$

3.15 MATRIX REPRESENTATION OF RELATIONS

Suppose A and B are both finite sets and R is a relation from A to B, then R may be represented as a matrix called the relation matrix of R. It is denoted by M_R.

If $A = \{a_1, a_2, \dots a_m\}$ and $B = \{b_1, b_2, \dots b_n\}$ are two finite sets containing m and n elements respectively and R is relation from A to B, then the Relation Matrix of R is the $m \times n$, matrix,

$M_R = [m_{ij}]_{m \times n}$ is defined by

$$m_{ij} = \begin{cases} 0 \text{ if } (a_i, b_j) \notin R \\ 1 \text{ if } (a_i, b_j) \in R \end{cases}$$

Where m_{ij} is the element in the ith row and jth column. M_R can be first obtained by first constituting a table, whose columns are preceded by a column consisting of successive elements of A and where rows are headed by a row consisting of successive elements of B. If $(a_i, b_i) \in R$, then we enter 1 in the ith row and jth column and if $(a_k, a_l) \notin R$, then we enter zero in the kth row and ith column.

Example 1: Let $A = \{1, 2, 3\}$ and $R = \{(x, y) \mid x < y\}$, find M_R.

Solution: We have, $R = \{(1, 2), (1, 3), (2, 3)\}$

The table and corresponding relation Matrix for the R are given below

	1	2	3
1	0	1	1
2	0	0	1
3	0	0	0

$$M_R = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Fig. 3.6

Example 2: Let $A = \{1, 4, 5\}$ and $\{(1, 4), (1, 5), (4, 1), (4, 4), (5, 5)\}$, find M_R.

Solution: Given that $R = \{(1, 4), (1, 5), (4, 1), (4, 4), (5, 5)\}$

The relation Matrix of R is

$$M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Note: If A and B are two finite sets with $|A| = m$; and $|B| = n$, then $a \;\; m \times n$ matrix, whose entries are zeros and ones determine a relation from A to B.

If R is symmetric relation on a set A, and M_R denotes the Matrix of relation R, then

$$m_{ij} = 1 \Rightarrow m_{ji} = 1$$

and $\qquad m_{ji} = 0 \Rightarrow m_{ji} = 0 \text{ in } M_R = [m_{ij}]$

i.e., $M_R = M_R^T$, where M_R^T denotes the transpose of M_R.

If R is an anti-symmetric relation on A, then $m_{ij} = 0$ or $m_{ji} = 0$ for all $i \neq j$ in M_R and if R is a transitive relation on A then

$m_{ij} = 1$ and $m_{jk} = 1 \Rightarrow m_{ik} = 1$ is satisfied by M_R. Moreover, if R is a relation from A to B and S is a relation from B to C, where A, B and C are finite sets m, n and p elements respectively, then $M_R \,.\, M_s$ can be computed. Provided M_R is $m \times n$ matrix and M_s is a $n \times p$ matrix. The Matrices $M_R \,.\, M_S$ and M_{soR} are equal.

Example 3: Let A = {1, 2, 3}

R and S be two relations defined A as follows:

$$R = \{(1,1), (1, 3), (2, 1), (2, 2), (2, 3), (3, 2)\}$$

and $$S = \{(1, 1), (2, 2), (2, 3), (3, 1), (3, 3)\}$$

then $$SoR = \{(1, 1), (1, 3), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$$

we get

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \quad M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

and $M_{SOR} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = M_R\, M_S$ can easily be verified

If

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } M_S = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

and the relational Matrices of the relation R and S defined on a set A = {1, 2, 3,4} for which

We know that

$$M_{SoR} = M_R \,.\, M_s$$

Therefore $$M_{SoR} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence $$M_{SoR} = \{(1, 1), (1, 3), (1, 4), (3, 3)\}$$

3.16 RELATIONS AND DIGRAPHS

A relation can be represented pictorially by drawing its graph. Let R be a relation on the set $A = \{a_1, a_2, \ldots a_n\}$. The element a_i of A are represented by points (or circles) called nodes (or vertices). If $(a_i, a_j) \in R_j$

then we connect the vertices a_i and a_j by means of an arc and put an arrow in the direction from a_i to a_j. If $(a_i, a_j) \in R$ and $(a_j, a_i) \in R$ then we draw two arcs between a_i and a_j (sometimes by one arc which starts from node a_i and relatives to node x_i (such an arc is called a loop). When all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, we get a graph of the relation R. If R is reflexive, then there must be a loop at each node in the graph of R. If R is symmetric, then $(a_i, a_j) \in R$ implies $(a_j, a_i) \in R$ and the nodes a_i and a_j will be connected by two arcs (edges) one from a_i to a_j and the other from a_j to a_i.

Example 1: Let $A = \{a, b, d\}$ and R be a relation on A given by

$$R = \{(a, b), (a, d), (b, d), (d, a), (d, d)\}$$

Construct the digraph of R.

Solution: The digraph of R is as shown in Fig. 3.7.

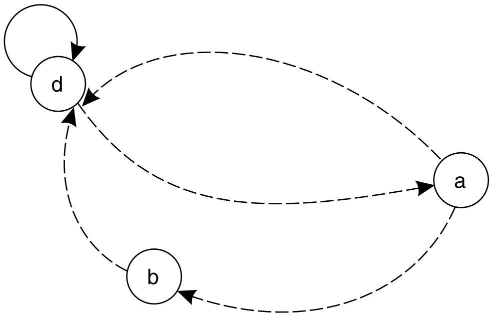


Fig. 3.7

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

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4, 1), (4, 4)\}$$

Construct the digraph of R.

Solution: The digraph of R is shown in Fig. 3.8.

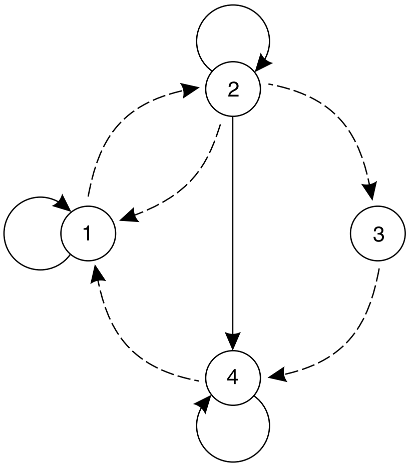


Fig. 3.8

Example 3: Find the relation determined by Fig. 3.9.

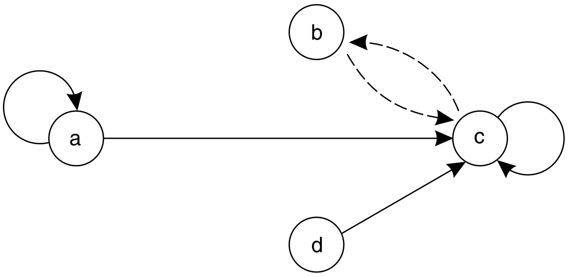


Fig. 3.9

Solution: The relation R of the digraph is

$$R = \{(a, a), (a, c), (b, c), (c, b), (c, c), (d, c)\}$$

Paths in Relation and Digraph

If R is a relation on a set A, a path of length n in R from a_i to a_j is a finite sequence P: a_i, a_1, a_2, … a_{n-1}, a_j, beginning with a_i and ending with a_j such that:

$$a_i\, Ra_1,\ a_1\, Ra_2,\ \ldots,\ a_{n-1}Ra_j$$

A path in a digraph of the relation R is succession of edges, where the indicated directions of the edges are followed. The length of a path in a digraph is the number of edges in the path. If n is a positive integer then the relation R^n on the set A can be defined as follows:

$(a_i , a_j) \in R^n$ means there is a path of length n from a_i to a_j in R. The relation R^∞ can be defined on A, by letting $(a_i , a_j) \in R^\infty$ means, that there is some path in R from a_i to a_j.

Definition 3.16: A cycle in a digraph is a path of length $n \geq 1$ from a vertex to itself.

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

$$R = \{(1, 1), (1, 2), (2, 3), (3, 5), (3, 4), (4, 5)\}$$

Compute (a) R^2 (b) R^∞.

Solution: The digraph of R is shown in Fig. 3.10.

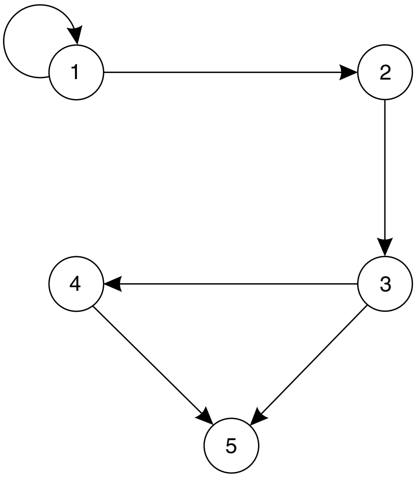


Fig. 3.10

$$(1, 1) \in R \text{ and } (1, 1) \in R \Rightarrow (1, 1) \in R^2$$
$$(1, 1) \in R \text{ and } (1, 2) \in R \Rightarrow (1, 2) \in R^2$$
$$(1, 2) \in R \text{ and } (2, 3) \in R \Rightarrow (1, 3) \in R^2$$
$$(2, 3) \in R \text{ and } (3, 5) \in R \Rightarrow (2, 5) \in R^2$$
$$(2, 3) \in R \text{ and } (3, 4) \in R \Rightarrow (2, 4) \in R^2$$
$$(3, 4) \in R \text{ and } (4, 5) \in R \Rightarrow (3, 5) \in R^2$$

Hence $R^2 = \{(1, 1), (1, 2), (1, 3), (2, 5), (2, 4), (3, 5)\}$

(*b*) There is a path from 1 to $4 \Rightarrow (1, 4) \in R^\infty$, whose length is 3.

There is a path from 1 to 5 $\Rightarrow \in R^\infty$, whose length is 3 and

There is a path from 1 to 5 whose length is 5

Hence $R^\infty = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$

Example 2: Give an example of a non-empty set and a relation on the set that satisfies each of the following combinations of properties: draw a digraph of the relation:

(1) Symmetric and reflexive but not transitive

(2) Transitive and reflexive; but not anti-symmetric

(3) Anti-symmetric and reflexive, but not transitive.

Solution: (1) Let $A = \{a, b, c\}$ and $R = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, a), (c, b)\}$ clearly R is symmetric and reflexive but not transitive. The digraph of R is given below:

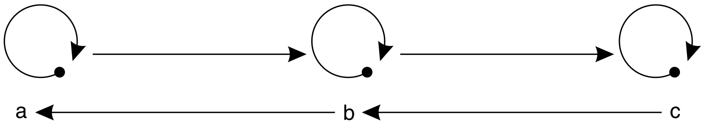


Fig. 3.11

(2) Let $A = \{a, b, c\}$, and

$$R = \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, c), (b, a), (c, b), (c, a)\}$$

The relation R is reflexive and transitive but not anti-symmetric.

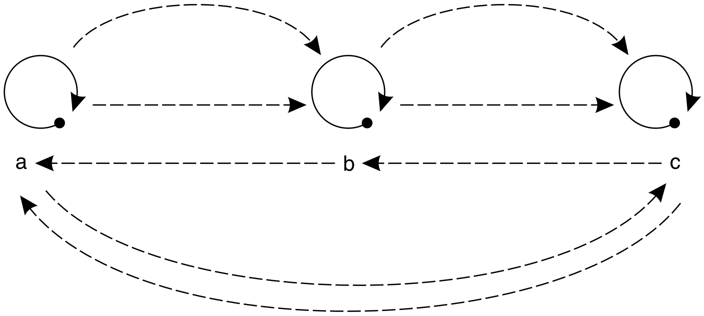


Fig. 3.12

Example 3: Let $A = \{a, b, c\}$ and $R = \{(a, b), (b, b), (c, c), (a, b), (b, c)\}$

The relation on A is symmetric and reflexive but not transitive. Figure 3.13 illustrates the relation.

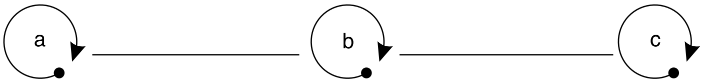


Fig. 3.13

Example 4: For the following digraph which of the special properties are satisfied by digraph's relation?

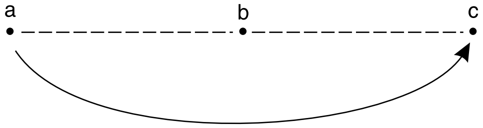


Fig. 3.14

Solution: $R = \{(a, b), (b, c), (b, c), (a, c)\}$

R is transitive and anti-symmetric on $A = \{a, b, c\}$.

3.17 COMPOSITION OF RELATIONS

Definition 3.17: Let R be a relation from A to B and S be a relation from B to C. Then we can define a relation, the composition of R and S written as SoR. The relations SoR is a relation from the set A to the set C and is defined as follows:

If $a \in A$, and $c \in A$, then $(a, c) \in S o R$ if and only if for some $b \in B$, we have $(a, b) \in R$ and $(b, c) \in S$.

Example: Let $A = \{1, 2, 3, 4\}$ and R, S be two relations on A defined by

$$R = \{(1, 2), (1, 3), (2, 4), (3, 2)\};$$

$$S = \{(1, 4), (4, 3), (2, 3), (3, 1)\} \text{ find } SoR.$$

Solution:

$$(1, 2) \in R \text{ and } (2, 3) \in S \Rightarrow (1, 3) \in S o R$$

$$(1, 3) \in R \text{ and } (3, 1) \in S \Rightarrow (1, 3) \in S o R$$

$$(3, 2) \in R \text{ and } (2, 3) \in S \Rightarrow (3, 3) \in S o R$$

$$(2, 4) \in R \text{ and } (4, 3) \in S \Rightarrow (2, 3) \in S o R$$

Thus $$S oR = \{(1, 3), (1, 1), (3, 3), (2, 3)\}$$

Theorem 3.3: If R is relation from A to B, S is a relation from B to C and T is a relation from C to D. Then

$$To\ (SoR) = (ToS)\ oR$$

Proof: Let M_R, M_S, M_T denote the Matrices related to relations R, S and T respectively, then

$$M_{To\ (SoR)} = M_{SoR} \,.\, M_T$$
$$= (M_R \,.\, M_S) \,.\, M_T = (M_R \,.\, M_S) \,.\, M_T$$

(Q Multiplication of matrices is associative)

$$= M_R \,.\, (M_{ToS}) = M_{(ToS)\ oR}$$
$$\Rightarrow\ To\ (SoR) = (ToS)\ oR$$

Theorem 3.4: Let R be a relation from the set A to the set B and S be a relation from the set B to set C, then

$$(SoR)^{-1} = R^{-1}\ oS^{-1}$$

Proof: Let $(c, a) \in (SoR)^{-1}$ for some $c \in C$ and $a \in A$. Then

$$(c, a) \in (SoR)^{-1} \text{ if } (a, c) \in SoR$$

$\therefore$ There is an element $b \in B$ with $(a, b) \in R$ and $(b, c) \in S$ now $(a, b) \in R$ and $(b, c) \in S$

$$\Rightarrow (b, a) \in R^{-1} \text{ and } (c, b) \in S^{-1}$$
$$\Rightarrow (c, b) \in S^{-1} \text{ and } (b, a) \in R^{-1}$$
$$\Rightarrow (c, a) \in R^{-1}\ S^{-1}$$

thus $(SoR)^{-1} = R^{-1}\ S^{-1}$

Example: Let $A = \{a, b\}$

$$R = \{(a, a), (b, a), (b, b)\} \text{ and } S = \{(a, b), (b, a), (b, b)\}$$

Then, verify $(SoR)^{-1} = R^{-1}\ oS^{-1}$

Solution:

$$S\ oR = \{(a, b), (b, a), (b, b)\}$$

$\Rightarrow$ $(S\ oR)^{-1} = \{(b, a), (a, b), (b, b)\}$

and $R^{-1} = \{(a, a), (a, b), (b, b)\}$, $S^{-1} = \{(a, a), (a, b), (b, b)\}$

$\Rightarrow$ $R^{-1}\ oS^{-1} = \{(b, a), (a, b), (b, b)\} = (SoR)^{-1}$

EXERCISE 3.1

1. Let $A = \{1, 2, 3, 4\}$, determine whether the relations are reflexive, symmetric, anti-symmetric or transitive.

1. $R = \varnothing$
2. $R = \{(1, 1), (2, 2), (3, 3)\}$
3. $R = \{(1, 3), (1, 1), (3, 1), (1, 2), (3, 3), (4, 4)\}$
4. $R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$
5. $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$
6. $R = \{(1, 3), (4, 2), (2, 4), (3, 1), (2, 2)\}$
7. $R = A \times A$
8. $R = \{(1, 2), (1, 3), (3, 1), (1, 1), (3, 3), (3, 2), (1, 4), (4, 2), (3, 4)\}$

2. Write down the relations in the square of the set $\{1,2, 4, 8, 16, 32, 64\}$.

3. The following relations in N, the set of natural numbers. Give their domains and ranges.

(*i*) $\{(1, 1), (16, 2), (81, 3), (256,\}$

(*ii*) $\{(2, 1), (4, 2), (10, 5), (18, 9), (20, 10)\}$

4. Determine the domain and range of relation R, on set of Integers $R = \{(x, y) \mid x$ is a multiple of 3 and y is a multiple of $5\}$.

5. Tabulate the element of the following relations from A to B:

(*a*) $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5, 6, 7\}$ and $R = \{(x, y) \mid y = x^2 + 3x + 3\}$

(*b*) $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5\}$ and $R = \{(x, y) \mid 5x + 2\,y$ is a prime number$\}$

6. Let f on a mapping of a set X onto a set R. Then if we define $(a, b) \in R$, for $a, b \in X$ provided $f(a) = f\ (b)$. Prove that R is an equivalence relation.

7. Determine whether the relation $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 1), (1, 4), (4, 1)\}$ is an equivalence relation in $\{1, 2, 3, 4\}$

8. Let R be the relation in the natural numbers $N = \{1, 2, 3, \ldots\}$ Define by "$x + 2y = 10$" i.e., let $R = \{(x, y) \mid x \in N,\ y \in N,\ x + 2y = 10\}$. Find (*a*) The domain and range of R (*b*) R^{-1}

9. Let $A = \{1, 2, 3, 4, 5, 6\}$, construct pictorial descriptions of the relation R on A for the following as:

(*a*) $R = \{(j, k) \mid j$ is a multiple of $k\}$

(*b*) $R = \{(j, k) \mid (j - k)^2 \in A\}$

(*c*) $R = \{(j, k) \mid (j$ divides $k\}$

(*d*) $R = \{(j, k) \mid j\,k$ is a prime

10. Let R be the relation from $A = \{1, 2, 3, 4, 5\}$ to $B = \{1, 3, 5\}$ which is defined by "x is less than y", write R as a set of ordered pairs:

11. Let L be the set of lines in the Euclidean plane and let R be the relation in L defined by "x is parallel to y". Is R a symmetric relation? Why? Is R a transitive relation?

12. Prove that if R is a symmetric relation, then $R \cap R^{-1} = R$.

13. Let $A = \{1, 2, 3\}$. Give an example of a relation R in A. Such that R is neither symmetric nor anti-symmetric.

14. If A is a set with the element and B is a set with a elements. Then find the number of relations possible firm A to B.

15. In $N \times N$ show that the relation defined by $(a, b)\ R\ (c, d)$ if and only if $ad = bc$ is an equivalence relation.

16. On the set of Natural numbers N, the relation R is defined "aRb" iff "a divides b". Show that R is anti-symmetric.

17. On the set of Integers, the relation R is defined by "aRb" iff "$(a - b)$ is even integer". Show that R is an equivalence relation.

18. Give an example of a non-empty set and a relation on the set that satisfies each of the following properties; draw a digraph of the relation.

(*a*) Reflexive (*b*) irreflexive (*c*) an anti-symmetric relation

19. Let $A = \{1, 2, 3\}$ determine whether the relation R whose matrix M_R is given is an equivalence relation:

$$(a)\ M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \qquad (b)\ M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

20. Determine whether the relation whose digraph is given below (Fig. 3.15) is an equivalence relation.

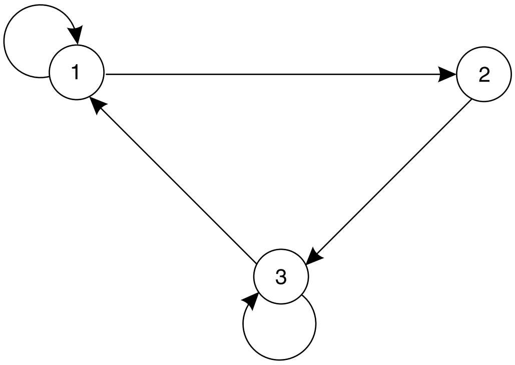


Fig. 3.15

21. Let $A = \{1, 2, 3\}$ and
$R = \{(1, 1), (1, 4), (4, 1), (4, 4), (2, 2), (2, 3), (3, 2), (3, 3)\}$
Write the Matrix of R and sketch its graph.

22. Let $R = \{(1, 2), (3, 4), (2, 2)\}$ and $S = \{(4, 2), (2, 5), (3, 1), (1, 3)\}$
Find $R\ oS$, $S\ oR$, $(S\ oR)$, $(R\ oS)\ oR$, $R\ oR$, $S\ oS$, and $(R\ oR)\ oR$.

23. Let R and S be two relations on a set of positive integers.
$= \{(x, 2x) \mid x \in I\},\ S = \{(x, 7x) \mid x \in 1\}$
Find $R\ oS$, $R\ oR$, $R\ oR\ oR$ and $R\ oS\ oR$.

24. Let $A = \{1, 2, 3, 4, 5, 6, 7\}$ and
$R = \{(x, y) \mid x - y \text{ is divisible by } 3\}$
Show that R is an equivalence relation. Draw the graph of R.

25. If $A = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4), (2, 1)\}$
Show that the transitive closure $R\infty$ is
$\{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4)\}$

26. $A = \{a, b, c\}$, and R, S are relations on A whose matrices are

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Show that $M_{SoR} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

27. Find all the partitions of $A = \{1, 2, 3\}$

28. Find the numbers of partitions on $A = \{a, b, c, d\}$

29. Let $N = \{1, 2, 3, \ldots\}$ and a relation R is defined in $N \times N$ as follows (a, b) is related to (c, d) if and only if

$$a + b = b + c$$

then show that R is an equivalence relation.

30. If a finite set A has n elements. Prove the following:

(*a*) There are $2^{n^2 - n}$ reflexive relations on A

(*b*) There are $2^{n^2 - n}$ irreflexive relations on A

(*c*) There are $2^{(n^2 + n)/2}$ symmetric relations on A

(*d*) There are $2^{(n^2 - n)/2}$ compatibility relations on A

(*e*) There are $2^n \cdot 3^{(n^2 - n)/2}$ anti-symmetric relations on A

Answers:

1. (1) Symmetric (2) Symmetric and transitive (3) Transitive (4) Transitive (5) Equivalence relation (6) Symmetric (7) Equivalence relation (8) Transitive.

2. $R = \{(1, 1), (4, 2), (16, 4), (64, 8)\}$

3. (*i*) Domain = {1, 16, 81, 256}

Range = {1, 2, 3, 4}

(*ii*) Domain = {2, 4, 10, 18, 20}

Range = {1, 2, 5, 9, 10}

4. Domain = $\{ x \in Z / x$ is multiple of 3}

$= \{\ldots -12, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Range = $y \in Z / y$ is a multiple of 5}

$= \{\ldots, -15, -10, -5, -0, -5, 10, 15, \ldots\}$

5. (*a*) {(1, 1), (2, 1), (3, 3), (4, 7)}

(*b*) {(1, 1), (1, 3), (1, 4), (3, 1), (3, 2), (3, 4)}

6. Yes, equivalence relation.

7. $R = \{(8, 1), (6, 2), (4, 3), (2, 9)\}$

$R^{-1} = \{(1, 8), (2, 6), (3, 4), (4, 2)\}$

9. $R = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}$

10. Symmetric and transitive; since:

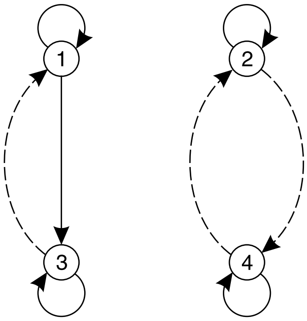
(*i*) *x* is parallel to *y P y* is parallel to *y*

(*ii*) if *x* is parallel to *y* and *y* is parallel to *z* then *x* is parallel to *z*.

17. (*a*) $R = \{(x, x), (y, y), (z, z) (z, y)\}$

19. (*a*) Yes (*b*) No

20. No.



21. $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

22. $R\, oS = \{(4, 2), (3, 2), (1, 4)\}$

$S\, oR = \{(1, 5), (3, 2), (2, 5)\}$

$(R\, oS)\, oR = \{(3, 2)\}$

$R\, oR = \{(1, 2)\}$;

$S\, oS = \{(4, 5), (3, 3)\}$

$(R\, oR)\ o\ R = \varnothing$

23. $R\, oS = \{(x, 14x) \mid x \in I\} = S\, oR$

$R\, oR = \{(x, 4x) \mid x \in I\}$

$R\, oR\, oR = \{(x, 8x) \mid x \in I\}$

$R\, oS\, oR = \{(x, 2x) \mid x \in I\}$

27. The different partitions of A are

{{1, 2, 3}}, {{1}, {2, 33}}, {{2}, {1, 33}}, {{3}, {1, 3}}, {{13, 52}, {3}}

28. Number of different partitions on A is 15.

4

Functions and Recurrence Relations

4.1 INTRODUCTION

The concept of relation was defined very generally in the preceding chapter. We shall now discuss a particular class of relations called Functions. They are widely used in Mathematics and the concept is basic to the idea of computation.

4.2 FUNCTION

Definition 4.1: Let A and B be any two sets. A relation f from A to B is called function if for every $a \in A$ there is a unique element $b \in B$, such that $(a, b) \in f$.

If f is a function from A to B, then f is a function from A to B such that

(*i*) Domain $f = A$

(*ii*) Whenever $(a, b) \in f$ and $(a, c) \in f$, then $b = c$

The notation $f: A \rightarrow B$, means f is a function from A to B.

Functions are also called Mappings or Transformations. The terms such as "correspondence" and "operation" are used as synonyms for "function".

Given any function $f: A \rightarrow B$, the notation $f(a) = b$ means $(a, b) \in f$. It is customary to write $b = f$ (a). The element $a \in A$ is called an argument of the function f, and f (a) is called the value of the function for the argument a or the image of a under f.

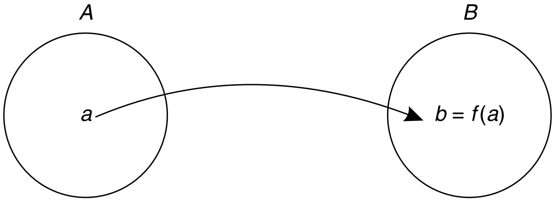


Fig. 4.1 Representation of a function

Example 1: Let $A = \{1, 2, 3\}$, $B = \{p, q, r\}$ and

$f = \{(1, p), (2, q), (3, r)\}$. Then $f(1) = p$, $f(2) = q$, $f(3) = r$, clearly f is a function from A to B.

Example 2: Consider the sets $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3\}$.

Let $f = \{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$ every element of A is related to exactly one element of B.

Hence f is function (*see* Fig. 4.2).

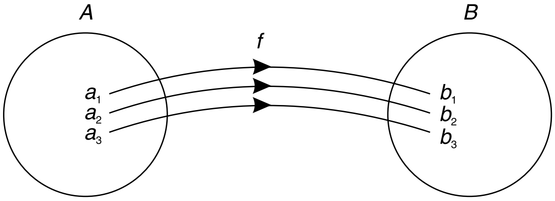


Fig. 4.2

If f: $A \to B$ is a function, then A is called the Domain of f and the set B is called the codomain of f. The range of f is defined as the set of all images under f.

It is denoted by $f(A) = \{b \mid \text{for some } a \text{ in } A, f(a) = b\}$ and is called the image of A in B. The Range f is also denoted by R_f.

If D_f denotes the domain of f: $A \to B$, and R_f denotes the Range of f, then $D_f = A$ and $R_f \subseteq B$.

A function need not be defined by a formula. While defining the property, it is customary to identify the function by a formula for example $f(x) = x^3$ for $x \in R$ represents the function $f = \{(x, x^3): x \in R\}$. Where R is the set of real numbers.

4.2.1 Restriction and Extension

Definition 4.2: If f: $A \to B$ and $P \subseteq A$, then $f \cap (P \times B)$ is a function from $P \to B$, called the Restriction of f to P. Restriction of f to P is written as $f \mid P$: $P \to B$ is such that $(f \mid P) = f(a) \; \forall \; a \in P$. If g is a restriction of f, then f is called the extension of g.

The domain of $f \mid P$ is P.

If g is a restriction of f, then $D_g \; \hat{I} \; D_f$ and $g(a) = f(a) \; a \; \hat{I} \; D_g$ and $g \; \hat{I} \; f$.

Example: Let $f: R \to R$, be defined by $f(x) = x^3$.

If N is the set of Natural numbers = $\{0, 1, 2, \ldots\}$ then $N \subseteq R$ and $f \mid N = \{(0, 0), (1, 1), (2, 2)\ldots\}$

4.3 ONE-TO-ONE MAPPING (INJECTION ONE-TO-ONE FUNCTION)

Definition 4.3: A mapping f: $A \to B$ is called one-to-one mapping if distinct elements of A are mapped into distinct elements of B,

i.e., f is one-to-one if

$$a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

or equivalently $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

Example: f: $R \to R$ defined by $f(x) = 3x \; \forall \; x \in R$ is one–one since

$$f(x_1) = f(x_2) \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2 \; \forall \; x_1, x_2 \in R.$$

4.4 ONTO-MAPPING (SURJECTION)

Definition 4.4: A mapping f: $A \to B$ is called onto-mapping if the range set $R_f = B$.

If f: $A \to B$ is onto, then each element of B is f-image of atleast one element of A.

i.e., $\{f(a) : a \in A\} = B$

If f is not onto, then it is said to be into mapping.

Example: f: $R \to R$, given by $f(x) = 2x \;\forall\; x \in R$ is onto.

4.5 BIJECTION (ONE-TO-ONE, ONTO)

Definition 4.5: A mapping f: $A \to B$ is called one-to-one, onto if it is both one-to-one and onto.

Example: f: $R \to R$, defined by $f(x) = 3x + 2$ is a bijection.

4.6 IDENTITY MAPPING

Definition 4.6: If f: $A \to A$ is a function such that every element of A is mapped onto itself then f is called an Identity mapping it is denoted by I_A.

i.e., $f(a) = a \;\forall\; a \in A$ then f: $A \to A$ is an Identity mapping.

We have $$I_A = \{(a, a) : a \in A\}$$

4.7 COMPOSITION OF FUNCTIONS

Definition 4.7: Let f: $A \to B$, and g: $B \to C$ be two mappings. Then the composition of two mappings f and g denoted by gof is the mapping from A into C defined by $gof = \{(a, c) \mid$ for some b, $(a, b) \in f$ some $(b, c) \in g\}$.

i.e., gof: $A \to C$ is a mapping defined by

$$(gof)(a) = g(f(a)) \text{ where } a \in A$$

Note: In the above definition it is assumed that the range of the function f is a subset of B (the Domain of g), i.e., $R_f \subseteq D_g$ If $R_f \subseteq D_g$, then gof is empty.

(*i*) The composition of functions is not commutative, i.e., $fog \neq gof$ where f and g are two functions.

(*ii*) gof is called the left composition g with f.

Example: Let f: $R \to R$; $g : R \to R$ be defined by $f(x) = x + 1$, $g(x) = 2x^2 + 3$, then

$$(gof)(x) = g[f(x)] = g[(x + 1)] = 2(x + 1)^2 + 3$$
$$(fog)(x) = f[g(x)] = f(2x^2 + 3) = 2x^2 + 3 + 1 = 2x^2 + 4$$

gof and fog are both defined but $gof \neq fog$

Theorem 4.1: Let f: $A \to B$, then g: $B \to C$ be both one-one and onto functions, then gof: $A \to C$ is also one-one and onto.

Proof:

Let $a_1,\ a_2 \in A$, then

$$\begin{aligned}(gof)\,(a_1) = (gof)\,(a_2) &\Rightarrow g\,[f\,(a_1)] = g\,[f\,(a_2)] \\ &\Rightarrow f\,(a_1) = f\,(a_2) \qquad (\because g \text{ is one-one}) \\ &\Rightarrow a_1 = a_2 \qquad (\because f \text{ is one-one})\end{aligned}$$

Hence *gof* is one-to-one

Now, from the definition, *gof*: $A \rightarrow C$ is a function g: $B \rightarrow C$ is onto, then $c \in C \Rightarrow$ There is some element $b \in B$ such that $\Rightarrow c = g\,(b)$ and f: $A \rightarrow B$ is onto, then by definition there exists an element $a \in A$, such that $f\,(a) = b$

We have $$c = g\,(b) = g\,[f\,(a)] = (gof)\,(a)$$
$$\Rightarrow (gof): A \rightarrow C \text{ is onto}$$

Hence *gof* is both one-one and onto.

4.8 ASSOCIATIVITY OF MAPPINGS

Definition 4.8: If f: $A \rightarrow B$, g: $B \rightarrow C$ and h: $C \rightarrow D$ are three functions, then *gof*: $A \rightarrow C$, *hog*: $C \rightarrow D$ and (*hog*) *of*: $A \rightarrow D$, can also be formed assuming that $a \in A$, we have

$$\begin{aligned}(hog)\ of\,(a) &= (hog)\,[f\,(a)] \\ &= h\,[gf\,(a)] \\ &= h[gof\,(a)] = ho(gof)\,(a)\end{aligned}$$

Thus the composition of functions is associative.

4.9 CONSTANT FUNCTION

Definition 4.9: Let f: $A \rightarrow B$, f said to be a constant function if every element of A is mapped on to the same element of B.

i.e., If the Range of f has only one element then f is called a constant mapping.

Example: f: $R \rightarrow R$, defined by

$f\left(x\right) = 5\ \forall\ x \in R$ is a constant mapping we have $R_f = \{5\}$

4.10 INVERSE MAPPING

Definition 4.10: Let f: $A \rightarrow B$, be one-one, onto mapping (bijection), then f^{-1}: $B \rightarrow A$ is called the inverse mapping of f.

f^{-1} is the set defined as

$$f^{-1} = \{(b,\, a) \mid (a,\, b) \in f\}$$

Note:

(*i*) In general the inverse f^{-1} of a function $f: A \to B$, need not be a function. It may be a relation.

(*ii*) If $f: A \to B$ is a bijection and $f(a) = b$, then $a = f^{-1}(b)$ where $a \in A$, and $b \in B$

Example:

(*i*) Let $A = \{a, b, c\}$, $B = \{1, 2, 3\}$ and $f = \{(a, 1), (b, 3), (c, 2)\}$ clearly f is both one-to-one and onto

$\therefore f^{-1} = \{(1, a), (2, c), (3, b)\}$ is a function from B to A.

(*ii*) Let R be a set of real numbers and $f: R \to R$ be given by

$$f(x) = x + 5 \ \forall \ x \in R \ \text{, i.e., } f = \{(x, x+5) \mid x \in R\}$$

then $f^{-1} = \{(x + 5, x) \mid x \in R\}$ is a function from R to R.

Theorem 4.2: If $f: A \to B$ be both one-one and onto, then $f^{-1}: B \to A$ is both one-one and onto.

Proof: Let $f: A \to B$ be both one-one and onto. Then there exist elements $a_1, a_2 \in A$, and elements $b_1, b_2 \in B$ such that

$$f(a_1) = b, \text{ and } f(a_2) = b_2$$

or $$a_1 = f^{-1}(b_1) = \text{ and } a_2 = f^{-1}(b_2)$$

Now, let $f^{-1}(b_2) = f^{-1}(b_2)$ then

$$f^{-1}(b_1) = f^{-1}(b_2)$$
$$\Rightarrow a_1 = a_2$$
$$\Rightarrow f(a_1) = f(a_2)$$
$$\Rightarrow b_1 = b_2$$

Thus f^{-1} is one-one

Again since f is onto, for $b \in B$, there is some element $a \in A$, such that $f(a) = b$.

Now $$f(a) = b$$
$$\Rightarrow a = f^{-1}(b)$$

$\Rightarrow f^{-1}$ is onto

Hence f^{-1} is both one-one and onto

Theorem 4.3: The inverse of an invertible mapping is unique.

Proof: Let $f: A \to B$

By any invertible mapping. If possible let

$$g: B \to A$$

and $$h: B \to A$$

be two different inverse mappings of f.

Let $b \in B$ and

$$g(b) = a_1, a_1 \in A$$

$$h(b) = a_2, a_2 \in A$$

Now $g(b) = a_1, \Rightarrow b = f(a_1)$

and $h(b) = a_2 \Rightarrow b = f(a_2)$

Furthermore $b = f(a_1)$ and $b = f(a_2)$

$$\Rightarrow f(a_1) = f(a_2)$$

$$\Rightarrow a_1 = a_2 \qquad (\because f \text{ is one-one})$$

This proves that $g(b) = h(b) \; \forall \; b \in B$

Thus, the inverse of f is unique

This completes the proof of the theorem.

Theoem 4.4: If $f: A \rightarrow B$ is an invertible mapping, then $f\, of^{-1} = I_B$ and $f^{-1}\, of = I_A$.

Proof: f is invertible, then f^{-1} is defined by $f(a) = b \Leftrightarrow f^{-1}(b) = a$ where $a \in A$ and $b \in B$

To prove that $f\, of^{-1} = I_B$

Let $b \in B$ and $f^{-1}(b) = a$, $a \in A$ then

$$f\, of^{-1}(b) = f[f^{-1}(b)]$$
$$= f(a) = b$$

Therefore $fof^{-1}(b) = b \; \forall \; b \in B$

$$\Rightarrow f\, of^{-1} = I_B$$

and $f^{-1}\, of(a) = f^{-1}[f(a)] = f^{-1}(b) = a$

Therefore $f^{-1}\, of(a) = a \; \forall \; a \in A$

$$\Rightarrow f^{-1}\, of = I_A$$

Theorem 4.5: If $f: A \rightarrow B$ is invertible then $f^{-1}\, of = I_{A'}$ and $f\, of^{-1} = I_B$

Proof: Left as an exercise.

Theorem 4.6: Let $f: A \rightarrow B$, and $g: B \rightarrow C$. The function $g = f^{-1}$, only if $gof = I_{A'}$ and $fog = I_B$.

Proof: Left as an exercise.

Theorem 4.7: If $f: A \rightarrow B$, and $g: B \rightarrow C$, are both one-one and onto, then $(gof)^{-1} = f^{-1}\, og^{-1}$.

Proof:

$f: A \rightarrow B$ is one-one and onto

$g: B \rightarrow C$ is one-one and onto,

Hence $gof: A \rightarrow C$ is one-one and onto

$\Rightarrow (gof)^{-1} : C \rightarrow A$ is one-one and onto

Let $a \in A$, then there exists and element $b \in B$ such that $f(a) = b \Rightarrow a = f^{-1}(b)$.

Now, $b \in B \Rightarrow$ there exists an element $c \in C$ such that $g(b) = c \Rightarrow b = g^{-1}(c)$

Then $(gof)(a) = g[f(a)] = g(b) = c \Rightarrow a = (gof)^{-1}(c)$ … (1)

$(f^{-1}\, og^{-1})(c) = f^{-1}[g^{-1}(c)] = f^{-1}(b) = a \Rightarrow a = (f^{-1}\, og^{-1})(c)$ … (2)

Combining (1) and (2), we have

$$(gof)^{-1} = f^{-1}\, og^{-1}$$

4.11 CHARACTERISTIC FUNCTION OF A SET

Definition 4.11: Let U be a universal set and A be a subset of U. Then the function

$$\psi_A : U \to [0, 1] \text{ defined by}$$

$$\psi_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

is called a characteristic function of the set A.

4.11.1 Properties of Characteristic Functions

Let A and B be any two subsets of a universal set U. Then the following properties hold for all $x \in U$:

(1) $\psi_A(x) = 0 \Leftrightarrow A = \varnothing$

(2) $\psi_A(x) = 1 \Leftrightarrow A = U$

(3) $\psi_A(x) \subseteq \psi_B(x) = \Leftrightarrow A \subseteq B$

(4) $\psi_A(x) = \psi_B(x) \Leftrightarrow A = B$

(5) $\psi_{A \cap B}(x) = \psi_A(x) \,.\, \psi_B(x)$

(6) $\psi_{A \cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A \cap B}(x)$

(7) $\psi_A(x) = 1 - \psi_A(x)$

(8) $\psi_{A-B}(x) = \psi_A(x) - \psi_{A \cap B}(x)$

The operations I, =, +, . and –, used above are the usual arithmetical operations.

The values of characteristic functions are always either 1 or 0. The properties (1) to (8) can easily be proved using the definition of characteristic functions.

Set identities can also be proved by using the properties characteristic functions.

Example: Show that $\overline{\overline{(A)}} = A$

Solution:

$$\begin{aligned} \psi\overline{(\overline{A})}(x) &= 1 - \psi\overline{(\overline{A})}(x) \\ &= 1 - (1 - \psi_A(x)) \\ &= \psi_A(x) \Rightarrow \overline{(\overline{A})} = A \end{aligned}$$

4.12 SOLVED EXAMPLES

Example 1: On which sets A will identity function $I_A : A \to A$ be (*i*) one-one (*ii*) an onto function.

Solution: A can be any set

(*i*) The identity function is always one-one and

(*ii*) The identity function is always onto.

Example 2: Can a constant function be (*i*) one-one (*ii*) onto.

Solution: If *f* is a constant function, the co-domain of *f* consists of single element. Therefore

(*i*) a constant function is one-one if the domain of *f* contains a single element.

(*ii*) a constant function is always onto.

Example 3: f: $R \rightarrow R$ is defined by $f(x) = a\,x + b$, where a, b, $x \in R$ and $a \neq 0$.

Show that *f* is invertible and find the inverse of *f*.

Solution: Firstly, we shall show that *f* is one-to-one.

Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$$\Rightarrow a\,x_1 + b = a\,x_2 + b$$

$$\Rightarrow ax_1 = ax_2$$

$$\Rightarrow x_1 = x_2$$

Thus *f* is one-one

To show that *f* is onto

Let $y \in R$ such that $y = f(x)$

$$\Rightarrow y = a\,x + b$$

$$\Rightarrow a\,x = y - b$$

i.e., given $y \in R$, there exists an element

$$x = \frac{1}{a}(y - b) \in R, \text{ such that } f(x) = y$$

this proves that *f* is onto

Hence *f* is one-one and onto

Hence *f* is invertible and

$$f^{-1}_{(y)} = \frac{1}{a}(y - b)$$

Example 4: Let $U = \{a, b, c, d, e, f\}$ and $A = \{a, d, e\}$ then find X_A, where X_A denotes the characteristic function of A.

Solution:

$$X_A = \{(a, 1), (b, 0), (c, 0), (d, 1), (e, 1), (f, 0)\}$$

Since $a \in A \Rightarrow X_A(a) = 1$, $d \in A \Rightarrow X_A(d) = 1$, and $e \in A \Rightarrow X_A(e) = 1$, b, c, f are not the members of A,

Thus $$X_A(b) = X_A(c) = X_A(f) = 0$$

Example 5: Let A and B be subsets of a universal set U then prove $X_{A} \cap_{B} = X_A\ X_B$.

Solution:

$$\Rightarrow X_A(a) = X_B(a) = 1$$

$$\Rightarrow X_A(a)\,X_B(a) = 1$$

Let $b \in (A \cap B)'$, then $b \notin A \cap B \Rightarrow X_A \cap X_B(b) = 0$

Now $b \in (A \cap B)' \Rightarrow X_A \cap X_B(b) = 0$

also $b \in (A \in B)' \Rightarrow b \in (A' \cup B')$

$\Rightarrow b \in A'$ or $b \in B'$

$\Rightarrow X_A(b) = 0$ or $X_B(b) = 0$

$\Rightarrow (X_A X_B)(b) = X_A(b) X_B(b) = 0$

Hence by definition

$$X_{A \cap B} = X_A X_B.$$

EXERCISE 4.1

1. Define the terms:

(*i*) Function

(*ii*) One-one function

(*iii*) Onto function

(*iv*) Identify function

2. Let f: $N \to N, f(x) = 2x + 3$, N being the set of natural numbers. Prove that f is injection but not surjection.

3. Show that the function f from the reals into the reals defined by $f(x) = x^2 + 1$ is one-to-one, onto function and find f^{-1}.

4. A binary operation b on a set A is said to be associative if $b(x, b(y, z)) = b(b(x, y), z)$ for all $x;\ y,\ z \in A$, which of the operations are associative?

(*a*) $b(x, y) = x - y$

(*b*) $b(x, y) = x^2 + y^2$

(*c*) $b(x, y) = max\ \{x, y\}$, where $max\ \{x, y\}$ denotes the larger of the two numbers x and y. (For example $max\ \{5, 7\} = 7$, $max\ \{-6, 2\} = 2$)

5. If $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, determine if the following functions are one-to-one or onto.

(*a*) $f = \{(1, a), (2, a), (3, b), (4, d)\}$

(*b*) $g = \{(1, e), (2, b), (3, a), (4, a)\}$

(*c*) $h = \{(1, d), (2, b), (3, a), (4, c)\}$

6. $A = \{-1, 0, 2, 5, 6, 11\ f : A \to B$ is a function given by $f(x) = x^2 - x - 2$ for all $x \in A$. Find the range of f. If f an onto function.

7. Let R_0 be the set of all non-zero real numbers, show that f: $R_0 \to R_0$ defined by $f(x) = \dfrac{1}{x}$ for all $x \in R_0$ is one-to-one and onto for all $x \in R_0$ is one-to-one and onto.

8. Let f: $S \to T$ be a function; Let A and B be subsets of S, and D and E be subsets of T. Prove the following theorems:

(*i*) $A \subset B$, then $f(A) \subset f(B)$

(*ii*) $D \subset E$, then $f^{-1}(D) \subset f^{-1}(E)$

(*iii*) $f(A \cap B) \subset f(A) \cap f(B)$

9. $A = \{1, 2, 3\}$, $B = \{p, q\}$, $C = \{a, b, f: A \to B$ and $g: B \to C$ are given by $f = \{(1, p), (2, q), (3, q)\}$, $g = \{(p, b), (q, b)\}$ show that: $gof = \{(1, b), (2, b), (3, b)\}$.

10. $X = \{1, 2, 3\}$ and f, g and h are function from X to X given by $f = \{(1, 2), (2, 3), (3, 1)\}$, $g = \{(1, 2), (2, 1), (3, 3)\}$, $h = \{(1, 1), (2, 2), (3, 1)\}$ find $f\,og$, $g\,of$, $f\,og\,of$, $h\,of$, $h\,oh$, and $g\,oh$.

11. R is the set of real numbers, given that $f(x) = x + 2$, $g(x) = x - 2$, and $h(x) = 3x\ \forall\ x \in R$.

Find $g\,of$, $f\,og$, $f\,of$, $g\,og$, $f\,oh$, $h\,og$, $h\,of$, and $f\,ogoh$

12. Let $A = \{1, 2, 3 \ldots, n\}$, $\{n \geq 2)$, and $B = \{a, b\}$ find the number of subjections from A onto B.

13. Let $f: R \to R$ be defined by $f(x) = 3x + 4$, show that f is one-one and onto. Give a formula that defines f^{-1}.

14. Let $A = R - \{3\}$, and let $f: A \to B$ be defined by $f(x) = \dfrac{x-2}{x-3}$, show that f is one-to-one and onto. Find f^{1}.

15. Let the functions $f: R \to R$ and $g: R \to R$ be defined by $f(x) = 2x + 1$, $g(x) = x^2 - 2$. Find formulas which define the functions $g\,of$ and $f\,og$.

16. Let $U = \{a, b, c, d, e\}$, $A = \{c, d\}$ and $B = \{a, d, e\}$, find (1) X_A (2) X_B.

17. Show that the functions $f: N \times N \to N$ and $g: N \times N \to N$ given by $f(x, y) = x + y$ and $g(x, y) = xy$ are onto but not one-to-one. ***(OU Mar. 2002)***

18. If x and y are finite sets, find a necessary condition for the existence of one-to-one mapping from x to y. ***(OU Mar. 2001)***

19. Let $A = B = R$, the set of real number. Let $f: A \to B$ be given by the formula $f(x) = 2x^2 - 1$ and let $g: B \to A$ be given by $g(y) = 3\sqrt{\frac{1}{2}y + \frac{1}{2}}$. Show that f is a bijection between A and B and g is a bijection between B and A. ***(OU Dec. 2000)***

Answers:

3. $f^{-1}(Y) = (Y-1)^{1/2}$.

4. (*c*)

5. (*c*)

6. $f(A) = B = \{-2, 0, 18, 28, 108\}$

10. $f\,og = \{(1, 3), (2, 2), (3, 1)\}$

$g\,of = \{(1, 1), (2, 3), (3, 2)\}$

$f\,og\,of = \{(1, 2), (2, 1), (3, 3)\}$

$h\,of = \{(1, 2), (2, 1), (3, 1)\}$

$h\,oh = \{(1, 1), (2, 2), (3, 1)\}$

$g\,oh = \{(1, 2), (2, 3), (3, 2)\}$

11. $g\ of\,(x) = x$

$f\,og\ (x) = kx$

$f\,of\,(x) = x + 4$

$go\ g\ (x) = x - 4$

$f\,oh\ (x) = 3x + 2$

$h\ og\ (x) = 3x - 6$

$h\ of\,(x) = 3x + 6$

$f\,ogoh\ (x) = 3x$

12. $2^n - 2.$

13. $f^1\ (y) = \dfrac{y-4}{3}$

14. $f^1\ (y) = \dfrac{2-3y}{1-4}$

15. $g\ of\,(x) = 4x^2 + 4x - 1, f\,og = 2x^2 - 2$

16. $X_A = \{(a, 0), (b, 0), (c, 1), (d, 1), (e, 0)\}$

$X_B = \{(a, 1), (b, 0), (c, 0), (d, 1), (e, 1)\}$

4.13 RECURSION AND RECURRENCE RELATIONS

Recursion is a technique of defining a function, a set or an algorithm in terms of itself. For example: consider the set of natural numbers, we introduce the method of generating the set of natural numbers by recursion.

The natural numbers (including zero) are those objects which can be generated by starting with an initial object 0 (zero) and from any object "*n*" already generated passing to another uniquely determined object n^+, the successor of *n*. The objects differently generated are always distinct. Thus the natural numbers appear as a set of objects 0, 0^+, 0^{++}, 0^{+++}, …

The transition to the usual notation is made upon introducing 1, 2, 3, 4, … to stand for 0^+, 0^{++}, $0^{+++,}$ 0^{++++}, … and then employing the notation. The set of Natural numbers is denoted by *N*.

The set of natural numbers can also be generated by starting with usual null set $\varnothing$ and notion of a successor set.

If *A* is a given set, then the successor of *A* is the set $A \cup \{A\}$. It is denoted by A^+

Thus $$A^+ = A \cup \{A\}.$$

Let $\varnothing$ be the null set, then find the successor sets of $\varnothing$ these sets are:

$$\varnothing, \varnothing^+ = \varnothing \cup \{\varnothing\}, \varnothing^{++} = \varnothing \cup \{\varnothing\} \cup \{\varnothing, \{\varnothing\}\}$$

They can also be written as $\varnothing, \varnothing^+ = \{\varnothing\},$

$$\varnothing^{++} = \{\varnothing, \cup \{\varnothing\}\}$$

renaming the $\varnothing$ as 0 (zero),

$$\varnothing^+ = 0^+ = \{\varnothing\} = 1$$

$$\varnothing^{++} = 1^+ = \{\varnothing, \{\varnothing\}\} = \{0, 1\} = 2, ...$$

We get the set {0, 1, 2, 3, …}. Each element in the above set is a successor set of the previous element, except for the element 0. (0 is not the successor of any element).

Now we consider recursion in terms of successor:

Let S denote the successor. We define

(*i*) $x + 0 = x$ (*ii*) $x + S(y) = S(x + y)$

In this definition (*i*) is the basis, and it defines addition of 0. The recursive part defines addition of the successor of y.

Example 1:

$$\begin{aligned} 3 + 2 &= 3 + S(1) \\ &= S(3 + 1) \\ &= S(S(3 + 0)) = S(S(3)) = S(4) = 5 \end{aligned}$$

Now we start with a set of three functions called basis functions or initial functions of:

1. Zero function: Z: $Z(x) = 0$
2. Successor function S: $S(x) = x + 1$
3. Projection function : $\cup_1^n : \cup_1^n \left(x_1, x_2, x_3, ...x_n\right) = x_1$ (or generalized identify function).

Example 2:

$S(3) = 3 + 1 = 4,\ S(4) = 4 + 1 = 5,$

$\cup_1^2 \left(x, y\right) = x,\ \cup_2^3 \left(\alpha, \beta, r\right) = \beta,\ \cup_3^5 \left(1, 7, 6, 2, 4\right) = 6,\ \cup_3^6 \left(9, 3, 2, 5, 6, 8\right) = 2$, etc.

The initial functions are used in defining other functions by induction.

4.13.1 Sequences

The idea of a sequences is important to computer science. *A* sequence is defined as the list of objects in order. There are several ways of representing a sequence. One way is to list first terms of the sequence till the rule for writing down other terms is obtained.

For example: The sequence {2, 4, 6, 8, …} is a sequence whose *n*th terms in 2*n*. Another way is to give a rule of writing the *n*th terms of the sequence.

The sequence {1, 4, 7, 10, …} can be written as

$$\{S_n\} \text{ where } S_n = 3n + 1, n = 0, 1, 2, ...$$

We can represent a sequence by using a recursive relation:

The recurrence relation

$a_n = a_{n-1} + 5$, with $a_1 = 6$, recursively defines the sequence 6, 11, 16, …

$a_1 = 6$ is called the initial condition.

4.13.2 Strings

Definition 4.12: Let A be a non-empty set, which we refer to as the alphabet. *A* string on the set A is a finite sequence of elements of A.

The set of all strings on A is denoted by A^* (or by A^+).

Example 1:

(*i*) $a_3\, a_2\, a_1\, a_4$ is a string on $A = \{a_1, a_2, a_3, a_4\}$

(*ii*) 246107 is a string on the alphabet consisting of the ten digits {0, 1, 2, 3, … 9}

Usually we write a string on A without using commas between the elements of the string.

If a_1, a_2, a_3, …, a_n is a string then the length of the string is n.

Example 2: The length of the string 621708 is 6

If $a_1, a_2, \ldots, a_n$ is a segment string, then $a_{r+1}\, a_{r+2} \ldots a_s$ where $1 \le r \le s \le n$ is called a (proper) segment of the string. If $r = 0$, then $a_{r+1}\, a_{r+2} \ldots a_s$ is called an initial segment of the string.

Example 3: 537 is an initial segment of the string 537108 and 710 is a segment of the string 537108.

Let $a_1\, a_2 \ldots, a_m$ and $b_1\, b_2 \ldots b_n$ be strings. There concatenation is $a_1\, a_2$ and $b_1\, b_2 \ldots b_n$. It is also called the product or Join and is a length $m + n$. For example: 537 and 108 are two strings and their catenation is the string 537108.

4.13.3 Floor and Ceiling Functions

Definition 4.13: Let x be any real number, then the greatest integer that does not exceed x is called the Floor of x.

The FLOOR of x is denoted by $\lfloor x \rfloor$

Examples:

$$\lfloor 5.14 \rfloor = 5$$

$$\lfloor \sqrt{5} \rfloor = 2$$

$$\lfloor -7.6 \rfloor = -8$$

$$\lfloor 6 \rfloor = 6$$

$$\lfloor -3 \rfloor = -3$$

Definition 4.14: Let x be a real number, then the least integer that is not less than x is called the CEILING of x.

The CEILING of x is denoted by $\lceil x \rceil$

Examples:

$$\lceil 2.15 \rceil = 3$$

$$\lceil \sqrt{5} \rceil = 3$$

$$\lceil -7.4 \rceil = -7$$

$$\lceil -2 \rceil = -2$$

Note: If x is an integer, then $\lceil x \rceil = \lfloor x \rfloor$

4.13.4 Integer Value of Function

Definition 4.15: Let x be any real number. The Integer value of x is the value of x converted into an integer by deleting the fractional part of x. It is denoted by $INT\ (x)$.

Example:

$$INT\,(2.33) = 2, INT\,(-6.4) = -6$$
$$INT\,(9) = 9$$

Note: If x is a positive Integer then $INT\,(x) = \lfloor x \rfloor$ and if x is a negative integer then $INT\,(x) = \lceil x \rceil$.

4.13.5 Absolute Value Function

Definition 4.16: Let x be a real number, then the absolute value of x denoted by $ABS\,(x)$ or $|\,x\,|$ is defined as follows:

$$|\,x\,| = -x \text{ if } x < 0$$
$$|\,x\,| = x \text{ if } x \geq 0$$

Example:

$$|\,4.14\,| = 4.12, |\,7\,| = 7$$
$$|\,-3.5\,| = 3.5, |\,-0.12\,| = 0.12$$

Note: $|\,x\,| = |\,-x\,|$

4.13.6 Logarithmic Function

Definition 4.17: Let M be positive number, then the Logarithm of M to the base a, written $log_a M$ represents the exponent to which a must be raised to obtain M. $a^x = M$ and $log_a M = x$ are equivalent statements.

Example:

If $\quad 3^4 = 81$ then $log_3 81 = 4$

$$log_{10} 0.01 = -2 \text{ since } 10^{-2} = 0.01$$

Note: Logarithms to base 10 are called common logarithms and logarithms to the base e are called natural logarithms where $e = 2.718281$.

Usually log x mean $log_{10} x$.

4.13.7 Partial and Total Functions

Definition 4.18: Let X and Y be sets and A be a subset of X. A function f from A to Y is called a partial function from X to Y. The set A is a called the domain of f. If the domain of f is the set X, then f is called a total function from X to Y.

Let f be a function from N (the set of Natural Numbers) to N given by $f\,(a) = b$ if $a = b^2$. Then the domain of the function f is the set of squares and f is a partial function. We define N^n to be the set of all n-tuples of elements of N. Any function $f: N^n \to N$ is a total function. If A is a subset of N^n, then the function $f: A \to N$ is a partial function. The function $f\,(x, y) = x + y$, for all elements $x, y \in N$ is a total function. But the function defined by $S\,(x, y) = x - y$, for all $x, y \in N$ is a partial functions.

4.13.8 Primitive Recursive Functions

Definition 4.19: Let g: $N^n \to N$ and h: $N^{n+2} \to N$ be functions. We say that f: $N^{n+1} \to N$ is defined from g and h by Primitive recursion if f satisfies the conditions:

$$f(x_1, x_2, \ldots, x_n, 0) = g(x_1, x_2, \ldots, x_n)$$

and $f(x_1, x_2, \ldots, x_n, y + 1) = h(x_1, x_2, \ldots, x_n, y, f(x_1, x_2, \ldots, x_n, y))$ (where y is the inductive variable).

From the above definition it is clear that Primitive recursion (or recursion) is the operation in the operation in which a function f of $(n + 1)$ variables is defined by using two other functions g and h of n and $(n + 2)$ variables.

Definition 4.20: A function f is said to be Primitive recursive if it can be obtained from the initial functions by a finite number of operations of composition and recursion (i.e., Primitive recursion).

Example 1: Show that addition is primitive recursive.

Solution: Addition is defined by $x + 0 = x$, $x + (y + 1) = (x + y) + 1$ for all natural numbers x, y

We define $f(x, y) = x + y$ such that

$$\begin{aligned} f(x, y + 1) &= x + y + 1 = (x + y) + 1 \\ &= f(x, y) + 1 \\ &= S(f(x, y)) \end{aligned}$$

also $f(x, 0) = x$

More formally we define $f(x, y)$ as

$$f(x, 0) = x = \cup_1^1(x)$$

$$f(x, y + 1) = S\left(\cup_3^3(x, y, f(x, y))\right)$$

If follows that f comes from Primitive recursion from $\cup_1^1$ and $\cup_3^3$ and so is f Primitive recursive

Example 2: Show that multiplication * defined by $x * 0 = 0$, $x_* (y + 1) = x_* y + x$ is Primitive recursive.

Solution: We define $\mu(x, y)$ to be $x_* \; y$. so that $\mu(x, 0) = 0 = Z(x)$,

$$\begin{aligned} \mu(x, y + 1) &= \mu(x, y) + x \\ &= f(x, \mu(x, y)) \end{aligned}$$

$$\mu(x, y + 1) = f\left(\cup_3^3\left(x, y, \mu(x, y), \left(\cup_1^3\left(x, y, \mu(x, y)\right)\right)\right)\right)$$

Where f is the addition function.

Example 3: Let x, y be positive integers and suppose Q is defined recursively as follows:

$$Q(x, y) = \begin{cases} 0 & \text{if } x < y \\ Q(x - y, y) + 1 & \text{if } y \le x \end{cases}$$

find (*i*) $Q(4, 7)$ (*ii*) $Q(14, 6)$.

Solution:

(*i*) $Q(4, 7) = 0$ since $4 < 7$

(*ii*) $$\begin{aligned} Q(14, 6) &= Q(14 - 6, 6) \\ &= Q(8, 6) + 1 \\ &= Q(8 - 6, 6) + 1 + 1 \\ &= Q(2, 6) + 2 \end{aligned}$$

$= 0 + 2$

$= 2$

Example 4: Compute (*i*) A (1, 1), (*ii*) A (1, 2), (*iii*) A (2, 1) where A: $N^2 \rightarrow N$, (called Ackerman's function) is defined by

$$A\ (0, y) = y + 1$$
$$A\ (x + 1, 0) = A\ (x, 1)$$
$$A\ (x + 1, y + 1) = A\ (x + 1, y)$$

Solution:

(*i*) $A\ (1, 1) = A\ (0 + 1, 0 + 1)$
$= A\ (0, A\ (1, 0))$
$= A\ (0, a\ (0, 1))$
$= A\ (0, 1 + 1)$
$= A\ (0, 2)$
$= 2 + 1 = 3$

(*ii*) $A\ (1, 2) = A\ (0 + 1, 1 + 1)$
$= A\ (0, A\ (1, 1))$
$= A\ (0, 3) = 3 + 1 = 4$

(*iii*) $A\ (2, 1) = A\ (1 + 1, 0 + 1)$
$= A\ (1, A\ (2, 0))$
$= A\ (1, A\ (1, 1))$
$= A\ (1, 3)$
$= A\ (0 + 1, 2 + 1)$
$= A\ (0, 4)$
$= 4 + 1 = 5$

The functions given below are Primitive recursive:

1. Sign function

   The sign of x, denoted by $S_g(x)$ is defined by

$$S_g(0) = 0$$
$$S_g(x) = 1 \text{ for } x \neq 0$$

or

$$S_g\ (0) = Z(0)$$
$$S_g\ (y+1) = S\left(Z\left(\cup_2^2\left(y,\ S_g\ (y)\right)\right)\right)$$

   Sign function is also called non-zero test function.

2. Zero test function:

   It is denoted by $\overline{S_g}$ and is defined as $\bar{S}_g\ (0) = 1,\ \bar{S}_g\ (y+1) = 0$

3. Predecessor function:

   It is denoted by P, and is defined as

$$P(0) = 0,\ P(y+1) = y = \cup_1^2\ (y,\ P(y))$$

4. Proper subtraction function:

   It is denoted by $\dot{-}$ and is given by

$$x \dot{-} 0 = x, x - (y + 1) = P\,(x - y)$$

   that is $x - y = x - y$ for $x > y$

   and $x \dot{-} y = 0$ for $x < y$

   ($x \dot{-} y$ does not map into N, so we do not consider it here)

5. Absolute function: $|\quad|$

   It is defined as

$$| x - y | = (x \dot{-} y) + (y \dot{-} x)$$

4.13.9 Hashing

Hashing Function

In this section, we discuss Hashing. A Hashing function is used to store and retrieve data. We know that ‘files; are used to store information on a computer. Each file contains many records and each record contains a field which is designated as a key to that record. The key has a value that identifies a record. Any transformation which maps the internal bit representation of the set of keys to a set of addresses is called a Hashing function. Ideally, each key would map to a unique hash address. A good hash function maps a random selection of keys uniformly across the hash table. A poor hash function results in frequent collisions. Various hash functions are available. Extraction and compression are two well-known methods of hashing which are practical for relatively small hash tables. Probabilistic hashing and virtual hashing are advanced methods for hashing. We now explain a method known as the division method, with the help of an example; in which the hashing function h defined by the division is

$$h(k) = k \ (\text{mod } n)$$

The set $\{0, 1, 2, \ldots, n - 1\}$ is the address set, and $h(k)$ is the remainder of dividing k by the integer n. The remainder is a member of the address set.

Example 1: Assume that there are 10,000 customer account records to be stored and processed. The company’s computer is capable of searching a list of 100 items in an acceptable amount of time and 101 lists are available for storage. If hashing function h is defined from the set of 7-digit account number to the set $\{0, 1, 2, \ldots, 100\}$ as

$$h(k) = k \ (\text{mod } 101)$$

The customer with account number 3563821 will be assigned to the list 36.

Example 2: Suppose that 7,500 customer account records must be stored and processed the company’s computer is capable of searching a list of 58 items in an acceptable amount of time. There are 59 linked lists of storage. A hashing function h is defined from the set of 7-digit account numbers to the set $\{0, 1, 3, \ldots, 58\}$ is defined as follows:

h takes the first three digits of the account number as one number and the last four digits as another number, adds them and then applies the mod 59 function. Determine which list the customer with customer account number (key) 2614902 should be attached.

Solution: Consider 2614902

We split up the number as 261 and 4902 adding we get 261 + 4902 = 5163.

Dividing by 59, we get 30 as the remainder the record with account number 2614902 will be assigned to the list 30

i.e., $h(2614902) = 30$

Folding: In this method of hashing, the key (customer record number) is divided in several parts. The parts are then added to for another number in the required range.

For example: Consider the customer record number 37124865 (having 8-digit key). If 3-digit address is to be obtained then $h(37124865) = 371 + 248 + 65 = 684$.

EXERCISE 4.2

1. Show that exponentiation defined by $f(x, y) = x^y$ is Primitive recursive.
2. Show that the function $[x / 2]$ which is equal to the greatest integer which is $< x/2$ is Primitive recursive.
3. Show that the cosine of x, $C\,ox$ defined by $C\,00 = 1$, $C\,ox = 0$ for $x > 0$ is Primitive recursive.
4. Prove that the square function given by $f(y) = y^2$ is primitive recursive.
5. Show that the Ackerman's function $A: N^2 \rightarrow N$ which is defined by:

$$A(0, y) = y + 1$$
$$A(x + 1, 0) = A(x, 1)$$

and $$A(x + 1, y + 1) = A(x + 1, y)$$

is not primitive recursive.

6. Show that the function

$$f(x) = \begin{cases} x/2 \text{ when } x \text{ is even} \\ (x-1)/2 \text{ when } x \text{ is odd} \end{cases}$$

is primitive recursive.

4.14 RECURRENCE RELATIONS AND SOLUTIONS OF RECURRENCE RELATIONS

In the previous section, we defined the set of recursive function. In this section we shall first explain what is meant by a numeric function and then study recurrence relations.

Functions whose domain is the set of natural numbers and whose range is the set of real numbers are called numeric function.

For example

$$a_r = \begin{bmatrix} 0,\ 0 \le r \le 2 \\ 2^{-r} + 5,\ r \ge 3 \end{bmatrix}$$

is a numeric function. Bold face lowercase letters are used to denote Numeric functions for example

$$a = \{a_0, a_1, a_2, a_3, \ldots a_r, \ldots\}$$

is a numeric function where $a_0, a_1, a_2, a_3, \ldots a_r, \ldots$ denotes the values a at 0, 1, 2, 3, … r, …. If a and b denote two numeric functions then their sum and product are also numeric functions. If k is a scalar and a is a numeric function. The k is also numeric function.

If $a = \{ a_0, a_1, a_2, a_3\}$ is a

If $a = \{ a_0, a_1, a_2, \ldots a_r, \ldots\}$ is a numeric function, then $a_{r+1} - a_r$ is called its forward difference at r. It is denoted by Δa_r . The backward difference at r 1 is $a_r - a_{r-1}$. The backward difference of a at r is denoted by ∇a_r .

The convolution of two numeric function a and b is a numeric function c such that

$$C_r = a_0\, b_r + a_1\, b_{r-1} + a_2\, b_{r-2} + .. + a_{r-1}\, b_1 + a_r\, b_0$$

$$= \sum_{i=0}^{r} a_i\, b_{r-i}$$

The convolution of a and b is denoted by $a * b$

For example, let a and b denote two numeric functions such that

$$a_r = 5^r\, r^3,\ r \geq 0$$

and $$b_r = 3^r\, r^3\ 0,\ r \geq 0$$

Then the convolution $a * b$ is given by

$$C_r = \sum_{i=0}^{r} 5^i\, 3^{i-1}$$

4.15 GENERATING FUNCTIONS

We introduce now an alternative way to represent numeric functions. For the numeric function

$$a = \{ a_0, a_1, a_2, \ldots a_r, \ldots\}$$

we define an infinite series

$a_0 + a_1 z + a_2 z^2 + \ldots + a_r z^r + \ldots$ which is called the generating function of a. It is denoted by A (Z). The coefficient of z^r is A (z) is the value of the numeric function a. For example, the generating function of $a = (2^0, 2^1, 2^2, \ldots 2^r, \ldots)$ is $z^0 + 2z + 2z^2 + 2^3 z^3 + \ldots + 2^r z^r + \ldots$

The above infinite series can be written in the closed form as

$$A(z) = \frac{1}{1 - 2z}$$

In $$A\ (z) = a_0\, z^0 + a_1\, z^1 + a_2\, z^2 + \ldots + a_r\, z^r + \ldots$$

The term $a_0\, z^0 = a_0$ is called the constant term, the term $a_r\, z^r$ is the term of degree r. Note that $A(z)$ generates its coefficients. If all the coefficients are zero from some point on, $A(z)$ is just a polynomial. If $a_r \neq 0$ and $a_s = 0$ for $s \geq r + 1$ then A (z) is a polynomial degree r.

Let $$A\ (z) = a_0\, z^0 + a_1\, z^1 + a_2\, z^2 + \ldots + a_r\, z^r + \ldots$$

and $$B\ (z) = b_0\, z^0 + b_1\, z^1 + \ldots + b_r\, z^r + \ldots$$

denote the generating functions. A (z) and B (z) are equal if $a_r = b_r$ for each

$$r \geq 0 \text{ and } A(z) + B(z) = \sum_{r=0}^{\alpha} (a_r + b_r)\, z^r$$

If k is a scalar then

$$k\,A\,(z) = k\,(a_0\,z^0 + a_1\,z^1 + \ldots + a_r\,z^r + \ldots)$$

$$= k\sum_{r=0}^{\alpha} a_r\ z^r$$

The product $A\,(z)\,B\,(z)$ is defined as

$$A\,(z)\,B\,(z) = a_0\,b_0\,z^0 + (a_0\,b_1 + a_1\,b_0)\,z + (a_0\,b_2 + a_1\,b_1 + a_2\,b_0)\,z^2 + \ldots + (a_0\,b_r + a_1\,b_{r-1} + \ldots + a_r\,b_0)\,z^r + \ldots$$

for example, the generating function of the Numeric function

$$a_r = 5.2^r,\ r \geq 0$$

is $$A(z) = \frac{5}{1-2z}$$

the generating function of the Numeric function

$$a_r = 5.2^r,\ r \geq 0$$

is $$A(z) = \frac{25}{1-5z}$$

also the generating function of the numeric function

$$a_r = 5^{r+2},\ r \geq 0$$

is $$A(z) = \frac{1}{1-2z} + \frac{1}{1-5z}$$

4.15.1 Asymptotic Behaviour of Numeric Function

Let a be a numeric function. By the asymptotic behaviour of a, we mean how the volume of the function a varies for large r.

For example: for

$$a_r = 3r^2,\ r \geq 0$$

The value of the Numeric function increases for increasing r, and for

$$b_r = \frac{2}{r},\ r > 0$$

The value of the function decreases for increasing r. Finally for

$$C_r = 7,\ r > 0$$

The value of the numeric function remains constant for increasing r.

Let a and b be two numeric functions.

If there exist two positive constants r and k such that

$|b_r| \geq |a_r|$ for $r \geq k$

then we say that the numeric function a asymptotically dominates b, or the Number function b is dominated by a.

For example, let a and b be two numeric functions such that

$$a_r = r + 5,\ r \geq 0$$

$$b_r = \frac{1}{r} + 9,\ r > 0$$

Then the numeric functions a dominates b.

If a is a numeric function then $|\ a\ |$ asymptotically dominates a and if the numeric function b is asymptotically dominated by a, then for any constant λ, $\lambda\ b$ is also dominated by a.

If a is a given numeric function, then the set of all numeric functions that are dominated by a is called the order *"a"* or "big – Oh *a*" and is denoted by $O\ (a)$.

4.15.2 Recurrence Relations

In Section 4.1, we have discussed recursive definition of a sequence. The recursive formula for defining a sequence (or numeric function) is called a recurrence relation. If $a = (a_0, a_1, \ldots, a_r, \ldots)$ a numeric function, then the recurrence relation for a is an equation relating a_r for any r, to one or more a_i 's $(i < r)$. Every recursive formula includes a starting point. The information accompanying a recursive formula about the beginning of the sequence (or numeric function) is called initial condition. A recurrence relation is also called a difference equation.

Example 1: The recurrence relation $a_n = a_{n-1} + 5$, with $a_1 = 2$ recursively defines the sequence 7, 12, 17, … where $a_1 = 2$ is the initial condition.

Example 2: The recurrence relation $a_n = a_{n-1} + a_{n-2}$, with $a_1 = a_2 = 1$ defines the Fibonacci sequence 1, 1, 1, 2, 3, 5, 8, 13, … $a_0 = 1$, $a_1 = 1$, are called the initial conditions.

4.15.3 Linear Recurrence Relations

Suppose r and k are non-negative integers. A recurrence relation of the form

$$c_0\ (r)\ a_r + c_1\ (r)\ a_{r-1} + \ldots + c_k\ (r)\ a_{r-k} = f\ (r) \text{ for } r \geq k$$

where $c_0\ (r)$, $c_1\ (r)$, … $c_k\ (r)$ and $f\ (r)$ are functions of r is said to be a recurrence relation. If $c_0\ (r) > 0$ and $c_k\ (r) > 0$, then it said to be a linear recurrence relation of degree k. If $c_0\ (r)$, $c_1\ (r)$, … $c_k\ (r)$ are constants then the recurrence relation is called a linear recurrence relation with constant coefficients. if $f\ (r) = 0$, then the recurrence relation is called a linear homogenous relation. A recurrence relation which is not homogeneous is said to be inhomogeneous relation.

Examples: the recurrence relations

$$a_n - 6a_{n-1} + 11a_{n-1} + 6a_{n-3} = 2n$$

$$a_n - 9a_{n-1} + 26a_{n-1} - 24a_{n-3} = 5n$$

are linear recurrence relations with constant coefficients

The relation

$$a_n - 6a_{n-1} + 11a_{n-2} + 6a_{n-3} = 0$$

is homogeneous and $a_r + 9a_{r-2} = 0$ is a second order recurrence relation with constant coefficients.

4.15.4 Solutions of Recurrence Relations

We shall now describe some methods of solving recurrence relations in this section. We know that every recurrence relation is accompanied by boundary condition. Any numeric function that can be described by a recurrence relation together with an appropriate set of boundary conditions is called a solution of the recurrence relation. If $a = (a_0, a_1, \ldots, a_r, \ldots)$ is a solution to a recurrence relation then it is said to satisfy the relation. A given recurrence relation may or may not have a solution. We shall now consider the methods of solving of Homogeneous recurrence relations (*i*) the intervention method (substitution method) of solving a recurrence relation. In this method the recurrence relation for a_r is used repeatedly to solve the recurrence for a general expression for a_r in terms of *r*. We illustrate this method in the examples given below:

Example 1: Solve the recurrence relation $a_r = 2a_{r-1} + 1$ with $a_1 = 7$ for $r > 1$ by substitution.

Solution:

$a_1 = 7$ the initial conditions

$$\begin{aligned} a_2 &= 2a_1 + 1 = 2\,.7 + 1 \\ a_3 &= 2a_2 + 1 = 2\,.(2.7 + 1) + 1 \\ &= 2^2\,.\,7 + 2 + 1 \\ a_4 &= 2a_3 + 1 = 2\,(2^2\,.\,7 + 2 + 1) + 1 \\ &= 2^3\,.\,7 + 2^2 + 2 + 1 \\ &\ldots \\ a_r &= 2^{r-1}\,.\,7 + 2^{r-2} + 2^{r-3} + \ldots + 2 + 1 \end{aligned}$$

We have

$$a_r = 7.2^{r-1} + 2^{r-1} - 1,\ r \geq 1 \qquad (\because\ 1 + 2 + \ldots + 2^{r-2} = 2^{r-1} - 1)$$

Example 2: Solve the recurrence relation $a_r = a_{r-1} + f(r)$ for $r \geq 1$ by substitution.

Solution: We have

$$\begin{aligned} a_1 &= a_0 + f(1) \\ a_2 &= a_1 + f(2) = a_0 + f(1) + f(2) \\ a_3 &= a_2 + f(3) = a_0 + f(1) + f(2) + f(3) \\ a_r &= a_0 + f(1) + f(2) + \ldots + f(r) \\ &= a_0 + \sum_{n=1}^{r} f(n) \end{aligned}$$

(*ii*) Method of generating functions

Recurrence relations can also be solved by using generating functions. Some equivalent expressions used are given below:

$$A(z) = \sum_{r=0}^{\infty} a_r\, z^r \text{ then}$$

$$A(z) = \sum_{r=k}^{\infty} a_r\, z^r = A(z) - a_0 - a_1\, z - \ldots - a_{k-1}\, z^{k-1}$$

$$A(z) = \sum_{r=k}^{\infty} a_{r-1} z^r = z(A(z) - a_0 - a_1 z - ... - a_{k-2} z^{k-2})$$

$$A(z) = \sum_{r=k}^{\infty} a_{r-2} z^r = z^2 (A(z) - a_0 - a_1 z - ... - a_{k-3} z^{k-3})$$

$$A(z) = \sum_{r=k}^{\infty} a_{r-k} z^r = z^k A(z)$$

Example 3: Solve the recurrence relation

$$a_r - 7a_{r-1} + 10a_{r-2} = 0 \text{ for } r \geq 2$$

Solution: Multiplying each term of the recurrence relation by z^r, we get

$$a_r z^r - 7a_{r-1} z^r + 10a_{r-2} z^r = 0$$

Taking the sum 2 to ∞, we get

$$\sum_{r=2}^{\infty} a_r z^r - 7 \sum_{r=2}^{\infty} a_{r-1} z^r + 10 \sum_{r=2}^{\infty} a_{r-2} z^r = 0$$

replacing each infinite sum by the corresponding equivalent expression given above, we get

$$[A(z) - a_0 - a_1 z] - 7z\{A(z) - a_0\} - 10z^2 A(z) = 0$$

Simplifying, we get

$$A(z)(1 - 7z + 10z^2] = a_0 + a_1 z - 7a_0 z$$

or $$A(z) = \frac{a_0 + (a_1 - 7a_0)z}{1 - 7z + 10z^2} = \frac{a_0 + (a_1 - 7a_0)z}{(1-2z)(1-5z)}$$

Decomposing $A(z)$ as a sum of partial fractions, we can write

$$A(z) = \frac{c_1}{1-2z} + \frac{c_2}{1-5z} = c, \sum_{r=0}^{\infty} 2^r z^r + c_2 \sum_{r=0}^{\infty} 5^r z^r$$

The solution is $a_r = c_1 2^r + c_2 5^r$

(*iii*) Method of characteristic roots

Now we explain the method of solving linear recurrence relation by the methods of characteristic roots:

Consider

$$c_0 a_r + c_1 a_{r-1} + c_2 a_{r-2} + \dots + c_k a_{r-k} = 0 \quad \dots (1)$$

Substituting $A\alpha^r$ for a_r in (1), we get

$$c_0 A\alpha^r + c_1 A\alpha^{r-1} + c_2 A\alpha^{r-2} + ... + c_k A\alpha^{r-k} = 0 \quad \dots (2)$$

(the constant A is to be determined by the boundary conditions)

(2) Can be simplified as

$$c_0 \alpha^k + c_1 \alpha^{k-1} + ... + c_k = 0 \quad \dots (3)$$

The equation (3) is called the characteristic equation of the difference equation.

Equation (3) is an equation of kth degree. It has k roots. Let $\alpha_1, \alpha_2, \ldots \alpha_k$ denote the roots. Let the k roots be distinct. If $\alpha_1, \alpha_2, \ldots \alpha_k$ are called characteristic roots and

$$a_r = A_1 \alpha_1^{\ r} + A_2 \alpha_2^{\ r} + \ldots + A_k \alpha_k^{\ r}$$

is a solution of the difference equation given by (*i*). The constants $A_1, A_2, \ldots, A_n$ are determined by boundary conditions. Some roots of the characteristic equation may be multiple roots: Let a_1 be a root of multiplicity p, then the corresponding solution is given by

$$[A_1 r^{p-1} + A_2 r^{p-2} + \ldots + A_r] a_1^{\ r}$$

where the constants A_i s are to be determined by boundary conditions.

Example 4: Solve $a_r - 7a_{r-1} + 12a_{r-2} = 0$

Solution: The characteristic equation is

$$\alpha^2 - 7\alpha + 12 = 0$$
$$\Rightarrow (\alpha - 3)(\alpha - 4) = 0$$

The characteristic roots are $\alpha = 3$ and $\alpha = 4$.

$$a_r = A_1 \cdot 3^r + A_2 \cdot 4^r \text{ is the solution.}$$

Example 5: Solve $a_r + 9a_{r-1} + 27a_{r-2} + 27a_{r-3} = 0$

The characteristic equation is

$$\alpha^3 + 9\alpha^2 + 27\alpha + 27 = 0$$

or $$(\alpha + 3)^3 = 0$$

The characteristic roots are –3, –3, –3

Thus $a_r = (A_1 r^2 + A_1 r + A_z)(-3)^r$ is a solution.

4.16 SOLUTION OF NON-HOMOGENEOUS LINEAR RECURRENCE RELATIONS

In this section, we learn how to solve the non-homogeneous recurrence relations. Any solution to the recurrence relation is the sum of two parts: the Homogenous solution and the particular solution. A solution that satisfies the recurrence relation when the right hand side of the recurrence relation is set to zero is called a Homogeneous solution. The solution which satisfies the recurrence relation with $f(r)$ on right hand side is called the particular solution. The homogeneous solution is denoted by $a^{(h)}$ and the particular solutions denoted by $a^{(h)}$. We follow the same procedure as in solving homogeneous recurrence relations for determining the homogeneous solution. But there is no general procedure for determining the particular solution. It depends on the nature of $f(r)$. The methods are described in terms of examples.
(*i*) When $f(r)$ is a constant. Then the particular solution is also a constant.

Example 1: Find the particular solution of the recurrence relation

$$a_r - 7\underline{a}_{r-1} + 12\underline{a}_{r-2} = 1$$

Solution: $f(r)$ is a constant. Therefore, the particular solution is also a constant P. Substituting P in the given equation, we get $P - 7P + 12P = 1$

We get $$P = \frac{1}{6}$$

The particular solution is $a_r^{(p)} = \frac{1}{6}$

(*ii*) $f(r)$ may be polynomial in r and is of degree m. say. In this case the corresponding particular solution is of the form

$$P_1 r^m + P_2 r^{m-1} + \ldots + P_{m+1}$$

Example 2: Find the particular solution of

$$a_r + 5a_{r-1} + 6a_{r-2} = 3r^2$$

Solution: Let the form of the particular solution be $P_1 r^2 + P_2 r + P_3$ where P_1, P_2 and P_3 are constants to be determined. Substituting the expression into the left hand side of given difference equation, we get

$$P_1 r^2 + P_2 r + P_3 + 5P_1 (r-1)^2 + 5 P_2 (r-1) + 5P_3 + 6P_1 (r-2)^2 + 6P_2 (r-1) + 6P_3 = 3r^2$$

Simplifying, we get

$$12P_1 r^2 - (34p_1 - 12p_2) r + (29P_1 - 17P_2 + 12P_3) = 3r^2$$

$$12P_1 = 3 \quad \ldots \text{(i)}$$

$$34P_1 - 12P_2 = 0 \quad \ldots \text{(ii)}$$

$$29P_1 - 17P_2 + 12P_3 = 0 \quad \ldots \text{(iii)}$$

solving we get

$$P_1 = \frac{1}{4},\ P_2 = \frac{17}{24},\ P_3 = \frac{115}{288}$$

The particular solutions is

$$a_r^{(p)} = \frac{1}{4} r^2 + \frac{17}{24} r + \frac{115}{288}$$

(*iii*) When $f(r)$ is of the form λ^r, and λ is not a characteristic root of the recurrence relation, the particular solution is of the form $P\lambda^2$ further more when $f(r)$ is of the form

$\left(b_1 r^m + b_2 r^{m-1} + \ldots + b_{m+1}\right)\lambda^r$, the corresponding particular solution is of the form

$\left(P_1 r^m + P_2 r^{m-1} + \ldots + P_{m+1}\right)\lambda^r$,

Where λ is not a characteristic root of the recurrence relation. When λ is a characteristic root with multiplicity and $f(r)$ is of the form

$$\left(b_1 r^m + b_2 r^{m-1} + \ldots + b_{m+1}\right)\lambda^r,$$

the corresponding particular solution is of the form

$$r^{p-1}\left(P_1 r^m + P_2 r^{m-1} + \ldots + P_{m+1}\right)\lambda^r.$$

Example 3: Find a general expression for a solution to the recurrence relation

$$a_n - 5a_{n-1} + 6a_{n-2} = 4^n,\ n \geq 2. \qquad \textbf{\textit{(OU Dec. 2000)}}$$

Solution: The characteristic equation of the given relation is

$$\alpha^2 - 5\alpha + 6 = 0$$

or $$(\alpha - 2)(\alpha - 3) = 0$$

$\alpha = 2, \alpha = 3$ are the characteristic roots

The homogeneous solution is

$$a_n^{(h)} = A_1 2^n + A_2 3^n$$

The particular solution $a_n^{(p)}$ will be of the form

$$a_n^{(p)} = \lambda \cdot 4^n$$

Substituting $a_n = \lambda \cdot 4^n$ in

$$a_n - 5a_{n-1} + 6a_{n-2} = 4^n$$

we get

$$\lambda 4^n - 5\lambda 4^{n-1} + 6\lambda 4^{n-2} = 4^n$$

or $$4^{n-2}[\lambda 4^2 - 5\lambda \cdot 4 + 6\lambda] = 4^{n-2} \cdot 4^2$$

or $$16\lambda - 20\lambda + 6\lambda = 16$$

or $$2\lambda = 16$$

or $$\lambda = 8$$

Therefore, the general solution of the given recurrence relation is

$$a_n = A_1 \cdot 2^n + A_2 \cdot 3^n + 8 \cdot 4^n$$

Example 4: Find the particular integral of $a_r + a_{r-1} = 3r\,2^r$.

Solution: The general form of the particular solution is $(p_1\, r + P_2)\, 2^r$ substituting into $a_r + a_{r-1} = 3\,r\,2^r$, we get $(P_1\, r + P_2)\, 2^r + (P_1\,(r-1) + P_2)2^{r-1} = 3r\,2^r$ simplifying, we get

$$\frac{3}{2}P_1 r + \left(-\frac{1}{2}P_1 + \frac{3}{2}P_2\right)2^r = 3r2^r$$

Comparing, we get

$$\frac{3}{2}P_1 = 3$$

$$-\frac{1}{2}P_1 + \frac{3}{2}P_2 = 0$$

Solving the above equation

$$P_1 = 2,\ P_2 = \frac{2}{3}$$

The particular solution is

$$a_r^{(p)} = \left(2r + \frac{2}{3}\right)2^r$$

Example 5: Find the general solution of

$$a_r - 7a_{r-1} + 10a_{r-2} = 7.3^r, r \geq 2$$

Solution: The characteristic equation is $\left(\alpha^2 - 7\alpha + 10\right) = 0$

or $$\left(\alpha - 2\right)\left(\alpha - 5\right) = 0$$

The characteristic roots are 2, 5 the homogeneous solution is

$$a_r^{(h)} = A_1 2^r + A_2 5^r$$

Let $P \cdot 3^r$ be the particular solution of the given recurrence relation substitution $P, 3^r$ for a_r in the recurrence relation given

$$P \cdot 3^r - 7 P 3^{r-1} + 10 P 3^{r-2} = 7.3^r$$

$$\Rightarrow (-2) P = 7.3^2$$

$$\Rightarrow P = -63/2$$

The particular solutions is $a_r^{(p)} = (-63/2)3^r$

The general solutions is

$$a_r = a_r^{(p)} + a_r^{(h)} = A_1 2^r + A_2 5^r \left(-63/2\right)3^r$$

Example 6: Solve $a_r - 6a_{r-1} + 8a_{r-2} = r.4^r$ where $a_0 = 8$ and $a_1 = 22$

Solution: The characteristic equation of the given relation is

$$\alpha^2 - 6\alpha + 8 = 0$$

$$\Rightarrow \left(\alpha - 2\right)\left(\alpha - 4\right) = 0$$

The characteristic roots are 2, 4 the homogeneous solution is

$$a_r^{(h)} = A_1 2^r + A_2 4^r$$

Hence, 4 is a characteristic root with multiplicity 1. The particular solution takes the form $r(P_1 + P_2 r) 4^r$

Substituting this expression into recurrence relation, we get

$$16r(P_1 + P_2 r) - 24(r)(r-1)[P_1 + P_2(r-1)] + 8(r-2)[P_1 + P_2(r-2)] = 16r$$

The above expression holds for all values of and in particular for $r = 0$.

We obtained the simplified equation $P_1 + P_2 = 0$ for $r = 1$, we get $P_1 + 3P_2 = 2$

Which give $P_1 = -1$, $P_2 = 1$

The particular solution is $a_r^{(p)} = r(-1 + r) 4^r = r(r - 1)4^r$

The general solution is $a_r = a_r^{(h)} + a_r^{(p)}$

$$= A_1 2^r + A_2 4^r + r(r - 1) 4^r$$

the initial conditions $a_0 = 8$, $a_1 = 22$ give $A_1 = 3$.

The general solution is $a_r = r(-1 + r) 4^r + 5.2^r + 3.4^r$.

EXERCISE 4.3

I. Solve the recurrence relations

(*a*) $a_r = 7a_{r-1} - 10a_{r-2}$, $a_0 = 4$, $a_1 = 17$

(*b*) $a_r - 8a_{r-1} + 16a_{r-2} = 0$, $a_2 = 16$, $a_3 = 80$

(*c*) $a_r - 4a_{r-1} - 11a_{r-2} + 30a_{r-3} = 0$
given the initial condition
$a_0 = 0$, $a_1 = -35$, and $a_2 = -85$

(*d*) $a_r - a_{r-1} - 6a_{r-2} = -30$ with $a_0 = 20$, $a_1 = -5$

II. Solve:

(*a*) $S_k - 2S_{k-1} + S_{k-2} = 2$, with $S_0 = 25$, $S_1 = 16$

(*b*) $G_k - 7G_{k-1} + 10G_{k-2} = 6 + S_k$ with $G_0 = 1$, $G_1 = 2$

(*c*) $a_r - 3a_{r-1} - 4a_{r-2} = 4^r$

(*d*) $a_r - 4a_{r-1} + 4a_{r-2} = 3r + 2^r$

Answers:

I. (*a*) $a_r = 1.2^r + 3.5^r$

(*b*) $a_r = (2 + r)\ 4^{r-1}$

(*c*) $a_r = 4\ (-3)^r + 1.2^r + (-5)\ .\ 5^r$

(*d*) $a_r = 11\ .\ (-2)^r + 4\ .\ 3^r + 5$

II. (*a*) $S_k = 25 - 10k + k^2$

(*b*) $G_k = -9.2^k + 2.5\text{k} + (8 + 2k)$

(*c*) $a_r = A_1\ .\ (-1)^{\text{r}} + A_2\ .\ 4^r + \dfrac{4r \cdot 4^r}{5}$

(*d*) $a_r = (r^2 + 7r - 22)\ .\ 2^{r-1} + (12 + 3k)$.

5

Boolean Algebra

5.1 INTRODUCTION

In this chapter, we study partially ordered sets, Lattices and Boolean algebras. George Boole in 1854 has introduced a new kind of algebraic system known as Boolean algebra. It is relatively very simple and can be used to analyse and design completes circuits. Before we study Boolean algebra in this chapter we consider ordering relations and Lattices.

5.2 PARTIAL ORDERING

Definition 5.1: A relation R on a set A is called a partial order relation in A if R is, Reflexive anti-symmetric and transitive.

If R is a partial order on a set A, then A is said to be partially ordered by R. The partial order R on A is simply called an order relation on A. The set A with partial order R on it is called a partially ordered set or *n* ordered set or a Poset. We write (A, R) when we want to specify the partial order relation R usually we denote a partial order relation by the symbol $\leq$. This symbol does not necessarily mean "less than or equal to".

Example 1: If A is a non-empty set and $P(A)$ denotes the power set of A, then the relation set inclusion denoted by $\leq$ in $P(A)$ is a partial ordering.

Example 2: Let $A = \{2, 3, 6, 12, 24, 36\}$ and R be a relation in A which is defined by "*a* divides *b*". Then R is a partial order in A.

5.2.1 Comparability

Definition 5.2: Let R be a partial order on A and $a, \ b \in A$ whenever $aR\,b$ or $bR\,a$, we say that a and b are comparable otherwise a and b are non-comparable.

5.3 TOTALLY ORDERED SET

Definition 5.3: Let $(A, \leq)$ be a partially order set. If for every $a, \ b \in A,$ we have $a \leq b$ or $b \leq a$, then $\leq$ is called a simple ordering (or linear ordering) on A, and the set $(A, \leq)$ is called a totally ordered set or a chain.

Note: If A is a partially ordered set, then some of the elements of A are non-comparable. On the other land, if A is totally ordered then every pair of elements of A are comparable.

Example 1: Let N be the set of positive integers ordered by divisibility. The elements 5 and 15 are comparable. Since 5/15 on similarly the elements 7 and 21 are comparable since 7/21. The positive integers 3 and 5 are non-comparable since neither 3/5 nor 5/3. Similarly the integers 5 and 7 are non- comparable.

Example 2: Let A be a non-empty set with two or more elements and $P(A)$ denote the power set of A. Then $P(A)$ is not linearly ordered.

Example 3: The set N of positive integers with the usual order $\leq$ (less than equal) is a linear order on N. The set $(N, \leq)$ is a totally ordered set.

5.4 DUAL ORDER

Definition 5.4: If $\leq$ is a partial order on a set A, then the converse of R is also a partial order on A. i.e., if $\leq$ is a partial ordering on A, then $\geq$ is also a partial ordering on A. $(A, \geq)$ is called the dual of $(A, \leq)$.

Corresponding to every partial ordering on $\leq$ on A, we can define another relation on A which is denoted by < and is defined as follows:

$$a < b \Leftrightarrow a \leq b\text{: for all } a,\ b \in A, \text{ where } a \neq b$$

Similarly corresponding to the partial ordering $\geq$, we can define the a relation >, such that $a > b \Leftrightarrow a \geq b$ for $b \in A$ where $a \neq b$. The relations < and > are irreflexive, but both the relations < and > are transitive.

5.5 HASSE DIAGRAM

Definition 5.5: A Hasse diagram is a pictorial representation of a finite partial order on a set. In this representation, the objects i.e., the elements are shown as vertices (or dots).

Two related vertices in the Hasse diagram of a partial order are connected by a line if and only if they are related.

Example 1: Let $A = \{3, 4, 12, 24, 48, 72\}$ and the relation $\leq$ be such that $a \leq b$ if a divides b. The Hasse diagram of $(A, \leq)$ is shown in Fig. 5.1.

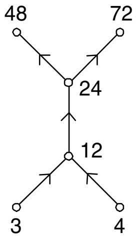


Fig. 5.1

We avoid arrows in a Hasse diagram and draw lines to show that the elements are related. Hasse diagrams can be drawn for any relation which is anti-symmetric and transitive but not necessarily reflexive.

Example 2: Let $A = \{1, 2, 3\}$, and $\leq$ be the relation "less than of equal to" on A. Then the Hasse diagram of $(A, \leq)$ is as shown in Fig. 5.2.

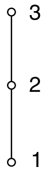


Fig. 5.2

Example 3: Let $A = \{a\}$, and $\leq$ be the inclusion relation on the elements of $P(A)$. The Hasse diagram of $(P(A), \leq)$, can drawn as shown in Fig. 5.3.

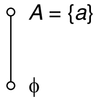


Fig. 5.3

Example 4: Draw the Hasse diagram representing the positive divisions of 36 (i.e., D_{36})
Solution: We have $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

Let R denote the partial order relation on D_{36}, i.e., aRb if and only a divides b. The Hasse diagram for R is shown in Fig. 5.3 (a).

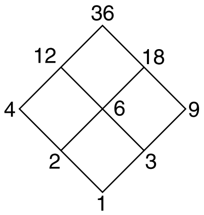


Fig. 5.3 (a)

Note:

(i) Two unequal relations R_1 and R_2 may have the same Hasse diagram.

(ii) The Hasse diagram of Poset A need not be connected.

If $(A, \leq)$ is partially ordered set, the Hasse diagram of $(A, \leq)$ is not unique. For example, consider the set $A = \{a, b\}$. The relation of inclusion $(\leq)$ on $P(A)$ is a partial ordering. The Hasse diagrams of $(P(A), \leq)$ are given in Fig. 5.4.

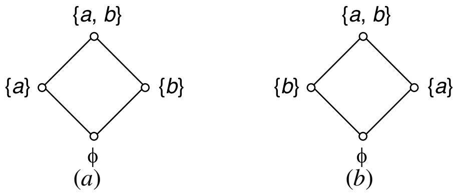


Fig. 5.4 Hasse diagram

The Hasse diagram which represent the partial ordered set $(A, \leq)$ show that the Hasse diagram of a poset is not unique.

If $(A, \leq)$ is a poset, the Hasse diagram of $(A, \geq)$ can be obtained by rotating the Hasse diagram of $(A, \leq)$ through 180°. So that the points at the top become the points at bottom. Some Hasse diagrams may have a unique point which is above all the other points in the diagram and in some cases, the Hasse diagrams have a unique point which is below all the other points.

Definition 5.6: A relation R on a set A is said to be connected if for every pair of distinct elements $a, b \in A$, either $aR\,b$ or $bR\,a$.

Definition 5.7: A partial ordering on a set A is said to be linear ordering if it is connected.

5.6 LEXICOGRAPHIC ORDERING

Let $(A, \leq)$ and $(B, \leq)$ be two partially ordered sets. We define another partial order on $A \times B$, denoted by $\prec$, and is defined as follows:

$(a, b) \prec (a', b')$ if $a < a'$ or if $a = a'$ and $b \leq b'$. The order $\prec$ is called Lexicographic ordering (or dictionary ordering). In the above ordering of elements in the first coordinate dominates except in case of ties. In this case of equality. We consider the second coordinate. The Lexicographic ordering defined above can be extended as follows:

Let $(A_1, \leq)$, $(A_2, \leq)$, ... $(A_n, \leq)$ denote partially ordered sets. We define a partial order $\propto$ on $A_1 \times A_2 \times ... A_n$ as follows:

$(a_1, a_{2,} ..., a_n) \prec (a_1', a_2', ..., a_n')$ if and only if

$a_1 < a_1'$ or

$a_1 = a_1'$ and $a_2' < a_2'$ or

$a_1 = a_1', a_2' = a_2'$, and $a_3 < a_3'$ or

$a_1 = a_1', a_2 = a_2' ... a_{n-1} = a_{n-1}'$and $a_n \leq a_n'$

in the above ordering:

The first coordinate dominates, in the case of equality, we consider the second coordinate, if the equality holds again, we pass to the next coordinate and so on.

The order in which the words in an English dictionary appear is an example of lexicographic ordering.

Example 1: Let $A = (a, b, c, ... z)$ and let A be linearly ordered in the usual way $(a \leq b), b \leq c, ... y \leq z)$. The set $A^n = A \times A \times ... \times A$ (n factors) can be identified with the set of all words having length n. The Lexicographic ordering on A^n has the S^n has the property that if $w_1 < w_2$ (where w_1 and w_2 are two words in S^n), then w_1 would precede w_2 in the dictionary listing.

Thus

Card $\prec$ Cart

Loss $\prec$ Lost

Park $\prec$ Part

Salt $\prec$ Seat
Mark $\prec$ Mast

We can extend Lexicographic order to posets. If A is a partially ordered set and A^* denotes the set of all finite sequences of elements of A we can extend Lexicographic order to A^* as follows:

Let $\alpha = a_1\, a_2 \ldots a_m$ and $\beta = b_1\, b_2 \ldots b_n$ belong to A^* with $m \leq n.$, we say that $\alpha \propto \beta$ if $(a_1, a_2, \ldots a_m) \propto (b_1, b_2, \ldots b_n)$ in $A^n = A \times A \times \ldots \times A$ (n factors) under the Lexicographic ordering of A^n.

Example 2: Let $A = \{a, b, c, \ldots z)$ and let R be a simple ordering on A denoted by $\leq$, where $(a \leq b \leq c \ldots \leq z)$

Let $S = A \cup A^2 \cup A^3$

Then S consists of all words (strings) of three or fewer than 3 letters from A. Let $\prec$ Denote the lexicographic ordering on S. We have

Be $\prec$ Bet
Leg $\prec$ Let
Peg $\prec$ Pet
Sea $\prec$ See
...

Lexicographic ordering is used in sorting character data on a computer. The Lexicographic ordering is also called dictionary ordering. We can use the names "Lexically less than" or "Lexically equal to" or "Lexically greater then" to denote a lexicographic ordering.

Example 3: Let $A = \{a, b, c, \ldots z)$ with simple alphabetical order and let $A^2 = A \times A$, then $bq > ae$, $df > ab$ and $dy < ez$.

5.7 COVER OF AN ELEMENT

Definition 5.8: Let $(A, \leq)$ be a partially ordered set. An element $b \in A$ is said to cover an element $a \in A$, if a $< b$ and if there does not exist any element $c \in A$ such that $a \leq c$ and $a \leq b$.

If b covers a, then a line is drawn between the elements a and b in the Hasse diagram of $(A, \leq)$.

5.8 LEAST AND GREATEST ELEMENTS

Definition 5.9: Let $(A, \leq)$ denote a partially ordered set. If there exists an element $a \in A$ such that $a \leq x \;\forall\; x \in A$, then a is called the least member in A, relative to the partial ordering $\leq$. Similarly, if there exists an element $b \in A$, such that $x \leq b \;\forall\; x \in A$, then b is called greatest member in A relative to $\leq$.

Note:

(*i*) The least member of is usually denoted by 0, and the greatest member in a poset is usually denoted by 1.

(*ii*) For a given poset, the greatest or least member may or may not exist.

(*iii*) The least member in poset, if it is unique, and the greatest member if it exists is unique.

(*iv*) In every chain, the least and greatest members always exist.

Example 1: Let $A = \{1, 2, 3, 4, 5\}$ and $\leq$ be the relation "less than or equal to" then the Hasse diagram of $(A, \leq)$ is as shown in Fig. 5.5.

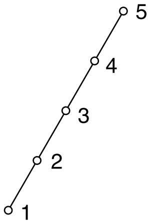


Fig. 5.5 Hasse diagram

From Fig. 5.5, it is clear that 1 is the least member and 5 is the greatest element in $(A, \leq)$.

Example 2: Let $A = \{a, b\}$ and $P(A)$ denote the power set of A. Then $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Let $\leq$ be the inclusion relation on the elements of $P(A)$. Clearly $\emptyset$ is the least member and $A = \{a, b\}$ is the greatest member in $(P(A), \leq)$.

We now discuss certain elements which are of special importance.

5.9 MINIMAL AND MAXIMAL ELEMENTS (MEMBERS)

Definition 5.10: Let $(A, \leq)$ denote a partially ordered set. An element $a \in A$ is called a minimal member of a relative to $\leq$ if for no $x \in A$, is $x < a$.

Similarly an element $b \in A$ is called a maximal member of A relative to the partial ordering $\leq$ if for no $x \in A$, is $b < x$.

The minimal and maximal members of a partially ordered set need not unique.

Example 1: Consider the poset shown in Fig. 5.6

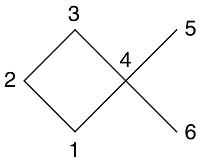


Fig. 5.6

There are two maximal elements and two minimal elements.

The elements 3, 5 are maximal and the elements 1 and 6 are minimal.

Example 2: Let $A = \{a, b, c, d, e\}$ and let Fig. 5.7 represent the partial order on A in the natural way. The element a is maximal. The elements d and e are minimal.

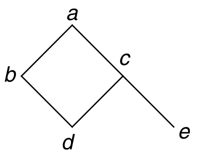


Fig. 5.7

Distinct minimal members of a partially ordered set are incomparable and distinct maximal members of a poset are also incomparable.

5.10 UPPER AND LOWER BOUNDS

Definition 5.11: Let $(A, \leq)$ be a partially ordered set and let $B \leq A$. Any element $m \in A$ is called an upper bound for B if for all $x \in A$, $x \leq m$. Similarly an element $l \in A$ is called a lower bound for B if for all $x \in A$, $l \leq x$.

Example 1: $A = \{1, 2, 3, ..., 6\}$ be ordered as pictured in Fig. 5.8.

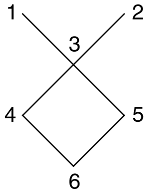


Fig. 5.8

If $B = \{4, 5\}$ then

The upper bounds of B are 1, 2, 3

The lower bound of B is 6.

Example 2: Let $A = \{a, b, c\}$ and $(P(A) \leq)$ be the partially ordered set. The Hasse diagram of the Poset be as pictured in Fig. 5.9.

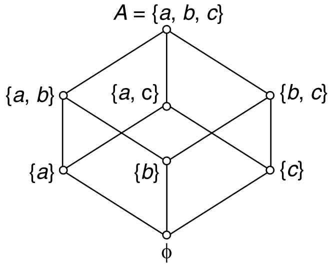


Fig. 5.9

If B is the subset $\{a, c\}$, $\{c\}$. Then the upper bounds of B are $\{a, c\}$ and A, while the lower bounds of B are $\{c\}$ and $\varnothing$.

From the above, it is clear that the upper and lower bounds of a subset are not unique.

5.10.1 Least Upper Bound (Supremum)

Definition 5.12: Set A be a partially ordered set and B a subset of A. An element $m \in A$ is called the least upper bound of B if M is an upper bound of B and $M \leq M'$ whenever M' is an upper bound of B.

A least upper bound of a partially ordered set if it exist is unique.

Example: Let $A = \{a, b, c, d, e, f, g, h\}$ denote a partially ordered set. Whose Hasse diagram is shown in Fig. 5.10:

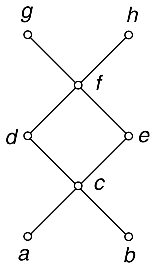


Fig. 5.10

If $B = \{c, d, e\}$ then f, g, h are upper bounds of B. The elements f is least upper bound.

5.10.2 The Greatest Lower Bound (Infimum)

Definition 5.13: Let A be a partially ordered set and B denote a subset of A. An element L is called a greatest lower bound of B if l is a lower of B and $L' \leq L$ whenever L' in a lower bound of B.

The greatest lower bound of a poset if it exists is unique.

Example: Consider the poset $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ whose Hasse diagram is shown in Fig. 5.11 and let $B = \{3, 4, 5\}$

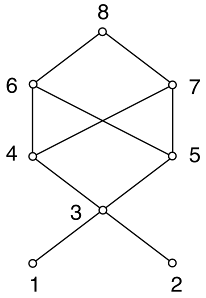


Fig. 5.11

The elements 1, 2, 3 are lower bounds of B. 3 is greatest lower bound.

The least upper bound (LUB) and the greatest lower bound (GLB) of subset B are also called the supremum and infimum of the subset B.

Note:

(*i*) The least upper bound of a set is abbreviated as $l \cdot u \cdot b$ or *sup* and the greatest lower bound is abbreviated as "$g \cdot l \cdot b$" or "*inf*".

(*ii*) If A is a chain, then every subset S: has a supremum and an infimum.

(*iii*) Let N be the set of positive integers and let N by ordered by divisibility. If a and b are two elements of N, then

$inf\,(a, b) = gcd\,(a, b)$

and Sup (a, b) = Lcm (a, b)

(*iv*) If $(A, \leq)$ is a poset, then its dual $(A, \geq)$ is also a poset. The least member of $(A, \leq)$ is the greatest member in $(A, \geq)$ relative to $\geq$ and vice versa. Similarly the $g \cdot l \cdot b$ of A with respect to the relation $\leq$ is the as $g \cdot l \cdot b$ of A with respect to the relation $\geq$ and vice versa.

(*v*) $g \cdot l \cdot b$ of a and b is called the meet or product of a and b and the l.u.b of a and b is called the join or sum of a and b where $a, b \in N$. The symbols such as * and $\oplus$ are also used to denote meet and join respectively.

Theorem 5.1: Let $(A, \leq)$ be a partially ordered set and S be a subset of A. Then

(*i*) The least upper bound of set, if it exists is unique.

(*ii*) The greatest lower bound of S, if it exists is unique.

i.e., S can have at most, one least upper bound and at most one greatest lower bound.

Proof: (*i*) If possible let there be two least upper bounds for S, say b_1 and b_2. Now b_2 is supremum and b_1 is an upper bound of $S \Rightarrow b_2 \leq b_1$. Similarly b_1 is supremum and b_2 is an upper bound of $S \Rightarrow b_1 \leq b_2$. $S \subseteq A$, therefore by symmetric property $b_2 \leq b_2, b_1 \leq b_2 \Rightarrow b_1 = b_2$. Hence, least upper bound of S is unique.

(*ii*) Left as an exercise.

Theorem 5.2: Let A be finite non-empty poset with partial order $\leq$. Then A has atleast, one maximal element.

Proof: Let $a \in A$. If a is not the maximal element. Then we can find an element $a_1 \in A$ such that $a < a_1$. It a_1 is not a maximal element of A, then we can find an element $a_2 \in A$ such that $a_1 < a_2$. Continuing this argument we get a chain

$$a < a_1 < a_2 < a_3 < \dots a_{r-1} < a_r$$

Since A is finite this chain cannot be extended and for any $b \in A$, we cannot have $a_r < b$. Hence a_r is a maximal element of $(A, \leq)$.

By the same argument, the dual poset $(A, \geq)$ has a maximal element such that $(A, \leq)$ has a minimal element.

Theorem 5.3: If $(A, \leq)$ and $(B, \leq)$ are partially ordered sets, then $(A \times B, \leq)$ is a partially ordered set with the partial order $\leq$, defined by $(a, b) \leq (a', b')$ if $a \leq a'$ in A and $b \leq b'$ in B.

Proof: $a \leq a'$ in A and $b \leq b'$ in B

$\therefore$ $(a, b) \in A \times B$ implies $(a, b) \leq (a, b)$

Hence $\leq$ satisfies reflexive property in $A \times B$.

Let $(a, b) \leq (a', b')$ and $(a', b') \leq (a, b)$ where a, a' are the members of A and b, b' are the members of B.

Then $a \leq a'$ and $a' \leq a$ in A and $b \leq b'$ and $b' \leq b$ in B

Now $a \leq a'$ and $a' \leq a \Rightarrow a = a'$

(since A is a partially ordered set)

and $$b \leq b' \text{ and } b' \leq b \Rightarrow b = b'$$

(since B is a partially ordered set)

$\therefore$ $\leq$ is anti-symmetric in $A \times B$

Also $(a, b) \leq a', b'$ and $(a', b') \leq (a'', b'')$ in $A \times B$ where $a, a', a'' \in A$ and $b, b', b'' \in A$ implies that

$$a \leq a' \text{ and } a' \leq a''$$

and $$b \leq b' \text{ and } b' \leq b''$$

by the transitive property of the partial orders in A and B, we have

$$a \leq a', a' \leq a'' \Rightarrow a \leq a''$$

and $$b \leq b', b' \leq b'' \Rightarrow b \leq b''$$

Hence $(a, b) \leq (a'', b'')$

Therefore transitive property holds for partial order in $A \times B$. Hence $A \times B$ is a partially ordered set.

5.11 WELL-ORDER SET

Definition 5.14: A set with an ordering relation is well-ordered if every non-empty subset of the set has a least element.

Example: The set of natural numbers is well-ordered.

5.12 BINARY AND N-ARY OPERATIONS

Definition 5.15: Let A be a non-empty set and f be a mapping $f: A \times A \to A$. Then f is called a binary operation on the set A and the mapping

$$f: A^n \to A$$

is called an n-ary operation on A. If, f is an n-ary operation; then n is called the order of the operation $f: A \to A$ (i.e., $n = 1$), is called a unary operation.

Examples: (*i*) Addition is a binary operation on the set of natural numbers.

(*ii*) Addition, multiplication and subtraction are binary operations on the set of integers.

It is customary to denote a binary operation by symbols such as +, –, 0, *, $\cup, \cap$, etc. A binary operation on the elements of a set produces images which are again the members of the same set. A given set with the given binary operation is said to be closed with respect to the binary operation.

5.13 CHOICE FUNCTIONS

Definition 5.16: Let $\{A_i : i \in I\}$ be a collection of non-empty disjoint sets and let $A_i \leq X \ \forall \ i.$ A function

$f: \{A_i\} \to \times$ defined by

$f(A_i) = a_i \in A_i$ is called a choice function.

5.14 AXIOM OF CHOICE

There exists a choice functions for any non-empty collection of non-empty sets.

We now state a theorem called the well-ordering theorem without proof.

5.15 WELL-ORDERING THEOREM

Theorem 5.4: Every set A can be well-ordered.

5.16 LATTICES

In this section, we introduce lattices which have important applications in the theory and design of computers.

Definition 5.17: A lattice is a partially ordered set $(L, \leq)$ in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

Example 1: Let Z^+ denote the set of all positive integers and let R denote the relation 'division' in Z^+. Such that for any two elements $a, b \in Z^+$, $aR\,b$, if a divides b. Then (Z^+, R) is a lattice in which the join of a and b is the least common multiple of a and b, i.e. $a \vee b = a \oplus b$ = LCM of a and b, and the meet of a and b, i.e. $a * b$ is the greatest common divisor (GCD) a and b i.e.,

$$a \wedge b = a * b = \text{GCD of } a \text{ and } b$$

We can also write $a + b = a \vee b = a \oplus b =$ LCM of a and b and $a \,.\, b = a \wedge b = a * b =$ GCD of a and b.

Example 2: Let S be a non-empty set and $L = P(S)$; $(P(S); \leq)$ i.e., $(L, \leq)$ is a partially ordered set. If A and B are two elements of L, then we have $A \cup B = A \vee B$ and $A \cap B = A \wedge B$

Hence the $(L, \leq)$ is a Lattice.

Example 3: Let $\cap$ be a positive integer and S_n be the set of all divisors of n ... S_n. If $n = 30$, $S_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$. Let R denote the relation division as defined in example 1. Then (S_{30}, R) is a Lattice see Fig. 5.12.

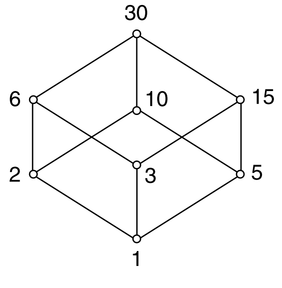


Fig. 5.12

Different lattices can be represented by the same, Hasse diagram. If $(L, \leq)$ is a lattice, then $(L, \geq)$ is also a lattice. The operations of meet and join on $(L, \leq)$ become the operations of join and meet on

$(L, \geq)$. The statement involving the operations * and $\oplus$ and $\leq$ hold if we replace * by $\oplus$, $\oplus$ by * and $\leq$ by $\geq$. The lattices $(L, \leq)$ and $(L, \geq)$ are duals of each other.

Example 4: Let A be a non-empty set and $L = P(A)$. Then $(L, \leq)$ is a lattice. Its dual $(L, \geq)$ is also a lattice.

5.17 SOME PROPERTIES OF LATTICES

Let $(L, \leq)$ be a lattice and '$\cdot$' and '+' denote the two binary operation meet and join on $(L, \leq)$. Then for any $a, b, c \in L$ we have

$(L-1)$ $a \cdot a = a$, $(L-1)'$ $a + a = a$ (Idempolint laws)

$(L-2)$ $a \cdot a = b \cdot a$, $(L-2)'$ $a + b = b + a$ (Commutative laws)

$(L-3)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $(L-3)'$ $(a + b) + c = a + (b + c)$ (Associative laws)

$(L-4)$ $a \cdot (a + b) = a$, $(L-4)'$ $a + (a \cdot b) = a$ (Absorption laws).

The above properties (*L*, – 1) to (*L*, – 4) can be proved easily by using definitions of meet and join. We can apply the principle of duality and obtain $(L-1)'$ to $(L-4)'$.

Theorem 5.5: Let $(L, \leq)$ be a lattice in which '$\cdot$' And '+' denote the operations of meet and join respectively. Then

$$a \leq b \Leftrightarrow a \cdot b = a \Leftrightarrow a + b = b \quad \forall\ a, b, c \in L$$

Proof: Let $a \leq b$

We know that $a \leq a$, therefore $a \leq a \cdot b$ but from the definition we have $a \cdot b \leq a$

$$\therefore \qquad a \leq b \Rightarrow a \cdot b = a$$

let us assume that $a \cdot b = a$

but this is possible only if $a \leq b$

i.e., $a \cdot b = a \Rightarrow a \leq b$

$$\therefore \qquad a \leq b \Rightarrow a \cdot b = a \textit{ and } a \cdot b = a \Rightarrow a \leq b$$

combining these two, we get

$$a \leq b \Leftrightarrow a \cdot b = a$$

now let $a \cdot b = a$, then we have

$$b + (a \cdot b) = b + a + a + b$$

but $b + (a \cdot b) = b$

Hence $a + b = b$

Similarly by assuming $a + b = b$ we can show that $a \cdot b = a$

Hence $a \leq b \Leftrightarrow a \cdot b = a \Leftrightarrow a + b = b \;\; = a$

Theorem 5.6: Let $(L, \leq)$ be a lattice. Then

$$b \leq c \Rightarrow \begin{cases} a \cdot b \leq a \cdot c \\ a + b \leq a + c \end{cases}$$

For all $a, b, c \in L$

Proof: From Theorem 5.4

$$b \leq c \Leftrightarrow b \cdot c = b$$

now $$(a \cdot b),\ (a \cdot c) = (a \cdot a)\ (b \cdot c) = a\ (b \cdot c)\ \ a \cdot b$$

$$\Rightarrow a \cdot b \leq a \cdot c$$

Similarly we can prove $a + b \leq a + c\ \forall\ a, b, c \in L$

Note: The above properties of a Lattice are called properties of Isotonicity

We now state the following theorem without proof:

Theorem 5.7: Let $(L, \leq)$ be a Lattice. Then

$$a + (b \cdot c) \leq (a + b) \cdot (a + c)$$

$$a \cdot (b + c) \leq (a \cdot b) + (a \cdot c)$$

for all $a, b, c \in L$

Proof: The proof is left as an exercise.

5.18 LATTICE AS AN ALGEBRAIC SYSTEM

We now define lattice as an algebraic system, so that we can apply many concepts associated with algebraic systems to lattices.

Definition 5.18: A lattice is an algebraic system $(L, \cdot, +)$ with two binary operation '·' and '+' on L which are both commutative and associative and satisfy absorption laws.

5.19 BOUNDED LATTICES

If L is a lattice, then every pair of elements of L has a least upper bound and a greatest lower bound. If A is a finite subset of A, then A has both least upper bound and greatest lower bound. This property may not hold if A is not a finite subset of L, we find greatest lower bound and least upper bound of a subset of a lattice as follows.

Let $(L, \cdot, +)$ be a lattice and $A \leq L$ be a finite subset of L. The greatest and least upper bound of A are defined as

$$glb\ \ A = \overset{n}{\underset{i=1}{\cdot}}\ a_i \text{ and } l \cup b\ \ A = \overset{n}{\underset{i=1}{+}}\ a_i$$

Where $A = \{a_1, a_2, \ldots a_n\}$

Example: Show that for a bounded, distributive lattice, complement of an element is unique.

(VTU Aug. 2000)

Solution: Let L be a bounded distributive lattice.

Let $e \in L.$ If possible let e' and e'' be the complements of e in L.

Then $e + e' = 1$ and $e + e'' = 1$

$$e \cdot e' = 0 \text{ and } e \cdot e'' = 0$$

now
$$\begin{aligned} e' &= e' + 0 \\ &= e' + (e \cdot e'') \\ &= (e' + e) \cdot (e' + e'') \\ &= (e + e') \cdot (e' + e'') \\ &= 1 \cdot (e' + e'') \end{aligned}$$

Thus $$e' = e' + e'' \qquad \text{... (1)}$$

Also
$$\begin{aligned} e'' &= e'' + 0 \\ &= e'' + (e \cdot e') \\ &= (e'' + e) \cdot (e'' + e') \end{aligned}$$

Definition 5.19: A lattice is called complete if each of its non-empty subsets has *a* least upper bound and a greatest lower bound.

The least and greatest elements of a lattice L, if they exist are called the bounds of the lattice L, they are denoted by 0 and 1 respectively. A lattice which has both 0 and 1 is called a bounded lattice. Every finite lattice must be complete, and every complete lattice must have a least element and a greatest elements. The bounds of L satisfy the following:

$$a + 0 = a, \ a \cdot 1 = a$$
$$a + 1 = 1, \ a \cdot 0 = 0 \text{ for any } a \in L$$

If L is a bounded lattice, then the elements 0 and 1 duals of each other. If L is a bounds lattice, then we denote it by (L, $\cdot$, +, 0, 1)

Definition 5.20: Let (L, $\cdot$, +, 0, 1) be a bounded lattice and $a \in L.$ If there exists an element $b \in L$ such that

$$a \cdot b = 0 \text{ and } a + b = 1$$

then b is called the complement of a

Example 1: Let A be a non-empty set and $L = P(A)$. Then the every element of L has a complement.

Example 2: In the lattice shown in Fig. 5.13 the elements a and d are complements of each other

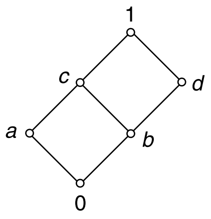


Fig. 5.13

Definition 5.21: A lattice L is complemented if it is bounded and if every element in L has a complement.

Example: If S is non-empty set and $L = P(S)$. Then each element of L has a unique complement in L. Therefore $L = P(S)$ is a complemented lattice.

5.20 SUB LATTICES, DIRECT PRODUCTS

Definition 5.22: Let $(L, \leq)$ be a lattice. A non-empty subset A of L is called a sub lattice of L if $a + b \in A$ and $a \cdot b \in A$ whenever $a \in A$ and $b \in A$.

If A is a sub lattice of L, then A is closed under the operations of '$\cdot$' and '+'.

Example 1: Let Z^+ be the set of all positive integers and let D denote the relation "division" in Z^+ such that for any $a, b \in Z^+$, $a\ D\ b$ if a divides 6. Then (Z^+, D) is a lattice in which $a + b$ = LCM of a and b and $a \cdot b$ = GCD of a and b.

Example 2: Let n be a positive integer and S_n be the set of all divisiors of n. If D denote the relation as defined above (in example 1). Then (S_n, D) is a sub lattice of (Z^+, D).

Example 3: Consider the lattice L shown in Fig. 5.14. The subset $A = \{a, c, d, y\}$ is a sub lattice of L.

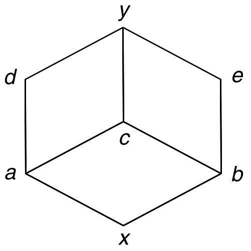


Fig. 5.14

Definition 5.23: Let $(L_1, *, +)$ and $(L_2, \wedge, \vee)$ be two lattices. The algebraic system $(L_1 \times L_2, ..., +)$ in which the binary operation + and '$\cdot$' are on $L_1 \times L_2$ defined as

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$$

$$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$$

for all (a_1, b_1) and (a_2, b_2) $(a_2, b_2) \in L_1 \times L_2$

is called the direct product of the lattices L_1 and L_2.

Example 4: Let $L_1 = \{1, 2, 4\}$ and $L_2 = \{1, 3, 9\}$, clearly L_1 and L_2 are chains and division is a partial ordering on L_1 and L_2 and L_1 consists of divisors of 4 and L_2 consists of divisor of 9. $L_1 \times L_2$ consists of 36 where each node in the diagram of $L_1 \times L_2$ is shown as (a, b) (instead of $a\ b$).

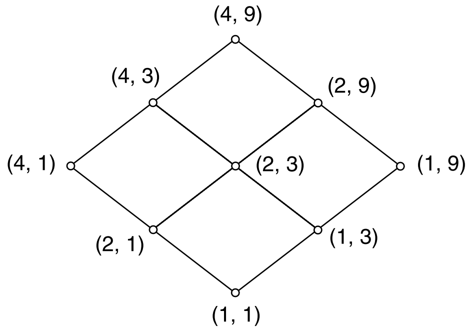
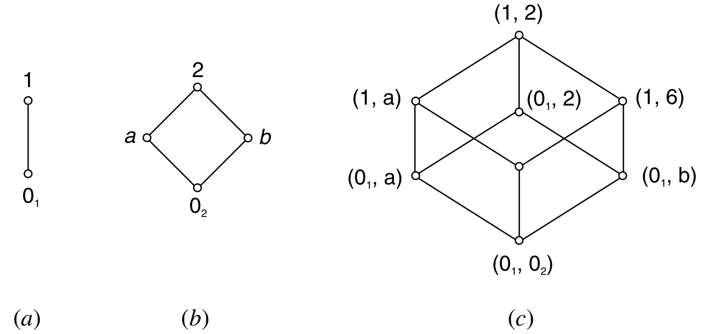


Fig. 5.15 Direct products of two lattices

Example 5: Let L_1 and L_2 be two lattices shown Fig. 5.16 (*a*) and (*b*) respectively. Then $L_1 \times L_2$ is the lattice shown Fig. 5.16. (*c*).



(*a*) (*b*) (*c*)

Fig. 5.16

We can use the direct product of lattices to construct larger lattices from the smaller ones. If L is a lattice we can form lattices $L \times L$, $L \times L \times L$, $L \times L \times L \times L$, ... which are denoted L^2, L^3, L^4, ... respectively.

Example 6: If $L = (0, 1)$ and $(L, \leq)$ is a lattice, then $(L^n, \leq_n)$ is a lattice of n-tuples of 0 and 1. Any element in the lattice $(L^n, \leq_n)$ can be written as $(a_1, a_2, \ldots a_n)$ in which a_1 is either 0 and 1 for $i = 1, 2, 3, \ldots, 4$.

The partial ordering relation on L^n can be defined for any a, b in L^n as

$$a \leq_n b \Leftrightarrow a_i, \leq_n b_i \text{ for } i = 1, 2, \ldots, n$$

where $$a = (a_1, a_2, \ldots a_n) \text{ and}$$

$$b = (b_1, b_2, \ldots, b_n)$$

In general the diagram of $(L^n, \leq_n)$ is an n-cube.

Definition 5.24: Let $(L, \cdot, +, 0, 1)$ be a lattice L is said to complemented lattice if every element has atleast one complement.

Example 7: Let $(L_3, \leq_3)$ be a lattice of 3-tuples of 0 and 1. The complement of an element of L_3 can be obtained by changing 1 by 0 and 0 by 1 in the 3-tuples representing the element.

The complement of (0, 1, 1) is (1, 0, 0), the complement of (1, 0, 1) is (0, 1, 0) and so an. The bounds of (0, 0, 0) and (1, 1, 1).

Definition 5.25: A lattice $(L, \cdot, +)$ is called a distributive lattice if for any $a, b, c \in L$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

Example 8: $(L_3, \leq_3)$ is distributive.

Example 9: The power set of a non-empty set *A* is a lattice under the operation $\cap$ and $\cup$ is a distributive lattice.

Definition 5.26: Let $(L, \leq)$ be a lattice, with a lower bound 0. An element $a \in L$ is said to be join irreducible if $a = x + y \Rightarrow a = x$ or $a = y$.

Example 10: $0 \in L$ is join irreducible.

Let $a \neq 0$ be an element of *L*. The element *a* is join irreducible if and only if *a* has unique immediate predecessor.

Definition 5.27: Let $(L, \leq)$ be a lattice, with an upper bound 1. An element $a \in L$ is said to be meet irreducible if $a = x \cdot y$ implies $a = x$ or $a = y$.

If $a \neq 0$ then *a* is meet irreducible if and only if *a* has unique immediate sucessor.

Example 11: Find the join irreducible and meet irreducible elements of the lattice shown in Fig. 5.17.

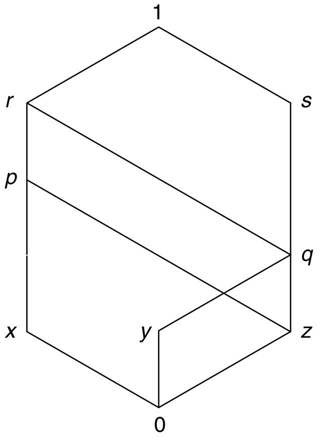


Fig. 5.17

Solution: The elements *x*, *y*, *z* and *s* are join irreducible. The elements *x*, *y*, *p*, *r* and *s* are meet irreducible.

Definition 5.28: The join irreducible elements of a lattice *L*, which immediately succeed 0 are called atoms.

Example 12: In the lattice shown in Fig. 5.18, 2 is the 0 element (lower bound) 3 succeeds 2, hence atom of L is the element 3.

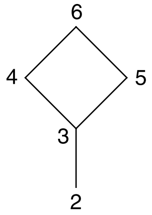
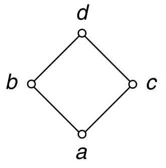


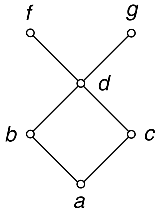
Fig. 5.18

EXERCISE 5.1

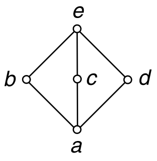
1. Define the terms
   (*a*) Partially ordered set
   (*b*) Linearly ordered set.
   Give examples.
2. Let $\leq$ be a Partial ordering of a set S. Define the dual order on S. How is the dual order related to the iverse of the relation $\leq$.
3. Define Lenilographical order on $A \times B$ where A and B are two linearly ordered sets.
4. Define the terms 'immediate predecessor' and 'immediate successor' and show that each element of a linearly ordered set can have at most one immediate predecessor.
5. What is meant by a 'Hasse diagram'? Draw the Hasse diagram of the relation R on A where $A = \{1, 2, 3, 4\}$ and
   $R = \{(1, 1), (1, 2), (2, 2), (2, 4), (1, 3), (3, 3), (3, 4), (1, 4), (4, 4)\}$.
6. Let n be a positive integer and S_n be the set of all divisors of n. Let D denote the relation of 'division' '*ns*, such that $a\ D\ b$' iff a divides b. Draw the Hasse diagram for (S_n, D).
7. Let $A = \{1, 2, 3, 4, 6, 8, 9, 12, 24\}$ be ordered by divisibility.
8. Determine the greatest and least elements, if they exist of the poset
   $A = \{2, 4, 6, 8, 12, 18, 24, 36, 72\}$ with the partial order of divisibility.
9. Which of the Hasse diagram in the figure given below represents lattices:



(*i*)



(*ii*)



(*iii*)

10. If $(L_1, \leq)$ and $(L_2, \leq)$ are two lattices, then show that $(L_1, \times L_2, \leq)$ is also a lattice.

11. Define that term ‘sub lattice’. Give an example.

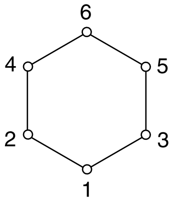
12. What is meant by a bounded lattice? If L is a finite lattice show that L is bounded.

13. Show that a subset of a linearly ordered poset is a sub lattice.

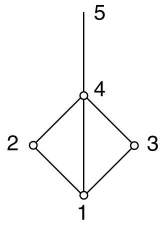
14. Show that a linearly ordered poset is a distributive lattice.

15. Let L be a bounded lattice with atleast two elements. Show that no two elements of L is its own complement.

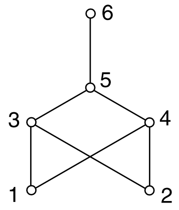
16. Which of the partially ordered sets shown in the figure below are lattices.



(*a*)

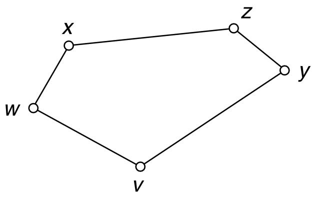


(*b*)



(*c*)

17. Consider the lattices $D = \{v, w, x, y, z\}$ shown in the figure given below. Find all the sub lattices with three or more elements.



18. Suppose the following collection of sets is ordered by set inclusion:

$$A = \{\{a\}, \{a, b\}, \{a, b, c, d\}, \{a, b, c, d, e, f\}\}.$$

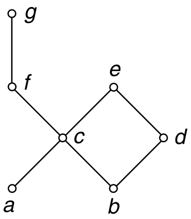
Is A well-ordered?

19. Define the dual of a statement in a lattice L. Why does principle of duality apply to L?

20. Suppose L is a linearly ordered set. Show that S has almost one maximal element.

21. $S = \{2, 4, 6, 12, 20\}$ is ordered by divisibility. Find the maximal and minimal elements of S.

22. Find all the maximal and minimal elements of the poset B diagrammed in the figure below:



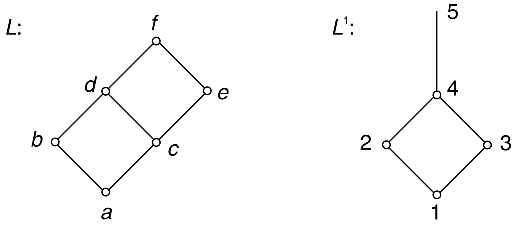
23. Show that every chain is a distributive lattice.

24. Show that the operations of meet and join in a lattice are, commutative, associative and idempotent.

25. If $(L, \leq)$ is a lattice in which * and $\oplus$ denote the operations of meet and join respectively then show that

$$a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$$
$$\forall\ a, b, c \in L$$

26. Define Isomorphic lattices. Show that the lattices L and L^1 given below are not isomorphic:



27. Define the terms

(*a*) Distributive Lattice.

(*b*) Join irreducible elements of a Lattice.

28. Show that if a bounded lattice has two or more elements then $0 \neq 1$.

29. L is a bounded lattice. If L is distributive and the complement of an element $a \in L$ exists, then show that it is unique.

5.21 BOOLEAN ALGEBRA

Definition 5.29: A Boolean algebra is a distributive complemented lattice having atleast two elements as well as 0 and 1.

A Boolean algebra is generally denoted by a 6-tuple, $(B, +, \cdot, {}^1, 0, 1)$ where $(B, +, \cdot)$ is a lattice with two binary operations + and ·, called the join and meet respectively is a unary operation in B. The elements 0 and 1 are the least and greatest elements of the lattice $(B, +, \cdot)$. The following axioms are satisfied:

1. There exist at least two elements a, b in B and that $a \neq b$.

2. $\forall\ a, b \in B$

   (*i*) $a + b \in B$

   (*ii*) $a \cdot b \in B$

3. for all $a, b \in B$

   $$\left.\begin{aligned} (i)\ & a + b = b + a \\ (ii)\ & a \cdot b = b \cdot a \end{aligned}\right\} \quad \text{commutative laws}$$

4. Associative laws: for all $a, b, c \in B$

   (*i*) $a + (b + c) = (a + b) + c$

   (*ii*) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

5. Distributive laws: for all $a, b, c \in B$

   (*i*) $a + (b \cdot c) = (a + b) \cdot (a + c)$

   (*ii*) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

6. (*i*) Existence of zero: There exists of *B* such that

$$a + 0 = a \ \forall \ a \in B$$

   The element 0 is called the zero element

   (*ii*) Existence of unit: There exists $1 \in B$ sum that

$$a \cdot 1 = a \ \forall \ a \in B$$

   The element 1 is called the unit element.

7. Existence of complement: $\forall \ a \in B$ there exists an element $a' \in B$ such that

   (*i*) $a + a' = 1$ and (*ii*) $a \cdot a' = 0$

Example 1: Let $A_1, A_2, ..., A_n$ be subsets of a universal set *X*. The set of all subsets of $\{ A_1, A_2, ..., A_n\}$. Which can be formed from A_i by union intersection and complement together with the binary operation $\cup$ and $\cap$, and the unary operation is a Boolean algebra.

Example 2: Let $B = \{0, 1\}$ and let +, $\cdot$ be two operations in *B* defined by the following operation tables (*a*) and (*b*):

+	1	0
1	1	1
0	1	0

(*a*)

·	1	0
1	1	0
0	0	0

(*b*)

Suppose that the complements are defined by $1^1 = 0$ and $0^1 = 1^1$, then *B* is a Boolean algebra.

Example 3: Let B_n denote the set of n-bit sequences. Let the operations of sum. Product and complement in B_n defined as follows:

For all $a, b \in B_n$ ... $a + b$ contains 1 if a, b contains 1, $a \cdot b$ contains 1 if *a* and *b* contain: *a* and *b* contains 1 if a contains 0, then B_n is a Boolean algebra.

Example 4: Let $\pi 1$ be the set of all propositions *T*1 is a Boolean algebra under the operations $\vee$ and *A* with ~ being the complement. The contradiction *f* is the zero element and the taulogy *T* is unit element of in $\pi 1$.

When $\cdot$ operations are performed before + operation the parentheses are not used, we use the letter *B* to represent a Boolean algebra $(B, +, \cdot, {}^1, 0, 1)$ and we often use the symbols $\vee$ and $\wedge$ in the place of + and operation. The dual of any statement *S* in *B* is the statement obtained by interchanging the operations + and $\cdot$ and interchanging the identity elements 0 and 1, in the original statement *S*. Also the dual of any theorem in *B* is also a theorem. We shall now prove some theorems.

Theorem 5.8: $\forall \ a \in B, a + a = 0$

Proof: $a + a = (a + a) \cdot 1$ (axiom 6 (ii))

$= (a + a) \cdot (a + a')$ (axiom 7(i))

$= a + a \cdot a^1$ (axiom 5(i))

$= a + 0$ (axiom 7(ii))

$= a$ (axiom 6(i))

Theorem 5.9: $\forall\ a \in B,\ a \cdot a = a$

Proof: $a \cdot a = a \cdot a + 0$ (axiom 6 (i))

$= a \cdot a + a \cdot a'$ (axiom 7(ii))

$= a \cdot (a + a')$ (axiom 5(ii))

$= a \cdot 1$ (axiom 7(i))

$= a$

Theorem 5.10: The elements 0 and 1 in *B* are unique.

Proof: Assume that 0_1 and 0_2 are two zero elements in *B*. Such that $a_1 + 0_1 = a_1$ and $a_2 + 0_2 = a_2$ $\forall\ a_1 \in B$ and $a_2 \in B$

Consider $a_1 + 0_1 = a_1$

taking $a_1 = 0_2$, we get

$0_2 + 0_1 = 0_2$

Similarly by taking $a_2 = 0_1$ in $a_2 + 0_2 = a_2$, we get $0_1 + 0_2 = 0_1$

Hence $0_2 + 0_1 = 0_1 + 0_2 \Rightarrow 0_1 = 0_2$

by the principle of duality we can easily show that the unit element 1 in unique in *B*.

Theorem 5.11: In each Boolean algebra

(*i*) $0' = 1$

(*ii*) $1' = 0$

Proof: (*i*) we have $0' = 0 + 0' = 1$

and (*ii*) $1' = 1 \cdot 1 = 0$

Theorem 5.12: For any $a \in B$, (*i*) $a + 1 = 1$ (*ii*) $a \cdot 0 = 0$

Proof: (*i*) $a + 1 = (a + 1) \cdot 1$

$= (a + 1) \cdot (a + a')$

$= a + 1 \cdot a'$

$= a + a'$

$= 0$

(*ii*) applying principle of duality, we get

$$a \cdot 0 = 0$$

Theorem 5.13: For any $a, b \in B$

(i) $a + a \cdot b = a$ (ii) $a \cdot (a + b) = a$ (absorption laws)

Proof: (i) We have

$$\begin{aligned} & a + a \cdot b \\ &= a \cdot 1 + a \cdot b \\ &= a \cdot (1 + b) \\ &= a \cdot 1 \\ &= a \end{aligned}$$

(ii) We have

$$\begin{aligned} a \cdot (a + b) &= (a + 0)\,(a + b) \\ &= a + 0 \cdot b \\ &= a + 0 \\ &= a \end{aligned}$$

Theorem 5.14: For each $a \in B$, there exists a unique complement.

Proof: Let a_1' and a_2' be two complements of a in B

then $$a + a_1' = 1, a + a_2' = 1$$

and $$a \cdot a_1' = 0, a \cdot a_2' = 0$$

now $$\begin{aligned} a_1' &= 1 \cdot a_1' \\ &= (a + a_2') \cdot a_1' \\ &= a \cdot a_1' + a_2' \cdot a_1' \\ &= 0 + a_2' \cdot a_1' \\ &= a\, a_2' + a_1' \cdot a_2' \\ &= (a + a_1') \cdot a_2' \\ &= 1 \cdot a_2' \\ &= a_2' \end{aligned}$$

Hence the complement a^1 for each $a \in B$ is unique.

Theorem 5.15: For each $a \in B$, $(a')' = a$ (Involution law)

Proof: By definition of complement

$$a + a' = 1 \text{ and } a' \cdot a = 0$$

now $$a + a' = a \Rightarrow a' + 1 \Rightarrow a' + a$$

and $$a \cdot a' = 0 \Rightarrow a' \cdot a = 0$$

by uniqueness a is the complement of a^1

hence $$(a')' = a \ \forall \ a \in B$$

Theorem 5.16: In a Boolean algebra B,

$$a + (b + c) = (a + b) + c$$

and $a \cdot (b \cdot c) = (a \cdot b) \cdot c \ \ \forall \ a \in B$, (Associative laws)

Proof: Left as an exercise

Theorem 5.17: For any $a; b \in B$

$$(a + b)' = a' \cdot b'$$

and $(a \cdot b) = a' + b'$ (De Morgan's laws)

Proof: (*i*) The theorem is proved if we show that

$$(a + b) = (a' \cdot b') = 1 \text{ and } (a + b), (a' \cdot b') = 0$$

Consider $(a + b)\ (a' \cdot b') = b + a + (a' \cdot b')$

$$= b + (a + a') \cdot (a + b')$$

$$= b + 1 \cdot (a + b')$$

$$= b + a + b'$$

$$= b + b' + a$$

$$= 1 + a$$

$$= 1$$

also

$$(a + b) \cdot (a' \cdot b')$$

$$= ((a + b) \cdot a') \cdot b'$$

$$= ((a \cdot a') + (b \cdot a')) \cdot b'$$

$$= (0 + (b \cdot a')) \cdot b'$$

$$= (b \cdot a') \cdot b'$$

$$= (b \cdot b') \cdot a'$$

$$= 0 \cdot a'$$

$$= 0$$

Hence $(a + b') = a' \cdot b'$

(*ii*) Follows from 5.15 (*i*) by the principle of duality.

5.22 SUB-BOOLEAN ALGEBRA

Definition 5.30: Let $(B, +, \cdot, ', 0, 1)$ be a Boolean algebra and $S \leq B$. If S contains the elements 0 and 1 and is closed under the operations +, and ·, then $(S, +, \cdot, ', 0, 1)$ is called a sub-Boolean algebra)

For any Boolean algebra, the set {0, 1} and *B* are both sub-Boolean algebra of *B*.

Example: Consider the Boolean algebra *B* shown in Fig. 5.19.

The subset $S_1 = \{a, a', 0, 1\}$ is a sub-Boolean algebra of *B*. The subset $S_2 = \{a \cdot b', b', 0, 1\}$ is not a sub-Boolean algebra.

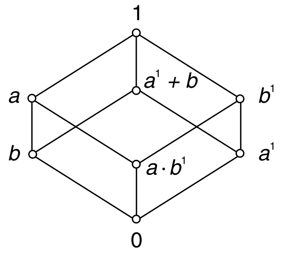


Fig. 5.19

5.23 DIRECT PRODUCTS

Definition 5.31: Let $(B_1, +_1, \cdot, ', 0_1, 1_1)$ and $(B_2, +_2, \cdot, '', 0_2, 1_2)$ be Boolean algebra. The direct product of the Boolean algebras denoted by $(B_1 \times B_2, +_3, \cdot_3, ''', 0_3, 1_3)$ is a Boolean algebra in which the operation are defined as follows:

$$(a_1, b_1) +_3 (a_2, b_2) = (a_1 +_1 a_2, b_1 +_2 b_2)$$

$$(a_1, b_1) \cdot_3 (a_2, b_2) = (a_1 \cdot_1 a_2, b_1 \cdot_2 b_2)$$

$$(a_1, b_1)''' = (a_1', b_1'') \; \forall \; (a_1, b_1), \text{ and } (a_2, a_2) \in B$$

also $\quad 0_3 = (0_1, 0_2)$ and $1_3 = (1_1, 1_2)$

using the definition given above we can generate new Boolean algebras. If B is a Boolean algebra we can generate the Boolean algebras $B \times B = B^2$, $B \times B \times B = B^3$, $B \times B \times B \times B = B^4$, ...

5.24 HOMOMORPHISM

Definition 5.32: Let $(B, +, \cdot, ', 0, 1)$ and $(B_1, +_1, \cdot_1, ^-, 0_1, 1_1)$ be two Boolean algebras. A function $f : B \to B,$ is called a Boolean algebra homomorphism, if f preserve the two binary operation and the unary operation i.e., for all $a, b \in B$

$$f(a + b) = f(a) +_1 f(b)$$

$$f(a \cdot b) = f(a) \cdot, f(b)$$

$$f(a') = f(\overline{a})$$

$$f(0) = 0_1$$

and $\quad f(1) = 1_1$

5.25 ATOMS OF BOOLEAN ALGEBRA

Let $(L, +, \cdot)$ be a lattice. An element $a \in L$ is called join-irreducible if it cannot expressed as the join of two distinct elements of L.

i.e., $a \in L$ is join irreducible, if for any $a_1, a_2, \in L$

$$a = a_1 + a_2 \Rightarrow (a = a_1) \text{ or } (a = a_2)$$

In the case of a Boolean algebra, the elements which cover the least element 0, are the only elements which are join irreducible. They are called atoms of the Boolean algebra. An element $a \in B$ is called an atom if $a \neq 0$, and either $a \cdot b = 0$ or $a \cdot b = 1 \;\; \forall \;\; b \in B$. The atoms a Boolean algebra are also called minterms. We can also represent the elements of a Boolean algebra in terms of the meet of their anti-atoms. The anti-atoms in Boolean algebra are those elements of the Boolean algebra which are covered by the greatest element 1. Anti-atoms are also called Maxterms. They are the complements of the atoms.

5.26 BOOLEAN EXPRESSIONS AND MINIMIZATION OF BOOLEAN FUNCTIONS

Boolean expressions are formed by application of the basic operations +, ·, and ^{1}, to one or more constants of variables. The simplest expression consists of a single constant or a variable such as 0 or *a*.

Definition 5.33: A Boolean expression or form, in *n* variables $x_1, x_2, ..., x_n$ is any finite string of symbols formed as given below:

1. 0 and 1 are Boolean expression.
2. $x_1, x_2, ..., x_n$ are Boolean expressions.
3. If α and β are Boolean expression, then $(\alpha) \cdot (\beta)$ and $(\alpha) + (\beta)$ are also Boolean expressions.
4. If α is a Boolean expression then $(\alpha)^1$ is also a Boolean expression.
5. No strings symbols except those formed in accordance with the above rules are Boolean expressions.

If α is a Boolean expression in *n* variables, say $x_1, x_2, ..., x_n$ then α can be written as $\alpha \;(x_1, x_2, ..., x_n)$. A Boolean expression in *n* variables may or may not contain all the *n* variables.

Some examples of Boolean expressions are

$$x_1 \, x_2', \; x_1(x_2 + x_3)', \; x_1 + x_1' \, x_2 + x_3 \, x_1'$$

Parentheses are added to specify the order in which the operations are performed and some of them can be dropped whenever possible.

0, 1, x_1, x_2, ... x_3 are Boolean expressions. If α and β are two Boolean expression, then $(\alpha), \alpha^1, \alpha + \beta$ and $\alpha \ldots \beta$ are also Boolean expression.

If $\alpha = (x_1, x_2, \ldots x_n)$ is a Boolean expression then we can assign values $a_1, a_2, \ldots a_n$ respectively to the variables where each a_i is either 0 or 1.

For example

Consider the Boolean expression

$$\alpha = (x_1, x_2, \ldots x_n) = [(x_1 \cdot x_2) + x_3]'$$

If $\quad x_1 = 1, x_2 = 0, \text{ and } x_3 = 0$, then

$$\alpha \;(x_1, x_2, x_3) = \alpha \;(1, 0, 0)$$

$$= [(1.0) + 0]$$

$$= (0 + 0)'$$
$$= 0'$$
$$= 1$$

Definition 5.34: Two Boolean expression α $(x_1, x_2, ..., x_n)$ and β $(x_1, x_2, ..., x_n)$ are said to be equal (or equivalent) if one can be obtained from the other by a finite number of application of the identities of Boolean algebra.

Definition 5.35: A literal is defined to be a Boolean variable or its complement.

Example 1: x, and x' are literals.

Definition 5.36: A literal or a product of two or more literals in which no two literals involve the same variable is called a fundamental product.

Example 2: $x_1\ x_2'\ x_3$, $x_1\ x_2\ x_3$, xy' are fundamental products.

Definition 5.37: A Boolean expression generated by $x_1, x_2, ..., x_n$ over B, which has the form of conjunction (product) of n literals is called a minterm.

The number of minterm generated by n variables in B_2 is 2^n.

The two variables x_1 and x_2 generate, the minterms x_1, x_2, $x_1' x_2$, $x_1 x_2'$, and $x_1' x_2$ in B_2. A minterm form of a Boolean expression is also called sum-of-products form or complete product of n variables.

We shall denote a particular *min* term by min_j or m_j where j is the decimal representation of $a_1\ a_2 \ldots a_n$ and each a_i is either 0 or 1 for $i = 1, 2, ..., n$. The minterms satisfies the following properties.

$$m_i \cdot m_j = 0 \text{ for } i \neq j$$

and
$$\underset{i=0}{\overset{2^n-1}{+}} m_i = 1$$

For $i \neq j$ the minterm m_i and m_j are not equal every Boolean expression except 0, can be expressed in an equivalent form consisting of the sums of minterms. When an expression is written as a sum of minterms, the equivalent form obtained is called a sum of products canonical form or a minterm expansion. In a minterm expansion any particular minterm may or may not be present. The number of different sum of products canonical forms is 2^{2^n}. These include minterms expansion of 0, in which no minterm is present in the sum, and also the minterm expansion of 1, where all the minterms are present in the sum. Therefore, the set of Boolean expression can be partitioned into 2^{2^n} equivalence classes. The set of Boolean expression under the operation +, $\cdot$ and ^{1}, form a Boolean algebra called a free Boolean algebra.

A Boolean expression can also be written as a product of sums of Maxterm, the equivalent expression obtained is called a product sums canonical form or maxterm expansion. Each maxterm is the complement of the corresponding minterm. In general, a maxterm of n variables is a sum of n literals in which each variable appears exactly once in either true or complement form, but not both. The maxterm expansion for an expression is unique.

The minterm expansion i.e., sum of products canonical form is called the disjunctive normal form and the maxterm expansion or products of sums canonical form is called the conjunction normal form.

Definition 5.38: Let $(B, +, \cdot, ', 0, 1)$ be a Boolean algebra. A function $f : B_n \to B$ which is associated with a Boolean expression in n variables is called a Boolean function.

Every function from B^n to B, may n of be Boolean, and there are functions from B^n to B which are not Boolean. Different expressions may determine the same Boolean functions. Absorption laws, De Morgan's laws, distributive laws and the other identities for Boolean algebras bring out the redundancy of Boolean expression. To transform Boolean expression E into a sums-of-products form; we first use De Morgan's laws and involution law, to convert E into a form which contains only sum and products of literals. We next use distributive law to transform E into a sums-of-products form. The next step is to transform each product in E into 0 or a fundamental product. This done by using the commutative, idempotent and complement laws. Finally, we use absorption law to get the sums-of-product form of E. To obtain complete sum-of-product form of E. We involve all the variables in each product of the sum-of-product form of E.

Example 3: Transform $((x_1 x_2)' x_3)' ((x_1' + x_3)(x_2' + x_3'))'$ into a sums-of-products form.

Solution: $((x_1 x_2)' x_3)' ((x_1' + x_3)(x_2' + x_3'))'$

$$= [((x_1 x_2)')' + x_3'] [(x_1' + x_3)' + (x_2' + x_3')']$$

$$= [x_1 x_2 + x_3'] [((x_1 x_3')')' + ((x_2 x_3)')']$$

$$= [x_1 x_2 + x_3'] [x_1 x_3' + x_2 x_3]$$

$$= x_1 x_2 x_1 x_3' + x_1 x_2 x_2 x_3 + x_3' x_1 x_3' + x_3' x_2 x_3$$

$$= x_1 x_2 x_3' + x_1 x_2 x_3 + x_1 x_3' + 0$$

$$= x_1 x_3' + x_1 x_2 x_3 + x_1 x_2 x_3'$$

Example 4: Express (*i*) $x_1 \cdot x_2$ (*ii*) $x_1(x_2' x_3)'$

In an equivalent sum-of-products canonical form in three variables x_1, x_2 and x_3.

Solution: (*i*) $x_1 \cdot x_2 = x_1 \cdot x_2 \cdot (x_3 + x_3')$

$$= x_1 \cdot x_2 \cdot x_3 + x_1 \cdot x_2 \cdot x_3' = m_7 + m_6$$

$$= m_6 + m_7$$

$$\therefore \quad x_1 \cdot x_2 = m_6 + m_7$$

(*ii*) $x_1(x_2' x_3)'$

$$= x_1[(x_2')' + x_3']$$

$$= x_1[x_2 + x_3']$$

$$= x_1 x_2 + x_1 x_3'$$

$$= x_1 x_2(x_3 + x_3') + x_1(x_2 + x_2')x_3'$$

$$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 \; x_2 \; x_3' + x_1 x_2' x_3'$$

$$= x_1 x_2 x_3 + x_1 x_2 x_3' + x_1 x_2' x_3'$$

$$= m_7 + m_6 + m_4$$

$$= m_4 + m_6 + m_7$$

$$= +4, 6, 7 = \sum m \; (4, 6, 7)$$

Example 5: Write $f(x_1, x_2, x_3) = x_1' x_2 x_3 + x_1 x_2' x_3 + x_1 x_2 x_3' + x_1 x_2 x_3 + x_1 x_2' x_3'$ in term of m-notation.

Solution: $f = x_1' x_2 x_3 + x_1 x_2' x_3 + x_1 x_2 x_3' + x_1 x_2 x_3 + x_1 x_2' x_3'$

$$= min_3 + min_5 + min_6 + min_7 + min_4$$
$$= min_3 + min_4 + min_5 + min_6 + min_7$$
$$= m_3 + m_4 + m_5 + m_6 + m_7$$
$$= \sum m \; (3, 4, 5, 6, 7)$$

Example 6: $f = x_1'(x_2' + x_4) + x_1 x_3 x_4'$

Solution: $f = x_1'(x_2' + x_4) + x_1 x_3 x_4'$

$$= x_1' x_2' + x_1' x_1' x_4 + x_1 x_3 x_4'$$

$$= x_1' x_2'(x_3 + x_3')\;(x_4 + x_4') + x_1(x_2 + x_2')\;(x_3 + x_3')x_4 + x_1(x_2 + x_2')x_3 x_4'$$

$$= x_1' x_2' x_3 x_4 + x_1' x_2' x_3' x_4 + x_1' x_2' x_3 x_4' + x_1' x_2' x_3' x_4' + x_1 x_2 x_3 x_4 +$$

$$x_1 x_2 x_3' x_4 + x_1 x_2' x_3 x_4 + x_1 x_2' x_3' x_4 + x_1 x_2 x_3 x_4' + x_1 x_2' x_3 x_4'$$

$$= m_0 + m_1 + m_3 + m_5 + m_7 + m_{10} + m_{14}$$

$$= \sum m \; (0, 1, 3, 5, 7, 10, 14)$$

Example 7: Write $Z = (x_1 + x_2 + x_3)\;(x_1 + x_2 + x_3')\;(x_1 + x_2' + x_3)$ in M-notation.

Solution: $Z = (x_1 + x_2 + x_3)\;(x_1 + x_2 + x_3')\;(x_1 + x_2' + x_3)$

$$= \text{Max}_0 \; \text{Max}_1 \; \text{Max}_3$$

$$= \prod M \;\; (0, 1, 2)$$

Example 8: $f = \sum m \; (0, 1, 2, 5)$ is a three input function. Transform f into its canonical sum-of-products form.

Solution: Let x_1, x_2 and x_3 denote the three inputs then

$$m_0 = 000 = x_1' x_2' x_3'$$

$$m_1 = 000 = x_1' x_2' x_3$$

$$m_2 = 010 = x_1' \, x_2 \, x_3'$$

$$m_3 = 101 = x_1 \, x_2' \, x_3$$

$\therefore$ Canonical sum-of-products form of the expression is

$$f = x_1' \, x_2' \, x_3' + x_1' \, x_2' \, x_3 + x_1' \, x_2 \, x_3' + x_1 \, x_2' \, x_3'$$

Example 9: Covert $f(x_1 \, x_2 \, x_3) = \prod (0, 2, 4, 5)$ into its canonical products-of-sums form.

Solution: $f(x_1 \, x_2 \, x_3) = \prod (0, 2, 4, 5)$

$$= M_0 \; M_1 \; M_2 \; M_5$$

we have
$$M_0 = 000 = x_1 \, x_2 \, x_3$$
$$M_1 = 000 = x_1 \, x_2' \, x_3$$
$$M_2 = 010 = x_1' \, x_2 \, x_3$$
$$M_3 = 101 = x_1' \, x_2 \, x_3'$$

$\therefore$ The required canonical product-of-sums form is

$$f = (x_1 \, x_2 \, x_3) \; (x_1 \, x_2' \, x_3) \; (x_1' \; x_2 \; x_3) \; (x_1' \, x_2 \, x_3')$$

Example 10: Obtain the three variable product-of-sums canonical form of the Boolean expression $x_1 \cdot x_2$.

Solution: Let x_3 denote the variable then

$$\begin{aligned} x_1 \cdot x_2 &= [x_1 + (x_2 \cdot x_2')] \, [x_2 + (x_1 \cdot x_1')] \\ &= (x_1 + x_2) \cdot (x_1 + x_2') \cdot (x_1 + x_2) \cdot (x_1' + x_2) \\ &= (x_1 + x_2) \cdot (x_1 + x_2') \, (x_1' + x_2) \\ &= [(x_1 + x_2) \cdot (x_3 + x_2')] \, [(x_1 + x_2') \cdot (x_3 \, x_3')] \, [(x_1' + x_2) \cdot (x_3 \, x_3')] \\ &= (x_1 + x_2 + x_3) \cdot (x_1 + x_2 + x_3') \cdot (x_1 + x_2' + x_3) \\ &\qquad (x_1 + x_2' + x_3') \, (x_1' + x_2 + x_3) \, (x_1' + x_2 + x_3') \\ &= \text{Max}_0 \cdot \text{Max}_1 \cdot \text{Max}_2 \cdot \text{Max}_3 \cdot \text{Max}_4 \cdot \text{Max}_5 \\ &= M_0 \cdot M_1 \cdot M_2 \cdot M_3 \cdot M_4 \cdot M_5 \\ &= \prod M \; (0, 1, 2, 3, 4, 5) \end{aligned}$$

Let $(B, +, \cdot, \,', 0, 1)$ be any Boolean algebra and $(a_1, a_2, \ldots, a_n) \in B^n$ where $a_i \in B$. If $\alpha \; (x_1, x_2, \ldots x_n)$ is a Boolean expression, we can find the value of $\alpha \; (x_1, x_2, \ldots x_n)$ for $(a_1, a_2, \ldots a_n)$ by replacing x_1 by a_1, x_2 by a_2, ..., x_n by a_n.

Example 11: Find the value of $x_1 + (x_1 \, x_2)$ over the ordered pairs of the two-element Boolean algebra.

Solution: Let $B = \{0, 1)$ then the (0, 0), (0, 1), (1, 0) and (1, 1) are the elements of $B^2 = B \times B$.

The values of $x_1 + (x_1 \cdot x_2)$ are listed in Table 5.1 given below.

Table 5.1

$(x_1 \cdot x_2)$	$x_1 + (x_1 \cdot x_2)$
(0, 0)	0
(0, 1)	0
(1, 0)	1
(1, 1)	1

Definition 5.39: Let P_1 and P_2 be fundamental products such that exactly one variable say x_i appears in complemented form in one of the products P_1 and P_2 and uncomplemented in the other. The consensus of P_1 and P_2 is the product of the literals P and the literals of P_2 after deleting x_i and x_i^1.

Example 12: (*i*) The consensus of $A\ B$ and $A'C$ is BC.

(*ii*) The consensus of $A\ B'C$ and $A'B'C'$ is 0.

(*iii*) The consensus of $x_1\, x_2\, x_3'\, x_4$ and $x_1\, x_2'\, x_5$ is $x_1\, x_3'\, x_4\, x_5$.

Consensus method is very useful in simplifying Boolean expressions. It is used to eliminate redundant terms in a Boolean expression. The redundant terms which are eliminated are called consensus terms.

Example 13: In the expression in $E = x_1\, x_2 + x_1'\, x_3 + x_2\, x_3$ the terms $x_2\, x_3$ is redundant. It is referred to as the consensus term. Eliminating $x_2\, x_3$ be can write $E = x_1\, x_2 + x_1'\, x_3$ as the simplified expression for E.

Definition 5.40: Let E be a Boolean expression. A fundamental product P is called a prime implicant of E if $P + E = E$ but no other fundamental product included in P has this property.

Example 14: $x_1\, x_3'$ is a prime implicant of the Boolean expression

$$E = x_1\, x_2' + x_1\ x_2\, x_3' + x_1'\, x_2\, x_3'.$$

5.27 MINIMIZATION OF BOOLEAN EXPRESSIONS

Boolean expressions are practically implemented in the form of gates. The cost of a circuit depends upon the number of gates in the circuit. Hence we reduce the member of gates in the circuit to a minimum so that the cost of the circuit is decreased to a miximum extent.

In this section, we explain to methods for simplification of Boolean expressions, namely (*i*) Algebraic method and (*ii*) Karnaugh map method.

5.27.1 Algebra Method

In this method, we make use of Boolean positates rules and theorem to simplify given Boolean expressions.

Example 1: Simplify

$$F = \overline{A}\ \overline{B}\ \overline{C} + \overline{A}\ B\ \overline{C} + A\ \overline{B}\ \overline{C} + A\ B\ \overline{C}$$

Solution:

$$\begin{aligned}
F &= \overline{A}\,\overline{B}\,\overline{C} + \overline{A}\,B\,\overline{C} + A\,\overline{B}\,\overline{C} + A\,B\,\overline{C}\\
&= (\overline{A}\,\overline{B} + \overline{A}\,B + A\,\overline{B} + A\,B)\,\overline{C}\\
&= (\overline{A}(\overline{B} + B) + A(\overline{B} + B))\,\overline{C}\\
&= (\overline{A}\cdot(1) + A\,(1))\cdot\overline{C}\\
&= (\overline{A} + A)\,\overline{C}\\
&= 1\cdot\overline{C}\\
&= \overline{C}
\end{aligned}$$

Example 2: Simplify $z\,(y + z)\,(x + y + z)$

Solution:

$$\begin{aligned}
&z\,(y + z)\,(x + y + z)\\
&= (z\,y + z\,z)\,(x + y + z)\\
&= (z\,y + z)\,(x + y + z)\\
&= z\,(y + 1)\,(x + y + z)\\
&= z\,(x + y + z)\\
&= z\,x + z\,y + z\,z\\
&= z\,x + z\,y + z\\
&= z\,(x + y + 1)\\
&= z\,(x + 1)\\
&= z
\end{aligned}$$

Example 3: Simplify $Y = (P + Q)\,(P + Q')\,(P' + Q)$

Solution:

$$\begin{aligned}
Y &= (P + Q)\,(P + Q')\,(P' + Q)\\
&= (P\,P + P\,Q' + P\,Q + Q\,Q')\,(P' + Q)\\
&= (P + P\,Q' + P\,Q + 0)\,(P' + Q)\\
&= (P + P\,Q' + P\,Q)\,(P' + Q)\\
&= P\,P^1 + P\,Q + P\,Q'\,P' + P\,Q'\,Q + P\,Q\,P' + P\,Q\,Q\\
&= 0 + P\,Q + 0 + 0 + 0 + P\,Q\\
&= P\,Q + P\,Q\\
&= P\,Q
\end{aligned}$$

Example 4: Show that $Y = P\,Q\,R + P\,Q'\,R + P\,Q\,R'$ can be simplifies as $Y = P\,(Q + R)$

Solution:

$$\begin{aligned}
Y &= P\,Q\,R + P\,Q'\,R + P\,Q\,R'\\
&= P\,R\cdot(Q + Q') + P\,Q\,R'\\
&= P\,R\cdot 1 + P\,Q\,R'\\
&= P\,(R + Q\,R')\\
&= P\,(R + Q)\\
&= P\,(Q + R)
\end{aligned}$$

Example 5: Minimize the expression $\overline{A\,B} + \bar{A} + A\,B$

Solution:

$$\begin{aligned} &\overline{A\,B} + \bar{A} + A\,B \\ &= \bar{A} + \bar{B} + \bar{A} + A\,B \\ &= \bar{A} + \bar{A} + \bar{B} + A\,B \\ &= \bar{A} + \bar{B} + A\,B \\ &= \bar{A} + A\,B + \bar{B} \\ &= (\bar{A} + \bar{\bar{A}}\,B)\;\bar{B} \\ &= \bar{A} + B + \bar{B} \\ &= \bar{A} + 1 = 1 \end{aligned}$$

Hence $\overline{A\,B} + \bar{A} + A\,B = 1$

5.27.2 Karnaugh Maps

A Boolean expression generally denoted the structure of a logical circuit, while the Boolean function describes the behaviour of the circuit. Many different circuits or programs can be used to compute the same Boolean function: It is often desirable to select the one that is simplest. The algebraic techniques used to simplify Boolean functions are difficult to apply in a systematic way. The Karnaugh method (named after Maurice Karnaugh) is a systematic method for simplifying switching (Boolean) functions.

The Karnaugh map is a graphical representation of the truth table with a square representing each minterm. If f is a function of n variables, then the Karnaugh map will have 2^n squares. 1-variable Karnaugh map is shown in Fig. 5.20. Note that the map has $2^1 = 2$ cells.

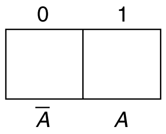
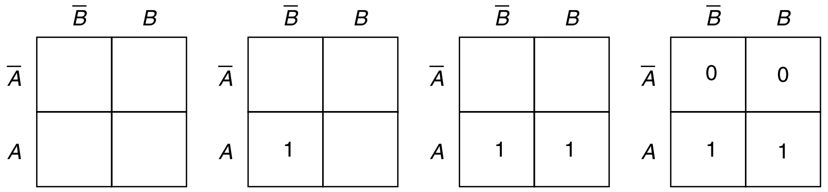


Fig. 5.20 Karnaugh map for 1-variable

Consider the Truth table shown in Table 5.2 for a function Z of two variables. To convert the table into its Karnaugh map, we begin by drawing 5.21 (a) (i.e., a blank map):

Table 5.2

A	B	Z
0	0	0
0	1	0
1	0	1
1	1	1



(*a*) (*b*) (*c*) (*d*)

Fig. 5.21

The first out put 1 appears for $A = 1$ and $B = 0$.

The input condition for this fundamental product is $A\overline{B}$. Enter this input condition in the Karnaugh map as shown in Fig. 5.21 (*b*). Table 5.2 has an output 1 appearing for $A = 1$ and $B = 1$. This fundamental product is $A\ B$. Enter this fundamental product (i.e., $A\ B$) as shown in Fig. 5.21 (*c*). Finally enter 0s in the remaining spaces (See Fig. 5.21 (*d*). A two variable Karnaugh map, can be represented as shown in Fig. 5.22:

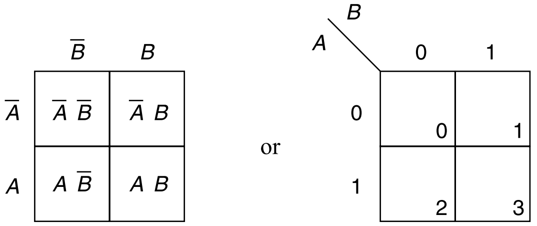

$\overline{B}$ B
$\overline{A}$ $\overline{A}\,\overline{B}$ $\overline{A}\,B$
A $A\,\overline{B}$ $A\,B$
or
B
A
0 1
0 0 1
1 2 3

Fig. 5.22 Two variable Karnaugh map representing minterms

If the top horizontal line represents $\overline{A}$ and A and the vertical line represents $\overline{B}$ and B, then the Karnaugh map, can be drawn as shown in Fig. 5.23:

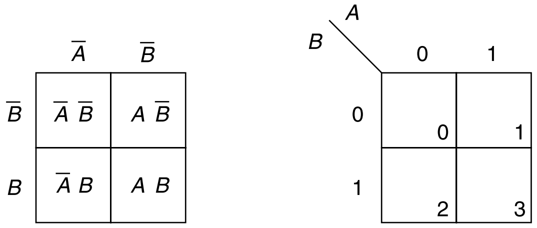

$\overline{A}$ $\overline{B}$
$\overline{B}$ $\overline{A}\,\overline{B}$ $A\,\overline{B}$
B $\overline{A}\,B$ $A\,B$
A
B
0 1
0 0 1
1 2 3

Fig. 5.23 2-Variable Karnaugh map

In the above Karnaugh map we observe that in every square a number is written. Each number is a minterm. If the number 0 is given to a square means it represents the minterm m_0. Similarly, a square (cell) with the number 1 represents the minterm m_1 a square with the number 2 represents m_2 and so on.

The binary number in the Karnaugh map differ by only one place, when moving from left to right. That is two adjust squares in Karnaugh map differ only by one variable.

The successive numbers are 00, 01, 11 and 10, where

00 represents $\overline{A}\,\overline{B}$

01 represents $\overline{A}B$

11 represents AB

and 10 represents $A\overline{B}$

In these products only one variable changes from complemented to uncomplemented form. The above code is called gray code. The Karnaugh map for the truth Table 5.3 is shown in Fig. 5.24.

Table 5.3

A	B	Z
0	0	1
0	1	1
1	0	0
1	1	0

	$\overline{B}$	B
$\overline{A}$	1	1
A	0	0

Fig. 5.24

Figure 5.25 shows a Karnaugh map for 3 variables.

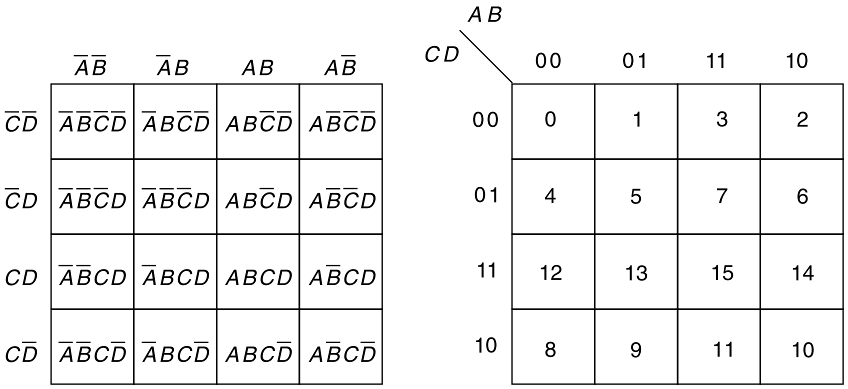
	$\overline{A}\,\overline{B}$	$\overline{A}B$	AB	$A\overline{B}$
$\overline{C}$	$\overline{A}\,\overline{B}\,\overline{C}$	$\overline{A}B\overline{C}$	$AB\overline{C}$	$A\overline{B}\,\overline{C}$
C	$\overline{A}\,\overline{B}C$	$\overline{A}BC$	ABC	$A\overline{B}C$

$C \backslash AB$	00	01	11	10
0	0	1	3	2
1	4	5	7	6

Fig. 5.25 Karnaugh map for 3 variables

Note that the numbering scheme here is 0, 1, 3, 2 then 4, 5, 7, 6.

Figure 5.26 shows a four variables Karnaugh map.



	$\overline{A}\overline{B}$	$\overline{A}B$	AB	$A\overline{B}$
$\overline{C}\overline{D}$	$\overline{A}\overline{B}\overline{C}\overline{D}$	$\overline{A}B\overline{C}\overline{D}$	$AB\overline{C}\overline{D}$	$A\overline{B}\overline{C}\overline{D}$
$\overline{C}D$	$\overline{A}\overline{B}\overline{C}D$	$\overline{A}\overline{B}\overline{C}D$	$AB\overline{C}D$	$A\overline{B}\overline{C}D$
CD	$\overline{A}\overline{B}CD$	$\overline{A}BCD$	$ABCD$	$A\overline{B}CD$
$C\overline{D}$	$\overline{A}\overline{B}C\overline{D}$	$\overline{A}BC\overline{D}$	$ABC\overline{D}$	$A\overline{B}C\overline{D}$

CD \ AB	00	01	11	10
00	0	1	3	2
01	4	5	7	6
11	12	13	15	14
10	8	9	11	10

Fig. 5.26 Karnaugh map for four variables

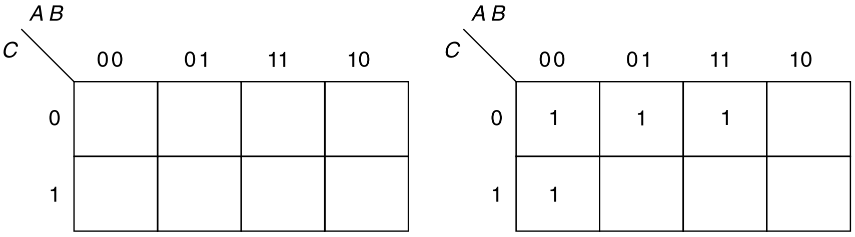
Example 1: Draw a Karnaugh map for Table 5.4:

Table 5.4

A	*B*	*C*	*Z*
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Solution: We first draw the blank map of Fig. 5.27 (*a*) output 1 appears *A B C* inputs of 000, 001, 010 and 110. The fundamental products for these conditions are $\overline{A}\,\overline{B}\,\overline{C}$, $\overline{A}\,\overline{B}\,C$, $\overline{A}\,B\,C$ and $A\,B\,\overline{C}$. Enter *Is* for these products on the Karnaugh map (Fig. 5.27 (*b*)).

Finally enter 0*S* in the remaining spaces as shown in Fig. 5.27 (*c*).

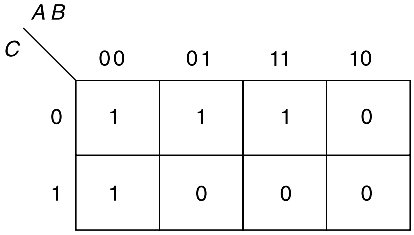


C \ AB	00	01	11	10
0				
1				

(*a*)

C \ AB	00	01	11	10
0	1	1	1	
1	1			

(*b*)



$C \backslash AB$	00	01	11	10
0	1	1	1	0
1	1	0	0	0

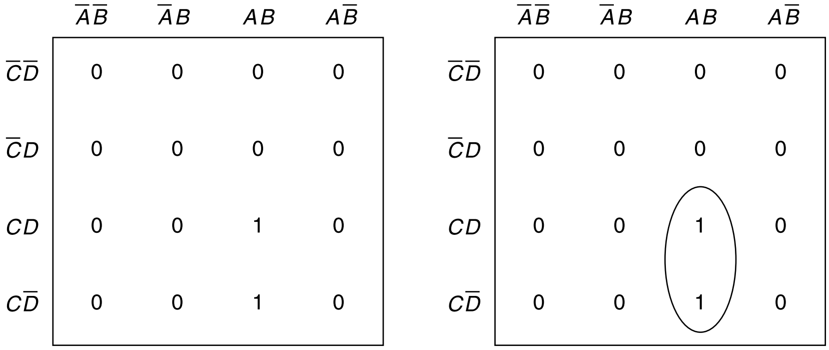
(*c*)

Fig. 5.27

Figure 5.27 (*c*) represents the Karnaugh map for Table 5.4.

Pair in a Karnaugh Map

Consider the Karnaugh map shown in Fig. 5.28. The map contains a pair is which are adjust to each other. The map represents the sum-of-products equation $Z = A\ B\ C\ D + A\ B\ C\ \overline{D}$. Where the first minterm represents the product $A\ B\ C\ D$ and the second minterm stands for the product $A\ B\ C\ \overline{D}$. The variable D in the uncomplemented form goes to the complemented form and the variables A, B and C remain uncomplemented. The variable D can be eliminated.



	$\overline{A}\overline{B}$	$\overline{A}B$	AB	$A\overline{B}$
$\overline{C}\overline{D}$	0	0	0	0
$\overline{C}D$	0	0	0	0
CD	0	0	1	0
$C\overline{D}$	0	0	1	0

	$\overline{A}\overline{B}$	$\overline{A}B$	AB	$A\overline{B}$
$\overline{C}\overline{D}$	0	0	0	0
$\overline{C}D$	0	0	0	0
CD	0	0	1	0
$C\overline{D}$	0	0	1	0

Fig. 5.28 Example of pair

In a pair, the variable which changes its state from complemented to uncomplemented (or vise versa) is removed. This rule is called pair reduction rule.

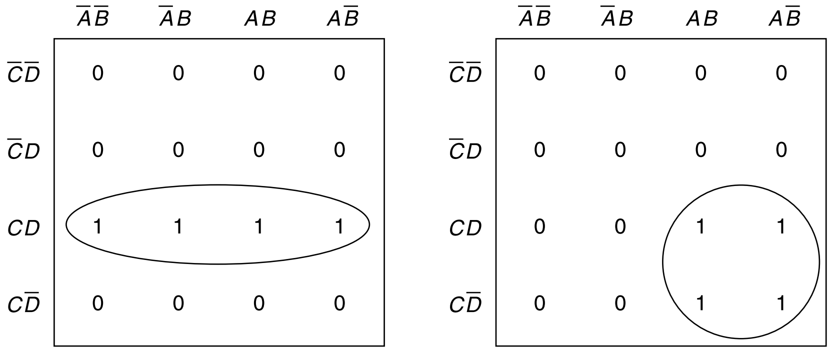
To draw a Karnaugh map for a truth table with don't care conditions; we first treat the don't conditions as 1s and encircle actual 1s in the largest groups. The remaining don't cares (which are not included in the groups) are regarded by visualizing them as 0*s*.

Thus, *A* pair in a Karnaugh map eliminates are variable and its complement.

In the above expression $Z = A\ B\ C\ D + A\ B\ C\ \overline{D}$ can be factored as $Z = A\ B\ C\ (D + \overline{D})$.

Quads

In a Karnaugh map, a quad is a group of four 1s that are horizontally or vertically adjacent. The 1s in a quad may be end-to-end or in the form of a square as shown in Fig. 5.29. A quad eliminates two variables and their complements. The rule is known as quad reduction rule. The quads in a Karnaugh map are always encircled as shown in Fig. 5.29.



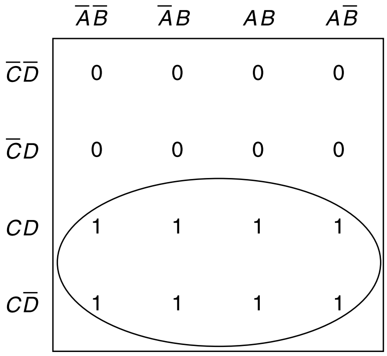
	$\bar{A}\bar{B}$	$\bar{A}B$	AB	$A\bar{B}$
$\bar{C}\bar{D}$	0	0	0	0
$\bar{C}D$	0	0	0	0
CD	1	1	1	1
$C\bar{D}$	0	0	0	0

	$\bar{A}\bar{B}$	$\bar{A}B$	AB	$A\bar{B}$
$\bar{C}\bar{D}$	0	0	0	0
$\bar{C}D$	0	0	0	0
CD	0	0	1	1
$C\bar{D}$	0	0	1	1

Fig. 5.29 Examples of quads

Octet

The octet in a Karnaugh map is a group of eight *Is*. An octet eliminates three variables and their complements.



	$\bar{A}\bar{B}$	$\bar{A}B$	AB	$A\bar{B}$
$\bar{C}\bar{D}$	0	0	0	0
$\bar{C}D$	0	0	0	0
CD	1	1	1	1
$C\bar{D}$	1	1	1	1

Fig. 5.30 Example of octet

Don't Care Conditions

In some problems certain input combinations may never occur in the circuit therefore the corresponding output never appears. But they appear in the truth table. In such case an *X* is entered in the truth table as functional value. *X* is called a don't-care condition. The logic designer can later assign a functional value 0 or 1 to the corresponding entries in the truth table (Table 5.5).

Table 5.5 *Don't care conditions*

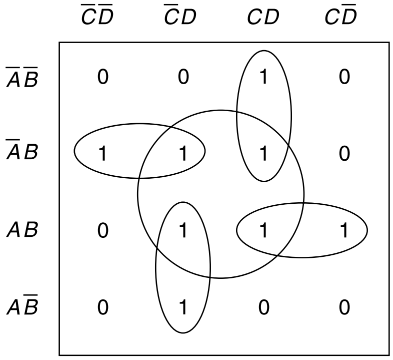
A	B	C	F
0	0	0	1
0	0	1	X
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	X
1	1	1	1

Rolling a Karnaugh Map

Pairs; quads and octets in a Karnaugh map are marked after rolling the map; in which we consider the map as if its left edge are touching the right edges and the top edges are touching the bottom edges.

Redundant Group

In a Karnaugh map, a group whose is are already used by others is called a redundant group (*See* Fig. 5.31). The removal of a redundant group leads to much simpler expression.



	$\overline{C}\overline{D}$	$\overline{C}D$	CD	$C\overline{D}$
$\overline{A}\overline{B}$	0	0	1	0
$\overline{A}B$	1	1	1	0
AB	0	1	1	1
$A\overline{B}$	0	1	0	0

Fig. 5.31 Karnaugh map with redundant group

In the Fig. 5.31 all the 1s of the quad are used by pairs of the map, therefore quad is redundant on Fig. 5.31 and it can be eliminated as shown in Fig. 5.32.

Summary of the rules for simplifying Boolean expression:

1. Construct the truth table for the given expression.
2. Begin with empty Karnaugh map and enter *a* 1 in the Karnaugh map for each fundamental product that produces *a* 1 output in the truth table. Enter 0s 1*s* elsewhere.
3. Encircle the octets, quads and pairs roll the Karnaugh map.
4. Eliminate redundant groups if any.

5. Write the simplified Boolean expression by ORing the products corresponding to the encircled groups.

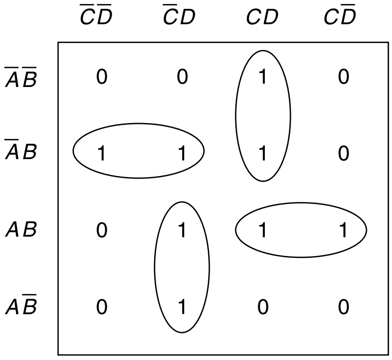


Fig. 5.32 Karnaugh map without redundant group

Example 2: Simplify the Boolean expression

$$Y = A\,B\,\overline{C} + A\,\overline{B}\,\overline{C} + A\,B\,C + A\,\overline{B}\,C$$

Solution: The truth table for Y is shown in Table 5.6:

Table 5.6

A	B	C	Y
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Figure 5.33 showns the Karnaugh map for Y.

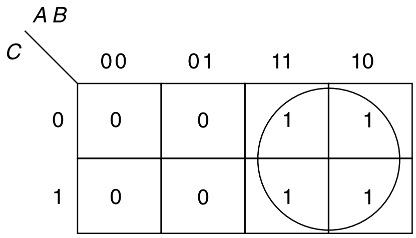


Fig. 5.33

There is quad in the map.

There are no redundant groups in the map A is the only variable which remained unchanged in the map.

$\therefore$ The simplified expression $Y = A$.

This can be proves as follows:

$$
\begin{aligned}
Y &= A\,B\,\overline{C} + A\,\overline{B}\,\overline{C} + A\,B\,C + A\,\overline{B}\,C \\
&= A(B\,\overline{C} + \overline{B}\,\overline{C} + B\,C + \overline{B}\,C) \\
&= A((B + \overline{B})\,\overline{C} + (B + \overline{B})\,C) \\
&= A(1 \cdot \overline{C} + 1 \cdot C) \\
&= A(\overline{C} + C) \\
&= A \cdot 1 \\
&= A
\end{aligned}
$$

Example 3: Obtain a simplified expression for a Boolean expression F (x. y. z) the Karnaugh map for which is given below:

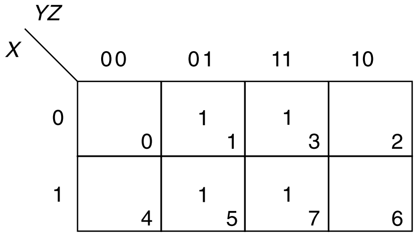


Fig. 5.34

Solution: Completing the given Karnaugh map by entering 0s in the empty square, we get the following Karnaugh map (See Fig. 5.35):

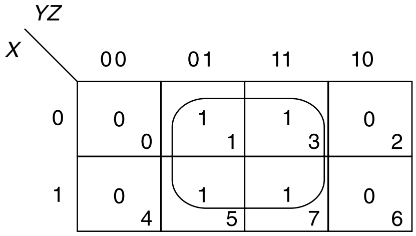


Fig. 5.35

There are no pairs, no octets. There is a quad in the map. The quad consists of the minterms m_1, m_3, m_5 and m_7. Moving horizontally from m_1 to m_3 i.e., $\overline{X}\;\overline{Y}\;Z$ to $\overline{X}\;Y\;Z$ we observe that Y changes from complemented form to uncomplemented for,... Therefore Y is eliminated. Moving vertically from m_1 to m_5 or m_3 to m_7, we find that the variable $\overline{X}$ changes to X. Hence we eliminate X.

$\therefore$ The simplified expression for $F(x, y, z)$ is

$$F(x, y, z) = Z$$

Example 4: Simplify $F(A, B, C, D) = \sum (0, 2, 7, 8, 10, 15)$ using Karnaugh map.

Solution: The minterms the function F are

$$m_0 = 0000 = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D}$$

$$m_2 = 0010 = \overline{A}\,\overline{B}\,C\,\overline{D}$$

$$m_7 = 0111 = \overline{A}\,B\,C\,D$$

$$m_8 = 1000 = A\,\overline{B}\,\overline{C}\,\overline{D}$$

$$m_{10} = A\,\overline{B}\,C\,\overline{D}$$

$$m_{15} = 1111 = A\,B\,C\,D$$

Karnaugh map of the given function is shown in Fig. 5.36:

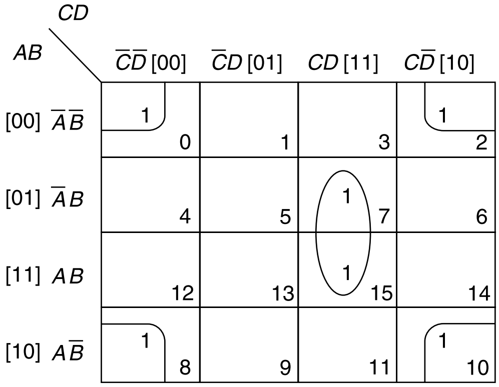


Fig. 5.36

The Karnaugh map has one pair, and one quad.

There are no over lappings.

Consider the pair $m_7 + m_{15}$.

A is the only variable which changes its form, have A is removed.

The reduced expression for the pair $m_7 + m_{15}$ is $B\ C\ D$ quad is $m_0 + m_3 + m_8 + m_{10}$ in the map moving horizontally we observe that the variable C changes its form and then moving vertically. We find that A changes its form. Therefore A and C are removed. The reduced expression for the quad $m_0 + m_3 + m_8 + m_{10}$ is $\overline{B}\,\overline{D}$.

Hence simplified expression for F is

$$B\,C\,D + \overline{B}\,\overline{D}$$

Example 5: Simplify

$$Y = \sum m\,(0, 1, 4, 5, 6, 8, 9, 12, 13, 14.)$$

Solution: The Karnaugh map can be constructed as shown in Fig. 5.37.

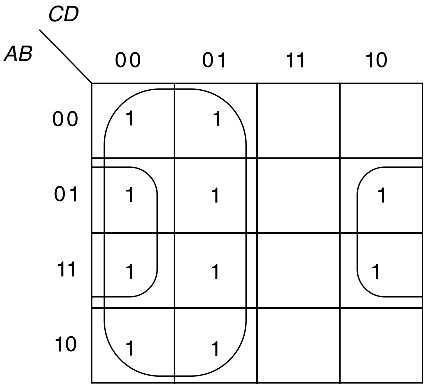


Fig. 5.37

There is one octet and a quad in the *K*-map. The quad is obtained by rolling vertically, such that the left and right edges are joined and over lappings. *A*, *B* and *D*, are the variables eliminated by the Octet in the map. Quad eliminated the variables *A* and *C*.

Octet gives $\overline{C}$ and quad gives $B\,\overline{D}$.

Hence, the reduced expression is $f = \overline{C} + B\,\overline{D}$.

Example 6: Simplify the Boolean function $f(A, B, C, D) = \sum m\,(1, 3, 7, 11, 15) + d\,(A, B, C, D)$ where the don't care conditions are given by $d\,(A, B, C, D) = \sum m\,(0, 2, 5)$.

Solution: The Karnaugh map for *f* can be constructed as shown in Fig. 5.38 (*b*).

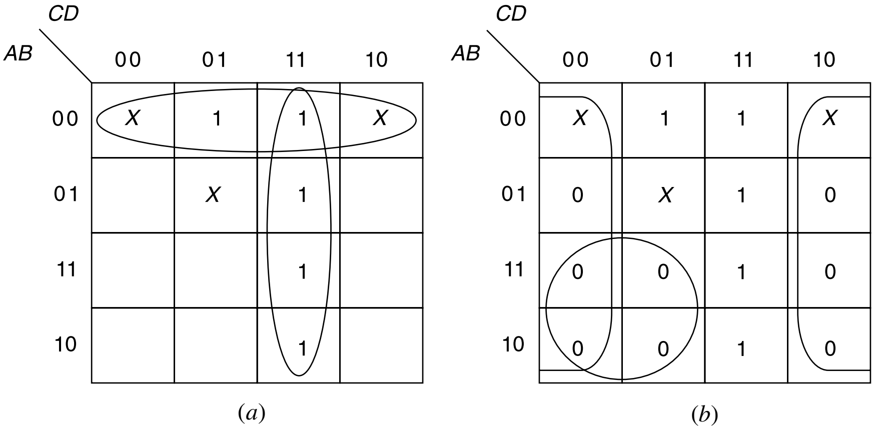


Fig. 5.38

The minterm for d may produce either 0 or 1 for f. The $I\ S$ and $X\ S$ are combined so as to endure maximum number of adjustment squares. The remaining cells are marked 0 as shown in Fig. 5.38 (b). There are two quads in Fig. 5.38 (a). The don't care condition in cell 5 is left free; as it does not contribute to any group in the map. The simplified expression in sum-of-products form is $f = \overline{A}\ \overline{B} + C\ D$. Combining $O\ S$ and $X\ S$ in Fig. 5.38 (b). We get the simplified products-of-sums equation as

$$f = \overline{(\overline{D} + A\ \overline{C})} = D(\overline{A} + C).$$

In this case, a variable can be taken for 0 and its complement is taken for 1.

EXERCISE 5.2

1. Define a Boolean algebra.

2. Define a sub algebra.

3. Define the dual of a statement S in a Boolean algebra.

4. Define an atom in a Boolean algebra B.

5. Define a Boolean expression and give examples.

6. Define a literal and a fundamental products and give examples.

7. What are idempotent laws for Boolean algebras?

8. What is involution law for Boolean algebras?

9. Write the dual of each statement:

(a) $(x + y)\,(x + 1) = x + x\,y + y$

(b) $\overline{(\overline{x} + \overline{y})} = x\,y$

(c) $x\,\overline{y} = 0$ if and only $x\,y = x$.

10. What is a minterm?

11. What is a maxterm?

12. Define a sum-of-products form.

13. Define a product-of-sums form.

14. Prove the following Boolean identities:

(i) $a + (\overline{a} \cdot b) = a + b$

(ii) $a \cdot (\overline{a} + b) = a \cdot b$

(iii) $(a \cdot b \cdot c) + (a \cdot b) = a \cdot b$

15. Simplify the following Boolean expressions:

(a) $(a \cdot b)' + (a \cdot b)'$

(b) $(a' \cdot b' \cdot c) + (a \cdot b' \cdot c) + (a \cdot b' \cdot c')$

16. Write the following Boolean expressions in equivalent sum-of-products form in three variables:

(a) $x_1\,x_2$ (b) $x_1 + x_2$

(*c*) $(x_1 \cdot x_2)' \cdot x_3$ (*d*) $x_1 + (x_2 \cdot x_3')$

(*e*) $(x_1 + x_2) + (x_1' \cdot x_3)$

17. Obtain the sum-of-products and product-of-sums of canonical forms of the following expressions:

(*a*) $x_1 \cdot x_2$ (*b*) $x_1\, x_2' + x_3$

18. Obtain simplified Boolean expressions which are equivalent to these expressions:

(*i*) $m_0 + m_1 + m_2 + m_3$

(*ii*) $m_0 + m_1 + m_2 + m_5 + m_6 + m_7$

(*iii*) $m_2 + m_3 + m_5 + m_6$

19. Express $F = x\,(y^1\ \ z)^1$ in complete sum-of-products form.

20. Write each of the following Boolean expressions in complete sum-of-products form:

(*i*) $E = x(x\,y' + x\,y' + y_2')$

(*ii*) $E = (x + y)'\,(x\,y')'$

(*iii*) $E = x_3\,(x_1' + x_2) + x_2'$

21. Simplify

(*i*) $X = \overline{A}\,\overline{B} + A\,\overline{B}$

(*ii*) $X = A\,B\,\overline{C} + A\,B\,C$

(*iii*) $X = \overline{A}\,\overline{B}\,\overline{C} + \overline{A}\,B\,\overline{C} + A\,B\,\overline{C} + A\,\overline{B}\,C$

(*iv*) $X = \overline{A}\,\overline{B}\,\overline{C}\,D + \overline{A}\,B\,\overline{C}\,D + A\,B\,\overline{C}\,D + A\,\overline{B}\,\overline{C}\,D$

(*v*) $X = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D} + A\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,\overline{B}\,\overline{C}\,D + A\,\overline{B}\,C\,\overline{D}$

(*vi*) $X = A\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,B\,\overline{C}\,D + \overline{A}\,B\,C\,D + A\,B\,\overline{C}\,D + A\,B\,C\,D$

22. Simplify the following Boolean function in product of sums form:

$$F\,(A, B, C, D) = \sum\ (0, 1, 2, 5, 8, 9, 10)$$

6

Logic Gates

6.1 INTRODUCTION

Boolean algebra can be applied to the solution of any electronic circuit involving two possible states. We begin our study by examining switching circuits. The most elementary circuit is shown in the figure given below (Fig. 6.1):

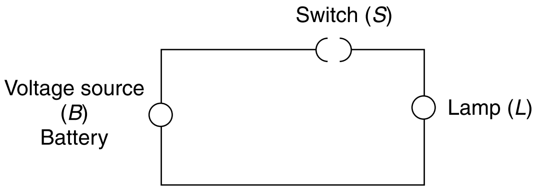
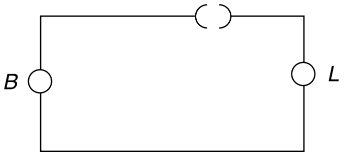


Fig. 6.1

The battery *B*, a single pole throw switch and an indicating lamp are connected in a simple switching circuit. The electronic circuit is a two-state device. It is for turning ‘on’ and ‘off’ an electronic light in the circuit. We can also construct a device which permit not only electric current but any quantity that can go through such as water, information etc. For general discussion we replace the word ‘switch’ by the word ‘gate’.

Consider the switching circuit displayed in Fig. 6.2 (*a*). When the switch *S* is open there is no current flowing in the circuit and the lamp *L* is off. This condition is indicated by the numeric value ‘0’. When the switch is closed the lamp *L* is on. This condition is indicated by the numerical value ‘1’. Therefore, the value 0 (or dark lamp) will show an open switch and the value 1 will show the closed switch in the circuit (the value 1 indicated a glowing lamp). The condition tables is the truth table which lists all the possible combinations of input binary variables is given in Fig. 6.2 (*b*):



(*a*) Simple switching circuit

S	*L*
0	0
1	1

(*b*) Condition table

Fig. 6.2

We can express the above condition table in different form as shown in Table 6.1:

Table 6.1

State of the switch	*State of the lamp*
Open	Off
Closed	On

Let P and Q denote the following statements:

P: The switch S is closed.

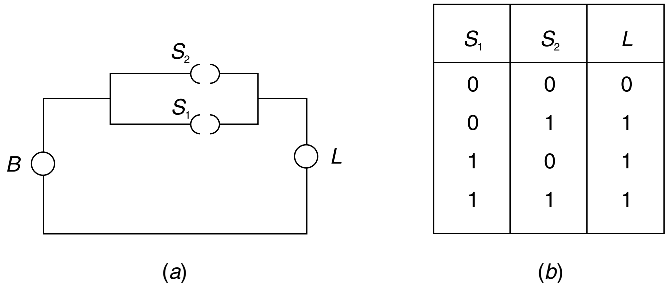
Q: The lamp L is on.

We can rewrite the condition table as follows:

Table 6.2

P(S)	*Q(L)*
0	0
1	1

Now consider the circuit shown in Fig. 6.3. The circuit has the switches S_1 and S_2 which are connected in parallel. When the switch S_1 is closed, the current flows exclusively through the upper branch, and the light (L) is on and when the switch S_2 is closed the current flows exclusively through the lower branch and the light is on. With both the switches closed the current divides equally between both branches still permitting the lamp to glow. If both the switches S_1 and S_2 are open the circuit becomes an open circuit and the light is off. This shows that an *OR* function can be obtained connected the switches in parallel. The light is or when either S_1 or S_2 is closed.



S_1	S_2	L
0	0	0
0	1	1
1	0	1
1	1	1

(*a*) (*b*)

Fig. 6.3

Let P: The switch S_1 is closed.

Q: The switch S_2 is closed.

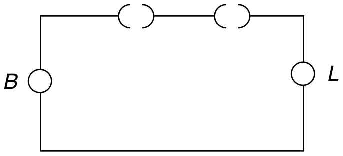
Y: The lamp L is on.

Then the truth Table 6.3 (*b*) can be written as:

Table 6.3

P	Q	Y
0	0	0
0	1	1
1	0	1
1	1	1

Fig. 6.4 (*a*) Contains the circuit in which two switches S_1 and S_2 are connected in 'series'. If both the switches S_1 and S_2 are closed then the circuit permits the flow of current in the circuit and the light is on. In all other combination the circuit is open and the light is off, showing that '*AND*' function is obtained (See Fig. 6.4):



(*a*)

S_1	S_2	L
0	0	0
0	1	0
1	0	0
1	1	1

(*b*)

Fig. 6.4

Let P: The switch S_1 is closed.

Q: The switch S_2 is closed.

Y: The light L is on.

The table of Fig. 6.4 (*b*) can be written as:

Table 6.4

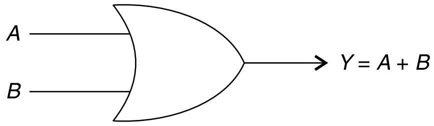
P	Q	Y
0	0	1
0	1	1
1	0	1
1	1	1

6.2 GATES AND BOOLEAN ALGEBRA

Boolean algebra is different from ordinary algebra. It is a system of mathematical logic. A switching network (governs) the flow of current through a circuit. Now we will discuss logic gates which are basically electronic circuits that can be used to actually implement the most elementary logical expressions, known as logic gates. There are three basic logic gates, the OR-gate, the AND-gate and the NOT-gate. Other logic gates that are derived from these three basic gates are NAND-gate, the NOR gate, the EX-OR gate and the EX-NOR gate.

6.2.1 OR-Gate

An OR-gate is a logic circuit with two or more than two inputs and outputs. The output of an OR-gate is '0' only when all of its inputs are at logic '0'. For all other input combinations the output is '1'. The symbol for the OR-gate is shown in Fig. 6.5. along with the associated truth table.



(*a*)

P	*Q*	*Y*
0	0	1
0	1	1
1	0	1
1	1	1

(*b*)

Fig. 6.5 OR-gate

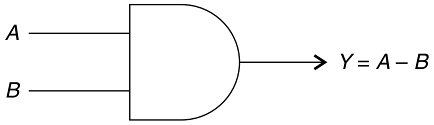
The operation of an OR-gate which is explained by the expression $Y = A + B$ is read as Y equal to A OR B.

Note: Performing OR operation is the same as taking the maximum of two bits.

6.2.2 AND-Gate

An AND-gate is a logic circuit having two or more than two inputs and one output. The output of an AND-gate is logic '1', only when all of its inputs are in '1' state. In all other possible combination the output is '0'. Fig. 6.6 (*a*) shows the symbol of an AND-gate. The truth table is given in Fig. 6.6 (*b*). The operation of an AND-gate is expressed by:

$$Y = A + B$$



(*a*)

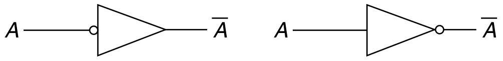
A	*B*	*Y*
0	0	0
0	1	0
1	0	0
1	1	1

(*b*)

Fig. 6.6

6.2.3 NOT-Gate (Inverter)

A NOT-gate is one input and one out put logic gate. The out put of a NOT-gate is always the complement of the input. A NOT-gate is also known as an inverter or a complementing circuit. Fig. 6.7 shows the NOT-gate with the associated truth table.



A	$\bar{A}$
0	1
1	0

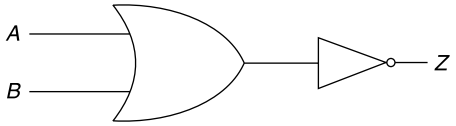
(*a*) (*b*) (*c*)

Fig. 6.7 A NOT-gate, equivalent symbol

6.2.4 NOR-Gate

The NOR-gate has two or more input, but produces only are output. The NOR operations is symbolised as $Z = A \downarrow B$.

NOR action is illustrated in Fig. 6.8. The equivalent symbol is shown in Fig. 6.9.



A	B	Z
0	0	1
0	1	0
1	0	0
1	1	0

Fig. 6.8 NOR-gate symbol

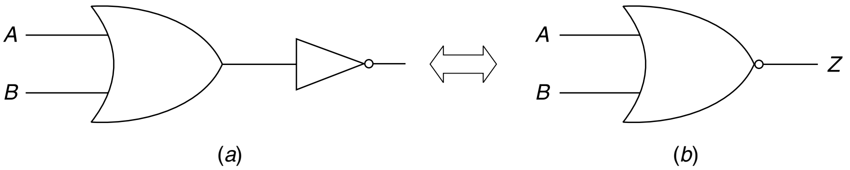
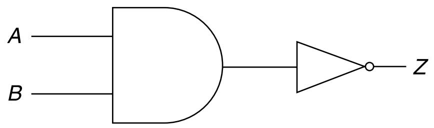


Fig. 6.9 NOR-gate equivalent symbol

6.2.5 NAND-Gate

NAND-gate function is a composite function. In this case an AND function is complemented to produce a NAND function placing an *N* in front of AND. The NAND-gate has two or more input signals but only one output signal. The NAND-gate is a contraction of NOT AND. It can have many inputs as desired. The symbol for NAND-gate along with the truth table is shown in Fig. 6.10.



A	B	Z
0	0	1
0	1	1
1	0	1
1	1	0

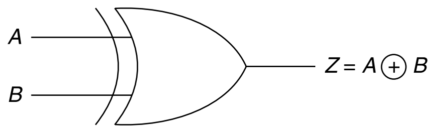
(*a*) (*b*)

Fig. 6.10 NAND-gate

NAND operation is symbolised as ↑ i.e., A NAND B is written as $A \uparrow B$.

6.2.6 Exclusive OR-Gate (EX-OR Gate or XOR Gate)

EX-OR stands for exclusive OR. It differs from an OR gate in only are of the entries in the truth table. The EX-OR gate can also L are have two or more inputs but produces one output signal. The symbol for Exclusive OR is shown in Fig. 6.11. Where the operation of the gate is expressed by $Z = A \oplus B$.



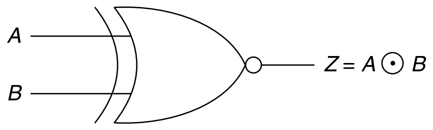
A	B	Z
0	0	0
0	1	1
1	0	1
1	1	0

(*a*) (*b*)

Fig. 6.11 Two input—EX-OR gate

6.2.7 Exclusive NOR Gate (EX-NOR Gate or XNOR Gate)

The EX-NOR gate is logically equivalent to an inverted EX-OR gate i.e., EX-OR gate followed by a NOT-gate. The symbol for EX-NOR is shown in Fig. 6.12. The operation of the gate is expressed by $Z = A \odot B$.



A	B	Z
0	0	1
0	1	0
1	0	0
1	1	1

(*a*) 2-input EX-NOR gate (*b*) Truth table for EX-NOR

Fig. 6.12

Sometimes it is convenient to use more than one representation for a given type of gate, Fig. 6.13 shows alternative symbols used for the logic gates.

We can use the above symbols to analyse and design complex digital systems. We can also apply the techniques of Boolean algebra to electronic logic. Generally a logic gate network is drawn so that the flow of information is from the left to right.

The inputs to a logic gate network will be formed on the left of schematic diagram and the outputs will be found on the right, which makes it easier for us to find the algebraic equation of the total network, Boolean algebra is useless unless it can be converted into hardware in the form of logic gates. Science of Boolean algebra can be a useful technique for analysing circuits only if the hardware can be translated into Boolean expression.

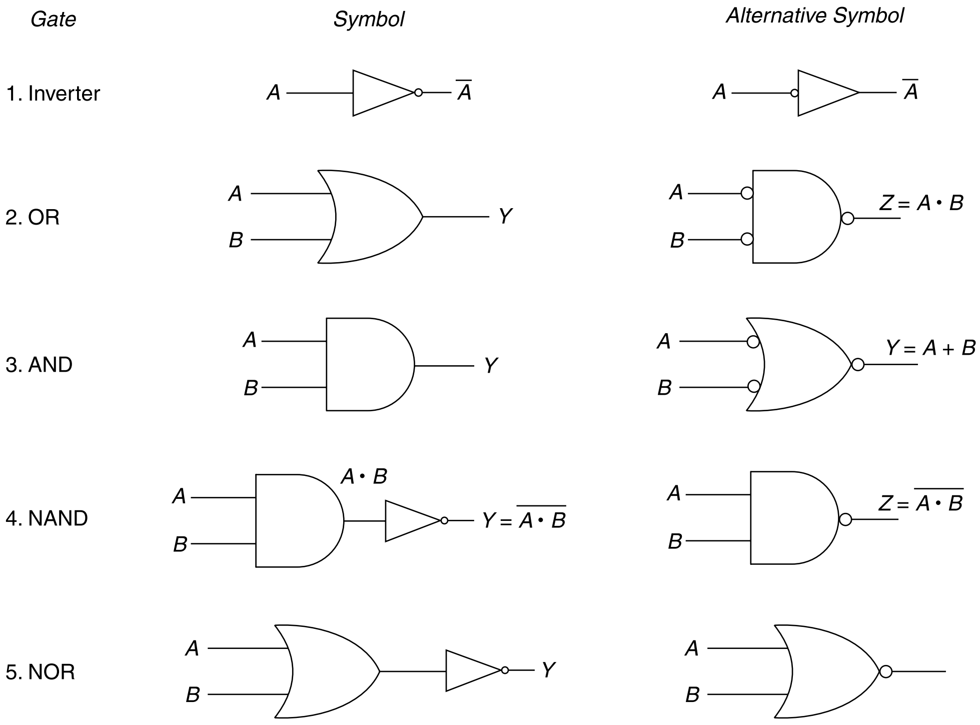


Fig. 6.13 Logic gates, equivalent symbols

Example 1: For the logic circuit shown in Fig. 6.14. write the input-output Boolean expression.

Solution: The output Boolean expression is

$$Z = (A + B) \cdot \left(\overline{A} + \overline{C}\right) \cdot (B + C).$$

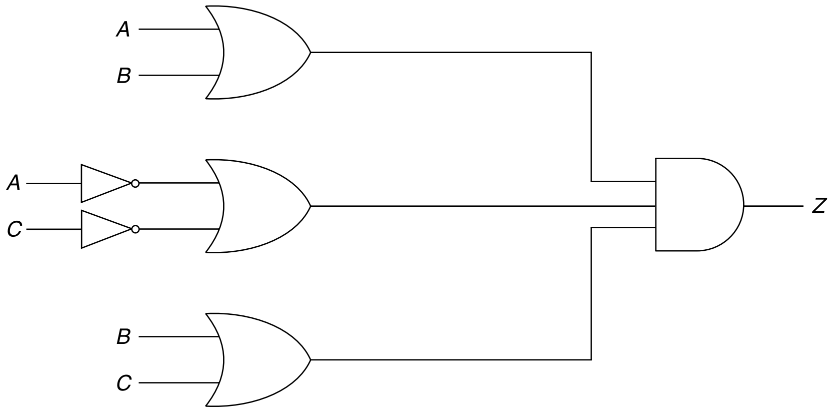


Fig. 6.14

Example 2: Represent $(A + B)\ (B + C)\ (C + A)$ in NOR-to-NOR form.

Solution: $(A + B)\ (B + C)\ (C + A) = (A$ NOR $B)$ NOR $(B$ NOR $C)$ NOR $(C$ NOR $A)$

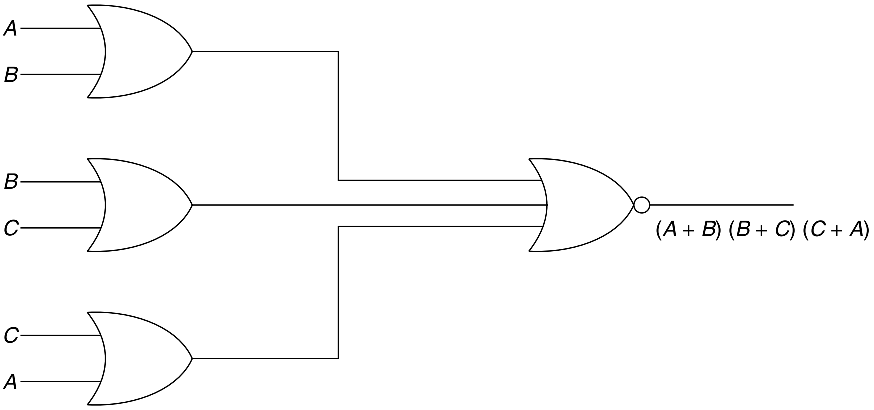


Fig. 6.15

Example 3: Implement the logic expression

$$F = \overline{A}\,\overline{B}\,C + \overline{A}\,B\,C + A\,\overline{B}$$

with logic gates.

Solution: The expression $F = \overline{A}\,\overline{B}\,C + \overline{A}\,B\,C + A\,\overline{B}$ requires three and gates and one OR-gate. It can be implemented as shown in Fig. 6.16:

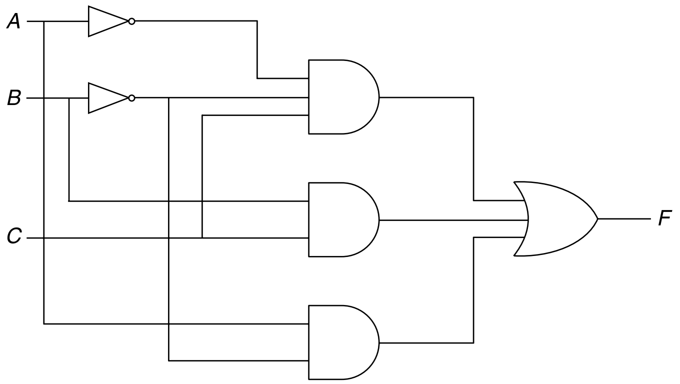


Fig. 6.16

Example 4: For the equation $Z = X\,Y + \overline{W}\,Y$ construct a gate structure and minimize it.

Solution: The gate structure for $Z = X\,Y\ +\ \overline{W}\,Y$ is shown in Fig. 6.17:

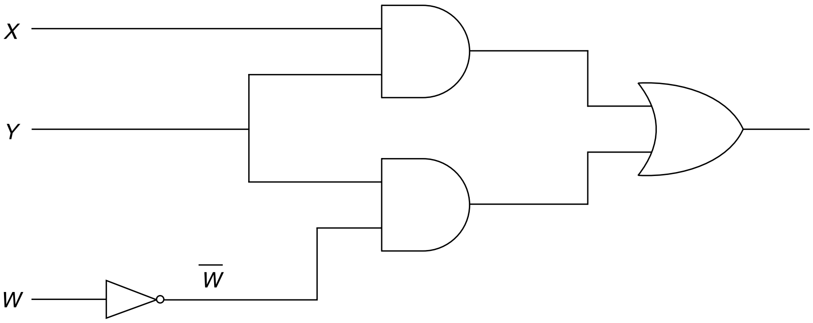


Fig. 6.17

Now consider $Z = X\,Y + \overline{W}\,Y$

The equation can be factored as $Z = Y\left(X + \overline{W}\right)$. The gate structure of Z has only two input gates.

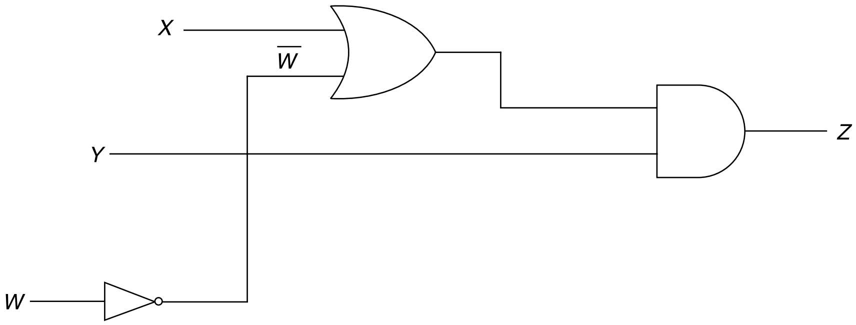


Fig. 6.18

Example 5: Construct a NAND-gate structure for the expression

$$Z = \left(\overline{A} + B\right) C + \overline{F} + D\ E$$

Solution: Figure 6.19 shows the NAND-gate network of *Z*:

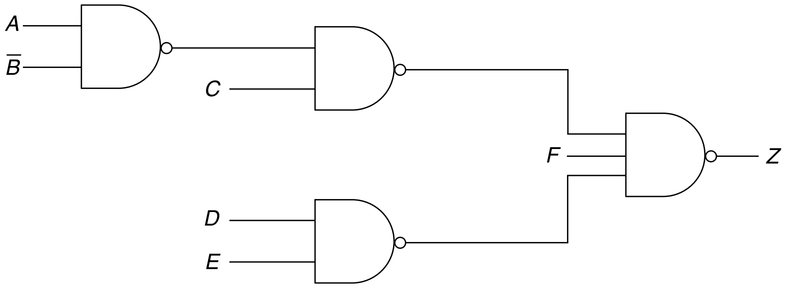


Fig. 6.19 NAND-gate network for *Z*

The equivalent AND-OR network is given in Fig. 6.20:

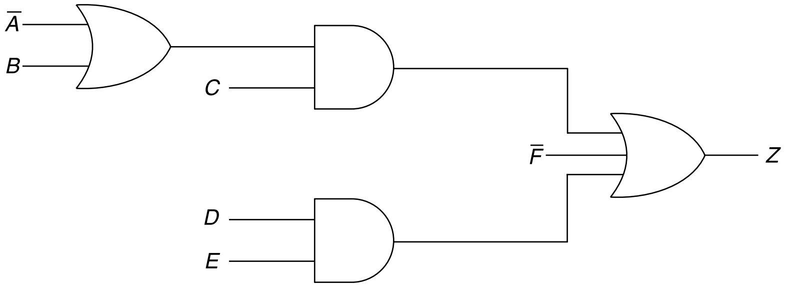


Fig. 6.20 Equivalent AND-OR network

Example 6: Use NAND-gates and draw a circuit diagram for $F = X\,\overline{Y}\,Z + \overline{Z}\,Y$.

Solution: $F = X\,\overline{Y}\,Z + \overline{Z}\,Y$

= (*X* NAND (NOT *Y*) (AND *Z*) NAND (NOT *C* NAND *B*)

The circuit diagram for *F* can be drawn as shown in Fig. 6.21:

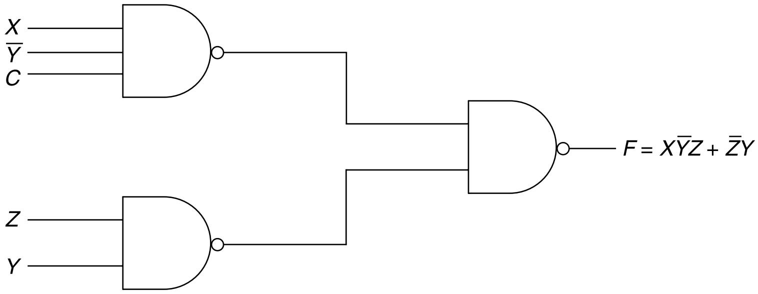


Fig. 6.21

Example 7: Show that the combination circuits of Fig. 6.22 are equivalent:

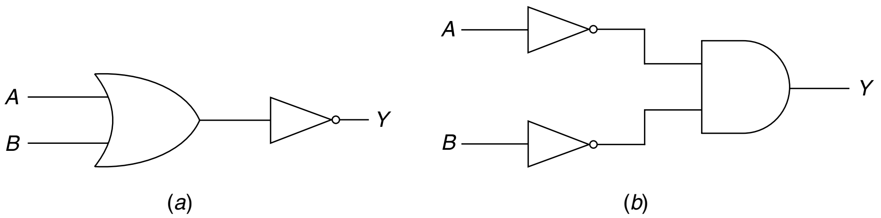


Fig. 6.22

Solution: The logic table for the circuit is shown in Fig. 6.22 (*a*) is:

Table 6.5

A	*B*	*Y*
1	1	0
1	0	0
0	1	0
0	0	1

(*a*)

A	*B*	*Y*
1	1	0
1	0	0
0	1	0
0	0	1

(*b*)

Table 6.5 (*a*) is logic table for the circuit Fig. 6.22 (*a*). The logic table for the circuit shown in Fig. 6.22 (*b*) is given in Table 6.5(*b*).

The logic table for the circuits is shown in Fig. 6.22 (*a*) and Fig. 6.22 (*b*) are identical. Hence the circuits are equivalent.

6.3 APPLICATIONS

Logic gates have several applications to the computers. They are used in the following:

1. Adders,
2. Encoder, and
3. Decoder

6.3.1 Adders

The application of binary bits consists the following elementary operations, namely

$$0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 10.$$

We observe that the left bit gives the carry. When the augend and addend numbers contain more significant digits, the carry obtained from the addition of two bits is added to the next higher order pair of significant digits.

6.3.1.1 Half adder

A logic circuit that performs the addition of two bits is called a half adder. The half adder circuit needs two binary inputs and two binary outputs. The inputs variables designate augend and addend bits, the output variables produce the sum and carry. It is necessary to specify two output variables because the sum of 1 + 1 is binary 10. We assign symbols *A* and *B* to the input variables, *S* for the sum function and *C* for carry function. Both *S* and *C* are out put symbols. The truth table for half adder is given below:

Table 6.6 *2-input Half Adder*

A	*B*	*Carry (C)*	*Sum (S)*
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

From the table, it is clear that half adder performs binary operation (electronically): at a faster rate.

Logic circuit for half adder is given in Fig. 6.23:

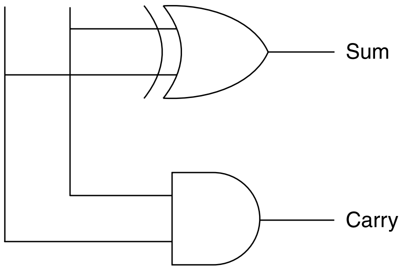


Fig. 6.23 (2-input) Half adder

6.3.1.2 Full adder

A logic circuit that performs the addition of three bits is a full adder. It consists of three inputs and two outputs. The two outputs are SUM and CARRY. Let us denote two of the input variables by A_1 and B_1, (to represent two significant bits to be adder) and the represents the carry from the previous lower significant position. The sum of three binary digits from 0 to 3. The binary numbers 2 and 3 need two binary digits. Hence we need two outputs designated by the symbols *S* (SUM) and *C* (CARRY). The truth table for the full adder is given below:

Table 6.7 *Full Adder*

A_1	B_1	C_1	C	S
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Logic circuit for Full adder is shown in Fig. 6.24.

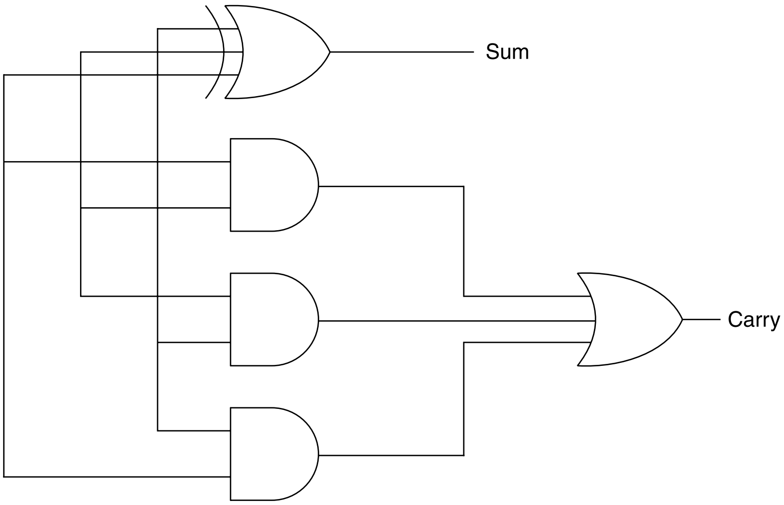


Fig. 6.24 (3-input) Full adder

6.3.2 Decoder

A decoder is a combinational logic circuit that converts *n* input lines to a maximum of 2^n unique output lines. In a 3 to 8 lines decoder three inputs are decoded into 8 outputs where each output represents one of the minterms of the 3 input variables. If the input variables represent a binary number then the outputs will be digits of octal system (contain 8 digits). *A* 3 to 8 lines decoder can also be used for decoding any 3 bit code to provide 8 outputs. The following is the diagram of 3 to 8 decoder:

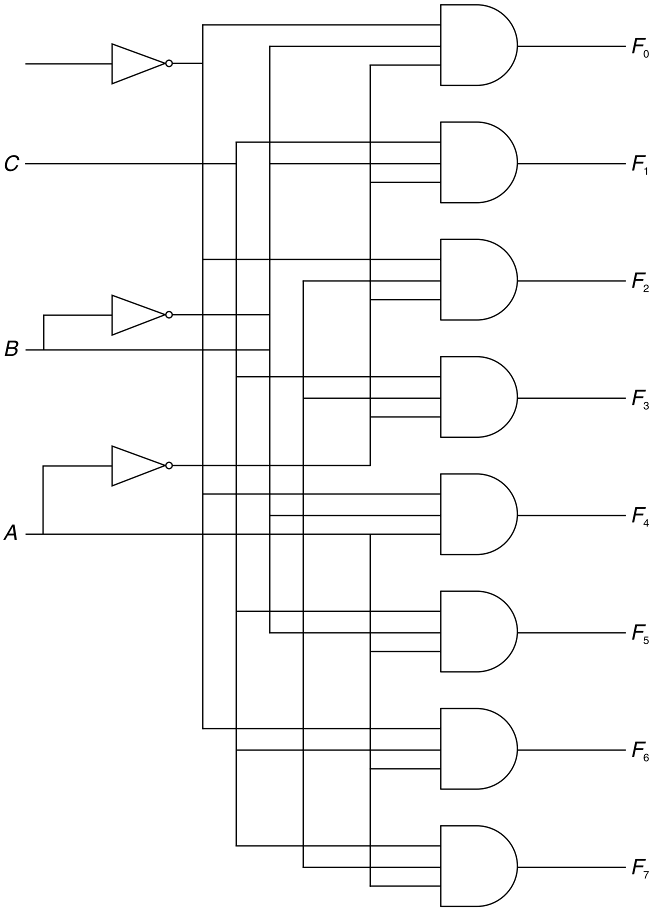


Fig. 6.25 A 3 to 8 decoder

The truth table of 3 to 8 lines decoder is given below:

Table 6.8

Inputs			*Outputs*							
A	*B*	*C*	F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7
0	0	0	1	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0
0	1	1	0	0	0	1	0	0	0	0
1	0	0	0	0	0	0	1	0	0	0
1	0	1	0	0	0	0	0	1	0	0
1	1	0	0	0	0	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1

We observe that the outputs variables are mutually exclusive. A decoder with n input variables can generate 2^n minterms.

6.3.3 Encoder

A logical circuit which performs the inverse operation of a decoder is called an Encoder. Decimal to binary encoder converts decimal numbers and a Hexadecimal to binary encoder converts Hexadecimal number to its binary equivalent. An encoder with 2^n input lines will have n output lines. The block diagram for 2^4 to 4 encoder is given in Fig. 6.26.

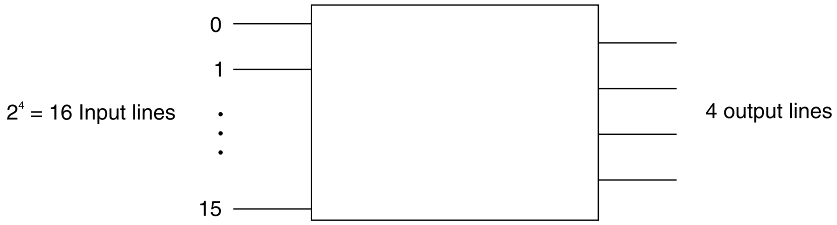


Fig. 6.26

6.3.4 Multiplexer (MUX)

Multiplexers are used to transmit large number of data over a small number of lines. Multiplex means many to one. A digital multiplexer is a combinational circuit that selects binary information from many input lines and directs it to a single output line. The selection of a particular input line is controlled by a set of selection lines. A multiplexer receives binary information from the 2^n lines and transmit information on a single output line (selected from the bit combination of n selection lines). The block diagram of 4 to 1 line multiplexer is shown in Fig. 6.27.

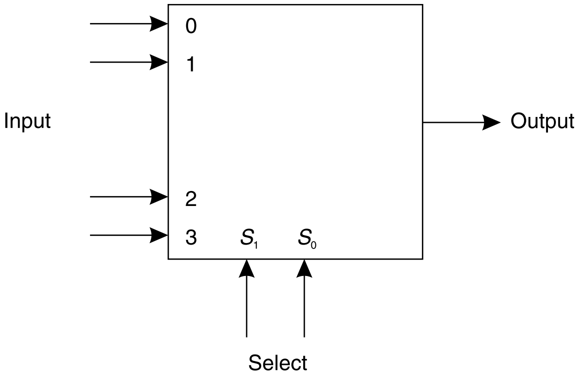


Fig. 6.27 Block diagram for 4 × 1 multiplexers

If a Boolean function F has n variables, we take $n - 1$ of these variables and connect them to the selection lines of a multiplexer. The remaining variable say X of the function F is used for the inputs of the multiplexer. The inputs of the MUX are chosen to be either X or X' or 1 or 0. We can implement F with a MUX by choosing the four values X, X', 1 and 0 for the inputs and by connecting the other variables to the selection lines. We now explain the method of implementing a Boolean function F of n variables with 2^{n-1} to 1 multiplexer, with the help of an example.

Example: Implement

$$F = (a, b, c) = \sum (0, 3, 6, 7)$$

With a multiplexer

Solution: We first express F in its sum of minterms form. The ordered sequence of variables chosen for the minterms is $a\ b\ c$. Where a is the left most variable in the ordered sequences. Thus, we have

$$n = 3 \text{ (no of variables)}$$
$$n - 1 = 3 - 1 = 2$$

we use 2^{n-1} to 1, i.e. 2^{3-1} to 1 i.e., 8 to 1 multiplexes for the implementation of F. The selected variable a is in the highest order position in the sequences of variables m_0, m_1, m_2, m_3, m_4, m_5, m_6, m_7 are the minterms. We list all the minterm in two rows as shown in Table 6.9. The singled out variable a will be in the complemented form in the first row and will be in the uncomplemented form in the second row.

Table 6.9

	I_0	I_1	I_2	I_3
a^1	⓪	1	2	③
a	4	5	⑥	⑦

We circle the minterms of the function F and inspect each column separately: we apply the following rules:

(*i*) If the two minterms in a column are not circle we apply 0 to the corresponding multiplexer input.

(*ii*) If the two minterms are circled, then we apply 1 to the corresponding input of MUX.

(*iii*) If the bottom row minterm in a column is circled and the top minterm is not circled, apply a to the corresponding multiplexer input.

(*iv*) If the minterm of top row is encircled and the bottom row minterm in a column is not encircled, then we apply a^1 to the corresponding multiplexer input applying the above rules we obtain the values as shown in Table 6.10.

Table 6.10 *Implementation table*

	I_0	I_1	I_2	I_3
a^1	⓪	1	2	③
a	4	5	⑥	⑦
	a^1	0	a	1

The inputs I_0, I_1, I_2, I_3, are applied the values as shown below:

Input	*Value applied to the input*
I_0	a'
I_1	0
I_2	a
I_3	1

The function F can be implemented by using MUX as shown in Fig. 6.28.

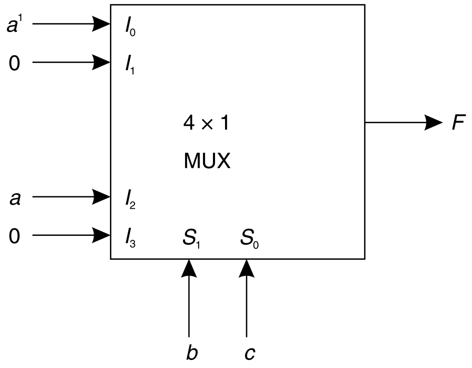


Fig. 6.28

6.4 SPECIAL SEQUENCES

If L is a logic circuit with n inputs devices and $A_1, A_2, \ldots A_n$ denote n-input sequences. Then each A_i must contain 2^n bits. There are many ways to form $A_1, A_2, \ldots A_n$, so that each A_i contain 2^n different possible combinations of input bits. One assignment scheme is as follows:

A_1: Assign 2^{n-1} bits which are 0's and 2^{n-1} bits which are 1*s*.

A_2: Repeatedly assign 2^{n-2} bits which are 0's followed by 2^{n-2} bits which are 1*s*.

A_3: Repeatedly assign 2^{n-3} bits which are 0's followed by 2^{n-3} bits which are 1*s*.

...

$A_1, A_2, A_s, \ldots$ are called special sequences. The complements of these special sequences can be obtained by replacing 0 by 1 and 1 by 0, in the sequences.

Example 1: Suppose a logic circuit has $n = 3$, input devices A, B and C, write down the special sequences for A, B and C and write their complements.

Solution: We have $n = 3$

There are $2^3 = 8$ bit special sequences for A, B and C. They can be written as follows:

$$A = 00001111$$
$$B = 00110011$$
$$C = 01010101$$

The special sequences for their complements are

$$\overline{A} = 11110000$$
$$\overline{B} = 11001100$$
$$\overline{C} = 10101010$$

Example 2: Determine how the pair of sequences 110001, 101101, is processed by an AND-gate.

Solution: 1's can occur as an outputs of an AND-gate. Only when both inputs are 1, therefore the pair 1100001, 101101, has the output 100001 by an AND-gate, (note that 1's occur in the first and last positions).

Example 3: How would a NOT-gate process the sequence 100011.

Solution: A NOT-gates changes 0 to 1 and 1 to 0. Hence the output of the given sequence is 01110000.

Example 4: If A = 1100110110, B = 1110000111 and C = 1010010110 find $A + B + C$.

Solution: 0s occur in the 4th, 7th positions. The remaining positions will have 1s.

Hence $A + B + C$ = 1110110111.

Example 5: If A = 00001111, B = 00110011 and C = 01010101 find $A\ B\ C$.

Solution: A, B and C have 1s in the 8th position.

Hence $A\ B\ C$ = 00000001

EXERCISE 6.1

I

1. What are logic gates? Name three basic logic gates.
2. What is an OR-gate? Explain in brief the function of an OR-gate.
3. What is an AND-gate.
4. What is an exclusive OR-gate? How does it differ from an OR-gate?
5. What is a NOT-gate? Explain its operations and draw its truth table.
6. Draw the circuit symbol of a NAND-gate.
7. Simplify:
   1. $P'\ Q + P'\ Q\ R'\ S' + P\ Q\ R\ S'$
   2. $(P' + Q' + R')\ (P' + Q' + R)\ (Q' + R)\ (P + R)\ (R + Q + R)\ (P' + Q)$
   3. $P\ Q\ R\ S + P'\ R\ S + P\ Q\ S + P\ Q\ R\ S' + Q\ R'\ S$

II

1. Simplify the following expressions:

   (a) $Z = \overline{(A \cdot B + B \cdot C)(B \cdot C + C \cdot D)(C \cdot D + A \cdot B)}$

   (b) $Z = (A + B) \cdot (A + \overline{B}) \cdot (\overline{A} + B)$

2. What is the significant of Principle of duality. Write the duals of

   (a) $(X + Y) * (Y + Z) * (Z + X)$

   (b) $A + (B + E) + B * (C + A) + C * (A + B)$

3. $D_{70} = \{1, 2, 5, 7, 10, 14, 35, 70\}$ (the division of 70} we define

$a + b = \text{lcm}(a, b)$

$a * b = \text{gcd}(a, b)$

$a' = {}^{70}\!/_{a}$

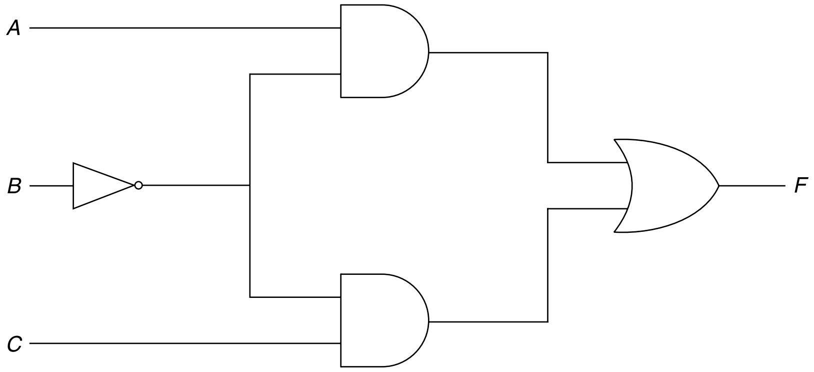
show that D_{70} is a Boolean algebra with 1 as the zero element and 70 as the unit element.

4. Find the sum of products form (disjunctive normal form) of the Boolean expression $E = ((xy)' z)$ $((n' + z)(y' + z'))$

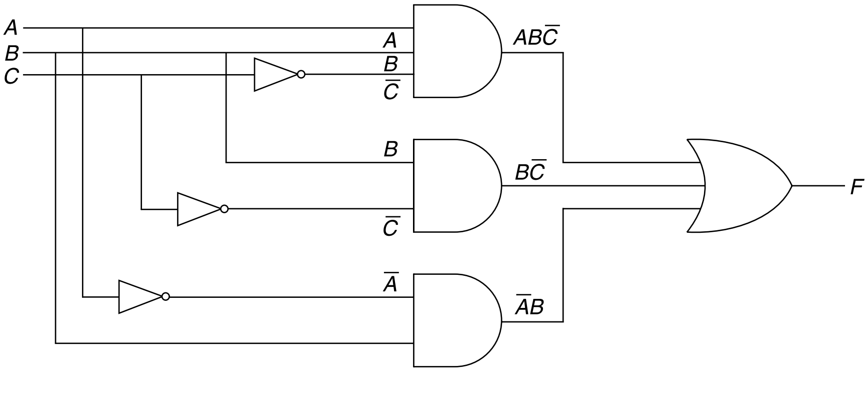
5. A logic circuit L has $n = 4$ inputs A, B, C, D write the 16 bit special sequence for A, B, C, D.

6. Given five inputs A, B, C, D and E find the special sequences which give all the different possible combinations of inputs bits.

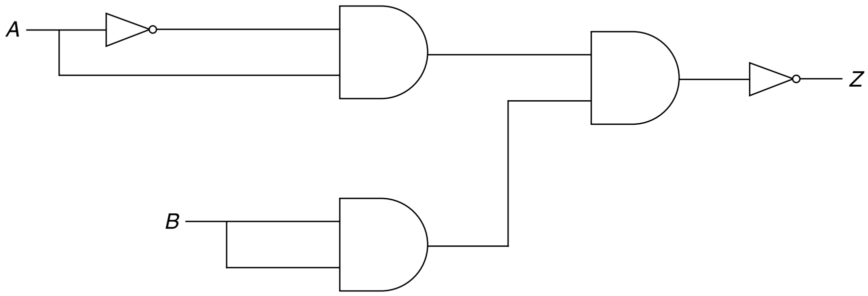
7. For each of the following networks find the output:



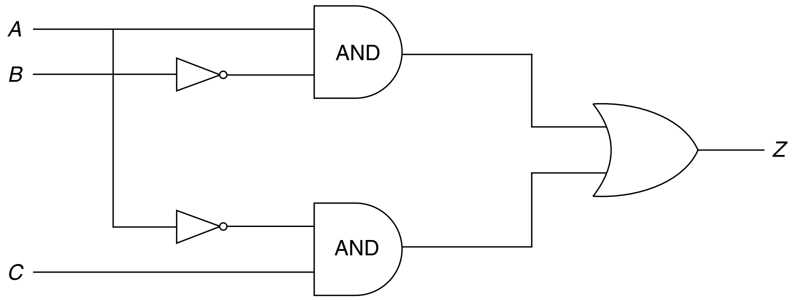
(*a*)



(*b*)



(*c*)

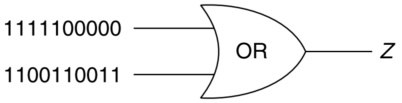


(*d*)

8. Simplify the Boolean expression and construct a network for the expression.

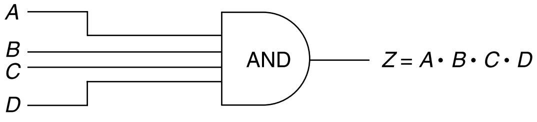
$$Z = \overline{A}BC + A\overline{B}\overline{C} + A\overline{B}C + AB\overline{C}$$

9. Determine the output of the gate



10. If $A = 11100111$
$B = 01111011$
$C = 01110011$
and $D = 11101110$

Determine the output of the gate



11. Implement $F(a, b, c) = \sum (1, 3, 5, 6)$ with a multiplexer.

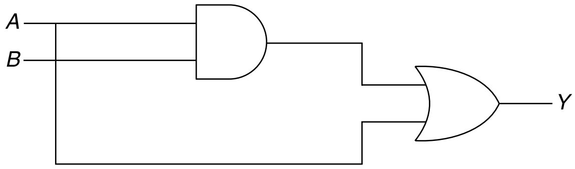
12. Implement the following functions with a multiplexer:

(*i*) $F(a, b, c) = \sum (1, 2, 5, 7)$

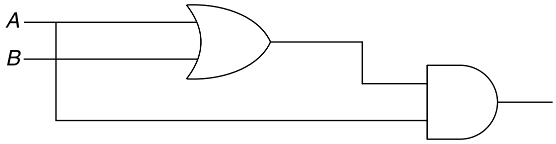
(*ii*) $F(a, b, c, d) = \sum (0, 1, 4, 8, 9, 14, 15)$

13. Show that the combinational circuits of exercise (*i*) to (*ii*) are equivalent

(*i*)

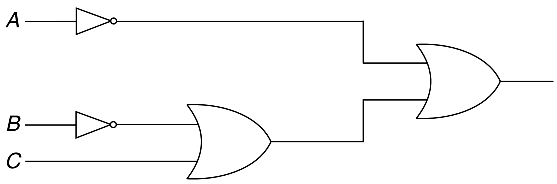


(*a*)

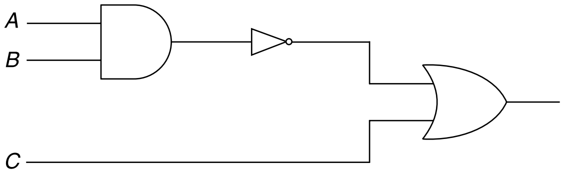


(*b*)

(*ii*)



(*a*)



(*b*)

14. A fundamental product P is called a prime implicant of a Boolean expression E if $P + E = E$. Find the prime implicant P of the expression

$$E = x\,y\,z + x'\,z' + x\,y\,z' + x'\,y'\,z + x'\,y\,z'$$

15. Draw a logic circuit corresponding Boolean expression

$$Y = \overline{A + BC} + B$$

7

Elementary Combinatorics

7.1 INTRODUCTION

Combinatorics deals with counting and enumeration of specified objects, patterns or designs. Techniques of counting are important in mathematics and computer science. In this chapter, we shall study basic of counting. We also develop basic ideas of permutations, combinations, Binomial theorem, power sets and pigeon hole principle. We begin our study with two basic counting principles.

7.2 BASICS OF COUNTING

7.2.1 Sum Rule (Principle of Disjunctive Counting)

Let S be a set and $|S|$ denote the number of elements in S. If S is a union of disjoint non-empty subsets $A_1, A_2, \ldots, A_n$ then

$$|S| = |A_1| + |A_2| + \ldots + |A_n|$$

In the above statement the subsets A_i of S are all disjoint i.e., they have no element in common. If A_i and A_j an two subsets of S, then

$$A_i \cap A_j = \varnothing \quad (\text{for} \quad i \neq j)$$

and we have

$$S = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n$$

that is each element of S is exactly in one of the subsets A_i. In other words, the subsets $A_1, A_2, \ldots A_n$ is a partition of S. We now state the sum rule for counting events.

Let S be a sample space. Two events E_1 and E_2 of X are said to be mutually exclusive if the events have no elements in common. If $E_1, E_2, E_3, \ldots E_n$, are mutually exclusive events of S, then we can state sum rule for counting events as follows:

If $E_1, E_2, \ldots E_n$ are mutually exclusive events of a sample space S and E_1 can happen in m_1 ways. E_2 can happen in m_2 ways, … , E_n can happen in m_n ways then E_1 or E_2 or … or E_n can happen $m_1 + m_2 + \ldots + m_n$ ways.

Example 1: How many ways can we get a sum of 7 or 1 when two distinguishable dice are rolled?

Solution: The two dice are distinguishable, therefore the ordered pairs (a, b) and (b, a) are distinct when $a \neq b$, i.e., $(a, b) \neq (b, a)$ for $a \neq b$.

The ordered pairs in which the sum is 7 are:

(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1). These ordered pairs are distinct.

∴ There are 6 ways to obtain the sum 7.

Similarly the ordered pairs: (5, 6), (6, 5) are all distinct.

∴ The number of ways in which we get a sum 11 with the two dice is 2.

Therefore, we can get a sum 7 to 11 with two distinguishable dice in 6 + 2 = 8 ways.

Example 2: How many ways can we draw a club or a diamond from a pack of cards?

Solution: There are 13 clubs and 13 diamonds in a pack of cards.

The number of ways a club or a diamond may be drawn 13 + 13 = 26.

Example 3: In how ways can be drawn an ace or a king from an ordinary deck of playing cards?

Solution:

Number of Aces in a pack = 4

Number of kings in a pack = 4

Number ways an Ace or a king can be drawn from the pack = 4 + 4 = 8

7.2.2 Product Rule (The Principle of Sequential Counting)

If $A_1, A_2, \ldots, A_n$ are non-empty sets, then the number of elements in the Cartesian product $A_1 \times A_2 \times \ldots \times A_n$ is the product $\prod_{i=1}^{n} |A_i|$

$$|A_1 \times A_2 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|$$

Product rule in terms of events:

If $E_1, E_2, \ldots, E_n$ are events, and E can happen in m_1 ways E_2 can happen m_2 ways, … E_n can happen in m_n ways, then the sequence of events E, first followed by E_2 followed by $E_3, \ldots$, followed by E_n can happen in $m_1 \times m_2 \times \ldots \times m_n$ ways.

Example 1: How many possible out comes are there when we roll a pair of dice, one red and one green?

Solution: The red die can land in any one of six ways and for each of there six ways, the green die can also land in six ways.

The number of possible out comes when two dice are rolled = 6 × 6 = 36.

Example 2: In how many different ways one can answer all the questions of a true-false test consisting of 4 questions?

Solution: There are two ways of answering each of the 4 questions. Therefore by product rule the number of ways in which all the 4 questions can be answered.

$$= 2 \times 2 \times 2 \times 2 = 16$$

Example 3: Find the number n of license plates that can be made where each plate contains two distinct letters followed by three different digits.

Solution: First letter can be printed in 26 different ways. Since the second letter must be different from the first, we have 25 contains for the second letter. Similarly the first digit can be printed in 10 ways, the second digit in the license plate can be printed in 9 ways and the third in 8 ways.

Therefore, the number of license plates that can be printed, so that each plate contains two distinct letters follower by three different digits 26 . 25 . 10 . 9 . 8 = 4,68,000.

EXERCISE 7.1

1. In how many ways can be draw a king or a queen from ordinary deck of playing cards?
2. How many ways can we draw a club or a spade from a pack of cards?
3. How many ways can we get a sum 6 or 9 when two distinguishable dice are rolled?
4. How many possible out comes are there when we roll a pair of dice, one yellow and one red?
5. In how many different ways are can answer all the questions of a true-false test consisting of 5 questions?
6. How many ways can we get a sum of 8 when two in distinguishable dice are rolled?
7. How many ways can we get a sum of 4 or 8 when two distinguishable dice are rolled? How many ways can we get an even sum?
8. In how many ways can an organisations containing 26 members elect a president, a treasurer and a secretary (assuming no person is elected to more than one position)?
9. In a railway compartment 6 seats are vacant on a bench. In how many ways can 3 passengers can sit on them?
10. There are 10 buses plying between on a bench. In how many ways can 3 passengers can sit on them?
11. Suppose a license plate contains two letters followed by three digits with the first digit not zero. How many different plates can be printed?
12. Suppose a license plate contains 3 English letters followed by 4 digits:
    (*a*) How many different license plates can be manufactured if repetition of letter and digits are allowed?
    (*b*) How many plates are possible if only the letters are repeated?
    (*c*) How many are possible if only the digits can be repeated?
13. How many different license plates are there that involve 1, 2 or 3 letters followed by 4 digits?
14. There are 10 true-false questions on an examinations. How many sequences are possible?
15. Suppose that a state's license plates consists of three letters followed by three digits. How many different plates can be manufactures (if repetitions are allowed)?
16. If there are 12 boys and 16 girls in a class find the number of ways of selecting one student as class representative.

Answers:

1. 8 **2.** 26 **3.** 9 **4.** 36 **5.** 32 **6.** 12 **7.** 8, 18 **8.** 15,600 **9.** 120
10. 90 **11.** 608400 **12.** $26^3 \times 10^4$, $26^3 \times 10 \times 9 \times 8 \times 7$, $26 \times 25 \times 24 \times 10^4$
13. $(26 + 26^2 + 26^3)\ 10^4$ **14.** 1024 **15.** $26^3 \times 10^3$ **16.** 28.

7.3 PERMUTATIONS AND COMBINATIONS

7.3.1 Permutations

Definition 7.1: A permutation of n objects taken r at a time is an arrangement of r of the objects ($r \leq n$).

A permutation of n objects taken r at a time is also called r-permutation or an r-arrangement. Various symbols are used to indicate the number of permutations of n things taken r at a time. The one we shall use in this text is $P\,(n, r)$, $(r \leq n)$. The symbols n_{P_r} or $P\,(^{n}_{r})$, $[n]_r$ or $n_{(r)}$ are also used to denote the number of permutations of n objects taken r at a time.

Example 1: Consider the three letters a, b, c. The arrangements of the letter a, b, c taken two at a time are.

$$ab,\ ba,\ ac,\ ca,\ bc,\ cb$$

$\therefore$ The number of 2-arrangements are 6 i.e., the number of permutation of 3 letters taken 2 at a time $= 3_{P_2} = P(3, 2) = 6$.

Notation

In this chapter, we use $\{P_1\,a, P_2\,b, P_3\,c, P_4\,d\}$ to indicate either:

(i) That we have $P_1 + P_2 + P_3 + P_4$ objects which include P_1 a's, P_2 b's, P_3 c's, P_4 d's.

(ii) That we have 4 objects a, b, c and d with the condition that:
a can be chosen at most P_1 times.
b can be chosen at most P_2 times.
c can be chosen at most P_3 times.
d can be chosen at most P_4 times.

The numbers P_1, P_2, P_3 and P_4 are called repetition numbers.

Example 2: The three permutations of $\{3\,a, 1\,b, 1\,c\}$ are *aaa*, *aab*, *baa*, *aac*, *aca*, *abc*, *acb*, *bac*, *bca*, *cab*, *cba*, *aba*.

7.3.2 Factorial Function

Definition 7.2: If n is a natural number, then the product of all the natural numbers from 1 to n is called "n-factorial". It is denoted by the symbol n! The symbols $\lfloor\underline{n}$ and $n_{(n)}$ are also used.

From the definition.

$$n! = n\,(n-1)\,(n-2)\ \ldots\ 3.2.1$$

The factorial function $n!$ can also be defined recursively as follows:

$$0! = 1$$

$$(n+1)! = n!\,(n+1),\ n \geq 0$$

From the above recursive definition, we get

$$1! = 0!\,(1) = 1$$

$$2! = 1!(2) = 1\cdot 2$$

$$3! = 2!(3) = 1.2.3$$

7.3.3 Falling and Rising Factorials

Definition 7.3: The number $n(n - 1)(n - 2) \ldots (n - r + 1)$ is called 'falling factorial'. It is denoted by $[n]_r$

The number $n(n + 1)(n + 2) \ldots (n + r - 1)$ is called 'rising factorial'. It is denoted by the symbol $[n]^r$

7.3.4 Stirling Numbers

Definition 7.4: The falling factorial $[x]_r$ is a polynomial of rth degree is x. Let us unite the polynomial as

$$[x]_r = S_r^0 + S_r^1\, x + S_r^2\, x^2 + \cdots + S_r^r\, x^r$$

The numbers $S_r^0, S_r^1, S_r^2, \ldots, S_r^r$ are called the stirling numbers of the first kind.

We have $S_r^0 = 0, S_r^r = 1, S_r^k = 0$, if $k > r$

The recurrence relation is

$$S_{r+1}^k = S_r^{k-1} - r\, S_r^k,\ S_r^0 = 0,\ S_r^r = 1$$

Let $n \geq r$ the number of distributions of n distinct objects into r non-distinct, boxes, no box being empty is denoted by S_n^r. It is called a stirling number of the second kind. We have the recurrence formula.

$$S_{n+1}^r = S_n^{r-1} + r\, S_n^r, \text{ if } 1 < r < n$$

$$S_1^1 = 1,\ S_n^n = 1,\ S_n^r = 0 \text{ if } r > n$$

$$S_0^0 = 1,\ S_0^r = S_n^0 = 0 \text{ if } r, n > 0$$

The number $S_n^1 + S_n^2 + \ldots + S_n^n$ is called nth Bell number. It is denote by B_n

Theorem 7.1: (Number of r-permutation without repetition). The number of r-permutations of n objects is $p(n, r) = n(n - 1)(n - 2)\ldots(n - r+1) = \dfrac{n!}{(n-r)!}$

Proof: The first element in an r-permutations of n objects can be chosen in n different ways. Once the first element has been selected, the second element can be selected in n–1 ways. We continue selecting the elements, having selected $(r - 1)$th element. We select rth element i.e., the last element. The rth element in the permutation can be selected in $n - r + 1$ ways. By product rule, the number of r-permutations of a set of n distinct objects is

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

We may also write $P(n, r)$ in factorial

$$P\,(n, r) = n\,(n-1)\,(n-2)\ldots(n-r+1) = \frac{n(n-1)\ldots(n-r+1)\,(n-r)\ldots 2\cdot 1}{(n-r)\ldots 2\cdot 1}$$

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

7.4 SOLVED EXAMPLES

Example 1: Find 8!

Solution: For $n \geq 0$, we have

$$(n + 1) = n!\,(n + 1)$$

Hence,

$$\begin{aligned} 8! &= (7 + 1)! \\ &= 7!\,8 \\ &= 6!\,7\cdot 8 \\ &= 5!\,6\cdot 7\cdot 8 \\ &= 4!\,5\cdot 6\cdot 7\cdot 8 \\ &= 3!\,4\cdot 5\cdot 6\cdot 7\cdot 8 \\ &= 2!\,3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8 \\ &= 1!\,2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8 \\ &= 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8 \\ &= 40{,}320 \end{aligned}$$

Example 2: Simplify $\frac{(n+1)!}{n!}$

Solution:

$$\frac{(n+1)!}{n!} = \frac{(n+1)\,n(n-1)\ldots 3\cdot 2\cdot 1}{n(n-1)\ldots 3\cdot 2\cdot 1} = n+1$$

or

$$\frac{(n+1)!}{n!} = \frac{(n+1)n!}{n!} = (n+1)$$

Example 3: Prove that $2\,P\,(n, n-2) = P\,(n, n)$

Solution:

$$= 2\,P\,(n, n-2) = 2\;\frac{n!}{(n-(n-2))!}$$

$$= 2\cdot\frac{n!}{n-n+2!} = \frac{2\cdot n!}{2!}$$

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

Example 4: How many words of three distinct letters can be formed form the letters of the word LAND?

Solution: The number of three distinct letter words that can be formed from the 4 letters of the word LAND is $P(4,3) = \frac{4!}{(4-3)!} = \frac{4!}{11} = 4! = 24$

7.5 PERMUTATIONS WITH LIKE ELEMENTS

Theorem 7.2: The number of permutations of n objects of which are q_1 are alike, q_2 are alike, …, q_r are alike is

$$P(n, q, q_2, \ldots, q_{r)} = \frac{n!}{q_1!\,\mathrm{q}_2!\ldots q_r!}$$

Where $n = q_1 + q_2 + \ldots + q_r$

Proof: Let the number of permutation be x.

If the q_1 like objects are unlike, then for each of these x arrangements, the q_1 like objects could be rearranged among themselves in q_1! Ways without altering the positions of the other objects.

∴ The number of permutations would be $x\, q_1!$

Similarly; if q_2 like objects were unlike; each of these $x\, q_1!$ Permutations would give rise to $q_2!$ Permutations

Therefore, the number of permutations would be $x\, q_1!\, q_2!$

Similarly, if all the objects were unlike number of permutations would be $x\, q!\, q_2! \ldots q_r!$

But if all the objects were unlike, the number of permutations with the n objects would be $n!$ Hence

$$x\, q!\, q_2! \ldots q_r! = n!$$

We have $$x = \frac{n!}{q_1!\,\mathrm{q}_2!\ldots q_r!}$$

i.e., $$P(n\, q_1, q_2, \ldots, q_r) = \frac{n!}{q_1!\,\mathrm{q}_2!\ldots q_r!}$$

Example: There are 4 black, 3 green and 5 red balls. In how many ways can they be arranged in a row?

Solution: Total number of balls = 4 black + 3 green + 5 red = 12

The black balls are alike,

The green balls are, and the red balls are alike,

∴ The number of ways in which the balls can be arranged in a row = $\frac{12!}{4!\,3!\,5!} = 27{,}720$

7.5.1 Ordered Samples

In combinational analysis, many problems are concerned with choosing a ball from an *urn* containing n balls or a card from a deck. When we choose one ball after the other from the *urn* (or a card from a deck) say r times, we call each choice an ordered sample of size r, we have two cases:

(*i*) Sampling with replacement

The drawn ball may be replaced in the *urn* before the next ball is drawn. There are *n* different ways to choose each ball, therefore by fundamental principle of counting (product rule); there are n^r different ordered sample with replacement of size *r*.

(*ii*) Sampling without replacement

When the ball drawn is not replaced in the *urn* after it is drawn; repetitions do not occur, in the ordered sample. In this case, an ordered sample of size *r* without replacement, is an *r*-permutation of the objects in the *urn*.

Hence there are $\dfrac{n!}{(n-r)!}$ different ordered samples of size *r* without replacement.

Example 1: Suppose an *urn* contain 5 balls. Find the number of ordered sample of size 2.

(*i*) With replacement (*ii*) Without replacement

Solution:

(*i*) There are 5 balls, and each ball in the ordered sample can be chosen in 5 ways.

Hence, there are 5.5 = 25; samples with replacement.

(*ii*) The first ball in the ordered sample can be chosen in 5 ways and the next ball in the ordered sample can be chosen in 4 ways (when the first drawn ball is not replaced).

There are 5 × 4 = 20, samples without replacement.

Example 2: In how many ways can one choose two cards in succession from a deck of 52 cards, such that the first chosen card is not replaced.

Solution: There are 52 cards in the deck of cards since the chosen card is not replaced the first can be chosen in 52 different ways and the second can be in 51 different ways.

$\therefore$ The number of ways in which the 2 cards are chosen = 52 × 51 = 2,652

Example 3: A box contains 10 light bulbs.

Find the number *n* of ordered samples of:

(*a*) Size 3 with replacement, and

(*b*) Size 3 without replacement.

Solution:

(*a*) $n = 10^r$

$= 10^3 = 10 \times 10 \times 10 = 1{,}000$

and (*b*) $P(10, 3) = 10 \times 9 \times 8 = 720$

7.6 CIRCULAR PERMUTATIONS

Definition 7.5: A circular permutation of *n* objects is an arrangement of the objects around a circle.

In circular arrangements, we have to consider the relative position of the different things. The circular permutations are different only when the relative order of the objects is changed otherwise they are same.

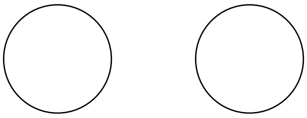


Fig. 7.1

7.6.1 Number of Circular Permutations

Definition 7.6: Let n distinct be given. If the n objects are to be arranged round a circle we take an objects and fix it in one position.

Now the remaining $(n - 1)$ objects can be arranged to fill the $(n - 1)$ positions the circle in $(n - 1)!$ ways.

Hence the number of circular permutations of n different objects = $(n - 1)!$

7.6.2 Number of Different Circular Permutations

We consider the order; clockwise or anti-clockwise of objects around a circle as the same circular permutation. Every arrangement with n objects round a circle is counted twice in $(n - 1)!$ circular permutations.

The total number of different permutations of n distinct objects is

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

Example 1: In how many ways can a party of 9 persons arrange themselves around a circular table?

Solution: One person can sit at any place in the circular table. The other 8 persons can arrange themselves in 8! ways i.e., the 9 persons can be arranged among themselves round the table in $(9 - 1)! = 8!$ ways.

Example 2: In how many ways 5 gents and 4 ladies dine at a round table, if no two ladies are to sit together?

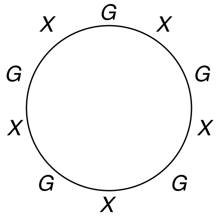


Fig. 7.2

Solution: Since no two ladies are to sit together, they should, seat themselves in between gents (i.e., a lady is to be seated in between two gents). The 5 gents can sit round the circular table in 5 positions (marked G in the Fig. 7.2). They can be arranged in $(5 - 1)! = 4!$ ways. The ladies can sit in the 4 out of 5 seats (marked X in Fig. 7.2). This can be done in P (5, 4) ways.

The required number of ways in which 5 gents and 4 ladies can sit round a table.

$$\begin{aligned} &= 4! \cdot P(5, 4) \\ &= (4 \cdot 3 \cdot 2 \cdot 1) \times (5 \cdot 4 \cdot 3 \cdot 2) \\ &= 2,880 \end{aligned}$$

Example 3: Twelve persons are made to sit around a round table. Find the number of ways they can sit such that 2 specified are not together.

Solution: 12 persons can sit round a table in (12 – 1)! = 11! ways.

The total number of ways in which 2 specified persons are together is 2! 10!.

The required number of seating arrangements in which 2 specified persons are not together.

$$= 11! - 2! \cdot 10!$$
$$= 11 \cdot 10! - 2! \cdot 10!$$
$$= 10\,!\,(11 - 2)$$
$$= 9 \cdot 10!$$

EXERCISE 7.2

1. In how many ways can 5 Telugu, 3 English, 2 Hindi books arranged on a shelf, if the books of each language are to be together?

2. Suppose a license plate contains two letters followed by three digits with the first digit not zero. How many different license plates can be printed?

3. How many license plates can be formed involving 3 English letters and 4 non-zero digits, if all the letters must appear either in the beginning or in the end.

4. From the digits 1, 2, 3, 4, 5, 6 how many three digit odd numbers can be formed, if the repetition of digits is not allowed?

5. There are 10 true-false questions on an examinations. How many sequences are possible?

6. Suppose that a state's license plates consists of three letter followed by three digits. How many different plates can be manufactured (if repetitions are allowed)?

7. Suppose a license plate contain 1 or 2 letters followed 3 digits. How many different license plates can be printed?

8. Suppose a license plate contains 3 English letters followed by 4 digits.

(*a*) How many different plates can be manufactured if repetition of letters and digits are allowed?

(*b*) How many plates are possible if only the letters are repeated?

(*c*) How many are possible if only the digits can be repeated?

9. Solve for n in $\dfrac{(n+2)!}{n!} = 56$

10. Find n if $\dfrac{(n+1)!}{(n-1)!} = 12$

11. A man wished to travel from one point in a city to a second point which is five blocks south and six blocks east of his starting point. In how many ways he make the journey if be always travels either south or east?

12. Find the number of ways of arranging the letter of the word TENNESSEE all at a time (*a*) if there no restriction (*b*) if the first two letters must be *E*.

13. Suppose a license plate contains three distinct letters followed by four digits with first digit not zero. How many different license plate can be printed?

14. In how many ways can 52 playing cards be distributed to four digits giving 13 cards each?

15. Find the number of arrangements that can be made out of the letters of the following words:

(*i*) Accountant

(*ii*) Independent

(*iii*) Assassination.

16. How many five digit numbers can be formed with the digits 2, 3, 5, 7, 9 which are:

(*a*) Odd

(*b*) Even

(*c*) Greater then 30,000

(*d*) Lie between 30,000 and 90,000.

17. In how many ways 6 rings be worn on 4 fingers when (*i*) there can be only one ring on each finger (*ii*) there can be any number of rings on each finger.

18. In how many ways 6 gents and 5 ladies dine at a round table, if no two ladies are to sit together?

19. If $P(n, 4)$: $P(n, 3) = 9$: 1 find n.

20. In how many ways 7 ladies and 7 gents can be seated at a round table; if no two ladies are to sit together?

21. In how many ways can 12 beads of which 3 are alike of one kind, 2 are alike of the another kind and the rest are different be formed into a ring?

22. In how many ways can 4 men and 3 ladies be arranged at a round table if the 3 ladies (*i*) never sit together (*ii*) always sit together?

23. How many words can be formed out of the letters of the word DAUGHTER, so that the vowels always occur together?

24. Suppose repetitions are not permitted.

(*a*) How many ways three digit numbers can be formed from the six digits 2, 3, 4, 5, 7 and 9?

(*b*) How many of these numbers are less than 400?

(*c*) How many are even?

(*d*) How many are odd?

(*e*) How many are multiples of 5?

25. Find the number of ways that three Americans, four French men, four Danes and two Italians can be seated in a row so that those of the same nationality sit together to solve the problem if they sit at a round table.

26. Find the member n of permutations that can be formal from all the letters of the word MISSISSIPPI.

27. Find n if $2\,P(n, 2) + 50 = P(2n, 2)$.

28. How many routes are there form the lower-left corner of an $n \times n$ square grid to the upper-right corner if we are restricted to travelling only to the right or, upward?

29. How many of the different permutations of the letters of word ENGLISH will (*i*) start with E (*ii*) start with E and end with N?

30. How many different numbers of six digits can be formed using the digits 0, 1, 2, 3, 4 and 5. How many of these are divisible by 5?

31. Twelve persons are made to sit around a table. Find the number of ways; they can sit such that 2 specifies persons are not together.

Answers:

1. 5! 3! 3! 2! **2.** 608400 **3.** $2 \times 26^3 \times 9^4$ **4.** 60 **5.** 1024 **6.** $26^3 \times 10^3$ **7.** $(26 + 26^2)\, 10^3$
8. $26^3 \times 10^4$, $26^3 \times 10 \times 9 \times 8\ 7$, $26 \times 25 \times 24 \times 10^4$ **9.** 6 **10.** 3 **11.** 924 **12.** (*a*) 3780 (*b*) 630
13. 14, 04, 00, 000 **14.** $52/(131)^4$ **15.** (*i*) 2,26,800, (*ii*) 7560 (*iii*) 10810800
16. (*a*) 96 (*b*) 24 (*c*) 96 (*d*) 72 **17.** 86, 200 **18.** 9 **19.** 3628800 **20.** 1663200 **21.** (*i*) 4320 (*ii*) 720
22. 4320 **23.** (*a*) 120 (*b*) 40 (*c*) 40 (*d*) 80 (*e*) 20

7.7 COMBINATIONS

Definition 7.7: A combination of *n* objects taken at a time is an unordered selection of *r* of the *n* objects ($r \leq n$).

A combination of *n* objects taken *r* at a time is also called *r*-combination of *n* objects.

Example 1: The two combinations of *a*, *b*, *c*, *d* taken two at a time are *ab*, *ac*, *ad*, *bc*, *bd* and *cd*.

Example 2: Consider the objects *a*, *b*, *c* from which the selections are to be made, by taking 2 objects at a time.

Solution: The 2-combinations are *ab*, *ac*, *bc*.

Example 3: The 3-combinations of four objects *a*, *b*, *c*, *d* taken 3 at a time are *abc*, *abd*, *acd*, *bcd*.

The number of combinations of *n* objects taken *r* at a time is demoted by *C* (*n*, *r*). The symbols $n_{(r)}$, n_{c_r}, $\binom{n}{r}$ and $c_{n,r}$ are also used to denote *r*-combinations of *n* objects.

Theorem 7.3: (Number of *r*-combinations without repetition). The number of *r*-combinations of *n* objects taken *r* at a time is

$$C(n_1\, r) = \frac{P(n,\, r)}{r!} = \frac{n!}{r!(n-r)!};\ (1 \leq r \leq n)$$

Proof: *r*-Combination means a selection of *r*-objects from the *n* objects, in which order of the objects does not matter. Each *r*-combination contains *r*-objects and these *r* objects can be arranged among themselves in *i*! ways. Hence each *r*-combination gives rise to *r*! permutations. Therefore, c(*n*, *r*) combinations will give rise to *c* (*n*, *r*). *r*! permutations. But the number of *r*-permutations of *n* objects is *P* (*n*, *r*).

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

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

$$= \frac{n!}{r!\,(n-r)!} \qquad \left(\therefore P(n,\, r) = \frac{n!}{(n-r)!}\right)$$

$$(1 \leq r \leq n)$$

Corollary 1:

$$C(n,\, n) = \frac{n!}{n!\,(n-n)!} = \frac{n!}{n!\ 0!} = 1 \qquad \text{(Boundary condition)}$$

Corollary 2:

$$C(n,0)=\frac{n!}{0!(n-0)!}=\frac{n!}{0!\ n!}=1 \qquad \text{(Boundary condition)}$$

Corollary 3: $C(n, r) = C(n, n - r)$ (Symmetric property)

Proof:

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

$$=\frac{n!}{(n-r)!\,\mathrm{r}!}=\frac{n!}{r!\,(n\bullet r)!}=c\,(n,r)$$

Corollary 4: If $C(n, x) = C(n, y)$ then either $x = y$ or $x + y = n$

Proof: $C(n, x) = C(n, y)$

$$\Rightarrow\ x=y \qquad \ldots \text{(i)}$$

and

$$C(n,x)=C(n,y)$$

$$\Rightarrow\ C(n,x)=C(n,n-y) \text{ (by cor. 3)}$$

$$\Rightarrow\ x=n-y$$

$$\Rightarrow\ x+y=n \qquad \ldots \text{(ii)}$$

from (*i*) and (*ii*) either $x = y$ or $x + y = n$

7.7.1 *r*-Subset

Definition 7.8: Let *A* be a set containing *n* elements. An *r*-subset of *A* is a selection of *r* elements of *A* without regard to the order.

Each *r*-subset is a *r*-combination and the number of r-subsets of *A* is

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

Combinationally $C(n, r)$ represents, the number of ways of choosing *r* objects from *n* distinct objects (i.e., number of ways of selecting *r* elements from the *n* elements of the set *A*).

7.8 POWER SET

Definition 7.9: If *A* is a set containing *n* objects, then the set containing all the subsets of *A* is called the power set of *A*.

The power set of *A* is denoted by $P(A)$ (or by 2^A).

Example 1: Set $A = \{1, 2\}$

Then $P(A) = \{\varnothing\ \{1\}, \{2\}, A\}$

Example 2: Let $A = \{a, b, c\}$

Then $P(A) = \{\varnothing\ \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

7.8.1 Number of Subsets of a Set

Let A be a non-empty set with n distinct objects: Each element of the set A either is a member of a particular subset of A or is not a member. The first element may either selected or not selected as a member of a subset. It can therefore be treated in two ways, selected or rejected. For each of these, the second element of the set may treated in two ways selected or rejected. Therefore, the first two elements may be treated in $2 \times 2 = 2^2$ ways. Similarly, the third element may be either selected or rejected in two ways for each of the 2^2 ways. Hence the first three elements may be treated in 2^3 ways. By continuing the argument, we can show the n elements of the set A can be treated in 2^{n} ways. Therefore, total number of subsets of A is 2^{n}.

i.e., if $$|A| = n,$$

then $$|P(A)| = 2^n$$

It may happen on certain occasions that we require the number of subsets of a set which contain repetitions of certain elements for example: consider the set $A = \{a, a, b, b, b, b, c\}$. A has seven elements of which 2 are alike of one kind and 4 are alike of a second kind.

For any subset we may select no, one or two a's. Hence a's may be selected in 3 ways. Similarly for each of these ways, the four b's may be selected in 5 ways. Therefore the a's and b's may be selected in $3 \times 5 = 15$ ways. The for each of these 15 ways the remaining element c can be selected in 2 ways. Therefore, the number of subsets of A is

$$3 \times 5 \times 2 = 30$$

In the same way, we may prove that the number of subsets of a set A of n elements, of which p are alike of one kind, q are alike of a second kind, and r are alike of a third kind, is

$$(p + 1)\,(q + 1)\,(r + 1)\,2^{n\text{-}p\text{-}q\text{-}r}$$

where $$(n \geq p + q + r)$$

Example 1: Find the number of subsets of

$$A = \{2, 2, 2, 3, 3, 5, 11\}$$

Solution: There are three 2's two 3's in the set. The remaining two elements i.e., 5 and 11 are distinct, we have $p = 3$, $q = 2$

The number of subsets of A is

$$(3 + 1)\,(2 + 1)\,2^{7-3-2}$$
$$= 4 \times 3 \times 2^2$$
$$= 48$$

Example 2: How many selections any number at a time, may be made from three white balls, four green balls, one red ball and one black ball, if atleast one must be chosen.

Solution: Total number of balls

$$= 3 \text{ white} + 4 \text{ green} + 1 \text{ red} + 1 \text{ black} = 9$$

we have $p = 3$, $q = 4$

Hence the number of selections that can be made is

$$(3 + 1)\,(4 + 1)\,2^{9-7}$$
$$= 4 \times 5 \times 2^2$$
$$= 80 \text{ (This includes the null set)}$$

If atleast are ball is to be chosen then the number of selections

$$= 80 - 1$$
$$= 79$$

7.8.2 Combinations of *n* things taking any number of them at a time when all the things are different

Each one of the n different things may either be selected or not selected i.e., there are two ways of selecting for each one of the n things.

$\therefore$ The total number of combinations of n things taking any number of things is 2^n.

But this includes the case in which all the things are rejected.

Hence the total number of ways in which one or more things are taken.

Corollary:

The total number of combinations of n things taken 1, 2, 3, …, n at a time i.e., $C(n, 1) + C(n, 1) + \ldots + C(n, n) = 2^n - 1$.

Example: In how many ways can a person invite one or more of his 5 friends to a party?

Solution: For every friend there are two possibilities i.e., he may be invited or he may not be invited to attend the party.

The number of ways in which we can invite his five friends at a party is 2^5.

But this includes the case when none of his friend is invited.

Hence, the number of ways in which he invites one or more of his five friends to a party is $2^5 - 1 = 32 - 1 = 31$

7.8.3 Combinations when all the given things are not different

Suppose that out of $m + n + p + \ldots$, things m are alike, and of one kind, n are alike and of second kind and the rest are different, say they are k in number.

Out of m things we may take 0, 1, 2, … or m. Hence there $(m + 1)$ ways of selecting the m things similarly, n things which are alike may be selected in $(n + 1)$ ways and, P things which are alike may be selected in $(P + 1)$ ways the remaing k different things may be selected in 2^k ways. These include the case in which all are rejected.

$\therefore$ The total numbers of combinations

$$= (m + 1)(n + 1)(p + 1)\, 2^k - 1$$

7.9 BASIC IDENTITIES

Example 1: Prove that $C(n, r) = C(n, n - r)$.

Solution:

Method 1: $C(n, r)$ denotes the number of selections of n objects when r-things are selected, and the remaining $(n - r)$ objects are not selected. Therefore, selecting of r-things is the same as discarding $(n - r)$ objects. For each selection of r things i.e., for each r-combination there is a discarding of $n - r$, remaing objects. The number of ways in which we discord $(n - r)$ objects is $C(n, n - r)$.

Since the set of r-combinations and the set of discarding of $(n - r)$ objects are in one-one corresponding we get

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

Method 2: See Corollary 3 of Theorem 7.

Example 2: (Pascal's Identity)

Show that $$C(n, r) = C(n - 1, r - 1) + C(n - 1, r)$$

Solution:

Method 1: $C(n, r)$ is the number of r-combinations of n objects. Let n be any one of the n objects. Fix the object x the $C(n, r)$ combinations can be grouped into:

(*i*) Those r-combinations that contain the objects x.

(*ii*) Those r-combinations that do not contain the object x.

Since the objects x is in all r-combinations of (*i*) we are to choose $(r - 1)$ objects in each combinations of (*i*) from the remaining $(n - 1)$ objects, this can be done in $C(n - 1, r - 1)$ ways.

The number of combinations that contain x, is

$$C(n - 1, r - 1)$$

To count the number of r-combinations of (*ii*) i.e., the number of r-combinations which do not contain x, we omit the objects x from n objects and choose r objects from the remaining $(n - 1)$ objects. Therefore, the number r-combinations that do not contain x is $C(n - 1, r)$.

Thus $$C(n, r) = C(n - 1, r - 1) + C(n - 1, r)$$

Method 2: Consider R.H.S.

$$C(n - 1, r - 1) + C(n - 1, r)$$

$$= \frac{(n-1)!}{(r-1)!\,(r-1-r+1)!} + \frac{(n-1)!}{r!\,(n-1-r)!}$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r)!} + \frac{(n-1)!}{r!\,(n-1-r)!}$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r)\,(n-r-1)!} + \frac{(n-1)!}{r\,(r-1)!\,(n-1-r)!}$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!}\left[\frac{1}{n-r} + \frac{1}{r}\right]$$

$$= \frac{(n-1)!}{(r-1)!\,(n-r-1)!}\left[\frac{r+n-r}{r\cdot(n-r)}\right]$$

$$= \frac{n\cdot(n-1)!}{r\cdot(r-1)!\,(n-r)\cdot(n-r-1)!}$$

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

Example 3: (Pascals row sum identity)

Show that $$C(n, 0) + C(n, 1) + \ldots + C(n, n) = 2^n$$

Solution: This is equivalent to finding the number of subsets of a set A with n elements. The number of subsets of A can be considered as follows:

The number of subsets having no elements (i.e., subsets with 0 elements is $C(n, 0)$

The number of subsets having 1 elements is $C(n, 1) \ldots$

The number of subsets with n elements is $C(n, n)$. Adding we get the number of elements in the power set of A.

i.e., $$|(A)| = C(n, 0) + C(n, 1) + \ldots + C(n, n)$$

but the number of elements in the power set of A is 2^n.

Hence $$C(n, 0) + C(n, 1) + \ldots + C(n, n) = 2^n$$

7.10 PARTITION AND CROSS PARTITIONS

7.10.1 Partition

Definition 7.10: Let S be a non-empty set. The collection $\{A_1, A_2, \ldots, A_r\}$ of subsets of S is a partition of S if and only if

(*i*) $S = A_1 \cup A_2 \cup \ldots \cup A_r$

(*ii*) For any $A_i, A_j \in S$

either $A_i = A_j$ or $A_i \cap A_j = \varnothing$

$A_1, A_2, \ldots, A_r$ are called cells of the partition and each A_i a non-empty subset of S.

7.10.2 Cross Partition

Definition 7.11: If $\{A_1, A_2, \ldots, A_r\}$ and $\{B_1, B_2, \ldots, B_p\}$ are both, partitions of a non-empty set S, then $\{A_i \cap B_j\}$ forms a partition of S. $\{A_i \cap B_j\}$ is called a cross-partition of S.

Example 1: Let $S = \{a, b, c, d, e, f, g, h\}$ and $A_1 = \{a, d, e\}$, $A_2 = \{b, c\}$, $A_3 = \{f\}$ $A_4 = \{g, h\}$ then $\{A_1, A_2, A_3, A_4\}$ forms a partition of S we observe that

(*i*) $A_1 \cup A_2 \cup A_3 \cup A_4 = S$, and

(*ii*) $A_i \cap A_j = \varnothing$ for all $A_i, A_j \in S$

7.10.3 Ordered Partition

Definition 7.12: A partition a non-empty set is called an ordered partition of S if there is a specified order on the subsets of S.

An ordered t-tuple of sets $\{A_1, A_2, \ldots, A_t\}$ is called a t-part ordered partition if the sets $A_1, A_2, \ldots, A_t$ form a partition of S.

Example 1: Let $S = \{a, b, c, d, e\}$ and $A_1 = \{a, b\}$, $A_2 = \{c\}$, $A_3 = \{d\}$, $A_4 = \{e\}$ $\{A_1, A_2, A_3, A_4\}$ is an ordered partition of S. It is a 4-part ordered partition.

Theorem 7.4: Let S contain n distinct objects. Then the number of ways S can be partitioned in r subsets $A_1, A_2, \ldots, A_r$ with P_1 objects in A_1, P_2 objects in $A_2 \ldots$, and P_r objects in A_r is

$$P(n; P_1, P_2, \ldots, P_r) = \frac{n!}{P_1!, P_2!, \ldots, P_r!}$$

Proof: Since the P_1 objects going into A_1 can be chosen in C (n, p_1) ways, the P_2 objects going into A_2 can be chosen in C $(n - p_1, p_2)$ ways, the P_3 objects going into A_3 can be chosen in $(n - p_1, - p_2, p_3)$ ways …, and the P_r objects going into A_r can chosen in C $(n - p_1, - p_2 - \ldots - p_{r-1}, p_r)$ ways the total number of partitions is

$$C\,(n, p_1)\; C\,(n - p_1, p_2)\; C\,(n - p_1, - p_2, p_3)\; C\,(n - p_1, - p_2 - \ldots, p_{r-1}, p_r)$$

$$= \frac{n!}{P_1!\,(n - P_1)!} \cdot \frac{(n - P_1)!}{P_2!\,(n - P_2)!} \cdot \frac{(n - P_1 - P_2)!}{P_3!(n - P_3)!} \cdots \frac{(n - P_1 - P_2 - \ldots, - P_{r-1})!}{P_r!\,0!}$$

$$= \frac{n!}{P_1!\,P_2! \ldots, P_r!}$$

Example 2: A farmer buys 4 cows, 2 goats and 5 ducks from a person who has 7 cows, 5 goats and 8 ducks. How many choices the farmer have:

Solution: The farmer can choose 4 cows from 7 cows in C (7, 4) ways, 2 goats from 5 goats in C (5, 2) ways and 5 ducks from 8 ducks in C (8, 5) ways.

∴ The farmer can choose 4 cows, 2 goats and 5 ducks in C (7, 4) C (5, 2) C (8, 5)

$$= \frac{7 \cdot 6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3 \cdot 4} \cdot \frac{5 \cdot 4}{1 \cdot 2} \cdot \frac{8 \cdot 7 \cdot 6}{1 \cdot 2 \cdot 3}$$

= 19,600 ways.

Theorem 7.5: The number of combination of $p_1 + p_2 + \ldots + p_r$ objects if p_1 are alike of one kind, p_2 are alike of another kind …, p_r are alike of rth kind is

$$(p_1 + 1)\,(p_2 + 1) \ldots (p_r + 1) - 1$$

Proof: Out of $(p_1, + p_2 + \ldots + p_r)$ objects, any number of objects can be selected, and each combination may contain any number of objects from 1 to $(p_1, + p_2 + \ldots + p_r)$ objects.

Consider P_1 objects out of the P_1 like things, none or 1 or 2 or 3 … all of the P_1 may be selected. Therefore, the number of combinations with P_1 like objects is $(P_1 + 1)$.

Similarly the number of possible combinations with P_2 like objects is $(P_2 + 1)$ …, the number of combinations of P_r objects is $(P_r + 1)$.

∴ The total number of combinations with $P_1 + P_2 + \ldots + P_r$ objects is

$$(P_1 + 1)\,(P_2 + 1) \ldots (P_r + 1)$$

but these combinations include the case in which all objects are rejected.

∴ The total number of combinations is

$$(P_1 + 1)\,(P_2 + 1) \ldots (P_r + 1) - 1$$

Example 3: There are twelve students in a class. Find the number of ways that the twelve students take three different tests if four students are to take each test.

Solution: We find the number of ordered partitions of twelve students into cells containing four students each. There are $\frac{12!}{4!\,4!\,4!}$ = 34,650 such partitions.

The required number of ways, the students can write the take the tests is 34,650.

Example 4: Find the number m of ways that a set X containing ten elements can be partitioned into two cells.

Solution: Let A denote a subset of X each A divides X into two disjoint sets A and (complement of A). Thus there are 2^{10} such divisions of X. This number includes the case in which $A = \varnothing$ and $A = X$ (i.e., improper subsets of X).

Hence the number of partitions $\left[A, \overline{A}\right]$ of X is $2^{10} - 2 = 1024 - 2 = 1022$ since each unordered partition determines two ordered partitions, we have

$$m = \frac{1022}{2} = 511$$

Thus, there are 511 partition of X into two non-empty disjoint cells.

7.11 PERMUTATIONS AND COMBINATIONS WITH UNLIMITED REPETITIONS

Let $U\left(n, r\right)$ denote r-permutations of n-objects with unlimited repetitions, and v (n, r) denote the number of r-combinations with unlimited repetitions, then

$$U\left(n, r\right) = n^r \text{ and } V\left(n, r\right) = C\left(n-1+r, n-1\right)$$

Consider the set $\left\{\infty \cdot a_1, \infty \cdot a_2, ..., \infty \cdot a_n\right\}$ where $a_1, a_2, \ldots, a_n$ are all distinct. Any r-combination is of the form $\left\{x_1 \cdot a_1, x_2 \cdot a_2, ..., x_n \cdot a_n\right\}$ where each x_i is a non-negative integer and $x_1 + x_2 + \ldots + x_n = r$.

The numbers $x_1 + x_2 + \ldots + x_n$ are called repetition numbers. Conversely any sequence of non-negative integers

$$x_1 + x_2 + \ldots + x_n, \text{ where } \sum_{i=1}^{n} x_i = r$$

corresponds to a r-combination $\left\{x_1 \cdot a_1, x_2 \cdot a_2, ..., x_n \cdot a_n\right\}$.

The following observations are made:

The number of r-combinations of $\left\{\infty \cdot a_1, \infty \cdot a_2, ..., \infty \cdot a_n\right\}$.

= The number of non-negative integers solution of $x_1 + x_2 + \ldots + x_n = r$.

= The number of ways of placing r indistinguishable balls in n numbered boxes.

= The number of binary numbers with $n - 1$ one's and r zeros.

$= C\ (n - 1 + r, r)$

$= C\ (n - 1 + r, n - 1)$

Example 1: Find the 4-combinations of {1, 2, 3, 4, 5, 6}.

Solution: The 4-combinations are

1234, 1235, 1236, 1245, 1246, 1256, 1345, 1346, 1356, 1456, 2345, 2346, 2456, 3456.

Example 2: Find the number of 3-combinations of $\left\{\infty \cdot a_1, \infty \cdot a_2, \infty \cdot a_3, \infty \cdot a_4\right\}$

Solution: We have $n = 4$, $r = 3$

The number of 3-combinations of the given set is $C\ (4 - 1 + 3, 3)$

$$= C\ (6, 3)$$
$$= 20$$

Example 3: Find the number of non-negative integral solutions to $n_1 + n_2 + n_3 + n_4 = 20$

Solution: We have $n = 4$, $r = 20$

The number of non-negative integral solutions

$$= C\ (4 - 1 + 20, 20)$$
$$= C\ (23, 20) = 1{,}771$$

Example 4: Find the number of 4-combinations of 5 objects with unlimited repetitions.

Solution: We have $n = 5$, $r = 4$

The number of 4-combinations

$$= C\ (5 - 1 + 4, 4)$$
$$= C\ (8, 4)$$
$$= 70$$

Example 5: Find the number of ways of placing 8 similar balls in 5 numbered boxes.

Solution: The number of ways of placing similar balls in 5 numbered boxes is

$$= C\ (5 - 1 + 8, 8)$$
$$= C\ (12, 8) = 495$$

Example 6: Find the number binary numbers with five 1's and three 0's.

Solution: The number of binary numbers with five 1's and three 0's is

$$= C\ (5 + 3, 3)$$
$$= C\ (8, 3)$$
$$= 56$$

Example 7: How many integral solutions are there to $x_1 + x_2 + x_3 + x_4 + x_5 = 16$, where each $x_i \geq 2$?

Solution: Let $x_i = y_i + 2$, where $y_i \geq 0$

We have $x_1 + x_2 + x_3 + x_4 + x_5 = 16$

$$\Rightarrow y_1 + 2 + y_2 + 2 + y_3 + 2 + y_4\ 2 + y_5 + 2 = 16$$
$$\Rightarrow y_1 + y_2 + y_3 + y_4 + y_5 = 6$$

The number of integral solutions of $x_1 + x_2 + x_3 + x_4 + x_5 = 16$ is the same as the number of integral solution of $y_1 + y_2 + y_3 + y_4 + y_5 = 6$.

$\therefore$ There are $C\ (\ 5 - 1 + 6, 6) = C\ (10, 6)$ such solutions.

Example 8: How many integral solutions are there of $x_1 + x_2 + x_3 + x_4 + x_5 = 30$, where $x_1 \geq 2, x_2 \geq 3, x_3 \geq 4, x_4 \geq 2, x_5 \geq 0$?

Solution: Let $x_1 = y_2 + 2$, $x_2 = y_2 + 3$, $x_3 = y_3 + 4$, $x_4 = y_4 + 2$, $x_5 = y_5 + 0$

$$x_1 + x_2 + x_3 + x_4 + x_5 = 30$$
$$\Rightarrow y_1 + 2 + y_2 + 3 + y_3 + 4 + y_4\ 2 + y_5 + 0 = 30$$
$$\Rightarrow y_1 + y_2 + y_3 + y_4 + y_5 = 19$$

The number of integral solutions of $x_1 + x_2 + x_3 + x_4 + x_5 = 30$, where $x_1 \geq 2, x_2 \geq 3, x_3 \geq 4, x_4 \geq 2, x_5 \geq 0$ is the same as the number of integral solutions of

$$y_1 + y_2 + y_3 + y_4 + y_5 = 19.$$

There are $C(5 - 1 + 19, 19) = C(23, 19)$ such solutions.

Example 9: How many outcomes are possible by costing a 6 faced die 10 times?

Solution: This is same as placing 10 similar balls into 6 numbered boxes.

There are $C(6 - 1 + 10, 10)$

$$= C(15, 10) \text{ possible outcomes.}$$

Example 10: Enumerate the number of non-negative integral solutions to the inequality.

$$x_1 + x_2 + x_3 + x_4 + x_5 \leq 19$$

Solution: We can express the problem as follows:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0$$
$$x_1 + x_2 + x_3 + x_4 + x_5 = 1$$
$$x_1 + x_2 + x_3 + x_4 + x_5 = 2$$
$$\ldots$$
$$x_1 + x_2 + x_3 + x_4 + x_5 = 19$$

The number of non-negative integral solutions of

$$x_1 + x_2 + x_3 + x_4 + x_5 = 0$$

is $C(5 - 1 + 0, 0)$.

The number of non-negative integral solutions of

$$x_1 + x_2 + x_3 + x_4 + x_5 = 1$$

is $C(5 - 1 + 1, 1)$.

∴ The number of non-negative integral solutions of

$$x_1 + x_2 + x_3 + x_4 + x_5 = 19$$

is $C(5 - 1 + 19, 19)$.

∴ The number of non-negative integral solutions of

$$x_1 + x_2 + x_3 + x_4 + x_5 \leq 19$$

is $C(5 - 1 + 0, 0) + C(5 - 1 + 1, 1) + \ldots + C(5 - 1 + 19, 19)$.

EXERCISE 7.3

1. If $C(n + 1, r + 1)$: $C(n, r)$: $C(n - 1, r - 1)$: 11:6:3, find n and r.

2. A committee of seven is to be formed from a boys and 5 girls. In how many ways can this be done, when the committee contains?

(*i*) Exactly three girls.

(*ii*) Atleast three girls.

3. Among 20 members of a team, there are two wicket keepers and five bowlers. In how many ways can eleven persons be chosen to include only one wicket keeper and atleast three bowlers?

4. How many different seven-person can be formed each containing 3 women from the available set of 20 women and 4 men from an available set of 30 men?

5. In how many ways can a person invite one or more of his seven friends to a party?

6. How many triangles can be formed by joining 12 points, 7 of which are in the same straight line?

7. In how many ways 5 white balls and 3 black balls can be arranged in a row so that no two black balls may be together?

8. In how many ways can a committee of 6 men and 2 women be formed out of 10 men and 5 women?

9. A student is two answer out of 10 questions in an examination

(*i*) How many choices he has?

(*ii*) How many, if he must answer the first three questions?

(*iii*) How many, if he must answer atleast four of the five questions?

10. Out of 4 officers and 10 clerks in an office, a committee consisting of 2 officers and 3 clerks is to be formed. In how many ways committee be done if:

(*i*) Any officers and any clerk can be included?

(*ii*) Are particular clerk must be on the committee?

(*iii*) Are particular officer cannot be on the committee?

11. If $C(n, 15) = C(n, 27)$ find the value of $C(n, 30)$.

12. If $P(n, r) = 5040$, and $C(n, r) = 210$, find n and r.

13. From 6 consonants and 4 vowels how many words can be made, each containing 4 consonants and 3 vowels?

14. A committee of 8 is to be selected out of 6 males and 8 females. In how many ways can it be formed so that the male way not be out numbered?

15. There are twelve points in a given plane, no three of them on the same time. How many lines are determined by these points?

16. In how many ways can three or more persons be selected from twelve persons?

17. Which regular polygon has the same number of diagonals as sides?

18. Find the regular polygon which has twice as many diagonals as sides.

19. Find the number of triangles that can be formed by the vertices of an octagon.

20. Find the number of ways in which 9 toys can be divided evenly among three children.

21. Find the number of ways in which fourteen people can be partitioned into six committees, where two of the committees contain three people each and the remaining four committees contain two people each.

22. In how many ways can a cricket eleven be selected out of 14 players when the captain is always to be included?

23. A box contains 2 white balls, 3 black balls and 4 red balls. In how many ways three balls be drawn from the box if atleast are black ball is to be included in the draw?

24. How many different possible outcomes are possible by tossing 6 similar coins?

25. There are 5 true and false questions in an examination. How many sequences of answers are possible?

26. Find the 3-combinations of $\{3\ a, 2\ b, 2\ c, 1\ d\}$.

27. There are 25 true or false questions on an examination. How many different ways can a students do the examination, if he or she can also choose to leave the answer blank?

28. Find the number of 4-combinations of $\{\infty \cdot a_1, \infty \cdot a_2, \infty \cdot a_3, \infty \cdot a_4, \infty \cdot a_5\}$.

29. Find the number of 3-combinations of 5-objects with unlimited repetitions.

30. Find the number of non-negative integral solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = 50$.

31. How many integral solutions are there to $x_1 + x_2 + x_3 + x_4 + x_5 = 20$, where each $x_i \geq 2$?

32. Find the number of integral solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = 20$,
where $x_1 \geq 3, x_2 \geq 2, x_3 \geq 4, x_4 \geq 6, x_5 \geq 0$.

33. Enumerate the number of placing 20 indistinguishable balls into 5 boxes, where each box is non-empty.

34. How many different outcomes are possible form tossing 10 similar dice?

35. Enumerate the number of non-negative integral solutions to the in equality $x_1 + x_2 + x_3 + x_4 + x_5 \geq 19$.

36. Find the number of integral solutions to $x_1 + x_2 + x_3 + x_4 + x_5 = 50$,
where $x_1 \geq 4, x_2 \geq 7, x_3 \geq -14, x_4 \geq 10$.

37. Find the number of 10-permutations of $\{3\ a, 4\ b, 2\ c, 1\ d\}$.

Answers:

1. $n = 10, r = 5$ **2**. (*i*) 1260, (*ii*) 1716 **3**. 54054 **4**. 31, 241, 700 **5**. 127 **6**. 185 **7**. 20
8. 2100 **9**. (*i*) 45 (*ii*) 21 (*iii*) 35 **10**. (*i*) 720 (*ii*) 210 (*iii*) 360 **11**. 496 **12**. $n = 10, r = 4$
13. 302400 **14**. 1414 **15**. 66 **16**. 4017 **17**. Pentagon **18**. 7 sides (Heptagon) **19**. 56
20. 1680 **21**. 3153150 **22**. $C(13, 10)$ **23**. 64 **24**. 7 **25**. 32
26. *aaa*, *aab*, *aac*, *aad*, *bba*, *bbd*, *cca*, *ccb*, *ccd*, *abc*, *abd*, *acd*, *bcd*. **27**. 3^{25} **28**. 70 **29**. 35
30. 316, 251 **31**. $C(14, 10)$ **32**. $C(9, 5)$ **33**. $C(19, 15)$ **34**. 3003
35. $C(5 - 1 + 0, 4) + C(5 - 1 + 1, 4) + \ldots + C(5 - 1 + 19, 4)$ **36**. $C(54, 3)$ **37**. 12, 600

7.12 THE PIGEONHOLE PRINCIPLE

In this section, we discuss the Pigeonhole principle. It is also known as the Dirichlet's drawer principle or the shoe box principle and it can be stated as follows:

Theorem 7.6: If n pigeons are assigned to m pigeonholes and $m < n$, then some pigeonhole contains atleast two pigeons.

Proof: Let $h_1, h_2, \ldots, h_m$ denote the m pigeonholes and $P_1, P_2, \ldots, P_m, P_{m+1}, \ldots, P_n$ denote the n pigeons (where $m < n$).We consider the assignment of the n pigeons to m pigeonholes as follows:

Assign pigeon p_1 to the pigeonhole h_1, pigeon p_2 to the pigeonhole h_2, …, and pigeon p_m to the pigeonhole h_m.

This assigns as many pigeons possible to individual pigeonholes. Since $m < n$, there are *pi* $(n - m)$ pigeons that have not yet been assigned. Atleast one pigeonhole will be assigned a second pigeon.

Example 1: If ten people are chosen in any way, show that atleast two of then will have been born on the same day.

Solution: There are ten people and the number of days in a week is only seven. If each person (pigeon) is assigned to the day of the week (pigeonhole) on which he or she is born, the pigeonhole principle tells us that two more people must be assigned to the same day of the week.

In the above example, the people (objects) are taken as the pigeons and the days of the week as taken as pigeonholes. In general, to apply pigeonhole principle, we must identify the pigeons i.e., the objects and the pigeonholes i.e., categories of the desired characteristic. Also we must be able to count the number of pigeons and pigeonholes.

Example 2: Show that if seven numbers from to 1 to 12 are chosen, then two of them will add upto 13.

Solution: Construct six different sets, each containing two numbers that add up to 13 as follows $x_1 = \{1, 12\}$, $x_2 = \{2, 11\}$, $x_3 = \{3, 10\}$, $x_4 = \{4, 9\}$, $x_5 = \{5, 8\}$, $x_6 = \{6, 7\}$. Each of the seven numbers belong to one of these six sets. Since there are six sets, the pigeonhole principle tells us that two of the numbers chosen belong to the same set. These numbers add upto 13.

Theorem 7.7: (The extended pigeonhole principle)

If n pigeons are assigned to m pigeonholes, then one of the pigeonholes must contain atleast $\lfloor n/m \rfloor + 1$ pigeons [$\lfloor p/q \rfloor$ denotes the largest integer less than or equal to the rational number p/q].

Proof: We prove the theorem by contradiction. Let each pigeonhole contain no more than $\lfloor (n-m)/m \rfloor$ pigeons. Then, there are at most $m \cdot \lfloor (n-1)/m \rfloor$ pigeons in all but $\lfloor (n-1)/m \rfloor \leq m\ (n-1)/m.$

$$\Rightarrow \lfloor (n-1)/m \rfloor = n-1$$

i.e., there $(n - 1)$ pigeons in all. This contradicts our assumption. Hence one of the pigeonholes must contain atleast $\lfloor (n-1)/m \rfloor + 1$ pigeons.

Example 3: Show that if any 26 people are selected, then we may choose a subset of 4 so that all 4 were born on the same day of the week.

Solution: We assign each person to the day of the week on which she or he was born. Then the number of pigeons (people) are to be assigned to 7 pigeonholes (days of the week). With $n = 26$ and $m = 7$.

Therefore atleast $\lfloor (26-1)/7 \rfloor + 1$, that is 4 people must have been born on the same day of the week.

Example 4: Show that there are atleast 6 different ways to choose 3 numbers from 1 to 10, so that all choices have the some sum.

Solution: Three numbers can be choses from the 10 numbers in $10_{C_3} = 120$ ways

The least sum = 1 + 2 + 3 = 6

The largest sum that we can get from this numbers 1 to 10 is 8 + 9 + 10 = 27

We have 22 such sums inclusive of 6 and 27

Let A be the set of sums obtained by taking three numbers from 1 to 10, then

$$A = \{6, 7, 8, ..., 27\}$$

If each sum is taken as a pigeonhole, then atleast one of the pigeonhole must contain

$$\left\lfloor \frac{120-1}{22} \right\rfloor + 1 = 5 + 1 = 6 \text{ pigeons,}$$

i.e., one pigeonhole contains atleast 6 different ways of 3 numbers having the same sum.

EXERCISE 7.4

1. Show that if any five numbers from 1 to 8 are chosen, then two of them will add upto 9.
2. If eight people are chosen, in any way from a group show that, atleast two of them will have been born on the same day of the week.
3. Show that if any 30 people are selected, then we may chose a subset of 5 so that all 5 were born on the same day of the week.
4. Prove that if any 14 numbers from 1 to 25 are chosen, then one of them is a multiple of another.
5. Show that if any 11 numbers are chosen from the set {1, 2, ..., 20}, then one of them will be a multiple of another.
6. If 20 processors are interconnected, show that atleast two processors are directly connected to the same number of processors.

7.13 BINOMIAL THEOREM

In this section, we obtain the formula for the expansion of $(a + b)^n$. The Binomial theorem gives a formula for the coefficients in the expansion of $(a + b)^n$. Since

$$(a + b)^n = \underbrace{(a + b)(a + b) \ldots (a + b)}_{n - \text{factors}}$$

the expansion results from selecting either a or a from each of the n factors. Multiplying the selection together, and then summing all such products obtained. Let us consider the expansion of $(a + b)^3$ as an example:

$$\begin{aligned}(a + b)^3 &= (a + b)\,(a + b)\,(a + b)\\ &= (a + b)\,[(a + b)\,(a + b)]\\ &= (a + b)\,[(a + b)\,a + (a + b)\,b]\\ &= (a + b)\,(aa + ba + ab + bb)\\ &= a\,[aa + ba + ab + bb] + b\,[aa + ba + ab + bb]\\ &= aaa + aba + aab + abb + baa + bba + bab + bbb\end{aligned}$$

There are eight terms in the expansions of which some are alike. Each term is a product three factors, the first being obtained from the first binomial; the second from the second binomial, and the third from the third binomial in $(a + b)\,(a + b)\,(a + b)$. All such possible selections are included in the eight terms. Each of the eight terms is a product of three letters are selected from each of the binomial factors. In the expansion a^3 (i.e., aaa) appears only once; $a^2\,b$ (i.e., aba, aab, bba) appears three times, ab^2 (i.e., abb, bba, bab) appears three times and b^3 (i.e., bbb) appears only once.

Therefore, we can write

$$(a + b)^3 = a^3 + 3a^2\,b + 3ab^2 + b^3$$

We observe that each term of this expansion is formed by selecting one and only one term from each of the three binomial factors; multiplying these together, and adding like products. We can select either none, one, two or three b's. If we select one a from each of factor. This can be done in only C (3, 0) one way. This gives the first term aaa i.e., a^3. If we select one b, we can select it from any one of the three factors. This can be done in C (3, 1) = 3 ways. For each of these selections. We must select one a from each of the other two factors, and this can be done in only one way. Hence, we have three terms each equal to $a^2\,b$ giving the second term $3a^2\,b$. We may how select two b's from the three factors in C (3, 2) = 3 ways, and an a must be selected in one way from the remaining factor. This gives the term $3ab^2$. Finally, we select three b's in C (3, 3) = 1 way and obtain the term $bbb = b^3$. Therefore, we can write

$$(a + b)^3 = C\,(3, 0)\,a^3 + C\,(3, 1)\,a^2\,b + C\,(3, 2)\,ab^2 + C\,(3, 3)\,b^3$$

$$= a^3 + 3a^2\,b + 3ab^2 + b^3$$

$$= \sum_{r=0}^{3} C(3, r)\,a^{3-r} \cdot b^r$$

we now consider the expansion of $(a + b)^n$ where a and b are real numbers and n is a positive integer.

Theorem 7.8: (The Binomial theorem)

Let n be a positive integer then for all a and b.

$$(a + b)^n = C\,(n, 0)\,a^n + C\,(n, 1)\,a^{n-1}\,b + C\,(n, 2)\,a^{n-2}\,b + \ldots + C\,(n, r)\,a^{n-r}\,b^r + \ldots + C\,(n, n)\,b^n$$

$$= \sum_{r=0}^{n} C(n, r)\,a^{n-r} \cdot b^r$$

Proof: **First Proof**

$$(a + b)^n = (a + b)\,(a + b)\,\ldots\,n \text{ factors}$$

Each term in the expansion is obtained by forming the product of one term each binomial factor.

Therefore each term in the expansion is of the form

$$a^{n-r}\,b^r\;(r = 0, 1, 2, \ldots, n)$$

The term $a^{n-r}\,b^r$ known as the general term is formed by selecting one b from each of r of the n factors. This can be done in C (n, r) ways. For each of these ways, the (n – r) a's can be selected, one from each of the remaining (n – r) binomial factors, in only one way. Hence coefficient of $a^{n-r}\,b^r$ is C (n, r). Therefore

$$(a + b)^n = \sum_{r=0}^{n} c(n, r)\,a^{n-r} \cdot b^r$$

$$= C\,(n, 0)\,a^n + C\,(n, 1)\,a^{n-1}\,b + C\,(n, 2)\,a^{n-2}\,b^2 + \ldots + C\,(n, r)\,a^{n-r}\,b^r + \ldots + C\,(n, n)\,b^n$$

Second Proof (Proof by mathematical induction)

Let r denote the set of all positive integers, we use the identities:

$$C\,(n, r) + C\,(n, r + 1) = C\,(n + 1, r + 1),$$

and

$$C\,(k, k) = C\,(k + 1, k + 1) = 1.$$

Let S be the set of positive integers for which:

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

Taking $x = 1$, we obtaining

$$\sum_{r=0}^{1} C(1, r) \cdot a^{1-r} \cdot b^r = C(1, 0)\, a^1\, b^0 + C(1, 1)\, a^0\, b^1$$

$$= a + b$$

The theorem holds for $x = 1$, i.e., $1 \in S$.

Assume that the theorem is true for $n = k$, i.e., $K \in S$, hence

$$\begin{aligned}(a+b)^k &= \sum_{r=0}^{k} C(k, r)\, a^{k-r} \cdot b^r \\ &= C(k, 0)\, a^k + C(k, 1)\, a^{k-1} b + \ldots + C(k, r-1) a^{k-r+1} b + C(k, r)\, a^{k-r} b^r + \ldots + C(k, k) b^k.\end{aligned}$$

Then

$$\begin{aligned}(a+b)^{k+1} &= (a+b)\,(a+b)^k \\ &= a\,(a+b)^k + b\,(a+b)^k \\ &= C(k, 0)\, a^{k+1} + C(k, 1)\, a^k b + C(k, 2)\, a^{k-1} b^r + \ldots + \\ &\qquad C(k, r-1) a^{k-r+1} b^{r-1} + C(k, r)\, a^{k-r+1} b^r + \ldots + C(k, k)\, ab^k. \\ &= C(k, 0)\, a^k b + C(k, 1)\, a^{k-1} b^2 + C(k, 2)\, a^{k-2} b^3 + \ldots + \\ &\qquad C(k, r-1) a^{k-r+1} b^r + C(k, r)\, a^{k-r+1} b^{r+1} + \ldots + C(k, k)\, b^{k+1}. \\ &= C(k, 0)\, a^{k+1} + [C(k, 0) + C(k, 1)]\, a^k b + [C(k, 1) + C(k, r)]\, a^{k-1} b^r + \ldots + \\ &\qquad [C(k, r-1) + C(k, r)]\, a^{k-r+1} b^r + \ldots + C(k, k)\, b^{k+1}. \\ &= C(k+1, 0)\, a^{k+1} + C(k+1, 1)\, a^k b + C(k+1, 2)]\, a^{k-1} b^r + \ldots + \\ &\qquad C(k+1, r)\, a^{k-r+1} b^r + \ldots + C(k+1, k+1)\, b^{k+1}. \\ &= \sum_{r=0}^{k+1} C(k+1, r)\, a^{k+1-r} \cdot b^r\end{aligned}$$

Therefore, the theorem is true for $x = k + 1$ also i.e., $k + 1 \in S$, if $k \in S$

Hence $S = N$

i.e., by the principle of mathematical induction the theorem is true for all positive integers and

$$(a+b)^n = \sum_{r=0}^{n} C(n, r)\, a^{n-r} \cdot b^r \text{ for all } n \in N$$

We note the following in the expansion:

(*i*) The number of terms in the expansion of $(a + b)^n$ is $n + 1$.

(*ii*) The general term is $C(x, r)\, a^{n-r}\, b^r$ (i.e., $(r + 1)$ the term is the general term). It is denote by T_{r+1}.

(*iii*) The coefficients of terms equidistant from ends of the expansion are equal.

7.13.1 Pascals Triangle

Consider the following expansions:

$$(a + b)^0 = 1$$
$$(a + b)^1 = a + b$$
$$(a + b)^2 = a + 2ab + b^2$$
$$(a + b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$$
$$(a + b)^4 = a^4 + 4a^3 b + 6a^2 b^2 + 4ab^3 + b^4$$
$$(a + b)^5 = a^5 + 5a^4 b + 10a^3 b^2 \ 10a^2 b^3 + 5ab^4 + b^5$$

It can be seen that the coefficients follow a definite pattern which can be most easily demonstrated by means of triangle known as Pascal's Triangle.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

Fig. 7.3

We can form the lines of the triangle by using the identity

$$C(x, r) + C(x, r + 1) = C(x + 1, r + 1).$$

Example 1: Expand $(2a + b)^4$.

Solution:

$$(2a + b)^4 = C(4, 0)(2a)^4 + C(4, 1)(2a)^3 b + C(4, 2)(2a)^2 b^2 + C(4, 3)(2a) b^3 + C(4, 4) b^4.$$
$$= 16a^4 + 32a^3 b + 24 a^2 b^2 + 8 ab^3 + b^4.$$

Example 2: Find the general term in the expansion of $\left(x^3 + \frac{1}{x}\right)^{10}$.

Solution:

$$\left(x^3 + \frac{1}{x}\right)^{10} = \left(x^3 + x^{-1}\right)^{10}$$

the general term in the expansion is

$$\begin{aligned} T_{r+1} &= C(10, r)(x^3)^{10-r}(x^{-1})^r \\ &= C(10, r)\, x^{30-3r}\, x^{-r} \\ &= C(10, r)\, x^{30-4r} \end{aligned}$$

Example 3: Find the term containing a^4 in the expansion of $\left(a - \frac{2}{a}\right)^8$.

Solution: The general term is

$$T_{r+1} = C(8,\, r)\, a^{8-r} \left(\frac{-2}{a}\right)^r$$
$$= C(8,\, r)\, a^{8-r} \left(-2a^{-1}\right)^r$$
$$= C(8,\, r)\, a^{8-r} (-2)^r \left(a^{-1}\right)^r$$
$$= C\ (8,\, r)\ (-2)^{\mathrm{r}}\, a^{8-\mathrm{r}}\, a^{-\mathrm{r}}$$
$$= C\ (8,\, r)\ (-2)^{\mathrm{r}}\, a^{8-2\mathrm{r}}$$

Putting $8 - 2r = 4$, we get $r = 2$

Hence the term containing a^4 is

$$T_{r+1} = T_3 = C\ (8,\, r)\ (-r)^{\mathrm{r}}\, a^4$$
$$= C\ (8,\, r)\ 4\ a^4$$
$$= 28\ 4\ a^4$$
$$= 112\ a^4$$

Example 4: Find the term independent of x in the expansion of $\left(x^2 + \frac{1}{x}\right)^{12}$.

Solution:

$$\left(x^2 + \frac{1}{x}\right)^{12} = \left(x^2 + x^{-12}\right)^{12}$$

The general term in the expansion of $(x^{\mathrm{r}} + x^{-1})^{12}$ is

$$T_{r+1} = C\ (12,\, r)\ (x^2)^{12-\mathrm{r}}\, (x^{-1})^{\mathrm{r}}$$
$$= C\ (12,\, r)\ x^{24-2\mathrm{r}}\, x^{-\mathrm{r}}$$
$$= C\ (12,\, r)\ x^{24-3\mathrm{r}}$$

If $\qquad 24 - 3r = 0$

$$3r = 24 \Rightarrow r = 8$$

Hence, the coefficient x^0 is C (12, 8)

i.e., the term independent of x is C (12, 8) = 495

7.13.2

Replacing a by x and b by 1 we can write binomial theorem as:

$$(x+1)^n = \sum_{r=0}^{n} C(n,\, r)\, x^{n-r} = \sum_{r=0}^{n} C(n,\, n-r)\, x^{n-r}$$

$$= \sum_{r=0}^{n} C(n, r)\, x^r = (1 + x)^n$$

Consider $$(1 + x)^n = \sum_{r=0}^{r} C(n, r)\, x^r$$

replacing x by $-x$, we have

$$(1 - x)^n = \sum_{r=0}^{n} C(n, r)(-x)^r = \sum_{r=0}^{n} C(n, r)(-1)^r\, x^r$$

taking $a = b = 1$ binomial theorem can be written as

$$(1 + 1)^n = C\,(n, 0) + C\,(n, 1) + \ldots + C\,(n, n)$$

$$2^n = C\,(n, 0) + C\,(n, 1) + \ldots + C\,(n, n)$$

(refer Example 3, Pascal's row sum identity under Section 7.9)

If we set $a = 1$ and $b = -1$ in the binomial theorem, we get.

$$(1 - 1)^n = C\,(n, 0) - C\,(n, 1) + C\,(n, 2) + \ldots + (-1)^n\, C\,(n, n)$$

or $$C\,(n, 0) - C\,(n, 1) + \ldots + (-1)^n\, C\,(n, n) = 0$$

which shows that the alternating sum of the members of any row of Pascal's triangle is zero. This can also be written as

$$C\,(n, 0) + C\,(n, 2) + C\,(n, 4) + \ldots = C\,(n, 1) + C\,(n, 3) + \ldots$$

The coefficients

$$C\,(n, 0), C\,(n, 1), C\,(n, 2)\,, \ldots, C\,(n, n)$$

are called Binomial coefficients. These coefficients can also be written as,

$$C_0, C_1, C_2, \ldots, C_n$$

7.14 SOLVED EXAMPLES

Example 1: Prove that $C\,(n, 1) + C\,(n, 3) + \ldots = C\,(n, 0) + C\,(n, 2) + \ldots = 2^{n-1}$.

Solution: We know that

$$n\,(C, 1) + n\,(C, 3) + n\,(C, 5) + \ldots = n\,(C, 0) + n\,(C, 2) + n\,(C, 4)$$

Let S denote the common total of these sums. Adding right-hand side to the left, we get

$$C\,(n, 0) + C\,(n, 1) + C\,(n, 2) + C\,(n, 4) + \ldots + C\,(n, n) = 2s$$

$$\Rightarrow\; 2^n = 2s$$

$$\Rightarrow\; S = 2^{n-1}.$$

Example 2: In the expansion of $(1 + x)^{\mathrm{n}}$, prove that

$$C_0^{\,2} + C_1^{\,2} + C_2^{\,2} + \ldots + C_n^{\,2} = \frac{2n!}{(n!)^2}$$

Solution: We have

$$(1 + x)^{\mathrm{n}} = C\,(n, 0) + C\,(n, 1)\,x + \ldots + C\,(n, n)\,x^n \qquad \ldots \text{(i)}$$

We know that the coefficients of the terms equivalent from the beginning and end are equal, therefore, we can write

$$(1 + x)^n = C(n, n) + C(n, n-1)\,x + \ldots + C(n, 0)\,x^n \qquad \ldots \text{(ii)}$$

multiplying (*i*) and (*ii*), we get

$$(1 + x)^{2n} = [C(n, 0) + C(n, 1)\,x + \ldots + C(n, n)\,x^n]\; x\; [\,C(n, n) + C(n, n-1)\,x + \ldots + C(n, 0)]\; x^n$$

from the right hand side, we see that the coefficients of x^{n} is

$$C(n, 0)^2 + C(n, 1)^2 + \ldots + C(n, n)^2.$$

But the coefficient of x^{n} in $(1 + x)^{2\mathrm{n}}$ is given by

$$C(2n, n) = \frac{2n!}{n!\cdot n!} = \frac{2n!}{(n!)^2}$$

$$C_0^{\,2} + C_1^{\,2} + C_n^{\,2} = \frac{2n!}{(n!)^2}$$

Example 3: If $(1 + x)^{\mathrm{n}} = C(n, 0) + C(n, 1)\,x + C(n, 2)\,x^2 + \ldots + C(n, n)x^n$.

Prove that $C(n, 1) + 2\,C(n, 2) + 3\,C(n, 3) + \ldots + n\,C(n, n) = n\,2^{n-1}$.

Solution:

$$C(n, 1)\,x + 2\,C(n, 2)\,x^2 + \ldots + n\,C(n, n)x^n$$

$$= nx + 2\cdot\frac{2(n-1)}{2\cdot !}\,x^2 + \ldots + n\,x^n$$

$$= nx + n\,(n-1)\,x^2 + \ldots + n\,x^n$$

$$= nx\,[1 + (n-1)\,x + \ldots + x^{n-1}]$$

$$= nx\,[C(n-1, 0) + C(n-1, 1)x + \ldots + C(n-1, n-1)x^{n-1}]$$

$$= nx\,(1 + x)^{n-1}$$

Putting $x = 1$ on both sides, we get

$$C(n, 1) + 2\cdot C(n, 2) + \ldots + n\cdot C(n, n) = n\cdot 2^{n-1}$$

Example 4: If $C(n, 0), C(n, 1), C(n, 2), \ldots, C(n, n)$ are the coefficients in the expansion of $(1 + x)^{\mathrm{n}}$, prove that:

$$C(n, 0)\,C(n, r) + C(n, 1),\,C(n, r+1) + \ldots + C(n, n-r)\,C(n, n) = \frac{2n!}{(n-r)!\,(\mathrm{n}+\mathrm{r})!}$$

Solution: We know that

$$(1 + x)^n = C(n, 0) + C(n, 1)\,x + C(n, 2)\,x^2 + \ldots + C(n, r)\,x^r + \ldots + C(n, n-1)\,x^{n-1} + C(n, n)\,x^n \qquad \ldots \text{(i)}$$

writing in the reverse order we get

$$(1 + x)^n = C(n, n)\,x^2 + C(n, n-1)\,x^{n-1} + \ldots + C(n-1)\,x + C(n, 0) \qquad \ldots \text{(ii)}$$

Since $\quad C(n, r) = C(n, n-r)$

we have $C(n, n) = C(n, 0)$, $C(n, n-1) = C(n, 1)$

we can therefore write

$$(1 + x)^n = C(n, 0)x^n + C(n, 1)\,x^{n-1} + C(n, 2)\,x^{n-2} + \ldots + C(n, n-1)\,x + C(n, n) \qquad \ldots \text{(iii)}$$

multiplying (i) and (ii) and equating the coefficient of x^{n+r} on both sides we get

$$C(n, 0) + C(n, r) + C(n, 1) + C(n, r+1) + C(n, 2)\, C(n, r+2) + \ldots + C(n, n-r)\, C(n, n)$$

$$= \text{Coefficient of } x^{n+r} \text{ in } (1+x)^{2\mathrm{n}}$$

$$= C(2n, n+r)$$

$$= \frac{2n!}{(n+r)!\,(\mathrm{n}-\mathrm{r})!}$$

Example 5: Prove that

$$\frac{C(n,1)}{C(n,0)} + 2\cdot\frac{C(n,2)}{C(n,1)} + 3\cdot\frac{C(n,3)}{C(n,2)} + \ldots + n\,\frac{C(n,n)}{C(n,n-1)} = \frac{n(n+1)}{2}$$

Solution: We know that

$$\frac{C(n,1)}{C(n,0)} = \frac{n}{1} = n,$$

$$2\cdot\frac{C(n,2)}{C(n,1)} = \frac{\frac{2\cdot(n-1)}{1\cdot 2}}{\frac{n}{1}} = \frac{n(n-1)}{n} = n-1$$

$$3\cdot\frac{C(n,3)}{C(n,2)} = \frac{\frac{3\cdot n(n-1)(n-2)}{1\cdot 2\cdot 3}}{\frac{n(n-1)}{1\cdot 2}} = n-2$$

$$n\,\frac{C(n,n)}{C(n,n-1)} = n\cdot\frac{1}{n} = 1$$

Adding, we get

$$\frac{C(n,1)}{C(n,0)} + 2\cdot\frac{C(n,2)}{C(n,1)} + 3\cdot\frac{C(n,3)}{C(n,2)} + \ldots + n\,\frac{C(n,n)}{C(n,n{-}1)}$$

$$= n + (n-1) + (n-2) + \ldots + 1 \leq 1 + 2 + 3 + \ldots + (n-1) + n$$

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

7.15 MULTINOMIAL THEOREM

The binomial theorem can be extended to give a formula powers of multinomials $(x_1 + x_2 + \ldots + x_t)^n$ as follows:

Theorem 7.9: The Multinomial Theorem

Let n be a positive integer, then for all $x_1 + x_2 + \ldots + n_t$

$$(x_1 + x_2 + \ldots + x_t)^{\mathrm{n}} = \sum P\ (n; q_1, q_2, \ldots, q_t)\ x_1^{q_1}\ x_2^{q_2} \ldots x_t^{q_t}$$

where the summation extends over all sets of non-negative integers $q_1, q_2, \ldots, q_t$ where $q_1 + q_2 + \ldots + q_t = n$.

Proof: The coefficient of $x_1^{q_1}\ x_2^{q_2}\ \ldots\ x_t^{q_t}$ is the number of ways of arranging n letters

$$\{q_1\, x_1, q_2\, x_2, \ldots, q_t\, x_t\}$$

The coefficient of $x_1^{q_1}\ x_2^{q_2}\ \ldots\ x_t^{q_t}$ is $(n; q_1, q_2, \ldots, q_t)$

Hence

$$(x_1 + x_2 + \ldots + n_t)^{\text{n}} = \sum P\ (x; q_1, q_2, \ldots, q_t)\ x_1^{q_1}\ x_2^{q_2}\ \ldots\ x_t^{q_t}$$

In the above expansion, $x_1^{q_1}\ x_2^{q_2}\ \ldots\ x_t^{q_t}$ is a selecting of n objects with repetition from t distinct types. The number of ways of selecting the objects is $C\ (n + t - 1, n)$.

Therefore, the number of terms in the expansion of $(x_1 + x_2 + \ldots + n_t)^{\text{n}}$ is $C\ (n + t - 1, n)$.

Example 1: Find the coefficients of $x^5\ y^{10}\ z^5\ w^5$ in the expansion of $(x + 7\,y + 3\,z + w)^{25}$.

Solution: We have $n = 25$, $x_1 = x_1$, $x_2 = 74$, $x_3 = 3\,z$, and $x_4 = w$

$\therefore$ The coefficients of $x^5\ y^{10}\ z^5\ w^5$ in the expansion of $(x + 7\,y + 3\,z + w)^{25}$ is

$$P\ (25, 5, 10, 5, 5) = \frac{20!\,1^5 \cdot 7^{10} \cdot 3^5 \cdot 1^5}{5!\,10!\,5!\,5!}$$

Example 2: Find the number of terms in the expansion of $(2x + 3y - 5z)^8$.

Solution: We have $n = 8$, $t = 3$

Hence the number of terms is

$$\begin{aligned} C\ (n + t - 1, n) &= C\ (8 + 3 - 1, 8) \\ &= C\ (10, 8) = 45 \end{aligned}$$

EXERCISE 7.5

1. Expand $(1 - x + x^{\text{r}})^4$ in ascending powers of x.
2. Find the 10th term of $\left(2x^2 + \frac{1}{x}\right)^{12}$.
3. Find the term independent of x in the expansion of $\left(2x^2 - \frac{1}{x}\right)^{12}$.
4. Prove that the term independent of x in the expansion of $\left(x - \frac{1}{x^2}\right)^{3n}$ is $(-1)^n\ \frac{3n!}{n!(2n)!}$.
5. Give a combinational proof for Pascal's column sum identify given by
$$C\ (r, r) + C\ (r + 1, r) + \ldots + C\ (n, r) = C\ (n + 1, r + 1)$$
6. Prove the Pascal's diagonal sum identity
$$C\ (n + 1, r) = C\ (n + 1, 1) + C\ (n + 2, 2) + \ldots + C\ (n + r, r)$$
7. Use the diagonal sum identity of Pascal to show that
$$1\ .\ 2 + 2\ .\ 3 + \ldots + n\ (n + 1) = n\ (n + 1)\ (n + 2)\ /3.$$

8. Prove that following by combinational argument:

(*i*) $C\,(2n, 2) = 2\,C\,(n, 2) + n^2$

(*ii*) $(n - r)\,C\,(n, r) = n\,C\,(n - 1, r)$

9. Show that

$$C\,(n, 0) + C\,(n + 1, 1) + C\,(n + 2, 2) + \ldots + C\,(n + r, r) = C\,(n + r + 1, r)$$

10. Prove that

$$C\,(n, 0) + 2\,C\,(n, 1) + 2^2\,C\,(n, 2) + \ldots + 2^{\text{n}}\,C\,(n, n) = 3^{\text{n}}$$

11. Show that

$$\frac{(1 + x)^n + (1 - x)^n}{2} = C\,(n, 0) + C\,(n, 2)\,x^2 + \ldots + C\,(n, q)\,x^{\text{q}}$$

where $q = n$ if n is even

$n - 1$ if n is odd

12. Show that the product of *r* consecutive integers is divisible by *r*!.

13. State and prove Binomial theorem.

14. State Multinomial theorem.

15. In the expansion of $(1 + px)^{\text{n}}$, the first three terms are 1, $5x$, $\frac{45x^2}{4}$. Find the values of *n* and *p*.

16. Find the coefficient of $x_1^{\,2}\,x_3\,x_4\,x_5^{\,4}$ in the expansion of $(x_1 + x_2 + x_3 + x_4 + x_5)^{10}$. Also find the number of terms in the expansion.

17. Find the coefficient of $x^3\,y^3\,z^2$ in the expansion of $(2x - 3\,y + 5\,z)^8$.

18. In the expansion of $\left(a^2 - \frac{1}{a^3}\right)^n$ the fifth term in $10a^{-4}$.

Find the value of *n*.

19. In the expansion of $(ax + by)^n$ the coefficients of the first three terms are 729, 486, and 135 respectively, if $a > 0$. Find the values of *a*, *b* and *n*.

20. Find the coefficient of $x^2\,y^3\,z^2$ in $(x + y + z)^7$.

Answers:

1. $1 - 4x + 10x^2 - 16x^3 + 19x^4 - 16x^5 + 10x^6 - 4x^7 + x^8$. **2**. $\frac{1760}{x^2}$ **3**.7920 **15**. $P = \frac{1}{2}$, $n = 10$

16. 12,600, 1001 **17**. $(2^3)\,(-3)^3\,(5)^2\,(560)$ **18**. $n = 8$ **19**. $a = 3$, $b = \frac{1}{3}$, $n = 6$ **20.** 210.

8

Graph Theory

8.1 INTRODUCTION

Graph theory is intimately related to many branches of mathematics. It is widely applied in subjects like, Computer Technology, Communication Science, Electrical Engineering, Physics, Architecture, Operations Research, Economics, Sociology, Genetics, etc. In the earlier stages it was called slum Topology.

Euler, Cayley, Sir William Hamilton, Lewin, and Kirchoff, laid foundations to the graph theory. Graph theory was born in 1736 with Euler's paper on Konigsberg bridge problem. The Konigsberg bridge problem is the best known example in graph theory. It was a long pending problem. Euler solved this problem by means of a graph. Euler became father of graph theory. Kirchoff, Cayley, Mobius, Hamilton and De Morgan have laid strong foundations and contributed much to the development of the subject. In this chapter, basic concepts and terms of graph theory have been introduced.

8.2 BASIC DEFINITIONS

8.2.1 Graph

Definition 8.1: A graph G is a pair of sets (V, E), where V is a non-empty set. The set V is called the set of vertices and the set E is called the set of edges (or lines).

A graph may be represented by a diagram in which each vertex is represented by a point in the plane and each edge is represented by a straight line (or curve) joining the points. The objects shown below (*see* Fig. 8.1) are graphs.

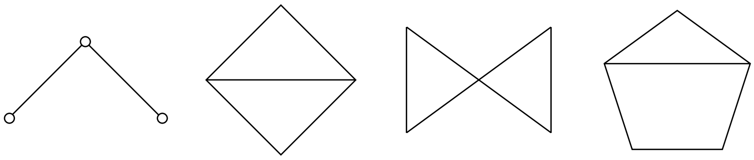


Fig. 8.1

Note:

(*i*) In a graph $G = (V, E)$, the sets V and E are assumed to be finite sets.

(*ii*) A vertex of a graph is called a node, a point; a junction or 0-cell. An edge of a graph is called a line, a branch, a 1-cell or an arc.

(*iii*) If $G = (V, E)$; {or $(V(G), E(G))$} is a graph, then the number of vertices in G is denoted by $|V|$ $(|V(G)|)$, and the number of edges in a is denoted by $|E|$ (or $|E(G)|$).

(*iv*) If $\{u, v\}$ is an edge in a graph G, then the vertices u and v are said to be adjacent.

8.2.2 Non-Directed Graph

Definition 8.2: Let $G = (V, E)$ be a graph. If the elements of E are unordered pairs of vertices of G then G is called a non-directed graph.

The graph in Fig. 8.2 are non-directed graphs

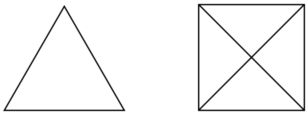


Fig. 8.2

Note: If e is an edge of a non-directed graph G, connecting the vertices u and v of G, then it is denoted by $e = \{u, v\}$. The points u and v are called the end points of the edge e.

8.2.3 Directed Graph (or Digraph)

Definition 8.3: Let $G = (V, E)$ be a graph. If the elements of E are ordered pairs of vertices, then the graph G is called a directed graph.

Note: If e is an edge of a directed graph G, denoted by $e = (u, v)$, then e is a directed edge in G. The edge e begins at the point u and ends at u. The vertex u is called the origin or initial point of the directed edge e and v is called the destination or terminal point of e. The graphs in Fig. 8.3 are directed graphs.

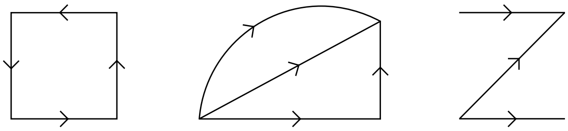


Fig. 8.3 Digraphs

8.2.4 Self-Loop

Definition 8.4: An edge associated with the unordered pair $\{v_i, v_i\}$ where $v_i \in V$ of a graph $G = (V, E)$ is called a self-loop in a graph G is an edge joining a vertex to itself.

In Fig. 8.4, there is a loop incident on the vertex v.

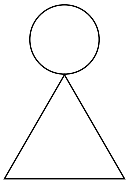


Fig. 8.4

8.2.5 Multigraph

Definition 8.5: A graph which allows more than one edge to join a pair of vertices is called a Multigraph.

Fig. 8.5 (*a*) is a multigraph in which, we have

$$G = \{\{a, b\}, \{a, d\}, 2\ (a, c), (c, d)\}$$

Fig. 8.5 (*b*) is a multigraph in which, we have

$$G = \{\{a, b\}, \{a, c\}, 3\ \{b, d\}, \{c, d\}, \{a, d\}\}$$

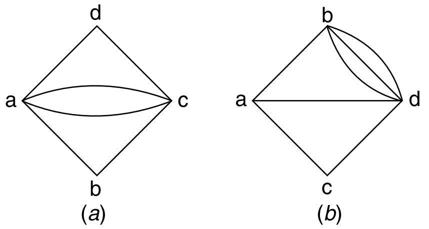


Fig. 8.5 Multigraph

8.2.6 Simple Graph

Definition 8.6: A graph *G* with no self-loops is called a simple graph.

The graphs in Fig. 8.6 are simple graphs.

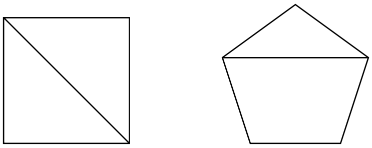


Fig. 8.6 Simple graphs

8.2.7 Non-Simple Graph

Definition 8.7: If graph *G* is not a simple graph, then it is called a non-simple graph (*see* Fig. 8.7)

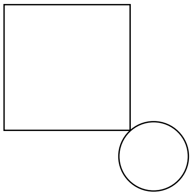


Fig. 8.7 Non-Simple graph

8.2.8 Null Graph

Definition 8.8: A graph *G* = (*V*, *E*) in which the set of edges *E* is empty is called a Null graph (*see* Fig. 8.8.)

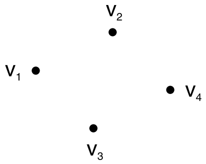


Fig. 8.8 Null graph

Note: A finite graph with one vertex and no edges is called a trivial graph.

8.2.9 Weighted Graph

Definition 8.9: A graph G is in which weight are assigned to every edge is called a weighted graph (Fig. 8.9)

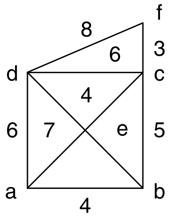


Fig. 8.9 Weighted graph

8.2.10 Finite Graph

Definition 8.10: A graph $G = (V, E)$ in which both $V(G)$ and $E(G)$ are finite sets is called a finite graph.

8.2.11 Pseudograph

Definition: A graph having loops but no multiple edges is called a Pseudograph (*see* Fig. 8.10)

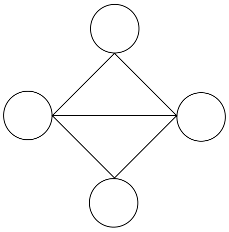


Fig. 8.10 Pseudograph

8.3 INCIDENCE AND DEGREE

Definition 8.11: Let G be a non-directed graph. An unordered pair $\{u, v\}$ is an edge incident on u and v. If G is a directed graph. An edge $\{u, v\}$ is said to be incident from u and to be incident to v.

8.3.1 Indegree

Definition 8.12: In a directed graph G, the number of edges ending at vertex v of G is called the indegree of v.

The indegree of a vertex v of G is denoted by $\deg^{+}_{G}(v)$ (or by indeg (v)).

Example: In the graph given below (Fig. 8.11) the indegree of the vertex V_1 is 3:

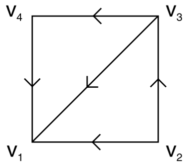


Fig. 8.11

8.3.2 Outdegree

Definition 8.13: Let G be a directed graph and v be a vertex of G. The outdegree of v is the number of edges beginning at v.

The outdegree of a vertex v in G is denoted by $\deg^{-}_{G}(v)$ (or by outdeg (v)).

In the Fig. 8.12, the outdegree of the vertex v_1 is 2.

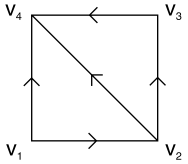


Fig. 8.12

8.3.3 Degree of a Vertex

In a non-directed graph G, the degree of a vertex v is determined by counting each loop incident on v twice and each other edge once. The degree of the vertex v in G is denoted by $d(v)$ or by $\deg_G(v)$ and is defined as follows:

Definition 8.14: The number of edges incident with a vertex v of a graph, with self-loops counted twice is called the degree of the vertex v. The degree of a vertex is sometimes referred to as its valency.

Note: A vertex of odd degree is an odd vertex of G and that of even degree is called even vertex.

Example 1: In the graph of Fig. 8.13

$$\deg(v_1) = 1, \deg(v_2) = 3, \deg(v_3) = 1, \deg(v_4) = 1,$$

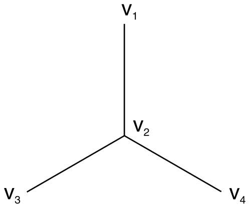


Fig. 8.13

Example 2: In the graph of Fig. 8.14, we have deg $(v_1) = 3$, deg $(v_2) = 4$, deg $(v_3) = 2$, deg $(v_4) = 3$ or $d_1 = 3, d_2 = 4, d_3 = 2, d_4 = 3$

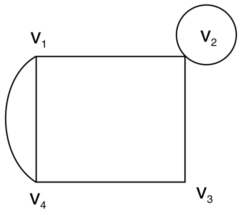


Fig. 8.14

8.3.4

Minimum degree and maximum degree: For a graph $G = (V, E)$, we introduce the following symbols:

δ (G) = Minimum of all the degrees of the vertices of a graph G.

Δ (G) = Maximum of all the degrees of the vertices of a graph G.

Thus

$$\delta\ (G) = \min \{\deg\ (v_i) : v_i \in V\}$$

$$\Delta\ (G) = \max \{\deg\ (v_i) : v_i \in V\}$$

8.3.5 Labeled Graph

Definition 8.15: A graph G in which each vertex is assigned a unique label is called a labeled graph.

The graph G in Fig. 8.15 is a labeled graph.

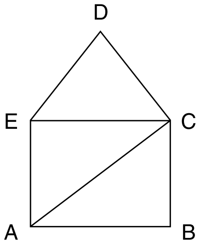


Fig. 8.15 Labeled graph

8.3.6 Isolated Vertex

Definition 8.16: A vertex of degree zero in a graph is called an Isolated vertex.

The vertex v_4 in Fig. 8.16 is an Isolated vertex.

Note: An Isolated vertex in a graph G has no edges incident with it. Every vertex in a null graph is an isolated vertex.

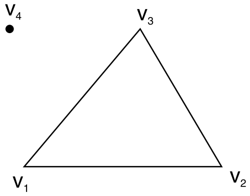


Fig. 8.16

8.3.7 Pendant Vertex

Definition 8.17: A vertex of a graph with degree one is called a pendant vertex. (or an end vertex). In the graph shown in Fig. 8.17, the vertices v_1 and v_4 are pendant vertices.

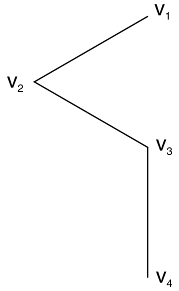


Fig. 8.17

8.3.8 *K*-regular Graph

Definition 8.18: A graph *G* is said to be *k*-regular, if every vertex of *G* has degree *k*.

Note:

(*i*) For a *k*-regular graph

$$\delta(G) = \Delta(G) = K$$

i.e., all the vertices (points) of *G* have the same degree *K*.

(*ii*) A regular graph of degree zero has no lines.

(*iii*) In a regular graph of degree 1, every component contains exactly one line.

(*iv*) If *G* is a 2-regular graph, then every component has a cycle.

(*v*) If *G* is a regular graph of degree 3, it is called a cubic graph. (*see* Fig. 8.18). Every cubic graph has an even number of points.

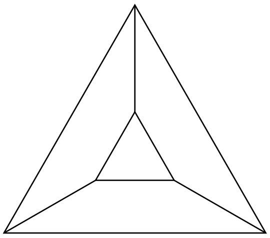


Fig. 8.18 Cubic graph

8.3.9 Complete Graph

Definition 8.19: A simple graph G, in which every pair of distinct vertices are adjacent is called a complete graph. If G is a complete graph of n vertices then it is denoted by k_n.

Figure 8.19 shows K_3 K_4 and K_5.

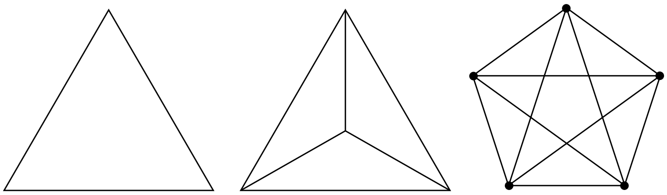


Fig. 8.19 Complete graphs K_3, K_4 and K_5.

Note:

(i) In a complete graph, there is an edge between every pair of vertices.

(ii) K_n is called $(n - 1)$-regular graph.

(iii) K_n has exactly $\frac{n(n-1)}{2}$ edges.

8.4 ORDER OF A GRAPH

Definition 8.20: If $G = (V, E)$ is a finite then the number of vertices denoted by $|V|$ is called the order of G.

Thus, the cardinality of the vertex set V of G the order of G.

Example: The graph shown in Fig. 8.20 is of order 6.

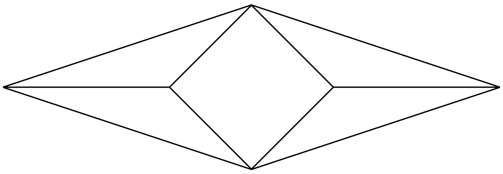


Fig. 8.20

8.5 SIZE OF A GRAPH

Definition 8.21: If $G = (V, E)$ is a finite graph, then the number of edges in G is called the size of G. It is denoted by $|E|$ (cardinality of E).

Example 1: The size of the graph shown in Fig. 8.21 is 6.

We shall often refer to a graph of order n and size m an (n, m)-graph.

If G is a (p, q) graph, then G has p vertices (points) and q edges (lines).

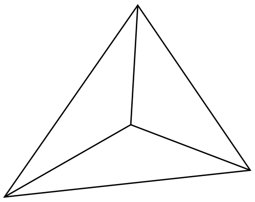


Fig. 8.21

Example 2: Let $V = \{v_1, v_2, v_3, v_4\}$, and

$E = \{(v_1, v_2), (v_1, v_3), (v_1, v_4)\}$

$G = (V, E)$ is a (4, 3) graph G can be represented by the Fig. 8.22.

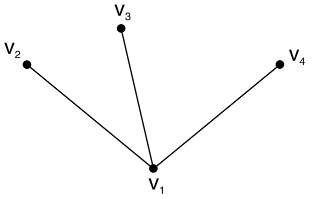


Fig. 8.22

8.5.1 Degree Sequence of a Graph

Definition 8.22: Let G be graph with $v = \{v_1, v_2, v_3, ..., v_n\}$ as the vertex set. Also let $d_i = \deg(v_i)$, then the sequence $(d_1, d_2, ..., d_n)$ in any order is called the degree sequence of G.

Note:

(*i*) The vertices of a graph G, are ordered so that the degree sequence is monotonically increasing so that

$$\delta(G) = d_1 \le d_2 \le d_3 \le ... \le d_n = \Delta(G)$$

(*ii*) The set of distinct non-negative integers occurring in a degree sequence of a graph G is called its degree set.

(*iii*) Two graphs with the same degree sequence are said to be degree equivalent.

(*iv*) It is customary to denote the degree sequence in power notation.

If (2, 2, 2, 3, 3, 4, 5, 5, 6) is the degree sequence of a graph G, then it is represented in power notation as $2^3\ 3^2\ 4^1\ 5^2\ 6^1$, the degree set being (1, 2, 3).

Example: Consider the graph shown in Fig. 8.23.

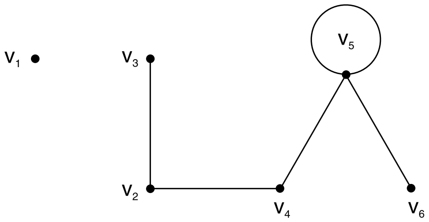


Fig. 8.23

We have $d(v_1) = 0$, $d(v_2) = 2$, $d(v_3) = 1$, $d(v_4) = 2$, $d(v_5) = 4$, $d(v_6) = 1$

v_1 is not adjacent with any other vertex of G, hence v_1 is an isolated vertex of G.

The degree sequence of G is (0, 1, 1, 2, 2, 4). There are two vertices of odd degree in G (The vertices v_3 and v_6 are odd).

Theorem 8.1:

(*i*) The sum of degrees of the vertices of a non-directed graph G is twice the number of edges in G i.e.,

$$\sum_{i=1}^{n} \deg(v_i) = 2|E|$$

(*ii*) If G is a directed graph

$$\sum_{i=1}^{n} \deg_G^-(v_i) = \sum_{i=1}^{n} \deg_G^+(v_i)$$

where $|V|$ = number of vertices in $G = n$

Proof:

(*i*) Let G be a non-directed graph. Each edge of G is incident with two vertices and hence contributes 2 to the sum of degree of all the vertices of the non-directed graph G.

Then the sum of degrees of all the vertices in G is twice the number of edges in G.

i.e.,
$$\sum_{i=1}^{n} \deg_G(v_i) = 2|E|$$

(*ii*) Let G be digraph and e be an edge associated with a vertex pair (v_p, v_q). The edge e contributes one to the outdegree of v_p and one to the indegree of v_q. This is true for all the edges in G.

Hence
$$\sum_{i=1}^{n} \deg_G^+(v_i) = \sum_{i=1}^{n} \deg_G^-(v_i) = |E|$$

Corollary 1: In a non-directed graph, the number of vertices of odd degree vertices is even.

Proof: Let $G = (V, E)$ be a non-directed graph. Let W denote the set of odd degree vertices and U denote the set of even degree vertices in G.

Then
$$\sum_{v_i \in V} \deg(v_i) = \sum_{v_i \in W} \deg(v_i) + \sum_{v_i \in U} \deg(v_i)$$

or
$$\sum_{v_i \in V} \deg(v_i) - \sum_{v_i \in U} \deg(v_i) = \sum_{v_i \in W} \deg(v_i) \qquad \text{... (i)}$$

$\sum_{v_i \in V} \deg(v_i)$ is even and $\sum_{v_i \in U} \deg(v_i)$ is also even, therefore

$\sum_{v_i \in V} \deg(v_i) - \sum_{v_i \in U} \deg(v_i)$ is even; i.e. L.H.S. of (*i*) is even

Thus each deg (v_i) on R.H.S. is odd the number of summands must be even.

$\therefore$ The number of odd degree vertices in G is even.

Corollary 2: If $K = \delta(G)$, is the minimum degree of the vertices of a non-directed graph $G = (V, E)$ then

$$K\,|V| \leq 2\,|E|$$

in particular, if G is a k-regular graph then

$$K\,|V| = 2\,|E|$$

If G is a simple graph, then G is without parallel edges or self-loops. Let G be a simple graph with one vertex. The number of edges in G is zero i.e., (1–1). The maximum degree of a vertex in a simple graph G with one vertex is zero. If G is a simple graph with 2 vertices then the maximum degree of any vertex in a is 1 = (2–1). In general it can be shown that the maximum degree of any vertex in a simple graph with n vertices is (n–1). This can be stated in the form a theorem as follows:

Theorem 8.2: The maximum degree of any vertex in a simple with n vertices is $n - 1$.

8.6 SOLVED EXAMPLES

Example 1: Draw a simple graph with 3 vertices.

Solution: The graph shown in Fig. 8.24 is a simple graph with 3 vertices.

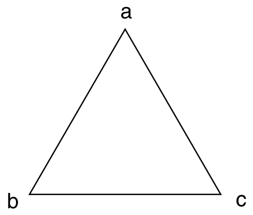


Fig. 8.24

Example 2: Draw a graph representing the problem of three houses and three utilities say water, gas and electricity.

Solution: Let H_1, H_2 and H_3 denote the houses. The utilities, water, gas and electricity be denoted by W, G and E respectively. The houses can be connected by the utilities as shown Fig. 8.25.

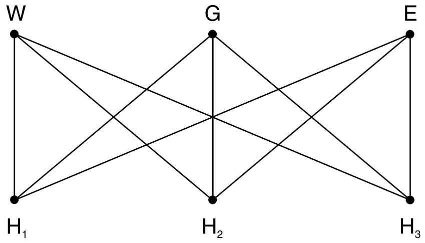


Fig. 8.25

Example 3: Draw the graphs of the chemical compounds.

(*a*) $C_2 H_6$ (*b*) $C_4 H_{10}$

Solution: (*a*) The graph of $C_2 H_4$ is

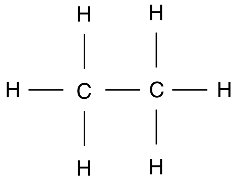


Fig. 8.26 (*a*)

(*b*) The graph of $C_4 H_{10}$ is

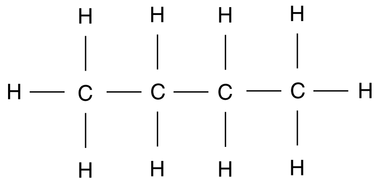


Fig. 8.26 (*b*)

Example 4: Represent the graph

$$G = \{(1, 2, 3, 4), (x, 4): |x - 4| \leq 1)\}$$

Solution: We have

$$V = \{1, 2, 3, 4\}$$
$$E = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3), (3, 4)\}$$

and $G = (V, E)$ is a non-directed graph. It can be represented as shown in Fig. 8.27.

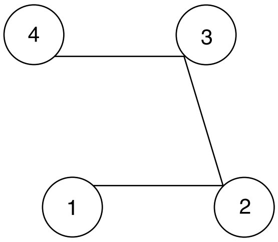


Fig. 8.27

Example 5: For the graph shown in 8.28. Verify $\sum \deg (v_i) = 2\,|E|$

Solution: We have $V = \{v_1, v_2, v_3, v_4, v_5\}$

$$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7)$$
$$d_1 = \deg (V_1) = 3, d_2 = \deg (V_2) = 4, d_3 = \deg (V_3) = 2,$$
$$d_4 = \deg (V_4) = 3, d_5 = \deg (V_5) = 1 \text{ and } |E| = 7$$

$$\sum \deg(v_i) = d_1 + d_2 + d_3 + d_4 + d_5$$

$$= 3 + 4 + 3 + 3 + 1 = 14$$

$$\therefore \quad \sum \deg(v_i) = 14 = 2 \times 7 = 2\,|E|$$

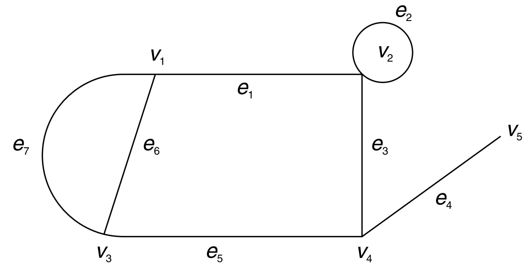


Fig. 8.28

Example 6: A sequence $d = (d_1, d_2, \ldots d_n)$ is graphic, if there is a simple non-directed graph with the degree sequence d. Show that the following sequences are not graphic:

(*i*) (2, 3, 4, 5, 6, 7) (*ii*) (2, 2, 4)

Solution: (*i*) The number of odd vertices in the degree sequence is 3 i.e., odd and the number of vertices in $G = 6$.

Maximum degree of any vertex in a simple graph is $= n - 1 = 6 - 1 = 5$. But the maximum degree in the given degree sequence is 7, therefore the given degree sequence is not graphic.

(*ii*) The graph contains 3 vertices. The maximum degree in the graph must be $(3 - 1) = 2$, but the maximum degree in the sequence is 4. Hence, the given degree sequences is not graphic.

Example 7: Draw a picture of the following graph and state whether it is directed or non-directed and whether it is simple:

$G = (V, E)$ where

$V = \{a, b, c, d, e\}$ and $E = \{(a, b), (a, c), (a, d), (a, e), (e, e), (c, d), (a, a), (b, c), (c, c)\}$.

Solution: The given graph G is a directed graph and is not simple:

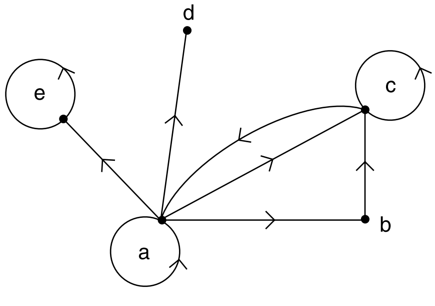


Fig. 8.29

Example 8: Find the order and size of the graph G shown in Fig. 8.30:

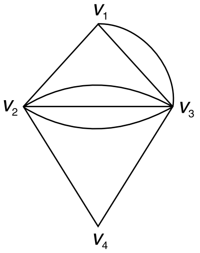


Fig. 8.30

Solution:

$$|V| = \text{order of } G = 4$$
$$|E| = \text{size of } G = 8$$

Example 9: Give an example of:

(*i*) A Simple graph,

(*ii*) A Pseudo graph, and

(*iii*) A Multigraph.

Solution:

(*i*) Figure 8.31 (*a*) is a Simple graph.

(*ii*) Figure 8.31 (*b*) is a Pseudo graph.

(*iii*) Figure shown in 8.31 (*c*) is a Multigraph.

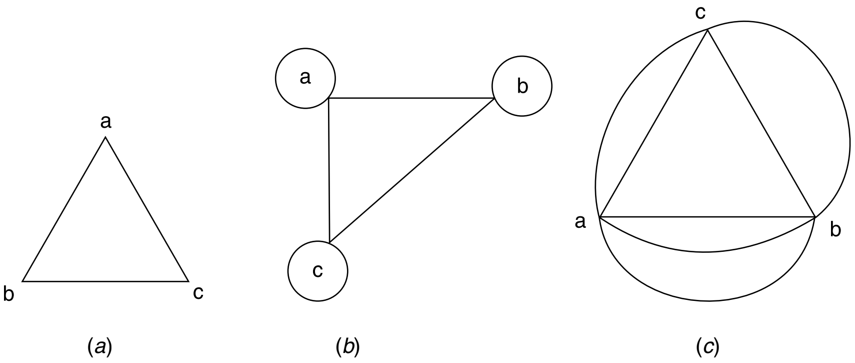


Fig. 8.31 (*a*) Simple Graph (*b*) Pseudo Graph (*c*) Multigraph

Example 10: Draw a non-simple graphs G with degree sequence (1, 1, 3, 3, 3, 4, 6, 7).

Solution: G is non-directed, therefore G permits self-loops in it. It be drawn as shown in Fig. 8.32.

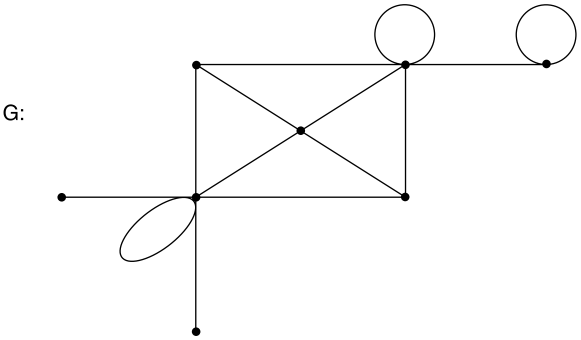


Fig. 8.32

Example 11: Show that every cubic graph has even number of vertices.

Solution: Let G be a cubic graph with p vertices.

The $$\sum \deg(v_i) = 3p \qquad \ldots \text{(i)}$$

L.H.S. of (i) is even, therefore R.H.S. i.e., $3p$ is even hence p is even.

Example 12: If $G = (V, E)$ is a (p, q) graph then show that $\delta \le \frac{2q}{p} \le \Delta$.

Solution: Let $V = \{v_1, v_2, ..., v_p\}$ then we have $\delta \le \deg(v_i) \le \Delta$

or $$p\,\delta \le \sum_{i=1}^{p} \deg(v_i) \le p\,\Delta$$

or $$p\,\delta \le 2\,q \le p\,\Delta$$

Hence $$\delta \le \frac{2q}{p} \le \Delta$$

Example 13: Suppose G is a non-directed graph with 12 edges. If G has 6 vertices each of degree 3 and the rest have degree less than 3, what is the minimum number of vertices G can have?

Solution: Number of edges in $G = 12$

Hence $$\sum \deg(v_i) = 2\,|E| = 2 \times 12 = 24$$

we have 6 vertices of degree 3. Let n denote the number of vertices each of whose degree is less than 3.

Then $$\sum \deg(v_i) < 6.3 + 3x$$

or $$24 < 18 + 3x$$

or $$3x > 6$$

or $$x > 2$$

The least positive integer for which the inequality $x > 2$ holds is $x = 3$.

Hence, the minimum number of vertices G can have is $3 + 6 = 9$.

Example 14: A non-directed graph G has 8 edges. Find the number of vertices, if the degree of each vertex is 2.

Solution: Given $|E| = 8$

We have

$$\sum_{i=1} \deg(v_i) = 2\,|E|$$

i.e., $2\,|V| = 2 \times 8$

or $|V| = 8$

Thus number of vertices in $G = 8$

Example 15: Show that a simple graph of order 4 and size 7 does not exist.

Solution: Let G be a group with order 4 and size 7, we have $|V| = n = 4$ and $|E| =$ number of edges = 7 Maximum number of edges in G

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

$$= \frac{1}{2}\,4(4-1)$$

$$= 6$$

Maximum number of edges, G can have is 6

It is given that number of edges in G is 7

$$|E| = 7 > 6$$

which is contradiction

Hence, G cannot exist

i.e., there cannot be a Simple graph with order 4 and size 7.

EXERCISE 8.1

1. Define:

(*a*) Graph

(*b*) Self-loop

(*c*) Digraph

(*d*) Multigraph

(*e*) Pseudo graph

(*f*) Order of a graph

(*g*) Size of a graph

Give examples.

2. Draw a diagram for each of the following graphs:

(*a*) $V = \{(a, d), (a, f), (b, c), (b, f), (c, e)\}$

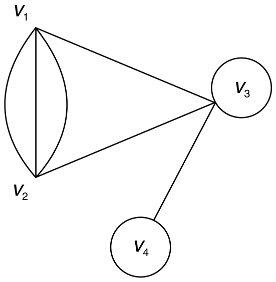
(*b*) $V = \{v_1, v_2, v_3, v_4, v_5), E = \{(v_1, v_1), (v_2, v_3), (v_2, {}_4v), (v_4, v_5)\}$

(*c*) $V = \{a, b, c, d, e\}$, $E = \{(a, a), \ldots (a, b), (b, c), (c, d), (c, e), (d, e)\}$

(*d*) $V = \{a, b, c, d\}$, $E = \{(a, a), (a, b), (b, c), (c, c), (c, d), (d, a)\}$

3. Describe the graph G, given below:

G:



4. (*a*) Give two example for a regular graph of degree 1.

(*b*) Give two examples for a regular graph of degree 2.

5. Draw a simple graph of

(*i*) Two vertices.

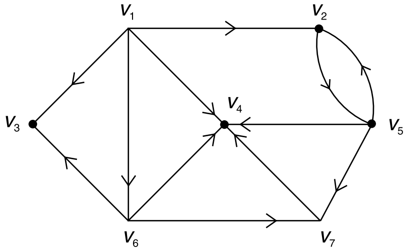
(*ii*) Four vertices.

6. Draw the graphs of the following chemical compounds:

(*a*) CH_4 (*b*) $C_2 H_6$

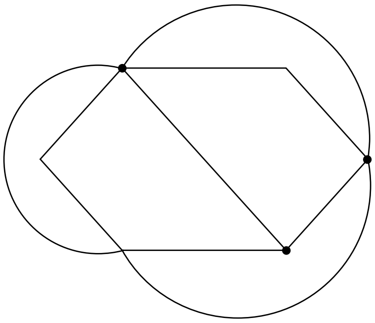
7. Find the indegree and the outdegree of each vertex in the graph G:

G:



8. Find the order and size of the graph G:

G:



9. Show that the maximum number of edges in a simple graph with n vertices is $\dfrac{n(n-1)}{2}$.

10. Nine members of a club meet each day for lunch at a round table. They decide to sit such that every member has different neighbours at each lunch. How many days can this arrangement last?

11. Show that every cubic graph has an even number of vertices (points).

12. Show that in any group of two or more people, there are always two with exactly the same number of friends inside the group.

13. Construct a cubic graph on 10 vertices. Draw three different representations.

14. Give an example of a 3-regular graph (cubic graph) on 6 vertices.

15. Show that the size of m-regular (p, q) graph is $\dfrac{P \cdot m}{2}$.

16. Suppose you are married and you and your husband visited a party with 3 other married couples no. one shakes hands with himself or his wife. How many hands you have shaken and how many did your husband shake? Give limits.

17. What is the largest number of vertices in a graph with 35 edges, if all vertices are degree atleast 3?

18. Show that there exists a 4-regular graph on 6 vertices. Construct a graph as an example.

19. Let G be a (p, q) graph all of whose points have degree or $k + 1$. If G has $k > 0$ points of degree k, show that $t = p\,(k + 1) - 2q$.

20. Is there a simple with the degree sequence:

(*i*) (1, 1, 3, 4, 6, 7)

(*ii*) (1, 2, 3, 3, 3, 4, 6, 7)

(*iii*) (1, 1, 2, 3)

(*iv*) (2, 3, 3, 4, 5, 6)

(*v*) (2, 2, 4, 8)

(*vi*) (6, 6, 6, 6, 4, 3, 3, 0)

(*vii*) (6, 6, 5, 4, 3, 3, 1)

21. Which of the following sequences are graphical? Construct a group in possible cases.

(*i*) 6, 5, 5, 4, 3, 3, 2, 2, 2

(*ii*) 5, 5, 4, 4, 3, 2, 2, 1, 1

(*iii*) 7, 6, 5, 4, 4, 3, 2, 1

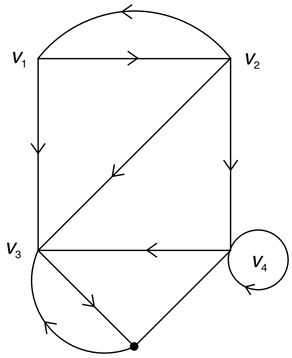
(*iv*) 4, 4, 4, 4, 3, 3

(*v*) 3, 3, 3, 3, 3, 3, 3, 3

22. A graph G has 21 edges, 3 vertices of degree 4 and other vertices are of degree 3. Find the number of vertices in G.

23. Show that there is no graph with the sequence (1, 1, 3, 3, 3, 4, 6, 7).

24. Find the indegree and out degree of each vertex of G.



Answers:

7.

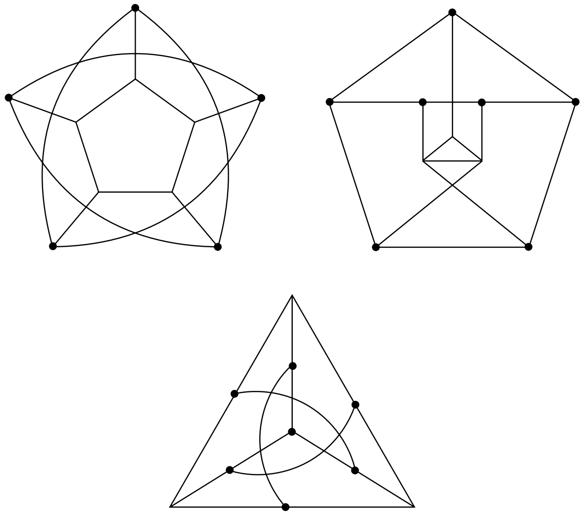
Vertex:	v_1	v_2	v_3	v_4	v_5	v_6	v_7
Indegree:	0	2	2	4	1	1	2
Outdegree:	4	1	0	0	3	3	1

8. Order of $G = 6$

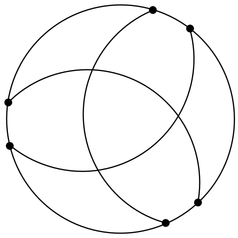
Size of $G = 10$

10. 4 days

13.



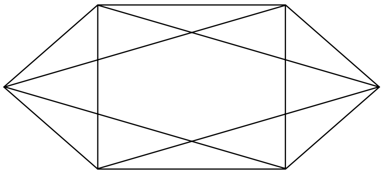
14.



15. 0 and 36

16. 23

17. 11



20. (*i*) to (*vii*) – No

21. (*i*) Yes (*ii*) No (*iii*) No (*iv*) Yes (*v*) Yes

22. 13

24.

Vertex:	v_1	v_2	v_3	v_4	v_5
Indegree:	1	1	4	3	1
Outdegree:	2	3	1	2	2

8.7 EDGES IN SERIES

In a graph *G* two edges are said to be in series if they have exactly one vertex in common.

In Fig. 8.33, the edges e_1 and e_2 are in series. v_1 is the common vertex. The edges e_3 and e_5 are in series.

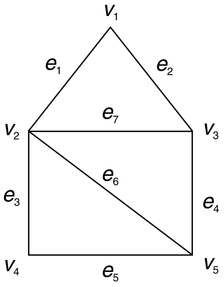


Fig. 8.33

8.8 ADJACENCY

In a graph *G*, if there is an edge *e* incident from the vertex *u* to the vertex *v* or incident on *u* and *v*, then the vertices *u* and *v* are said to be adjacent.

In the graph of Fig. 8.34 (*i*) The vertices v_1 and v_2 are adjacent.

Two non-parallel edges in a graph *G*, are said to be adjacent, if they are incident on the same vertex.

In the graph of Fig. 8.34 (*ii*) The edges e_1 and e_2 are adjacent.

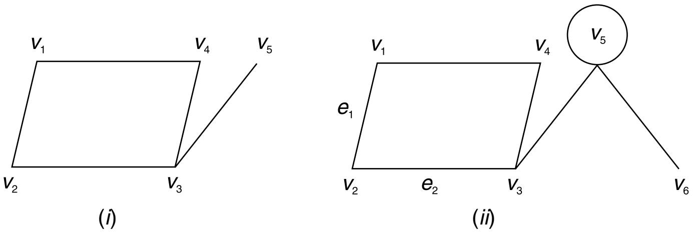


Fig. 8.34

8.9 MATRIX REPRESENTATION OF GRAPHS

A graph can be represented by a matrix. There are two ways of representing a graph by a matrix; namely (*i*) Adjacent matrix and (*ii*) Incidence Matrix.

8.9.1 Adjacency Matrix of a Non-Directed Graph

Definition 8.23: Let G be a graph with n vertices and no parallel edges. The adjacency matrix of G in a $n \times n$ symmetric binary matrix $A(G) = [a_{ij}]_{nxn}$ where

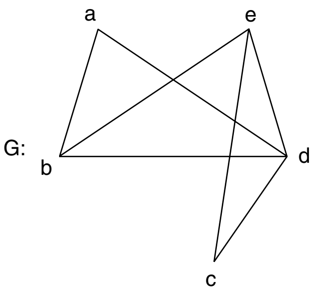
$a_{ij} = 1$ if v_i and v_j in G are adjacent

$a_{ij} = 0$ if v_i and v_j in G are adjacent

where v_i and v_j are vertices of G .

The adjacency matrix $A(G)$ of a graph G with n vertices is (*i*) Symmetric (*ii*) The principal diagonal entries are all 0's if and only if G has no self-loops and (*iii*) *i*th row sum and *i*th column of $A(G)$ is the degree of v_i.

Example 1: The adjacency matrix of the simple graph G shown in Fig. 8.35 (*i*) is given in 8.35 (*ii*):



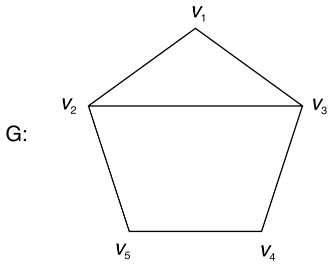
(*i*)

$$\text{Adjacency matrix } x;\ A\,(G) = \begin{array}{c c} & \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \\ e \end{array} & \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

(*ii*)

Fig. 8.35

Example 2: The adjacency matrix of the graph G, shown Fig. 8.36 (*a*) is given in 8.36 (*b*):



(*a*)

$$A(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(*b*)

Fig. 8.36

8.9.2 Adjacency Matrix of a Digraph

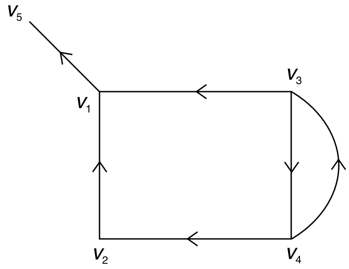
Definition 8.24: Let G be a digraph with n vertices, containing non-parallel edges. The adjacency matrix $A(G)$ of the digraph G is an $n \times n$ matrix defined by

$$A(G) = [a_{ij}]_{nxn}$$

Where $a_{ij} = 1$ if there is an edge directed from v_i to v_j
= 0 otherwise.

Example 1: Consider the digraph shown in Fig. 8.37 (*a*)

The Adjacency matrix is given in 9.37 (*b*):



(*a*)

$$A(G) = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

(*b*)

Fig. 8.37

The adjacency matrix of a graph is also called the connection matrix. It has different names in different disciplines.

In the adjacency matrix of a graph, every non-zero element on diagonal represents a self-loop at the corresponding matrix. We can find the adjacency matrices of multigraph; but we avoid parallel edges in the definition of *A* (*G*).

Example 2: Find the adjacency matrix or the graph shown in Fig. 8.38.

Solution: The adjacency matrix *A* (*G*) of the given multigraph is:

$$A(G) = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

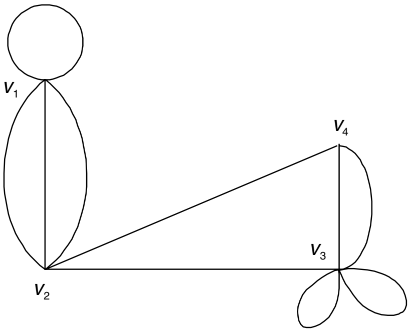


Fig. 8.38

8.9.3 Incidence Matrix of a Non-Directed Graph

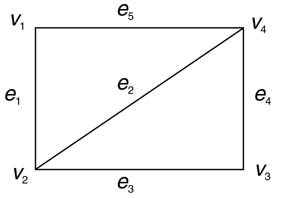
Definition 8.25: Let G be a graph with n vertices and m edges. The incidence matrix denoted by $X(G)$ is defined as the matrix $X(G)$ is defined as the matrix

$$X(G) = [x_{ij}]_{nxn}$$

Where $x_{ij} = 1$, if jth edge e_j is incident on ith vertex v_i, and

$= 0$, otherwise

$X(G)$ is an n by m matrix whose n rows correspond to the n vertices, and m columns correspond to m edges. A graph and its incidence matrix are shown in Fig. 8.39:



$$X(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Fig. 8.39 Graph and its incidence matrix

The incidence matrix contains only two elements 0 and 1. Each column in the incidence matrix of a graph has exactly two 1's appearing in that column. The sum of 1's in each row represents the degree of a vertex corresponding to the row. A row with all 0's in the incidence matrix represents an isolated vertex. Two identical columns in an incidence matrix correspond to parallel edges in the graphs G.

8.10 LINKED REPRESENTATION (OR ADJACENCY STRUCTURE)

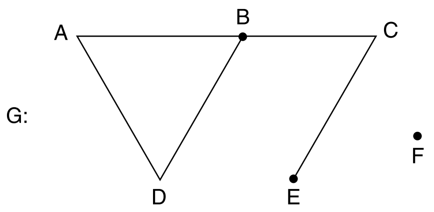
There are two ways of maintaining a given graph G in the memory of a computer; namely

(*i*) Sequential representation of G

and (*ii*) Linked representation of G.

Sequential representation of a graph in the memory of a computer uses the Adjacency matrix $A(G)$ of G. This type of representation has a number of major draw backs. Hence linked representation, also called the Adjacency structure, is described below by means of an example.

Consider the graph G shown in Fig. 8.40 (*a*)



(*a*)

Vertex	*Adjacency list*
A	B, D
B	A, C, D
C	B, E
D	A, B
E	C
F	ϕ

(*b*)

Fig. 8.40

The graph G may equivalently defined by the table in 8.40 (*b*). Which shows that each vertex in a followed by its list of adjacent vertices. Here the symbol ϕ is used to denote the empty list. The table may also be presented in the form shown below:

$$G = [A: B, D; B: A, C, D; C: B, E; D: A, B; E: C; F: \varnothing]$$

Where a colon ":" seperates a vertex from its list of adjacent vertices and a semicolon ";" seperates the different lists. The linked representation of a graph G, maintains G in the memory by using its adjacency lists and will contain two files namely (*i*) Vertex file and (*ii*) Edge file. The vertex file will contain the list of vertices of G, usually maintained by a linked list and the edge file will contain all the edges of G. Each record of the edge file will correspond to a vertex in an adjacency list and hence, indirectly to an edge of the graph G.

Example 1: Suppose a graph G is presented by the following table:

$$G = [A: D; B: C; C: E; D: B, D, E; E: A]$$

Draw the graph also find the number of vertices and edges in G.

Solution: The graph of G can drawn as shown in Fig. 8.41.

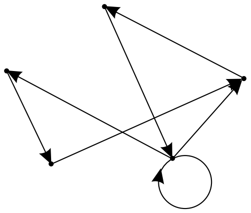


Fig. 8.41

Number of vertices in $G = 5$

Number of edges in $G = 6$

8.11 THE CYCLE MATRIX

Definition 8.26: Let G be a graph whose edges are labeled. The cycle matrix $C = [C_{ij}]$ of the graph G has a row for each cycle and a column for each edge with

$$C_{ij} = 1 \text{ , if the } ci\text{th cycle contains edge } e_j$$
$$= 0, \text{ otherwise}$$

Example: Consider the graph shown in the figure given below

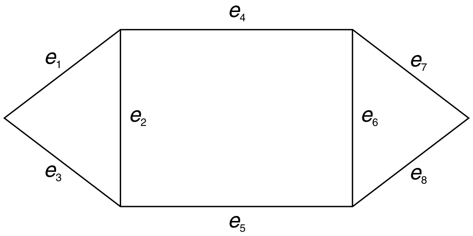


Fig. 8.42

The cycles in the graph are

$$z_1 = \{e_1, e_2, e_3\}$$
$$z_2 = \{e_2, e_4, e_5, e_6\}$$
$$z_3 = \{e_6, e_7, e_8\}$$
$$z_4 = \{e_1, e_3, e_4, e_5, e_6\}$$
$$z_5 = \{e_2, e_4, e_5, e_7, e_8\}$$
$$z_6 = \{e_1, e_3, e_4, e_5, e_7, e_8\}$$

The cycle matrix of *G* is:

$$\begin{array}{c|cccccccc|} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\ z_1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ z_2 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ z_3 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ z_4 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ z_5 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ z_6 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{array}$$

8.12 PATH MATRIX

Definition 8.27: Let *G* be a connected graph. Let *u* and *v* be any vertices of *G*. If $P_1, P_2, \ldots, P_r,\ r \geq 1$, denote distinct paths from *u* to *v* in *G*, then the path matrix

$P_{(u,\,v)} = [p_{ij}]$ is defined as follows

$P_{ij} = 1$, if *j*th edge lies in a *i*th path

$= 0$, otherwise

Example: Consider the graph *G*, given below:

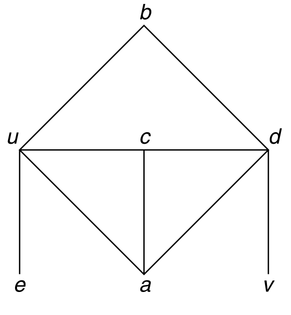


Fig. 8.43

The distinct paths in the graph *G* between the vertices *u* and *v* are:

$P_1 : u - b - d - v$

$P_2 : u - \mathrm{c} - \mathrm{d} - v$

$$P_3 : u - c - a - d - v$$
$$P_4 : u - a - d - v$$
$$P_5 : u - a - c - d - v$$

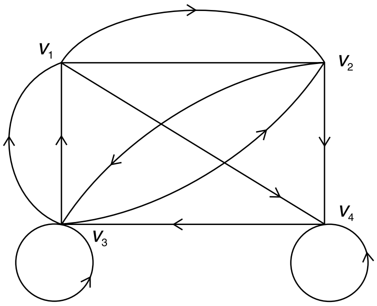
$$\begin{array}{c|ccccccccc|}
 & ua & ub & uc & ue & ac & ad & bd & cd & dv \\
p_1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
p_2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
p_3 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
p_4 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
p_5 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1
\end{array}$$

The path matrix of a tree is a row matrix.

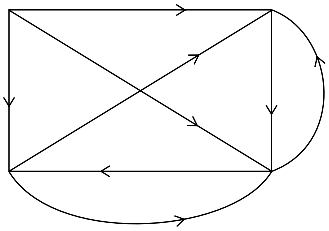
Exercise 8.2

I. Find the Adjacency Matrix *A* (*G*) of the following graphs:

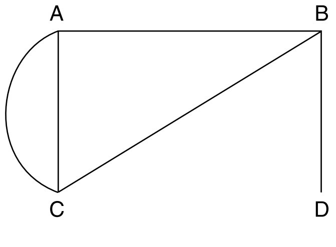
(*a*)



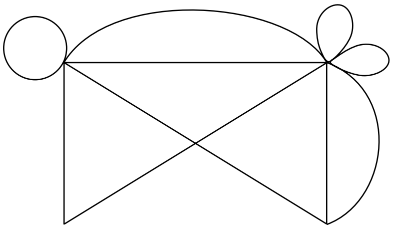
(*b*)



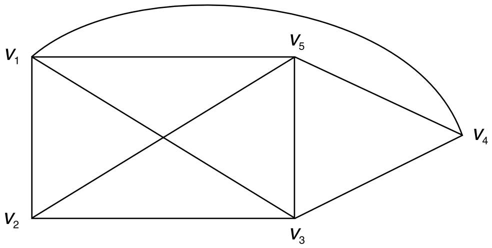
(*c*)



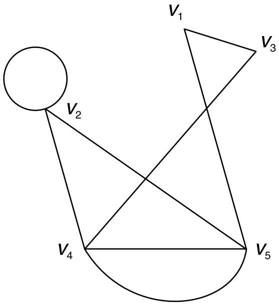
(*d*)



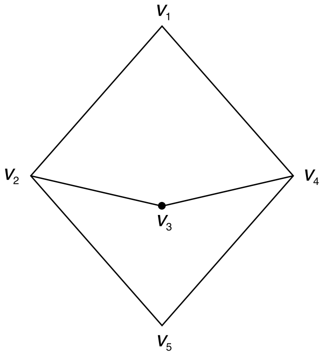
(*e*)



(*f*)

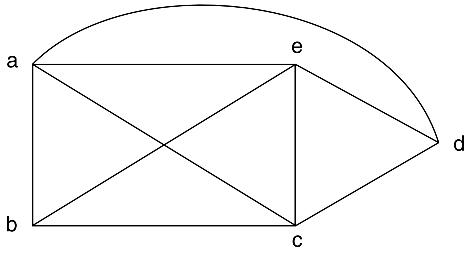


(*g*)

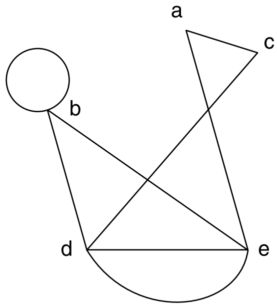


II. Write the incidence matrix for the graph G.

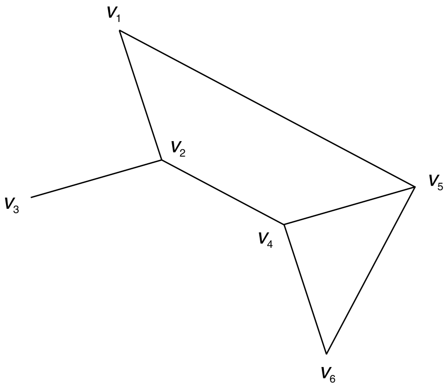
(*i*)



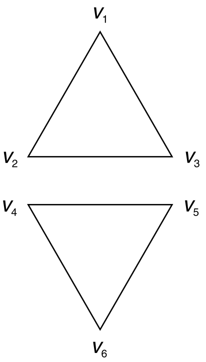
(*ii*)



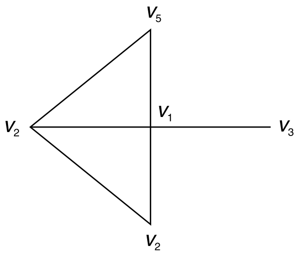
(*iii*)



(*iv*)



(*v*)



III. Draw the graph *G*, corresponding to each Adjacency matrix.

$$(a)\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad (b)\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$(c)\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad (d)\begin{pmatrix} 1 & 1 & 1 & 2 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 2 \end{pmatrix}$$

IV. Draw the digraph of the incidence matrix.

$$(a)\quad X(G) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \qquad (b)\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

V. The adjacency structure of a graph *G* is given as
G = [*A*: *B*, *E*; *B*: *A*, *E*, *F*, *G*; *C*: *D*, *G*, *H*; *D*: *C*, *H*; *E*: *A*, *B*; *F*: *G*; *G*: *B*, *C*, *F*; *H*: *C*, *D*]

Answers Exercise 8.2:

I.

$$(a)\quad A(G) = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad (b)\quad A(G) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$(c)\quad A(G)=\begin{pmatrix}0&1&2&0\\1&0&1&1\\2&1&0&0\\0&1&0&0\end{pmatrix}\qquad (d)\quad A(G)=\begin{pmatrix}1&1&1&2\\1&0&0&0\\1&0&0&2\\2&0&2&2\end{pmatrix}$$

$$(e)\quad A(G)=\begin{pmatrix}0&1&1&1&1\\1&0&1&0&0\\1&1&0&1&1\\1&0&1&0&1\\1&0&1&1&0\end{pmatrix}\qquad (f)\quad \begin{pmatrix}0&0&1&0&1\\0&1&0&1&1\\1&0&0&1&0\\0&1&1&0&2\\1&1&0&2&0\end{pmatrix}$$

$$(g)\quad A(G)=\begin{pmatrix}0&1&0&1&0\\1&0&1&0&1\\0&1&0&1&0\\1&0&1&0&1\\0&1&0&1&0\end{pmatrix}$$

II.

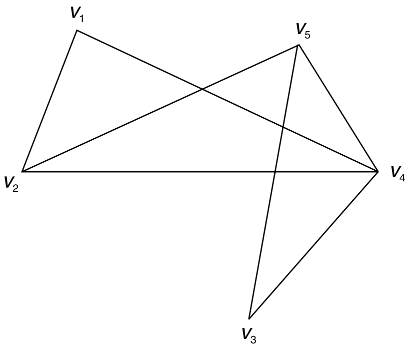
$$(i)\quad \begin{pmatrix}1&1&1&0&1&0&0&0\\1&0&0&1&0&0&0&0\\0&0&1&1&0&0&1&1\\0&0&0&0&1&1&0&1\\0&1&0&0&0&1&1&0\end{pmatrix}\qquad (ii)\quad \begin{pmatrix}1&1&0&0&0&0&0&0\\0&0&1&1&1&0&0&0\\1&0&0&0&0&1&0&0\\0&0&0&0&1&1&1&1\\0&1&0&1&0&0&1&1\end{pmatrix}$$

$$(iii)\quad \begin{pmatrix}1&0&0&0&0&0&1\\1&1&1&0&0&0&0\\0&1&0&0&0&0&0\\0&0&1&1&1&0&0\\0&0&0&0&1&1&1\\0&0&0&1&0&1&0\end{pmatrix}\qquad (iv)\quad \begin{pmatrix}1&0&1&0&0&0\\0&1&1&0&0&0\\1&1&0&0&0&0\\0&0&0&1&0&1\\0&0&0&1&1&0\\0&0&0&0&1&1\end{pmatrix}$$

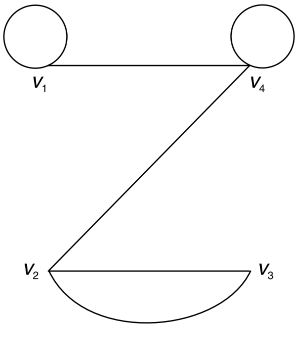
$$(v)\ \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

III.

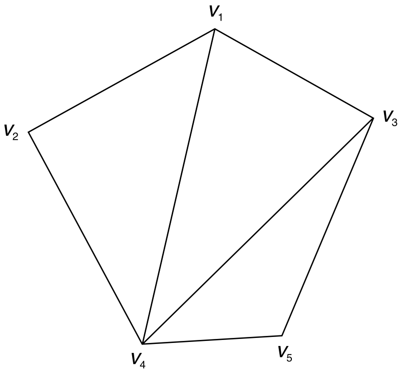
(*a*)



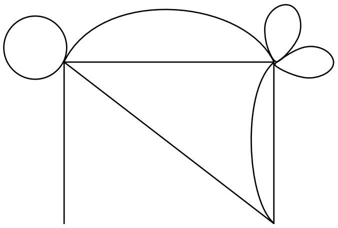
(*b*)



(*c*)

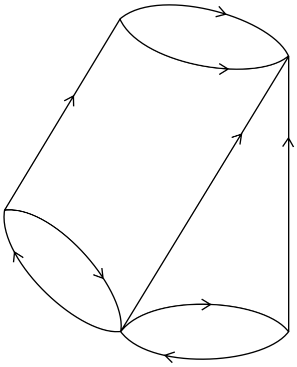


(*d*)

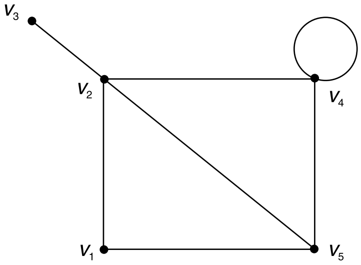


IV.

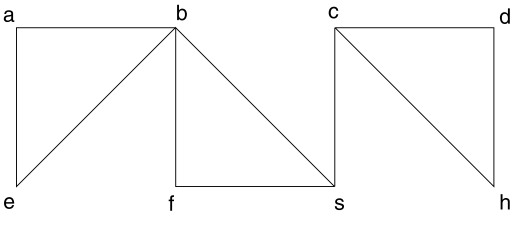
(*a*)



(*b*)



V.



8.13 WALKS, PATHS AND CIRCUITS

Definition 8.28: A walk in a graph is defined as a finite alternating sequences of vertices and edges v_0, e_1, v_1, e_2, v_2, e_3, ..., v_{n-1}, e_n, $v_{n,}$ beginning and ending with points (vertices) in which each edge is incident with two points immediately proceeding and following it.

A walk in a graph is denoted by w.

The walk v_0, e_1, v_1, e_2, ..., v_{n-1}, e_n, $v_{n,}$ may be written as v_0–v_1–v_2 ..., –v_{n-1}, – v_n, and is called $v_0 - v_n$ walk. The vertices v_0 and v_n with which the walk begins and ends are called the initial and the terminal vertices (i.e., v_0 is called initial vertex v_n is called the terminal vertex). If , $v_0 \neq v_n$ then the walk is called an open walk. $v_0 = v_n$ then the walk is called a closed walk. A walk is also called a chain.

Definition 8.29: A walk in a graph; in which no edge is repeated is called a trail.

Definition 8.30: A closed trail is called tour in a graph G.

Definition 8.31: The number of edges in walk is called the length of the walk.

Example 1:

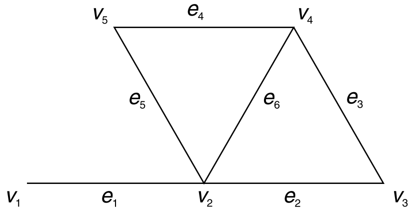


Fig. 8.44

Consider the graph G in Fig. 8.42

W_1: v_1 e_1 v_2 e_2 v_3 e_3 v_4 e_4 v_5; is called a walk

The length of the walk is 4.

Since the edges are not repeated the walk w, is a trail.

W_2: v_2 e_2 v_3 e_3 v_4 e_5 v_2; is called a closed walk

No edge in W_2 is repeated therefore W_2 is closed trail, hence a tour.

Definition 8.32: Let G be a non-directed graph. A sequence P of zero or more edges of the form $\{v_0, v_1\}$,$\{v_1, v_2\}$, $\{v_2, v_3\}$, ..., $\{v_{n-1}, v_n\}_,$ where v_0, v_1, v_2 ..., $v_{n,}$ are the vertices of G is called a path in G. It is denoted by P.

The vertex v_0 is called the initial vertex and the vertex v_n is called the terminal vertex of the path P.

The path P can also be written as $v_0 - v_1 - v_2 - ... - v_n$, is called $v_0 - v_n$ path.

If $v_0 \neq v_n$ the path P is called an open path and if $v_0 = v_n$, the path P is called a closed path.

The number of occurrences of edges in a path P is called the length of the path.

Note:

(*i*) A path in a graph is an open walk which no vertex (and no edge) appears more than once.

(*ii*) The terminal vertices of an open path are of degree one.

(*iii*) If P is a path in $G = (V, E)$, then $V(P) \subseteq V(G)$ and $E(P) \subseteq E(G)$ also $1 \leq |V(P)| \leq |E(P)| \leq n$.

(*iv*) Any $v_0 - v_n$ contains a $v_0 - v_n$ path.

Definition 8.33: If all the edges and vertices in a path P are distinct except possibly the end points then the path P is called a simple path.

If P is an open simple path of length n then P has $(n + 1)$ distinct vertices, and if P is a closed path of length n, then P has n distinct vertices and n distinct edges.

Definition 8.34: A closed walk in which no vertex (except its terminal vertices) appear more than once is called a circuit.

A circuit in a graph is a closed non-intersecting walk in which every vertex is of degree two (*see* Fig. 8.45). A circuit with no other repeated vertices except its end points is called a cycle. The terms a circuit and cycle or synonymous.

In the Fig. 8.46 (*a*) $v_3 - v_4 - v_5 - v_3$ is a cycle and in the Fig. 8.46 (*b*), $v_1 - v_2 - v_4 - v_5 - v_1$ is a cycle.

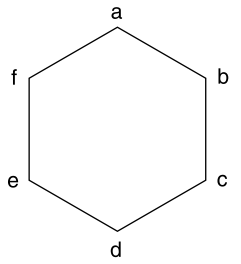


Fig. 8.45

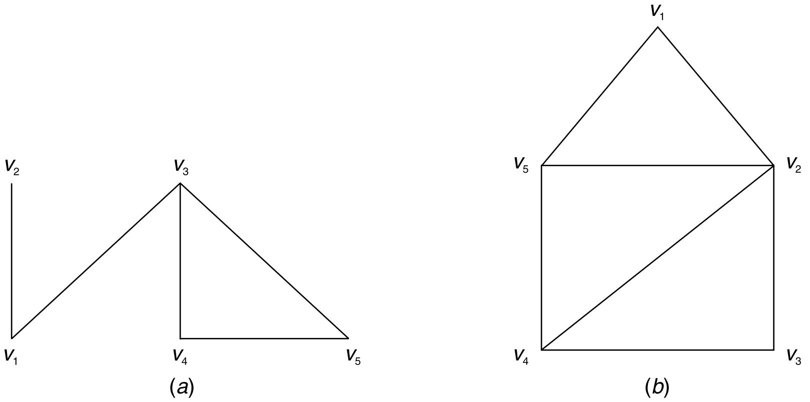


Fig. 8.46

Theorem 8.3: In a graph G, any $v_0 - v_n$ walk contains a path.

Proof: We prove the theorem by induction on the length of the walk.

If the length of the $v_0 - v_n$ path 0 or 1, then the walk is obviously a path.

Now, let us assume that the result holds for all walks of length less than n.

Let v_0, v_1, v_2, ... v_n be a walk of length n. If all the vertices v_i ; $1 \leq i \leq n$ are distinct then the walk is a path, if not there exists i and j such that $v_i = v_j$ for some i, j such that ; $1 \leq i \leq j \leq n$.

Now the walk $v_0 - v_1 - v_2 - ... v_i, v_{j+r}, ... v_n$ is a $v_0 - v_n$ walk, whose length is less then n, which by induction hypothesis contains a $v_0 - v_n$ path.

Theorem 8.4: If $\delta(G) \geq K$; then graph G has a path of length k.

Proof: Let v_1 be an arbitrary vertex in G, choose a vertex say v_2, which is adjacent to v_1. Since $\delta(G) \geq K$, there exist atleast $k - 1$ vertices other them v_1, which are adjacent to v_2. Choose another vertex $v_3 \neq v_1$ such that v_3 is adjacent to v_2. In this may we can find vertices v_4, v_5, v_6, ... v_i, where $1 \leq i \leq \delta(G)$. Having chosen the vertices $v_1, v_2, \ldots v_i$, where $1 \le i \le \delta(G)$. We can find another vertex v_{i+1} which is different from the vertices $v_1, v_2, \ldots v_i$, such that v_{i+1} is adjacent to v_i. Proceeding in this way. We can find a path of length k in G.

We now state the following theorem without proof:

Theorem 8.5: A closed walk of odd length in a graph G contains a cycle.

8.14 SUBGRAPHS

Definition 8.35: Let G and H be two graphs. H is called a subgraph of G if $V(H)$ is a subset of $V(G)$ and $E(H)$ is a subset of $E(G)$.

If H is a subgraph of G then

(*i*) All the vertices of H are in G.

(*ii*) All the edges of H are in G.

(*iii*) Each edge of H has the same end points in H as in G.

Example 1: In Fig. 8.47 the graph H is a subgraph of G.

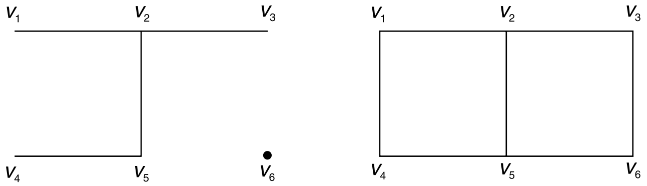


Fig. 8.47

Example 2: In Fig. 8.48 H is a subgraph of G.

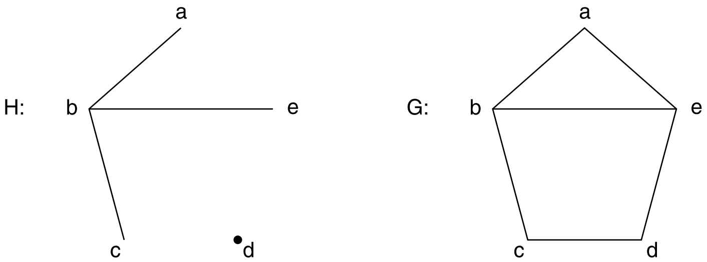


Fig. 8.48 Subgraph

8.14.1 Spanning Subgraph

Defintintion 8.36: A subgraph H of a graph G is called a spanning subgraph of G if $V(H) = V(G)$: i.e., H contains all the vertices of G.

In the graphs shown in Fig. 8.49 H is a spanning subgraph of G.

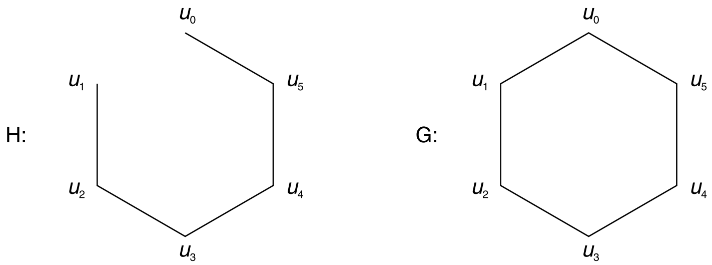


Fig. 8.49 Spanning subgraph

Two subgraphs H_1 and H_2 of a graph G are said to vertex disjoint if $V(H_1) \cap V(H_2) = \varnothing$.

8.14.2 Edge Disjoint Subgraph

Definition 8.37: Two subgraphs H_1 and H_2 of a graph G are said to be edge disjoint subgraphs of G if H_1 and H_2 do not share any edges in common.

8.15 REMOVAL OF VERTICES AND EDGES FROM A GRAPH

Definition 8.38: The removal of a vertex v_i from a graph G results in a subgraph of G; consisting of all points of G except v_i and all edges of G not incident with v_i. The obtained is denoted by $G–v_i$ and is the maximal subgraph of G not containing v_i (Fig. 8.50 (*a*)).

The removal of an edge e_j from a graph results in the spanning subgraph of G which containing all the edges of a G except the edge e_j. It is denoted by $G – e_j$ and is the maximal subgraph of G not containing e_j. (Fig. 8.50 (*b*)).

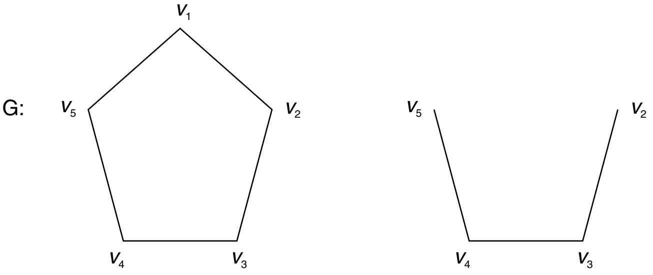


Fig. 8.50 (*a*) Graph minus a vertex v_1

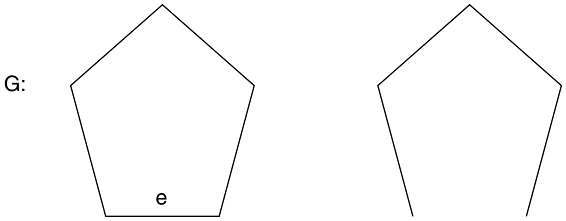


Fig. 8.50 (*b*) Graph minus edge *e*

8.16 ADDITION OF A VERTEX

Definition 8.39: Let G be a graph and v be a vertex which is not in G then the graph obtained by joining v with each vertex of G, is the sum graph $G + K_1$. It is denoted by $G + v$ (*see* Fig. 8.51).

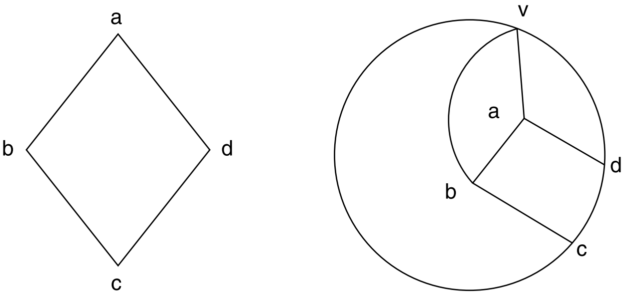


Fig. 8.51

8.17 OPERATIONS ON GRAPHS

8.17.1 Union of Graphs

Definition 8.40: Let $G = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs whose vertex sets v_1 and v_2 are disjoint. Then the union of G_1 and G_2 denoted by $G_1 \cup G_2$ is defined as the graph $G = (V, E)$ such that

(*i*) $V(G) = V(G_1) \cup V(G_2) = V_1 \cup V_2$

(*ii*) $E(G) = E(G_1) \cup E(G_2) = E_1 \cup E_2$

Example 1: If

G_1 is the graph

and G_2 is the graph

then $G_1 \cup G_2$

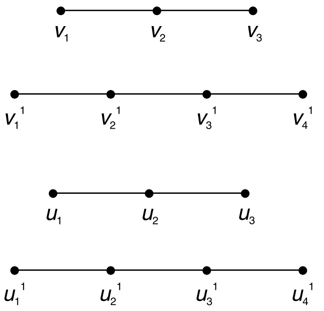
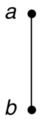
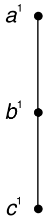


Fig. 8.52

8.17.2 Sum of Two Graphs

Definition 8.41: Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, V_2)$ denote two vertex disjoint graphs. Then the sum of G_1 and G_2 denoted by $G_1 + G_2$ is defined as $G_1 \cup G_2$ together with all the edges joining vertices of V_1 to vertices of V_2.

Example: If

G_1 is the graph  and G_2 is the graph 

then $G_1 + G_2$ is the graph given below:

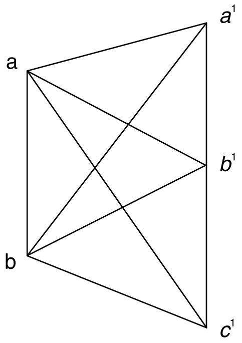


Fig. 8.53 Sum of two graphs

8.17.3 Intersection of Graphs

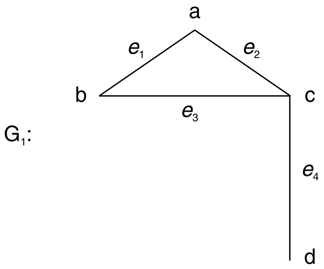
Definition 8.42: Let G_1 and G_2 be two graphs. Then the intersection of G_1 and G_2 denoted by $G_1 \cap G_2$ is defined as the graph G such that

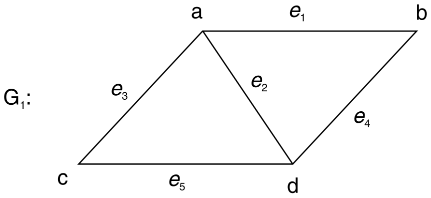
(*i*) $V(G) = V(G_1) \cap V(G_2)$.

(*ii*) $E(G) = E(G_1) \cap E(G_2)$.

Example:

Let





then $G_1 \cap G_2$ is the graph

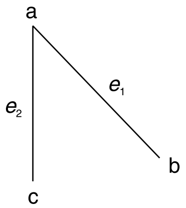
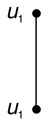


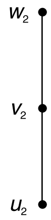
Fig. 8.54 Intersection of two graphs

8.17.4 Product of Two Graphs

Definition 8.43: Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be two graphs with $V_1 \cap V_2 = \varnothing$. Then the product of G_1 and G_2 denoted by $G_1 \times G_2$ is the graph having $V = V_1 \times V_2$ and $u = \{u_1, u_2\}$ and $V = \{u_1. u_2\}$ are adjacent if $u_1 = v_1$ and u_2 is adjacent to V_2 is G_2 or u, is adjacent to V_1 and G_1 and $u_2 = v_2$.

Example: If

G_1 is the graph 

and G_2 is the graph 

then $G_1 \times G_2$ is the graph given below:

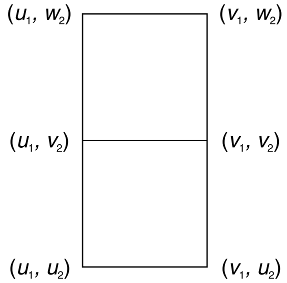


Fig. 8.55

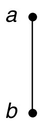
8.17.5 Composition (Lexicographic Product) of G_1 with G_2

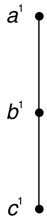
Definition 8.44: Let G_1 and G_2 be two graphs. The composition of G_1 and G_2 denoted by $G_1[G_2]$ is a graph $G = G_1[G_2]$ such that

(*i*) $V(G) = \{(u, v) : u \in v(G_1), u \in V(G_2)\}$

(*ii*) $E(G) = \{\{(u_1, v_1), (u_2, u_2)\}$: either $u_1 u_2 \in E(G)$ or $u_1 = u_2$ and $v_1 v_2 \in E(G_2)\}$

Example:

Let G_1: 

and G_2: 

then $G = G_1[G_2]$ is the graph

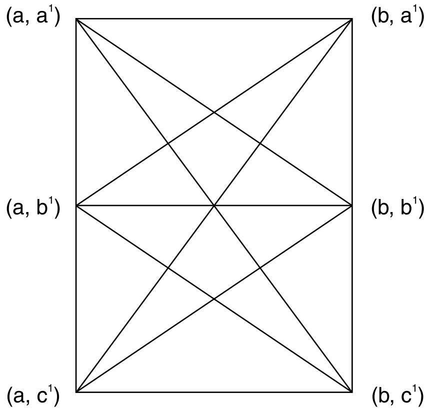


Fig. 8.56

Now we state the following theorem without proof:

Theorem 8.6: Let G_1 be a (p, q) graph and G_2 be (p_2, q_2) graph then:

(i) $G_1 \cup G_2$ is $(p_1 + p_2, q_1 + q_2)$ graph

(ii) $G_1 + G_2$ is a $(p_1 + p_2, q_1 + q_2 + p_1 p_2)$ graph

(iii) $G_1 \times G_2$ is a $(p_1 p_2, q_1, p_2 + q_2 p_1)$ graph

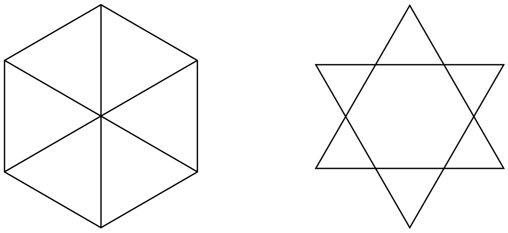
and (iv) $G_1[G_2]$ is a $(p_1, p_2, p_1, q_2 + p_2^2, q_1)$ graph

The proof is left to the reader as an exercise.

8.18 COMPLEMENT OF A GRAPH

Definition 8.45: Let G be a graph with n vertices then $K_n - G$ is called the complement of G. It is denoted by $\overline{G}$.

A graph and its complement are shown in Fig. 8.57.



(a) Graph G (b) Complement $\bar{G}$ of G

Fig. 8.57 A graph and its complement

8.18.1 Complement of a Subgraph

Definition 8.46: Let G be a graph and H be a subgraph of G. The complement H in G is the graph obtained by deleting the edges of H from those of G.

The complement of H in G is denoted by $\overline{H}$ (or $\overline{H}$ (G)). In Fig. 8.58 (a) G is a given graph, and in Fig. 8.58 (b): H is a subgraph of G. The complement of H in G is shown in Fig. 8.58 (c).

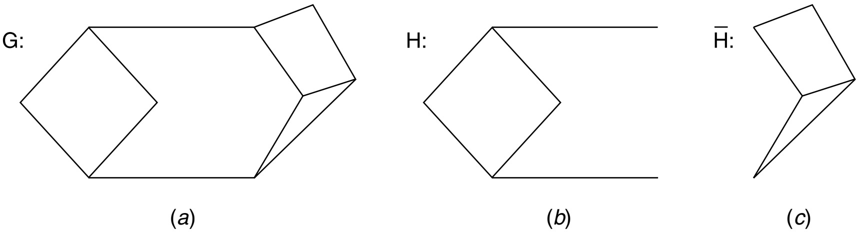


Fig. 8.58 Complement of a subgraph

8.19 CONNECTED GRAPH

A graph G is said to be connected if every pair of points in G are joined by a path. If G is not connected then G is called a disconnected graph.

A maximal connected subgraph of G is called a component of G. If G is disconnected then G has atleast two components.

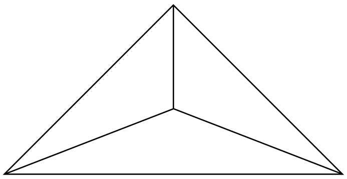


Fig. 8.59 A connected graph

Clearly a graph G is connected iff it has exactly one component.

Theorem 8.7: If G is a graph with n with points and $\delta(G) \geq \frac{n-1}{2}$ then G is connected.

Proof: Let assume that G is not connected. Then G has more than one component. Consider any component $G_1 = (V_1, E_1)$ of G.

Let $v_1 \in v_2$ since $\delta(G) \geq \frac{n-1}{2}$ there exist atleast $\frac{n-1}{2}$ points in G_1 which are adjacent to v_1 in G_1.

Then we have
$$|V| \geq \frac{n-1}{2} + 1$$
or
$$|V| \geq \frac{n+1}{2}$$

Thus each component of G has atleast $\frac{n+1}{2}$ points and G has least two components.

Hence the number of points (vertices) in $G \geq 2\,\frac{(n+1)}{2}$ i.e., $|V(G)| \geq (n+1)$ which is a contradiction.

Thus G is connected.

8.20 PARTITIONS

Definition 8.47: Let $G = (V, E)$ be a graph. A partition of the vertex set $V(G)$ is a collection $\{V_i\}_{1 \le i \le \alpha}$ of non-empty subsets of V such that

(*i*) $V_1 \cup V_2 \cup V_3 \cup ... \cup V_\alpha = V, \;\; (\alpha \ne 1)$

and (*ii*) $V_i \cap V_j = \varnothing$ whenever $i \ne j$

A partition of the edge set $E(G)$ is a collection $\{E_i\}$ of non-empty subsets of E such that $1 \le i \le \beta$.

(*i*) $E_1 \cup E_2 \cup E_3 \cup ... \cup E_\beta = E, \;\; (\beta \ne 1)$

(*ii*) $E_i \cap E_j = \varnothing$ whenever $i \ne j$

The partition of the edge set E is also called edge decomposition of G.

Example: Consider the graph shown in Fig. 8.60.

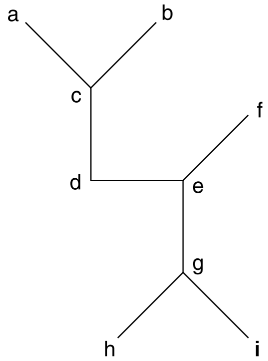


Fig. 8.60

$V_1 = \{a, b, c\}$, $V_2 = \{d, e, f, g\}$, $V_3 = \{h, i\}$ is a vertex partition of the vertex set $V(G)$.
and $E_1 = \{(a, c), (c, b)\}$, $E_2 = \{(c, d), (d, e), (e, f)\}$ $E_3 = \{(e, g)\}$, $E_4 = \{(g, h)\}$, $E_5 = \{(g, i)\}$is an edge decomposition of G.

Theorem 8.8: A graph G is connected if and only if for any partition of V into subsets V_1 and V_2 there is an edge joining a vertex of V_1 to a vertex of V_2.

Proof: Let G be a connected graph and $V = V_1 \cup V_2$ be a partition of V into two subsets.

Let $u \in V_1$ and $v \in V_2$. Since the graph G is connected there exists a $u - v$ path in G say $u = v_0, v_1, v_2, ... v_n = v$. Let i be the least positive integer such that $v_i \in v_2$. Then $v_{i-1} \in V_1$ and the vertices v_{i-1}, v_i are adjacent. Thus there is an edge joining $v_{i-1} \in V_1$ and $v_i \in V_2$.

Conversely

Let G be a disconnected graph.

Then G contains atleast two components.

Let V_1 be the set of all vertices of one component and V_2 be the set of remaining vertices of G. clearly $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \varnothing$.

The collection $\{V_1, V_2\}$ is a partition of V and there is no edge joining any vertex of V_1 to any vertex of V_2.

Hence the theorem.

Theorem 8.9: If G is a simple graph with n vertices and k components; then G can have at most $(n - k)(n + k + 1)/2$ edges.

Proof: Let G be a simple graph with n vertices and $G_1, G_2, G_3, \ldots G_k$ be the k components of G. Let the number of vertices in ith component G_i be $n_{i.}$

Then

$$|V(G_1)| + |V(G_2)| + \ldots + |V(G_k)| = n_1 + n_2 + \ldots + n_k = |V(G)| = n \text{ where } n_i > 1$$

and max $|E(G_i)| \leq \dfrac{n_i(n_i - 1)}{2}$

$$\therefore \qquad |E(G)| \leq \sum_{i=1}^{k} max\, |E(G_i)|$$

$$= \sum_{i=1}^{k} \frac{n_i(n_i - 1)}{2}$$

$$= \frac{1}{2}\left[\sum_{i=1}^{k} n_i^2 - \sum_{i=1}^{k} n_i\right]$$

$$= \frac{1}{2}\left[\sum_{i=1}^{k} n_i^2 - n\right]$$

i.e.,
$$|E(G)| \leq \frac{1}{2}\left[\sum_{i=1}^{k} n_i^2 - n\right] \qquad \ldots (1)$$

Now

$$\sum_{i=1}^{k}(n_i - 1) = (n_1 - 1) + (n_2 - 1) + \ldots + (n_k - 1)$$

$$= (n_1 + n_2 + \ldots + n_k) - (1 + 1 + \ldots k \text{ times})$$

$$= n - k$$

squaring on both sides

$$\left[\sum_{i=1}^{k}(n_i - 1)\right]^2 = (n - k)^2 = n^2 + k^2 - 2nk$$

or
$$\sum_{i=1}^{k}(n_i - 1)^2 + 2 \text{ (non-negative terms)} = n^2 + k^2 - 2nk$$

or
$$\sum_{i=1}^{k}(n_i - 1)^2 = n^2 + k^2 - 2nk - 2 \text{ (non-negative terms)}$$

or $$\sum_{i=1}^{k}(n_i - 1)^2 \le n^2 + k^2 - 2nk$$

or $$\sum_{i=1}^{k} n_i^2 + \sum_{i=1}^{k} 1 - 2\sum_{i=1}^{k} n_i \le n^2 + k^2 - 2nk$$

or $$\sum_{i=1}^{k} n_i^2 + k - 2n \le n^2 + k^2 - 2nk$$

or $$\sum_{i=1}^{k} n_i^2 - n \le n^2 - nk + n - nk + k^2 - k$$

$$= n\,(n - k + 1) - k\,(n - k + 1)$$

$$= (n - k)\,(n - k + 1)$$

i.e., $$\sum_{i=1}^{k} n_i^2 - n \le (n - k)(n - k + 1) \qquad \text{... (2)}$$

from (1) and (2), we get

$$|E(G)| \le (n - k)\,(n - k + 1)/2$$

Hence proved

Corollary: If $m > \frac{1}{2}(n - 1)(n - 2)$, then a simple graph with n vertices and m edges are connected.

Proof: Let G be a simple graph with n vertices and m edges.

Let us assume that G is disconnected. Then we have

$$m > \frac{1}{2}(n - 1)(n - 2)$$

Since G is a disconnected graph, G has at least two components. Therefore for $k \ge 2$, we have

$$m \le \frac{1}{2}(n - k)(n - k + 1)$$

Hence $$m \le \frac{1}{2}(n - 2)(n - 1)$$

Contradicting our assumption that

$$m > \frac{1}{2}(n - 1)(n - 2)$$

Therefore graph G is a connected graph.

Theorem 8.10: If G is not connected then $\overline{G}$ is connected.

Proof: Let G be disconnected graph. Then G has more than one component.

Let u, v be any two vertices of G. The theorem is proved if we show that there is a $u - v$ path in $\overline{G}$.

If u,v are in different components of G, then u,v are not adjacent in G. Hence, they are adjacent in $\overline{G}$.

If u, v are in the square components of G. Choose a vertex w in a different component of G. Then $u - w - v$ is a $u - v$ path in $\overline{G}$. Hence $\overline{G}$ is connected.

8.21 CYCLE GRAPH

Definition 8.48: A cycle graph of order n is a connected graph whose edges form a cycle of length n.

Cycle graph of order n is denoted by c_n. The graph shown in Fig. 8.61 is a cycle graph of order 5.

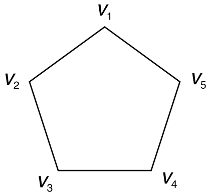


Fig. 8.61 Cycle graph of order 5 (c_5)

8.22 PATH GRAPH

Definition 8.49: Let G be a cycle graph order n. The graph obtained by removing an edge from G is called a path graph of order n. It is denoted by P_n.

The graph shown in Fig. 8.62 is a path graph order 5.

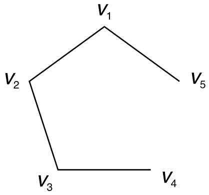


Fig. 8.62 Path graph of order 5 (P_5)

8.23 WHEEL GRAPH

Definition 8.50: Let G be a cycle graph order $(n - 1)$. The graph obtained by joining a single new vertex v to each vertex of G is called a wheel graph of order n.

A wheel graph of order n is denoted by w_n. The new vertex v is called the "*hub*". The graph shown in Fig. 8.63 is a wheel graph.

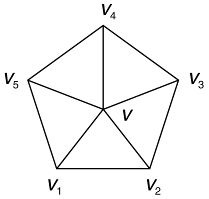


Fig. 8.63 Wheel graph (W_6)

Theorem 8.11: If G is a graph with 6 points then G or $\overline{G}$ contains a triangle.

Proof: Let $G = (V, E)$ be a graph with 6 points and $v \in V$. The vertex v is adjacent either in G or in $\overline{G}$ to the other five points of G. Let us assume u_1, u_2 and u_3 are three adjacent vertices of v in G. If any two of these vertices are adjacent then the 2 adjacent vertices and v form a triangle. If no two of the points u_1, u_2, u_3 are adjacent in G. Then they are adjacent in G and form a triangle in $\overline{G}$.

8.24 BIPARTITE GRAPH

There are a number of special classes of graph. One example is the bipartite graph. We now introduce, few more graphs which are important.

Definition 8.51: A graph G is called a bipartite graph if its vertex set V can be partitioned into two disjoint subsets A and B such that every edge in G, joins a vertex in A to a vertex in B. The graph shown in Fig. 8.64 is a bipartite graph.

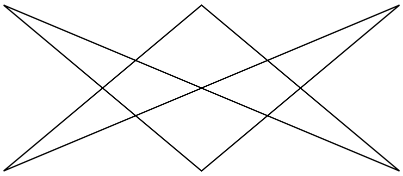


Fig. 8.64 Bipartite graph

A bipartite graph can have no self-loop.

8.24.1 Complete Bipartite Graph

Definition 8.52: A bipartite graph G in which every vertex of A is adjacent to every vertex in B is called a complete bipartite graph. Where A and B are partitioned subsets of the vertex V of G.

If $|A| = m$ and $|B| = n$, then the complete bipartite graph is denoted by $k_{m,\,n}$ and has $m\ n$ lines. The graphs in Fig. 8.65 are complete bipartite.

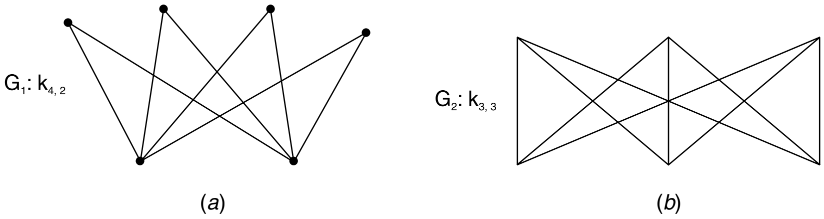


Fig. 8.65 Complete Bipartite graphs

8.24.2 Star Graph

Definition 8.53: A complete bipartite graph $k_{1,\,n}$ is called a star graph (*see* Fig. 8.66).

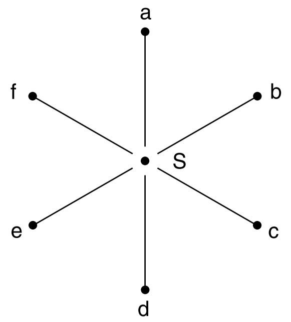


Fig. 8.66 Star graph ($k_{1,6}$)

8.25 SOLVED EXAMPLES

Example 1: Draw the complement of the graphs G shown in Fig. 8.67.

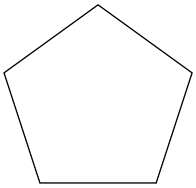


Fig. 8.67

Solution: The complement of G is shown in Fig. 8.68:

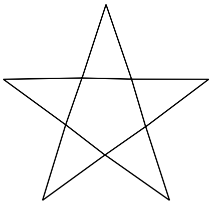


Fig. 8.68 Complement of G

Example 2: Draw simple unlabeled graphs of 3 vertices.

Solution: The graphs shown in Fig. 8.69 are simple graphs with three vertices.

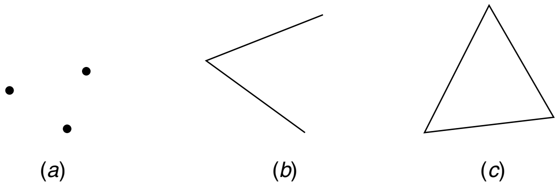


Fig. 8.69 Simple unlabeled graphs

Example 3: Find the number of connected graphs with four vertices and draw them.

Solution: There five connected graphs with four vertices (*see* Fig. 8.70):

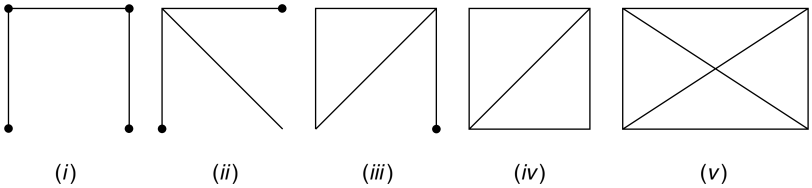


Fig. 8.70

Example 4: Draw the graph $K_{2,5}$

Solution: The graph $K_{2,5}$ has 2 × 5 = 10 edges and 7 vertices. It is shown in Fig. 8.71. The partitioned sets are $A = \{u_1, u_2\}$ and $B = \{v_1, v_2, v_3, v_4, v_5\}$.

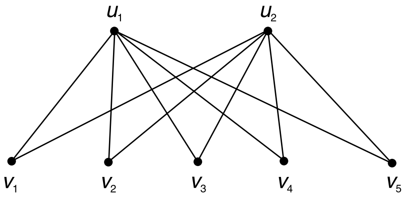


Fig. 8.71

8.26 ISOMORPHISM

Definition 8.54: Two graphs G and G' are isomorphism if there is a function $f: V(G) \to V(G')$, from the vertices of G to the vertices of G' such that

(*i*) f is one-one,

(*ii*) f is onto, and

(*iii*) For each pair of vertices u and v of G, $\{u, v\} \in E(G)$ if and only if $\{f(u), f(v)\} \in E(G')$ (i.e., f-preserves adjacency).

If $f: G \to G'$ is an isomorphism, then G and G' are said to be isomorphic and if two graphs G and G' are isomorphic then there may be several isomorphisms from G to G'.

If two graphs G and G' are isomorphic and $f: G \to G'$ is an isomorphic then

(*i*) $|V(G)| = |V(G')|$

(*ii*) $|E(G)| = |E(G')|$

(*iii*) The degree sequences of G and G' are the same.

(*iv*) If $v_0 - v_1 - v_2 - \ldots - v_{k-1} - v_1$ is a cycle of length G,
then $f(v_0) - f(v_1) - f(v_2) - \ldots - f(v_{k-1}) - f(v_1)$ is a cycle in G'.

Two graphs G and G' may have same number of vertices and same degree sequence, but they may not be isomorphic. The graphs shown in Fig. 8.72 have same degree sequence, send same number of vertices. But are non-isomorphic.

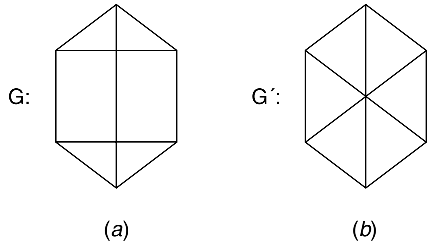


Fig. 8.72 Non-isomorphic graphs with same degree sequence

Usually we employ the adjacency matrix to check whether or not the given G and G' are isomorphic suppose $f: G \to G'$ is a one-to-one onto function. Let $v_0 - v_1 - v_2 - ... - v_n$ be the vertex ordering of G and $f(v_0) - f(v_1) - f(v_2) - ... - f(v_n)$ be the corresponding vertex ordering of G'. Let A (G) denote the adjacency matrix for the vertex ordering $v_0 - v_1 - ... - v_n$ of G and $A(G')$ denote the adjacency matrix for the vertex ordering $f(v_0) - f(v_1) - ... - f(v_n)$ of G'. If A $(G) = A(G')$; then we conclude that the graphs G and G' are isomorphic and if $A(G) \neq A(G')$ then f is not an isomorphism.

Theorem 8.12: Let $G = (V, E)$ and $G' = (V', E')$ be any two graphs and $f: G \to G'$ an isomorphism. If $v \in V$ then $\deg(v) = \deg\ f(v)$.

Proof: Two points u^1 and v^1 of v are adjacent in the graph G if and only if $f(u^1)$ and $f(v^1)$ are adjacent in G'. Also f is one-to-one and onto. Therefore the number of vertices which are adjacent to $v \in V$ is equal to the number of vertices in v^1 which are adjacent to $f(v)$. Hence deg (v) = deg $f(v)$.

Definition 8.55: An isomorphism of a graph G onto itself is called an automorphism of G.

8.27 SOLVED EXAMPLES

Example 1: Show the graphs G and G' shown in Fig. 8.73 are isomorphic.

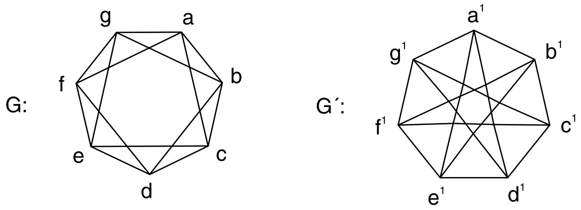


Fig. 8.73

Solution: Define a mapping $\varnothing$: $G \to G'$ such that

$$\varnothing\ (a) \to a^1$$

$$\varnothing\ (b) \to c^1$$

$$\varnothing\ (c) \to b^1$$
$$\varnothing\ (d) \to f^1$$
$$\varnothing\ (e) \to c^1$$
$$\varnothing\ (f) \to g^1$$
$$\varnothing\ (g) \to d^1$$

clearly the mapping $\varnothing$ is one-to-one and onto. $\varnothing$ preserves the adjacency.

$\varnothing\ G \to G'$ is an isomorphism note that both G and G' have 7 vertices and 14 edges each. Every vertex in G and G' is of degree 4.

Example 2: Show that the graphs G and G' (in Fig. 8.74) are isomorphic.

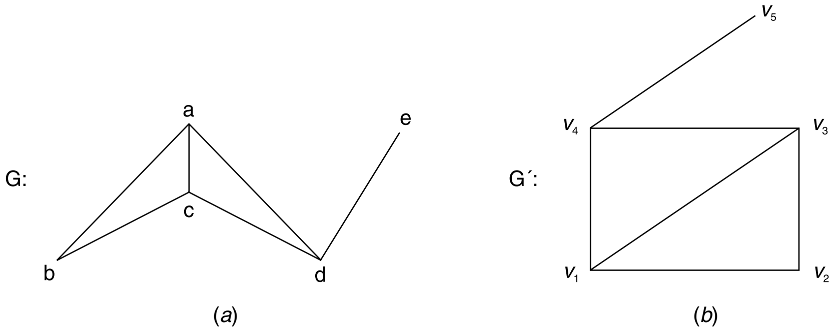


Fig. 8.74

Solution: Consider the map $f: G \to G'$ defined as follows:

$f(a) = v_1$, $f(b) = v_2$, $f(c) = v_3$, $f(d) = v_4$, $f(e) = v_5$. The adjacency matrix of G for the ordering a, b, c, d, e and the adjacency matrix of G' for the ordering.

$a \to v_1, b \to v_2, c \to v_3, d \to v_4, e \to v_5$ is the matrix.

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

i.e., $$A(G) = A(G')$$

Hence G and G' are isomorphic.

Example 3: Show that the graph G in Fig. 8.75 has a sub-graph isomorphic to $K_{3,\,3}$. Identify the sub-graph.

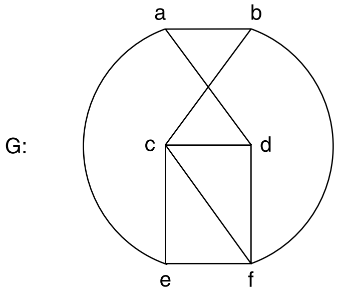


Fig. 8.75

Solution: Delete the edge $\{c, f\}$ from G. We get a sub-graph of G whose vertex set can be partitional into the sets.

$A = \{a, c, f\}$, $B = \{b, d, e\}$ and the sub-graph obtained can be drawn as follows:

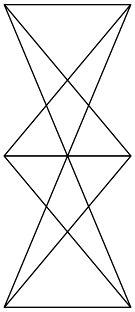


Fig. 8.76

Clearly the sub-graph obtained is $K_{3,\,3}$. Hence G has a sub-graph which is isomorphic to $K_{3,\,3}$.

Definition 8.56: A graph G is said to be self-complementary, if G is isomorphic to its complement $\overline{G}$ graphs G shown in Fig. 8.77 is self-complementary.

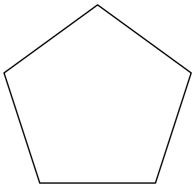


Fig. 8.77 Self-Complementary graph

Example 4: Show that a graph G is self-complementary if it has $4n$ or $4n + 1$ points (n is a non-negative integer).

Solution: Let $G = (V, E)$ be a self-complementary graph with m points.

Since G is self-complemary, G is isomorphic to $\overline{G}$.

We have $$|E(G)| = |E(\overline{G})|$$

or $$|E(G)| = |E(\overline{G})| = \frac{m(m-1)}{2}$$

or $$2\,|E(G)| = \frac{m(m-1)}{2}$$

i.e., $$|E(G)| = \frac{m(m-1)}{4}$$

$\frac{m(m-1)}{4}$ is an integer and one of m or $(m - 1)$ is odd.

i.e., m or $(m - 1)$ is a multiple of 4.

Hence n is of the form $4n$ or $4n + 1$.

Note: From the above it is clear that; a graph G with n vertices is isomorphic to its complement of n or $n - 1$) is a multiple of 4 and number of edges in G = number of edges in $\frac{n(n-1)}{4}$

Example 5: Can be graph with seven vertices be isomorphic to its complement.

Solution: We have $n = 7$

Since $$n - 1 = 7 - 1 = 6$$

Neither 7 n or 6 is a multiple of 4.

Hence a graph with 7 vertices cannot be isomorphic to its complement.

Example 6: Show that the graphs shown in Fig. 8.78 are isomorphic.

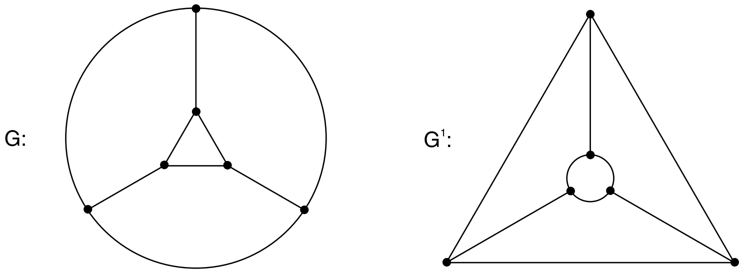


Fig. 8.78

Solution:

(*i*) Both the graphs G and G^1 have same number of vertices i.e., $|V(G)| = |V(G^1)| = 6$.

(*ii*) Both the graphs G and G^1 have same number of edges i.e., $|E(G)| = |E(G^1)| = 9$.

(*iii*) The degree sequences of G and G^1 are same i.e., (3, 3, 3, 3, 3, 3).

But the graphs are not labeled. We label the vertices of the graphs as shown in Fig. 8.79:

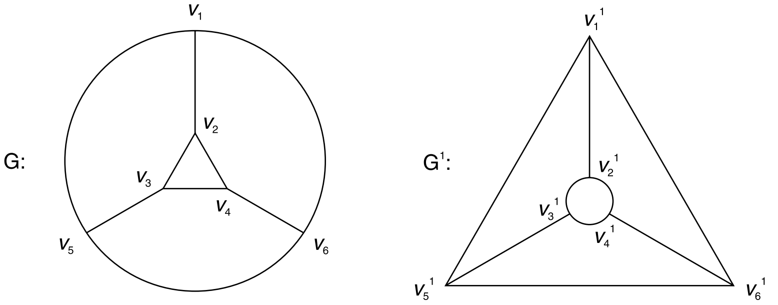


Fig. 8.79

Define a mapping $\varnothing: G \to G'$ by $\varnothing(v_i) = v_i'$

The mapping $\varnothing$ – preserves adjacency.

Hence G and G' are isomorphic.

Example 7: Show that graphs G_1 and G_2 are not isomorphic (Fig. 8.80).

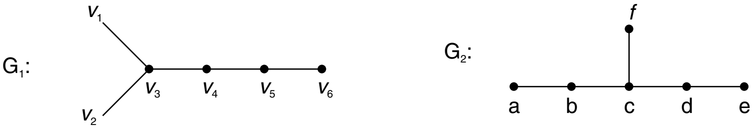


Fig. 8.80

Solution: We have number of vertices in G_1 = number of vertices in G_2 and number of edges in G_1 = number of edges in G_2. In the graph G_1, we have a vertex V_3 of degree 3.

There are two pendant vertices adjacent to V_3 in G_1 but in the graph G_2, the C which is of degree 3 has only are pendant vertex adjacent to it. Hence adjacency is not preserved in the graphs.

$\therefore$ G_1 and G_2 are not isomorphic.

Example 8: Give an example to show that two graphs of same order and same size need not be isomorphic.

Solution: Consider the graphs G_1 and G_2 as shown in Fig. 8.81.

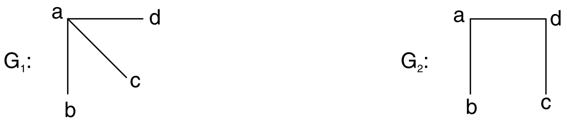


Fig. 8.81

Both the graphs G_1 and G_2 have same number of vertices and same number of edges, but adjacency is not preserved.

The degree sequence of G_1 is (1, 1, 1, 3)

The degree sequence of G_2 is (1, 1, 2, 2)

Therefore, G_1 and G_2 are not isomorphic.

EXERCISE 8.3

1. A graph G has 16 edges and each vertex is of degree 2. Find the number of vertices in G.

2. Draw the following graphs:

(*a*) 2-regular graph

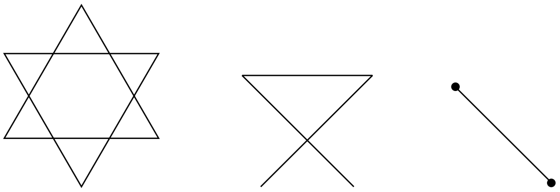
(*b*) 3-regular graph

(*c*) $K_{2,5}$ (*d*) $K_{3,3}$ (*e*) N_5 (null graph having 5 vertices)

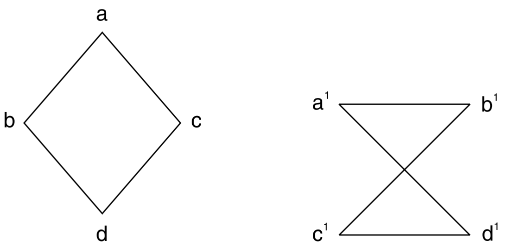
(*f*) W_5 (*g*) K_4 (*h*) K_5

3. A graph G has 35 edges and each vertex of G has degree atleast 3. Show that maximum number of (Possible) vertices that G can have is 23.

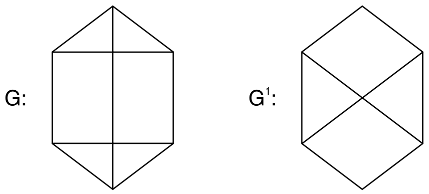
4. Draw the complement of the graph:



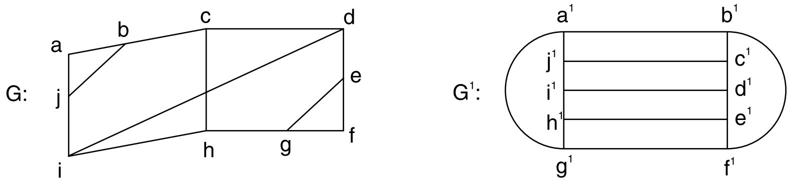
5. Show that the graphs G and G^1 are isomorphic:



6. Show that the graphs G and G^1 have the same degree sequence but are not isomorphic:

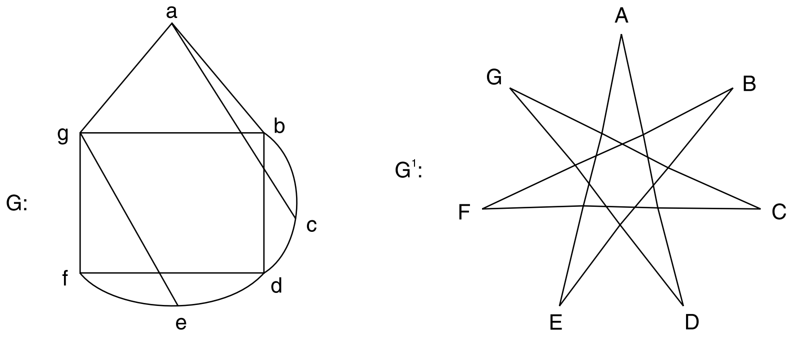


7. Show that the following graphs are not isomorphic:

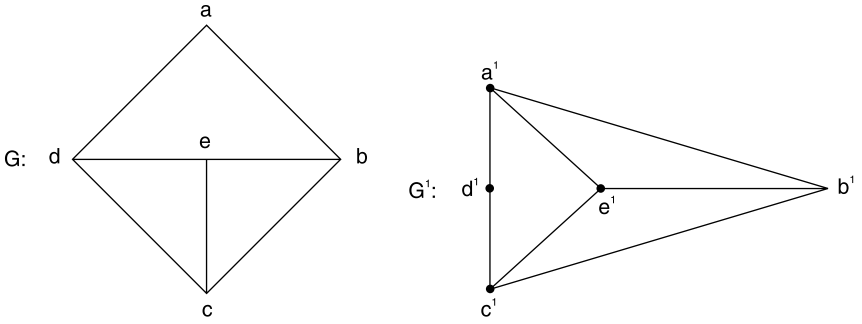


8. Show that the graphs G and G^1 are isomorphic:

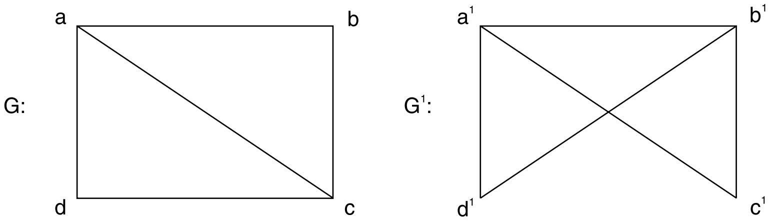
(*a*)



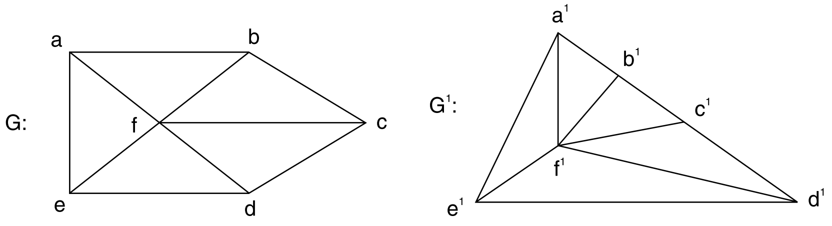
(*b*)



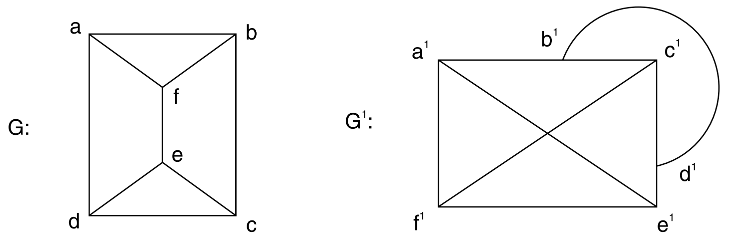
(*c*)



(*d*)

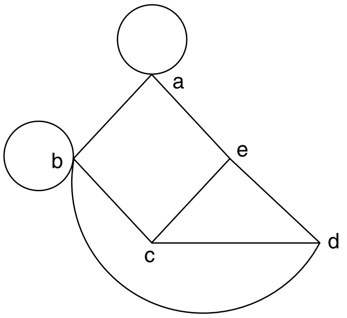


(*e*)

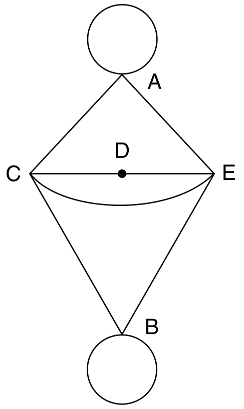


9. In the following graphs group those which are isomorphic to each other:

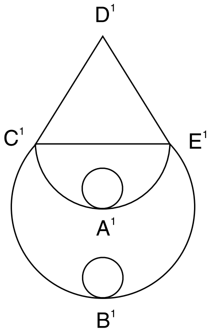
(O.U., MCA, 1991)



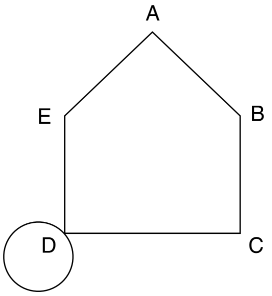
(*i*)



(*ii*)



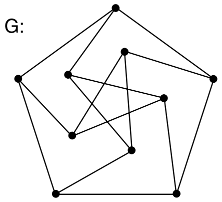
(*iii*)

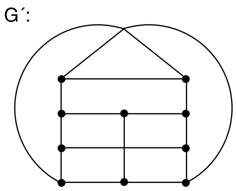


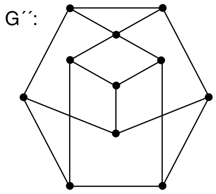
(*iv*)

10. Let C_n be a cycle graph with *n* vertices. Prove that C_5 is the only cycle graph isomorphic to its complement.

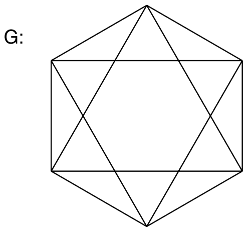
11. Prove that the following three graphs are isomorphic:

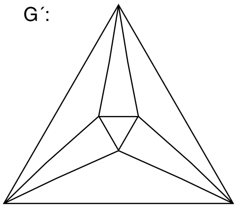






12. Show that the following graphs are isomorphic:





13. Show that every cubic (3-regular) graph has even number of points.

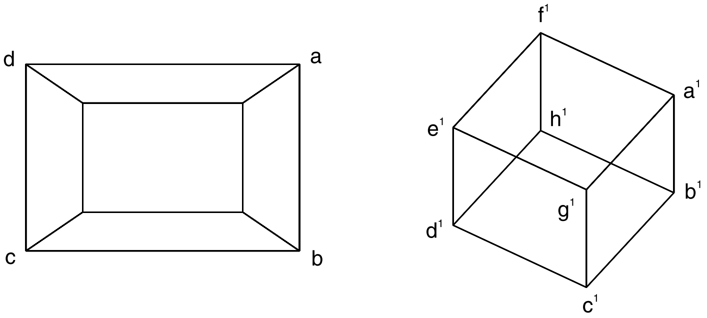
14. Prove that two graphs are isomorphic if and only if their complements are isomorphic. ***(O.U., MCA, 1995)***

15. G_1 and G_2 are two isomorphic graphs. Show that G_2 is connected if G_1 is connected.

16. If a graph of n vertices is isomorphic to its complement how many vertices must it have.

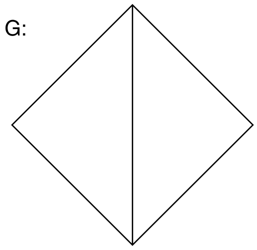
17. Prove that the cycle graph C_5 is isomorphic to its complement.

18. Show that the graphs G and G^1 are isomorphic.



19. Prove that a simple graph with n vertices must be connected if it has more than $\dfrac{(n-1)(n-2)}{2}$ edges.

20. Write down all possible non-isomorphic sub-graphs of the graph G. How many of them are spanning sub-graphs?



21. Show that maximum number of lines among all p point graphs with no triangle is $[P^2/4]$.

22. Define isomorphic graph. Give example. ***(MKU, 2001)***

8.28 FOREST

Definition 8.57: A graph is acyclic if it has no cycles. A forest is an acyclic graph.

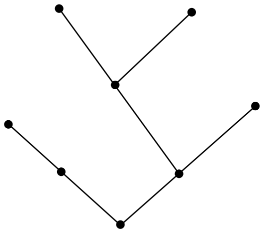


Fig. 8.82 A Forest

8.29 CUT VERTEX

Definition 8.58: Let G be a connected graph. If v is a vertex of G such that $G - v$ is not connected then, the vertex v is called a cut vertex.

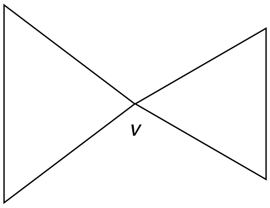


Fig. 8.83

If v is a cut vertex of G, then the removal of the vertex v increase the number of components in G. A cut vertex is also called a cut point.

Theorem 8.13: A vertex v in a connected graph G is a cut vertex if and only if there exist vertices u and w distinct from v such that every path connecting u and w contains the vertex v.

Proof: Let v be a cut vertex in a connected graph G. Then $G - v$ is disconnected and $G - v$ contains atleast two components say A and B. Let u be a vertex of A and W be a vertex of B. There is no path in $G - v$ connecting u and w. Since G is connected there exists a path P from u to w in G. If the path does not contain v, then the removal of v from G will not disconnect the vertices u and w, which is a contradiction to the fact that u and v lie is two different components of $G - v$.

Conversely; if every path from y to w contains the vertex v, then removal of v from the graph G disconnects u and w. Hence u and w lie in different components of G. Which shows that $G - v$ is a disconnected graph. Thus v is a cut vertex of G.

8.30 CUT EDGE (BRIDGE)

Definition 8.59: Let G be a connected graph. If e is an edge of G, such that G-e is not connected, the edge e is called a cut edge (or bridge). In the graph of Fig. 8.84, the edge e is a cut edge.

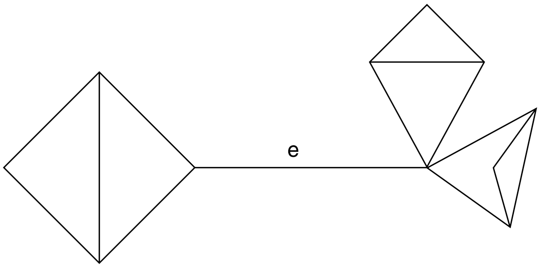


Fig. 8.84

8.31 CUT SET

Definition 8.60: Let G be a connected graph. A cut set in G is a set of edges whose removal from G leaves the graph G disconnected provided no proper subset of these edges disconnects the graph G.

A cut set in a graph always breaks the graph G into two parts. Every edge in a tree is a cut set, since the removal of any edge from a tree breaks the tree into two parts. In the graph shown in Fig. 8.85, the set of edges $\{a, c, d, f\}$ is a cut set.

Cut sets are of great importance in studying the properties of networks.

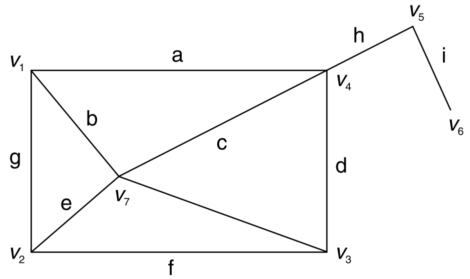


Fig. 8.85

8.32 SEPARABLE AND NON-SEPARABLE GRAPHS

Definition 8.61: A connected graph with at least one cut vertex is called a separable graph.

If G is a separable graph, then G is connected and there exists a subgraph H of G such that H and $\overline{H}$ (complement of H in G) have only one vertex in common.

Definition 8.62: A graph G is called a non-separable graph if it is connected, non-trivial and has no cut points. It is often called a block.

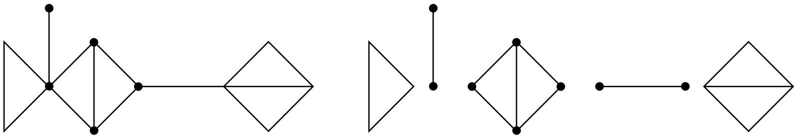


Fig. 8.86 A graph and its blocks

8.33 LABELED AND WEIGHTED GRAPHS

A graph in which each vertex is assigned a unique label is called labeled graph. Labeled graphs are useful in counting the number of different graphs. The graph G in Fig. 8.87 is a labeled graph.

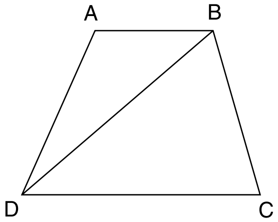


Fig. 8.87 A Labeled graph

A graph is called a weighted graph is each edge e is assigned a non-negative number w (e) called the weight of e. The graph G in Fig. 8.88 is a weighted graph.

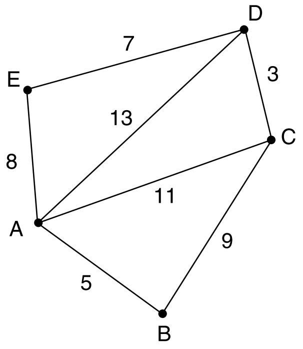


Fig. 8.88 A Weighted graph

If G is weighted graph and P is path G, then the weight of the path P is the sum of weights of the edges in the path.

8.34 CONNECTIVITY

8.34.1 Edge Connectivity

Definition 8.63: Let G be a connected graph. The edge connectivity of G is the minimum number of lines (edges) whose removal results in a disconnected or a trivial graph.

The edge connectivity of a connected graph G is denoted by $\lambda(G)$. If G is a disconnected graph, then $\lambda(G) = 0$. If G connected graph G has a bridge, then the edge connectivity of G is one.

From the definition, edge connectivity is the minimum cardinality of a cut set among all the cut sets of a connected graph.

8.34.2 Vertex Connectivity

Definition 8.64: Let G be a connected graph. The minimum number of vertices whose removal results in a disconnected or trivial graph is called the vertex connectivity of G.

The vertex connectivity of G is denoted by k (G). If k (G) then G has a vertex v such that $G - v$ is not connected and the vertex v is called a cut vertex or articulation point. If $G = K_n$ the complete graph with n vertices then k (G) $n - 1$. The vertex connectivity C_n (cycle graph with n vertices) is two. (for $n \geq 4$). If a graph G has a bridge then the vertex connectivity of G, i.e., k $(G) = 1$.

Theorem 8.14: The edge connectivity of a connected graph G cannot exceed the minimum degree of G, i.e., $\lambda(G) \leq \delta(G)$.

Proof: Let G be a connected graph and v be a vertex of minimum degree in G. Then the removal of edges incident with the vertex v disconnects the vertex v from the graph G. Thus the set of all edges incident with the vertex v forms a cut set of G. But from the definition, edge connectivity is the edge connectivity of G cannot exceed the minimum degree of v, i.e., $\lambda(G) \geq \Delta(G)$.

Theorem 8.15: The vertex connectivity of a graph G is always less then or equal to the edge connectivity of G i.e., $k(G) \leq \lambda(G)$.

Proof: If graph G is disconnected or trivial then $k(G) = \lambda(G) = 0$. If G is connected and has a bridge e, then $\lambda = 1$. In this case $K = 1$, since either G has a cut point incident with e or G is K_2.

$\therefore$ $k(G) \le \lambda(G)$ when $\lambda(G) = 0$ or 1, finally let us suppose that $\lambda(G) \ge 2$. The G has λ lines whose removal disconnects G. Clearly the $\lambda - 1$ of these edges produces a graph with a bridge $e = \{u, v\}$. For each of these $\lambda - 1$ edges select an incident point which is different from u or v. The removal of these points (vertices) also removes $\lambda - 1$ edges and if the resulting graph is disconnected then $k \le \lambda - 1 < \lambda$. If not the edge $e = \{u, v\}$ is a bridge and hence the removal of u and v will result in either a disconnected or a trivial graph. Hence $k \le \lambda$ in each case and this completes the proof of the theorem.

Thus, the vertex connectivity of a graph does not exceed the edge connectivity and edge connectivity of a graph cannot exceed the minimum degree of G. Hence the theorem given below:

Theorem 8.16: For any graph G, $k(G) \le \lambda(G) \le \delta(G)$

A graph G is n-connected if $K(G) \ge n$ and n-edge connected if $\lambda(G) \ge n$. Thus a non-trivial graph is 1-connected if and only if is connected and 2-connected if and only it is a block having more than one edge.

A maximal n-connected sub-graph G is called an n-component of G. Two distinct n-components of a graph G have at most $n - 1$ points in common. The graph shown in Fig. 8.89 is a 3-component graph.

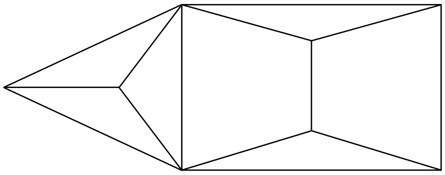


Fig. 8.89 A graph with two 3-components

Example 1: G is (p, q), prove that, if G is K-connected then $q \ge \dfrac{pk}{2}$.

Solution: Let G be K-connected graph.

Then $q \le \delta(G)$

We have
$$q \ge \frac{1}{2} \sum \deg(v_i) \ge \frac{1}{2}\, p\, \delta(G)$$

or
$$q \ge \frac{pk}{2}$$

Example 2: Find the edge connectivity and the vertex connectivity of the graph in Fig. 8.90.

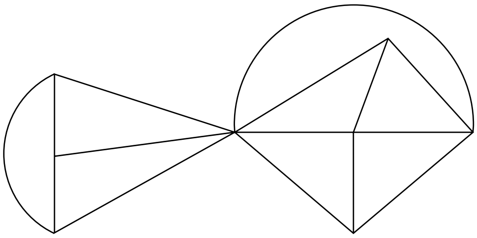


Fig. 8.90

Solution: The minimum number of edges removal disconnects the graph is 3 and the minimum number of vertices required to disconnect the graph is 1.

$\therefore$ Edge connectivity $\lambda(G) = 3$

Vertex connectivity $k(G) = 1$.

8.34.3 Girth, Circumference and Diameter

Let G be a graph. The length of the largest simple parts between any two vertices of G is called the girth of G, while the length of the longest cycle between any two vertices in G is called the circumference of G. The length of the longest path between any two vertices of a connected graph G is called the diameter of G.

If G is a cycle graph with n vertices (i.e. C_n), then the diameter of G is $(n-1)$ and the circumference of G is n.

If G is a complete graph within vertices (i.e. k_n), then the circumference of G is n and the diameter of G is $(n–1)$.

The girth of C_3 is 2.

The circumference of C_3 is 3 and diameter of C_3 is 3/2.

The girth of k_4, (complete graph with 4 vertices) is 3.

The circumference of k_4 is 4 and the diameter of k_4 is 2.

The girth of $k_{m,m}$ (complete Bipartite graph) is $2m–1$.

The circumference of $k_{m,m} = 2m$ if $m > 1$
$= 0$ if $m = 1$

The diameter of $k_{m,m} = m$ if $m > 1$
$= 0$ if $m = 1$

Example 1: The girth of $k_{1,1}$ is 1

The circumference of $k_{1,1} = 0$

The radius of $k_{1,1} = 0$

Example 2: The Girth of $k_{3,3} = 2 \cdot 3 - 1 = 5$

The circumference of $k_{3,3} = 2 \cdot 3 = 6$

The diameter of $k_{3,3} = m = 3$

EXERCISE 8.4

1. Define

(*a*) The edge connectivity of a connected graph. ***(MKU, MCA, 2002)***

(*b*) The vertex connectivity of a graph.

2. Prove that there is no 3-connected graph with 7 edges.

3. If a graph G is not connected then show that $\overline{G}$ is connected.

4. Let G be a connected graph and v is a point of G, then show that the following are equivalent:

(*a*) v is a cut point of G.

(*b*) There exists a partition $V - \{v\}$ into subsets U and W such that for each $u \in U$ and $w \in W$ the points v is on every $u - w$ path.

(*c*) There exists two points u and w distinct from v such that v is on every $v - w$ path.

5. If e is an edge of a connected graph. Show that the following statements are equal:

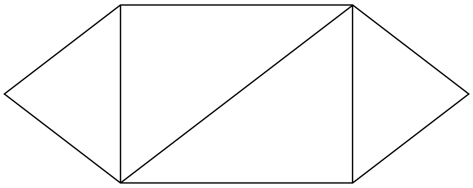
(*a*) e is bridge of G.

(*b*) There exists a partition of V into two subsets A and B such that for every point $u \in A$ and $w \in B$ the edge e is on every $u - w$ path.

(*c*) There exist two points, u and w such that the edge e is on every $u - w$ path.

6. Show that every non-trivial connected graph has atleast two points which are not cut points.

7. Find the edge connectivity and vertex connectivity of the graph given below:



8. Prove that the vertex connectivity of a graph G can never exceed the edge connectivity of G.

9. Define a connected graph. ***(MKU, MCA, May 2002)***

8.35 TREES AND SOME PROPERTIES OF TREES

The concept of a tree is important for these interested in applications of graphs. The important applications of trees include searching, sorting, syntax checking and database management. The tree is one of the most non-linear structures used for algorithm development in computer science. In this section, we shall define a tree and study its properties.

8.35.1 Tree

Definition 8.65: A tree is a connected graph without any circuits.

From the definition, it is clear that a tree is a connected and a cyclic graph. It has neither self-loops nor parallel edges and is denoted by the symbol T. Since trees are a cyclic, we adopt a convention similar to that used for Hasse diagrams. Trees may be directed or non-directed.

8.35.2 Directed Tree

Definition 8.66: A connected, a cyclic, directed graph is called a directed tree.

The graph in Fig. 8.91 (*a*) is a non-directed tree and graph shown in Fig. 8.91 (*b*) is a directed tree:

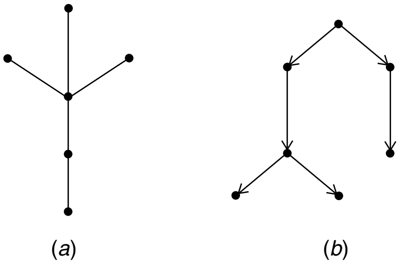


Fig. 8.91 Tree

If T is a tree, then it has a unique simple non-directed path between each pair of vertices. A tree with only are vertex is called trivial tree. If T is a not a trivial tree then it is called a non-trivial tree. The vertex set (i.e., the of nodes) of a tree is a finite set. In most cases the vertices of a tree are labeled.

Theorem 8.17: A simple non-directed graph G is a tree if and only if G is connected and has no cycles.

Proof: Let G be a tree. Then each pair of vertices of G are joined by a unique path, therefore G is connected. Let u and v be two distinct vertices of G. Such that G contains a cycle containing u and v. Then u and v are joined by atleast two simple paths, one along one portion of the cycle and the other path completing the cycle. This contradicts our hypothesis that there is a simple unique path between u and v. Hence tree has no cycle.

Conversely let G be a connected graph having no cycles. Let v_1 and v_2 be any pair of vertices of G and let there be two different simple paths say P_1 and P_2 from v_1 to v_2. Then we can find a cycle in G as follows: Since the paths P_1 and P_2 are different, there must be a vertex say u, which is on both P_1 and P_2 but its successor on P_1 is not on P_2. If u' is the next point on P_1 which is also on P_2, the segments of P_1 and P_2 which are between P_1 and P_2 form a cycle in G. A contradiction. Hence there is atmost one path between any two vertices of G, which shows that G is a tree.

Theorem 8.18: Any non-trivial tree has atleast one vertex of degree 1.

Proof: Let G be a non-trivial tree, then G has no circuits. Let v_1 be any vertex of G. If deg $(V_1) = 1$, then the theorem is at once established. Let $\deg(v_1) \neq 1$ move along any edge to a vertex V_2 incident with v_1. If $\deg(v_2) \neq 1$ then continue to another vertex say v_3 along a different edge. Continuing the process, we get a path $v_1 - v_2 - v_3 - v_4 - ...$ in which none of the $v_i^1\ s$ is repeated. Since the number of vertices in a graph is finite, the path must end some where. The vertex at which the path ends is of degree are, since we can enter the vertex but cannot leave the vertex.

Theorem 8.19: A tree T with n vertices has exactly $(n - 1)$ edges.

Proof: The theorem will be prove by mathematical induction on the number of vertices of a tree. If $n = 1$ then there are no edges in T. Hence the result is trivial.

If $n = 2$ then the number of edges connecting the vertices is one i.e., $n - 1$. Hence the theorem is true for $n = 2$. Assume that the theorem holds for all trees with fewer than n vertices. Consider a tree T with n vertices. Let V be a vertex in T of degree 1 and let T' denote the graph obtained by removing the vertex v and edge e associated with it from T. Consider $T' = T - e$.

T' has $n - 1$, vertices and fewer edges than T. If v_1 and v_2 are any two vertices in T', then there is a unique simple path from v_1 to v_2 which is not affected by the removal of the vertex and edge.

T' is connected and no edges in it, therefore T' is a tree. T' has $n - 1$ vertices and $n - 1 - 1 = n - 2$ edges. T has are more edge than T'.

$\therefore$ Number of edges in $T = n - 2 + 1 = n - 1$. Hence T has exactly $n - 1$ edges.

Theorem 8.20: Every non-trivial tree has atleast 2 vertices of degree 1.

Proof: Let m denote the number of vertices of degree 1 (i.e., pendant vertices) and n be the number of vertices in the tree T (where $n \geq 2$).

Let $v_1, v_2, v_3, ..., v_m$ denote the m vertices of degree 1 in T. Then each of the remaining $n - m$ vertices $v_{m+1}, v_{m+2}, ...,$ has degree atleast two.

Thus $\deg(v_i) = 1$ for $i = 1, 2, ..., m$

≥ 2 for $i = m + 1, m + 2, ..., n$

We have $$\sum_{i=1}^{n} \deg(v_i) \geq n + 1 \cdot (n - m)$$

or $$2(n - 1) \geq 2n - m$$

or $$2n - 2 \geq 2n - m$$

or $$-2 \geq -m$$

or $$m \geq 2$$

Thus T contains atleast two vertices of degree 1.

Theorem 8.21: A graph G is a tree if and only if G has no cycled and $|E| = |V| - 1$.

Conversely, let G be a graph such that G has no cycles and $|E| = |V| - 1$. Clearly G is connected.

Let $G_1, G_2, G_3, ... G_k$ be k components of G where $K > 1$.

G has no cycles, therefore each G_i, is connected and each G_i has no cycle in it.

Number of edges in each $G_i = |V_i| - 1$

Hence number of edges in G

$$= |V_1| - 1 + |V_2| - 1 + ... + |V_k| - 1$$
$$= |V_1| + |V_2| + ... + |V_k| - K$$
$$= |V| - K$$

by hypothesis G has $|V| - 1$edges

Thus $$|V| - k = |V| - 1$$

or $$K = 1$$

The number of components in G is one and G is connected.

Hence G is a tree.

8.36 DISTANCE

If u and v are two vertices of a connected graph G, there may be more than one path joining u and v. Various concepts can be defined based on the lengths of such paths between vertices of G. The simplest is given below:

Definition 8.67: If G is connected graph and u and v are any two vertices of G, the length of the shortest path between u and v is called the distance between u and v and is denoted by $d\,(u, v)$.

The distance function on defined above has the following properties. If u, v and w are any three vertices of a connected graph then.

(*i*) $d\,(u, v) \geq$ and $d\,(u, v) = 0$ iff $u = v$

(*ii*) $d\,(u, v) = d\,(v, u)$

and (*iii*) $d\,(u, v) \leq d\,(u, w) + d\,(w, v)$

from the above, it is clear that distance in a graph is a metric.

Example 1: In the graph shown in Fig. 8.92.

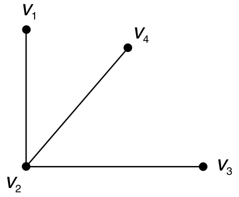


Fig. 8.92

Definition 8.68: Let G be a connected graph. For any vertex v on G, the eccentricity of v denoted by $e\,(v)$ is

$e\,(v) = \max \{d\,(u, v) : u, v \in v\}$

$e\,(v)$ is the length of the longest path in G starting from the vertex v.

Example 2: In the graph shown in Fig. 8.93. $e\,(v_1) = 3$

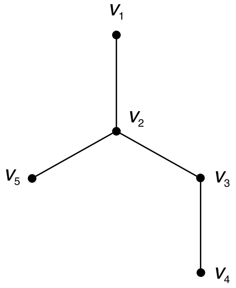


Fig. 8.93

Definition 8.69: The diameter of a connected r graph G is defined as the maximum eccentricity among all vertices of the graph G. It is denoted by d.

Hence d = diameter of G = max $\{e(v): v \in V\}$

Definition 8.70: The radius of a connected graph G is defined as the maximum eccentricity among all vertices of the graph. It is denoted by r.

Thus r = radius of G = min $\{e(v): v \in V\}$

Note: The radius of connected graph may not be half of its diameter.

Example 3: Consider the tree T shown in Fig. 8.94.

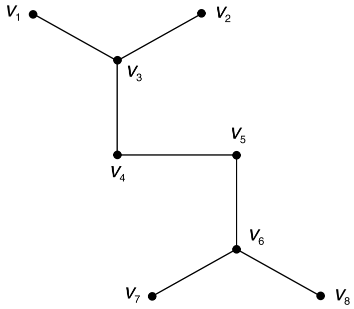


Fig. 8.94

We have $e(v_1) = 5$, $e(v_2) = 5$, $e(v_3) = 4$,
$e(v_4) = 3$, $e(v_5) = 3$, $e(v_6) = 4$,
$e(v_7) = e(v_8) = 5$

The radius of $T = r = 3$
and the diameter of $T = 5$

Definition 8.71: The centre of connected graph G is defined as the set of vertices having minimum eccentricity among all vertices of the graph. It is denoted by C or $C(G)$.

$$C = C(G) = \text{centre of } G = \{v \in V : e(v) = r\}$$

Example 4: Consider the graph shown in Fig. 8.93.

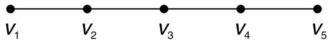


Fig. 8.95

$e(v_1) = 4$, $e(v_2) = 3$, $e(v_3) = 2$,
$e(v_4) = 3$, $e(v_5) = 4$, radius of $G = i = 2$.
Hence centre of $G = \{v_3\}$.

Note:

(1) Let G be a connected graph and $v_1, v_2, ..., v_n$ be 'n' vertices of G $e(v_1)$, $e(v_2)$, ... $e(v_n)$ is called the eccentricity sequence of G.
(2) The distance between two adjacent vertices of a connected graph G is 1.
(3) The maximum distance from each vertex of G occurs at a pendant vertices of G.
(4) If $C(G) = V(G)$ then G is called self-centred graph.
(5) If P is a path of even length the P has only one vertex at the centre.
(6) If P is a path of odd length this centre of P contains two adjacent vertices.

Example 5: In the graph shown in Fig. 8.96:

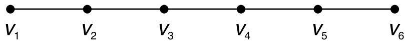


Fig. 8.96

Centre of $G = \{v_3, v_4\}$

Example 6: In the graph shown in Fig. 8.97. $C(G) = \{v_4, v_5\}$:

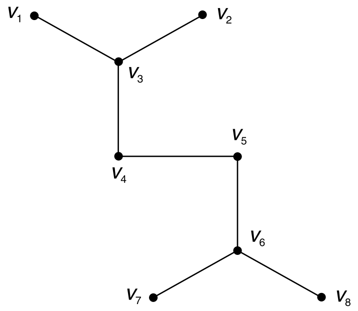


Fig. 8.97

Theorem 8.22: If r is the radius and d is the diameter of connected graph G then $r \leq d \leq 2r$.

Proof: From the definition of 'r' and 'd', we have $r \leq d$ ... (1)

Let u, v be the ends of a diametral path and w be the central vertex then

$$D = d(u, v) \leq d(u, v) + d(w, v) \leq r \text{ (Triangle inequality)}$$

or $$d \leq 2r \qquad \text{... (2)}$$

From (1) and (2)

$$r \leq d \leq 2r$$

8.37 SPANNING TREE

Definition 8.72: Let G be a connected graph. The sub-graph H of G is called a spanning tree of G if

(*i*) H is a tree

and (*ii*) H contains all the vertices of G.

A complete graph k_n has n^{n-2} different spanning trees.

Example 1: In the Fig. 8.98 H is spanning tree of G.

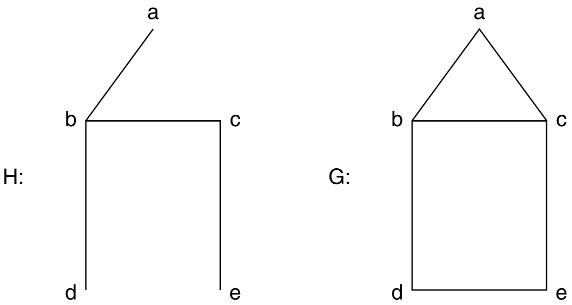


Fig. 8.98

Example 2: Find all the spanning trees of the graph G shown in the Fig. 8.99.

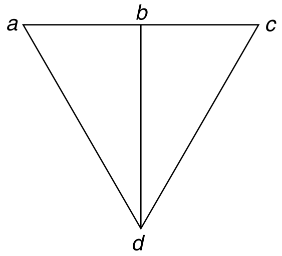


Fig. 8.99

Solution: The spanning trees of G are given below (Fig. 8.100):

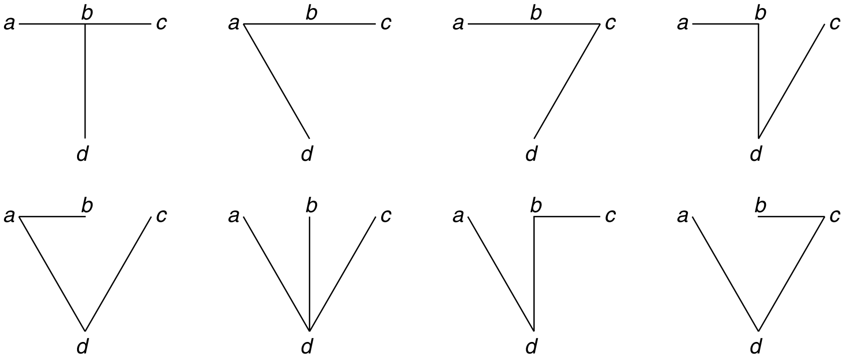


Fig. 8.100

Theorem 8.23: A non-directed graph G is connected if and only f G contains a spanning tree.

Proof: Let T be a spanning tree of G. There exists a path between any pair of vertices in G along the tree T. G is connected.

Conversely let G be a connected graph and K be the number of cycles in G. If $K = 0$, then G has no cycles and G is connected. Therefore G is a tree when $K = 0$.

Let us suppose that all connected graphs with fewer than K cycles have a spanning tree. Let G be a connected graph with n cycles. Let e be an edges in one of the cycle. $G - e$ is a connected graph and $G - e$ contains all the vertices of G.

$\therefore$ The spanning tree if $G - e$ is also spanning tree for G.

Hence by mathematical induction the result holds for all connected graphs.

If G is a connected graph and T is a spanning tree of G. Edges of G present in T are called the branches of G with respect to T_j and the edges of G which do not belong to T are called the chords of G with respect to T. If G has n vertices and e edges then, the number of branches with respect to the spanning tree T of G is $n - 1$ and the number of chords is $e - n + 1$.

The number of branches in a connected graph G is called the rank of G and the number of chords is called the nullity of G. If G has k components then the rank of G is defined as the sum of ranks of the components; i.e.,

$$\text{rank }(G) = \sum_{i=1}^{k} \text{rank}\,(G_i)$$

$$= \sum_{i=1}^{k}(n_i - 1) = \sum_{i=1}^{k} n_i - \sum_{i=1}^{k} 1$$

$$= n - k$$

where G_i, $i = 1, 2, ..., K$ are K components of G.

and nullity of $(G) = \sum_{i=1}^{k}$ nullity (G_i)

$$= \sum_{i=1}^{k}(e_i - n_i + 1)$$

$$= \sum_{i=1}^{k} e_i - \sum_{i=1}^{k} n_i + \sum_{i=1}^{k} 1$$

$$= e - n + 1$$

8.37.1 Minimal Spanning Tree

Definition 8.73: Let G be a connected weighted graph. A minimal spanning tree of G is a spanning tree of G whose total weight is as small as possible.

There are various methods to find a minimal spanning tree in connected weighted graph. Here we consider algorithms for generating such a minimal spanning tree.

8.37.2 Algorithm

A connected weighted graph with n vertices.

Step 1: Arrange the edges of G in the order of decreasing weights.

Step 2: Proceed sequentially, and delete each edge of G, that does not disconnect the graph G until $n - 1$ edges remain.

Step 3: Exit.

Example 1: Consider the graph G given below:

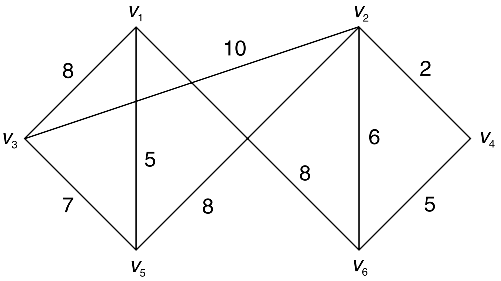


Fig. 8.101

Number of vertices in $G = n = 6$.

We apply the algorithm given above.

We order the edged by decreasing weights and delete the edges of G until $n - 1 = 6 - 1 = 5$ edges remain.

Edges	(v_2, v_3)	(v_1, v_6)	(v_1, v_3)	(v_2, v_5)	(v_3, v_5)	(v_2, v_6)
delete	yes	yes	yes	no	no	yes
Edges	(v_1, v_5)	(v_4, v_6)	(v_2, v_4)			
delete	no	no	no			

The minimal spanning tree of G is shown in Fig. 8.102:

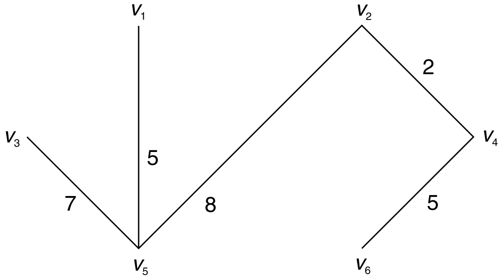


Fig. 8.102

The weight of the minimum spanning tree = 8 + 7 + 5 + 5 + 2 = 27.

8.37.3 Kruskals Algorithm

Input: A connected weighted graph G with n vertices.

Step 1: Arrange the edges of in order of increasing weights and select the edge with minimum weight.

Step 2: Proceed sequentially, add each edge which does not result in a cycle until $n - 1$, edges are selected.

Step 3: Exit.

Example 1: Consider the graph in Fig. 8.101.

We have $n = 6$

We order the edges by increasing weights (v_2, v_4) is edge with minimum weight. Select the edge (v_2, v_4) we successively add edges to (v_2, v_4), without forming cycles until $6 - 1 = 5$ edges are selected. This yields:

Edges	(v_2, v_4)	(v_1, v_5)	(v_4, v_6)	(v_2, v_6)	(v_3, v_5)	(v_1, v_3)	(v_1, v_6)	(v_2, v_5)	(v_2, v_3)
Weight	2	5	5	6	7	8	8	8	10
Add?	Yes	Yes	Yes	No	Yes	No	Yes	No	No

Edges in the minimum spanning tree are

$$(v_2, v_4), (v_1, v_5), (v_4, v_6), (v_3, v_5), (v_1, v_6).$$

The resulting minimal (optimal) spanning tree is shown in Fig. 8.103.

We apply the steps of Kruskal's algorithm to the graph of Fig. 8.101; as follows:

(v_2, v_4) is the edge with minimum weight, therefore we select the edge (v_2, v_4).

The next edge with minimum weight is (v_1, v_5), selection of (v_1, v_5) does not result in a cycle.

$\therefore$ edge (v_1, v_5) is selected.

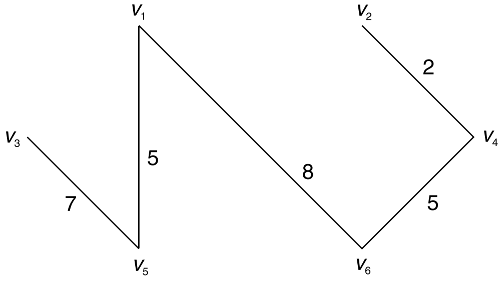


Fig. 8.103

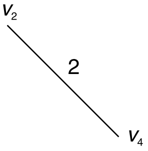


Fig. 8.104 (*a*)

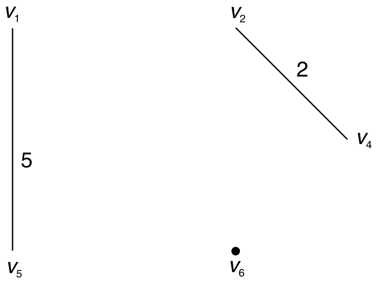


Fig. 8.104 (*b*)

The edge to be considered, next is (v_4, v_6).

The next edge to be selected is (v_4, v_6).

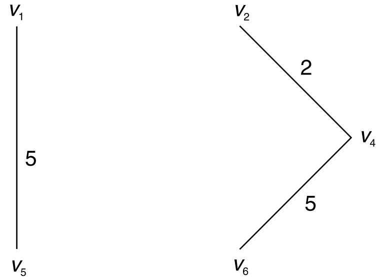


Fig. 8.104 (*c*)

Selection of the edge (v_2, v_6) for the spanning tree results in a cycle. Therefore (v_2, v_6) is not selected we consider the edge (v_3, v_5) selection of edge (v_3, v_5) does not result in a cycle. Hence (v_3, c_5) is selected.

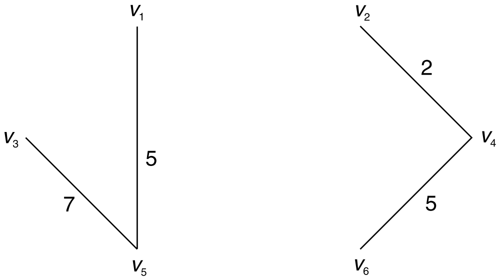


Fig. 8.104 (*d*)

Next we consider the edge (v_1, v_3) from the list. Selection of the edge (v_1, v_3) results in a cycle. Therefore edge (v_1, v_3) is not selected. Consider the edge (v_1, v_6) selection of edge (v_1, v_6) does not result in a cycle. Hence (v_1, v_6) is selected.

Number of edges selected is 5. We stop, and obtain the spanning trees as shown in Fig. 8.104 (*e*).

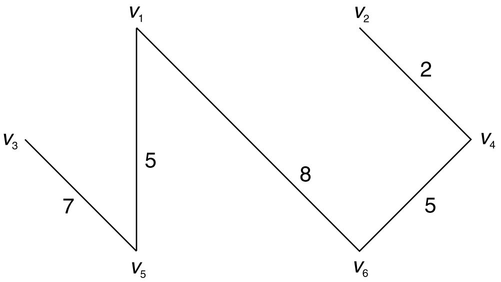


Fig. 8.104 (*e*)

The weight of the minimal spanning tree.

$$= 2 + 5 + 5 + 7 + 8$$
$$= 27$$

8.37.4 Prims Algorithm

Input: A connected weighted graph G with n vertices.

Step 1: Select an arbitrary vertex v_1 and an edge e_1 with minimum weight incident with vertex v_1.

Step 2: Having selected the vertices $v_1, v_2, ..., v_\text{i}$ and $e_1, e_2, ..., e_{i-1}$; select an edge e_i such that e_i connects a vertex of the set $(v_1, v_2, ..., v_i)$ and a vertex of $V = (v_1, v_2, ..., v_i)$ and of all such edges e_i has the minimum weight.

Step 3: Stop if $n - 1$, edges are selected, else go to step 2.

Example 1: Consider the graph shown in Fig. 8.105:

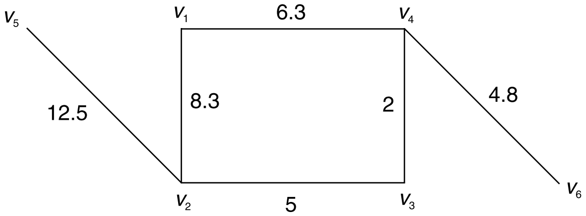


Fig. 8.105

Let
$$e_1 = (v_1, v_2), e_2 = (v_2, v_3)$$
$$e_3 = (v_3, v_4), e_4 = (v_4, v_1)$$
$$e_5 = (v_2, v_5) \text{ and } e_6 = (v_4, v_6).$$

Denote the edge of G.

We apply Prims algorithm to the graph as follows:

The edge $e_3 = (v_3, v_4)$ is an edge with minimum weight. Hence, we start with the vertex v_3 and select the edge e_3 incident with v_3.

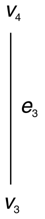


Fig. 8.106 (*a*)

We next consider the edges connecting a vertex $\{v_3, v_4\}$ with the vertex of the set $V - \{v_3, v_4\}$. We observe that e_6 the edge with minimum weight.

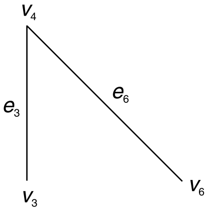


Fig. 8.106 (*b*)

Consider the edges connecting the vertices of the set $\{v_3, v_4, v_6\}$ with the vertices of $V - \{v_3, v_4, v_6\}$. The edge e_2 has the minimum weight. The edge e_2 is selected.

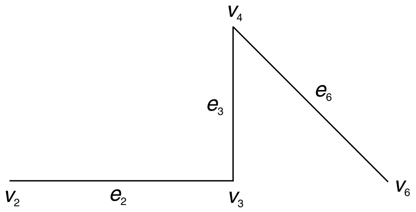


Fig. 8.106 (*c*)

of the connecting the vertices of $\{v_2, v_3, v_4, v_6\}$; with the vertex set $V - \{v_2, v_3, v_4, v_6\}$, e_4 has minimum weight, therefore e_4 is selected.

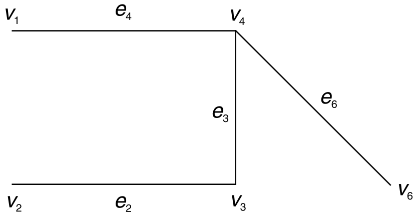


Fig. 8.106 (*d*)

e_1, e_5 are the edges remaining. e_5 is the only edge connecting $\{v_1, v_2, v_3, v_4, v_5, v_6\}$ and $\{v_5\}$ such that the inclusion of e_5 does not result in a cycle. Hence e_5 is selected.

Since number of edges selected is 5 we stop.

The minimal spanning tree obtained is shown in Fig. 8.106 (*e*).

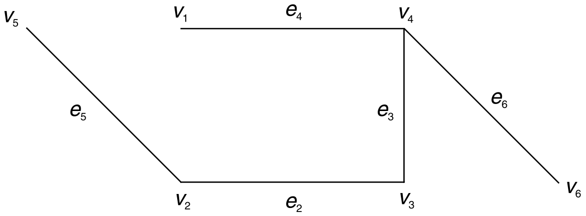


Fig. 8.106 (*e*)

Weight of the minimal spanning tree

$$= 2 + 4.8 + 5 + 6.3 + 12.5$$
$$= 30.6$$

8.38 ROOTED TREE

Definition 8.74: A rooted tree is a tree with a designated vertex called the root of the tree.

Any tree may be made into a rooted tree by selecting one of the vertices as the root. A rooted is a directed tree if there is a root from which there is a directed path to each vertex of the tree. The graphs in Fig. 8.107 are rooted trees in which the root of each is at the top.

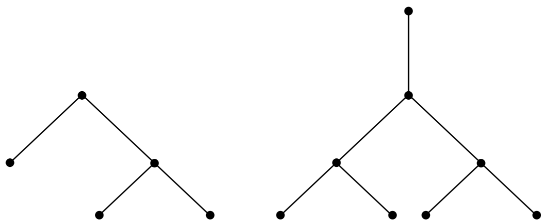


Fig. 8.107 Rooted trees

The level of a vertex in a rooted tree is the length of the path (number of edges) to v from the root. If T is a rooted tree with designated root v_0 and $v_0 - v_1 - v_2 - ... -v_{n-1} - v_n$ is a simple path in T, then v_{n-1} is called the parent of V_n and $v_0, v_1, v_2, ..., v_{n-1}$ are called the ancestors of v_n.

v_1 is a child of v_0, v_2 is a child of v_1, ...

If T is a rooted tree with designated vertex v_0 and u and v are two vertices (nodes) in T, then

(*i*) u is called a leaf of T, if it has no children (i.e., leaves of T are vertices of T with degree 1).

(*ii*) y is a descendant of u, if u is an ancestor of v.

(*iii*) Is an internal vertex of T, if v is not a leaf of T.

(*iv*) The sub-graph of T consisting of v and all its descendants with v as the designated root is a sub-tree of T rooted at v.

If T is a rooted tree then the maximum vertex level of T is called the depth of the tree. We usually adhere to the universal convention of representing the root of the tree as the top vertex (apex) of the tree. Rooted trees are useful in enumerating all the logical possibilities of a sequence of events where each event can occur in finite number f ways. If edges leaving each vertex of a rooted tree T are labeled, then T is called an ordered rooted tree. The vertices of an ordered to rooted can be labeled as follows: we assign 0 to the root of the tree. We next assign 1, 2, 3, 4, ... to the vertices immediately following the root of T according as the edges were ordered. The remaining vertices can be ordered as follows: If p is the label of a vertex v of T then p_1, p_2, p_3, ... are assigned to the vertices immediately following v according as the edges were ordered. The tree in Fig. 8.108 is an ordered rooted tree.

r is the root of the tree in Fig. 8.108. The vertices of T are labeled with their addresses. The system is known as universal address system for an ordered rooted tree.

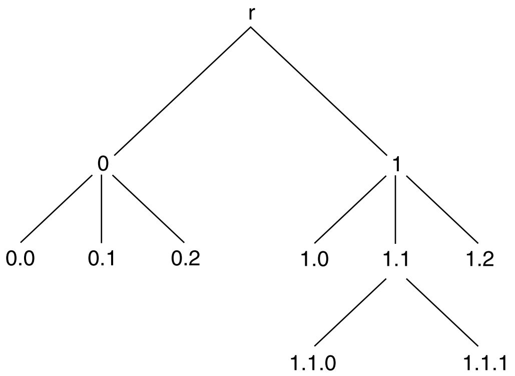


Fig. 8.108 Ordered rooted tree

8.39 EXPRESSION TREES

Algebraic expressions involving addition, subtraction, multiplication and division can be represented as ordered rooted trees called expression trees. The arithmetic expression $3 + 5 \times 9 - 7 \times 6^2$ can be represented as the tree shown in Fig. 8.109.

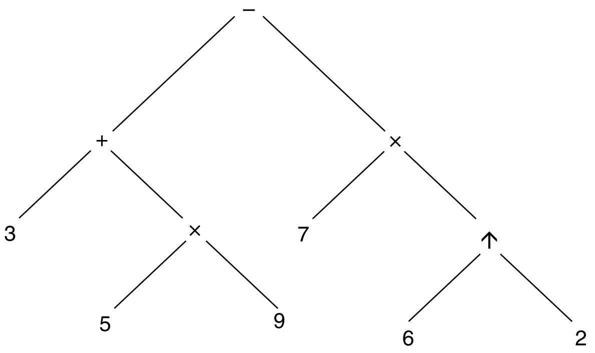


Fig. 8.109

The variables in the algebraic expression appear as the other vertices. In the polish prefix representation, we place the binary operational symbol before the argument and avoid parentheses. The expression $(a - b)/((c \times d) + e)$ can be expressed *as* $/ - ab + \times cde$.

Example: Write the following expression as a tree:

$$[(a \times b) \times c + (d + e) - (f - - (g \times h))]$$

Solution: The arithmetic expression $[(a \times b) \times c + (d + e) - (f - - (g \times h))]$ can be represented as the tree.

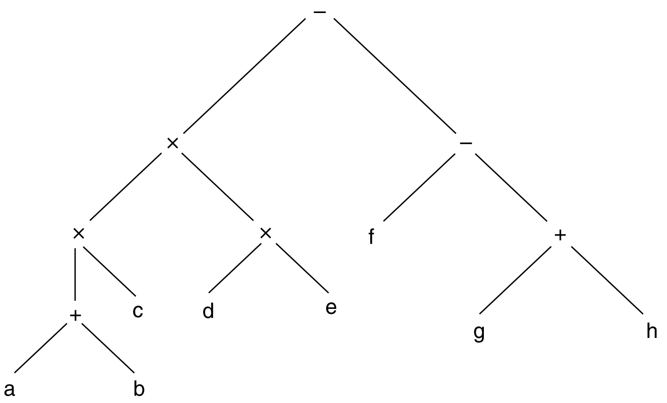


Fig. 8.110

8.40 BINARY TREE

So far we have discussed the tree, and its properties. Now we shall study about a special class of trees known as binary trees. They are special class of rooted tree. Binary trees play an important role in decision-making. They are extensively used in the study of computer search methods, binary identification problems and coding theory.

Definition 8.75: A tree in which there is exactly one vertex of degree two, and each of the remaining vertices of degree one or three, is called a binary tree.

If T is a binary tree, the vertex of degree two which is distinct from all the other vertices of T serves as a root of T. Thus every binary tree is a rooted tree. The vertices of degree one in a binary tree are called external vertices and all the remaining vertices are called internal vertices. The number of internal vertices in a binary tree is one less than the number of pendant vertices.

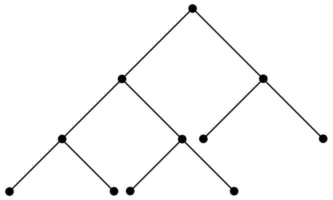


Fig. 8.111 Binary tree

The leaves of binary tree are vertices of degree one. Usually the roots in graph theory are portrayed, with the root and the leaves at the bottom. The direction from the root to leaves is taken as the down direction and the direction from the leaves to the root is taken as the up direction. The number of internal vertices in a binary tree is one less than the number of external vertices (pendant vertices). If v_i is vertex of a binary tree. v_i is said to be at a level l_i if v_i is at a distance l_i from the root of the binary tree. Thus the root a binary tree is at level 0.

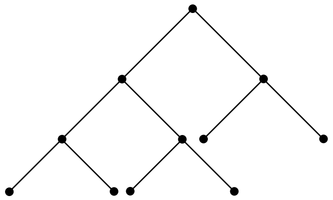


Fig. 8.112 A 11-vertex 3-level binary tree

The maximum level occurring in a binary tree is called the height of the binary tree. A binary tree with minimum height contains maximum number of vertices at each level. The root of a binary tree is at level 0 and there can be only one vertex at 0 level. The maximum number of vertices at level is 2^1, at level 2 is 2^2 and soon. By induction we can prove that the maximum number of vertices possible at level k in a binary tree is 2^k. We now state the following theorem on the minimum possible height of a binary tree:

Theorem 8.24: The minimum height of a binary tree on n vertices is $\lceil \log_2 (n+1) - 1 \rceil$ (where $\lceil m \rceil$ is the smallest integer $> m$) and maximum possible height is $\frac{n-1}{2}$.

Proof: The root of T is at level 0. We know that every vertex of T at level k can have 2^k. successors. Therefore we have

2 vertices at level 1

2^2 vertices at level 2

Hence the maximum number of vertices in the binary tree of height l is

$$1 + 2 + 2^2 + ... + 2^l$$

but T has n vertices, therefore

$$1 + 2 + 2^2 + ... + 2^l \geq n$$

or $$\frac{2^{l+1} - 1}{2 - 1} \geq n$$

or $$2^{l+1} - 1 \geq n$$

or $$2^{l+1} \geq n + 1$$

Hence $$l \geq \log_2 (n + 1) - 1$$

but l is an integer

The smallest possible value for 1 is

$$\lceil \log_2 (n + 1) - 1 \rceil$$

The minimum possible height of a binary tree T is

$$\lceil \log_2 (n + 1) - 1 \rceil$$

Now let denote the maximum possible height of T. We have the root of T at zero level, 2 vertices at level, 2 vertices at level 2, ...

2 vertices at level l.

When T is of height l, we have atleast 1 + (2 + 2 + ...l times) vertices in T.

i.e., $1 + 2l$ vertices in T

Hence $$1 + 2l \leq n$$

$$\Rightarrow 2l \leq n - 1$$

$$\Rightarrow l \leq \frac{n - 1}{2}$$

but n is odd

$\frac{n-1}{2}$ is an integer. Hence

The maximum possible value of l is $\frac{n-1}{2}$.

Thus, we have

$$\min l = [\log_2 (n + 1) - 1]$$

and $$\max l = \frac{n-1}{2}$$

A binary tree can also be defined as follows:

A binary tree is a directed tree, $T = (V, E)$ together with an edge labelling f: $E \to \{0, 1\}$, such that every vertex of T has at most one edge incident from it is labeled 0, and at most are edge incident from it labeled with 1.

If T is a binary tree, then each edge (u, v) labelled with 0 is called a left edge. u is called the parent of V and v is called the left child of u. Each edge (u, v) labelled with 1 is called a right edge in T. The vertex u is called the parent of v and u is called the right child of u.

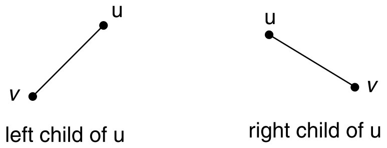


Fig. 8.113

8.41 SOLVED EXAMPLES

Example 1: Show that the number of vertices in a binary tree is odd.

Solution: Let T be a binary tree with n vertices. T contains exactly one vertex of degree 2 and the remaining vertices of T are of degree one or three. Therefore number of odd degree vertices in T is $n - 1$. But the number of odd degree vertices in a graph is even. Therefore $n - 1$ is even. Hence n is odd.

Example 2: T is a binary tree on n vertices and p is the number of pendant vertices in T. Show that the number of vertices of degree 3 in T is $n - p - 1$.

Solution: T has p vertices of degree one and one vertex in T is of degree two. Hence the number of remaining vertices (i.e., vertices of degree 3) is $n - p - 1$.

Example 3: T is a binary tree on n vertices. Show that the number of pendant vertices in T is $\frac{n+1}{2}$.

Solution: Let p denote the number of pendant vertices in T.

The number of edges in T is $n - 1$

The degree sum in $T = 2\,(n - 1)$

Therefore $\quad P \times 1 + (n - p - 1) + 2 = 2\,(n - 1)$

or $\quad P + 3n - 3p - 3 + 2 = 2n - 2$

or $\quad n + 1 = 2p$

Hence $\quad P = \frac{n+1}{2}$

Example 4: Find the maximum possible height of a binary with 13 vertices and draw graph of the tree.

Solution: We have $n = 13$

Maximum possible height of the binary tree $\frac{n-1}{2} = \frac{13-1}{2} = 6$

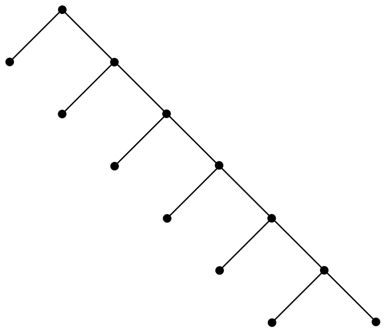


Fig. 8.114 Binary tree of maximum height with 13 vertices

Example 5: Find the minimum height of the tree with 9 vertices.

Solution: We have $n = 9$

The minimum height of the binary tree

$$= \lceil \log_2 (n+1) - 1 \rceil = \lceil \log_2 (9+1) - 1 \rceil = 3$$

8.42 COMPLETE BINARY TREE

Definition 8.76: A binary for which the level order indices of the vertices form a complete interval 1, 2, ..., n of the integers is called a complete binary tree.

If T is a complete binary tree, then all its levels except possibly the last, will have maximum number of possible vertices, and all the vertices at the last level appear as far left as possible. The tree shown in Fig. 8.115 is a complete binary tree.

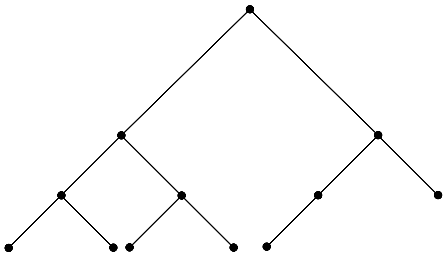


Fig. 8.115 A complete binary tree

If T is a complete binary tree with n vertices, then the vertices at any level l are given the label numbers ranging from 2^l to $2^{l+1} - 1$ or from 2^l to n if n is less than $2^{l+1} - 1$.

8.43 HEIGHT BALANCED BINARY TREE

Definition 8.77: A binary tree T in which the heights of left and right subtrees of every vertex differ by at most one is called a height balanced binary tree.

Every complete as a height balanced binary tree. Height balanced trees are important in computer science and are more general than complete binary tree. We state the following theorem without proof on the number of vertices in a height balanced binary tree.

Theorem 8.25: There are atleast $\frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2}\right]^{h+3} - 2$ vertices in any height balanced binary tree with height *h*.

8.44 B-TREE

Definition 8.78: Let *T* be a directed tree of order *k*.

T is said to said to be a B-tree of order *k*, if

(*i*) all the leaves are at the same level;

(*ii*) every internal vertex, except possibility the root has atleast $\lceil k/2 \rceil$ children (where $\lceil x \rceil$ means the least integer $\geq x$);

(*iii*) The root is a leaf or has atleast two children; and

(*iv*) no vertex has more than *k* children.

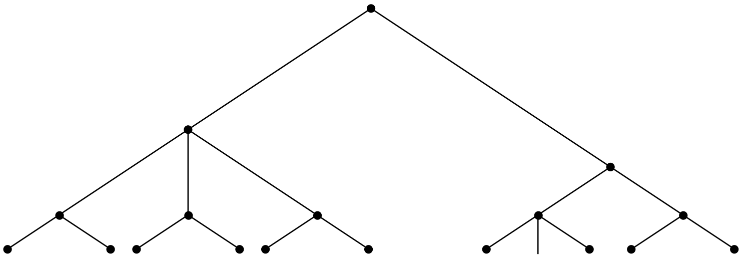


Fig. 8.116 B-tree

If the height of B-tree of order *k* is $h \geq 1$, then the B-tree atleast $2\lceil k/2 \rceil^{h-1}$ leaves.

8.45 DISTANCE BETWEEN SPANNING TREES OF A GRAPH

Definition 8.79: Let T_i and T_j be two spanning trees of a graph *G*. The distance between T_i and T_j is defined as the number of edges of group *G*, present in T_i but not in T_j.

Example: Consider the graph *G* as shown in the Fig. 8.117 below:

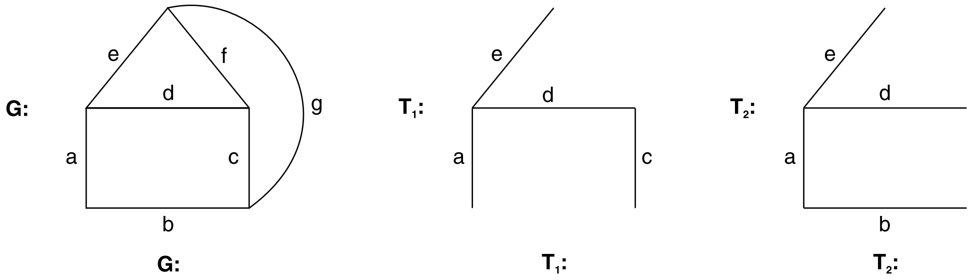


Fig. 8.117 Graph G and two spanning trees T_1 and T_2.

The distance between the spanning trees T_1 and T_2 is one.

8.46 CHORD OF A GRAPH

Definition 8.80: Let G be a graph and T be a spanning tree of G. An edge of G, that is not in T is called a Chord of G.

8.47 RANK AND NULLITY

Definition 8.81: Let G be a graph, with a vertices $(i.e., |V| = n)$. Let e be the number of edges in G, and k be the number of components of G. Then the rank of G in defined as follows:

$$r = \text{rank} = n - k$$

$(i.e., r = |V| - k)$

The nullity of G is defined as

$$\text{nullity} = \mu = e - n + k$$

$(i.e., \mu = |E| - |V| - |k|\,)$

If $k = 1$, the graph G is connected. Then the rank of G is $n - 1$ and the nullity of G is $e - n + 1$ $(i.e., |E| - |V| + 1)$

The nullity of a graph G is also referred to as its first Betti number.

EXERCISE 8.5

1. Define the terms

(*i*) Connected graphs ***(MKU, MCA, May 2002)***

(*ii*) Tree

(*iii*) Rooted tree

give examples

2. Define

(*a*) Cut vertex

(*b*) Cut edge

(*c*) Cut set

and give examples

3. Show that every non-trivial has atleast one vertex of degree 1.

4. Prove that a tree with n vertices has exactly $(n - 1)$ edges.

5. Define

(*a*) Spanning tree ***(MKU, MCA, May 2002)***

(*b*) Binary tree

(*c*) Eccentricity

(*d*) Leaf

(*e*) Forest

(*f*) Centre of a tree

(*g*) Radius of a tree

(*h*) Diameter of a tree

6. Show that the number of vertices of a binary tree is odd.

7. Show that the number of pendant vertices in a binary tree with *n* vertices is

$$\frac{n+1}{2}.$$

8. Define the term minimal spanning tree of a graph.

9. Define

(*a*) Complete binary tree

(*b*) Height balanced binary tree and

show that there are atleast

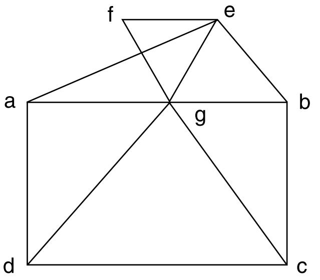
$$\frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2}\right]^{h+3} - 2$$

vertices in a height balanced tree of height *h*.

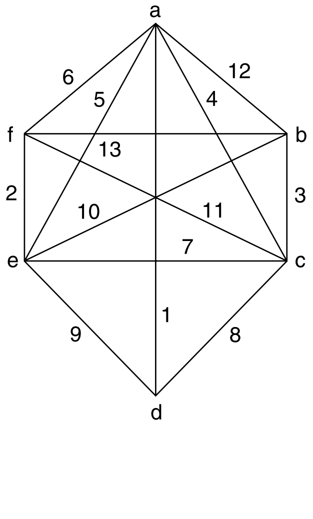
10. How many non-isomorphic trees are there with the number of vertices equal to

(*a*) 2 (*b*) 3 (*c*) 4 (*d*) 5

11. Find the spanning trees of the graph *G*.



12. Find the minimal and maximal spanning trees of *G*.



13. Prove that there is one and only one path between every pair of vertices in a tree.

14. If in a graph *G*, there is one and only are path between every pair of vertices then show that *G* is a tree.

15. Show that any connected graph with *n* vertices and *n* – 1, edges is a tree.

16. If two adjacent vertices of a tree are connected by adding an edge, then show that the resulting graph is a cycle.

17. State Kruskal's algorithm for find the minimal spanning tree. ***(O.U., MCA, 1998)***

18. Define term (*i*) Connected graph (*ii*) Spanning tree prove that every connected graph has one spanning tree. ***(O.U., MCA, 1991)***

19. Prove that every non-trivial tree contain atleast 2 vertices of degree 1. ***(O.U., MCA, 1991)***

20. Define a binary tree and desire a formula for the maximum possible height of a binary tree with *n* vertices.

21. How many different non-isomorphic trees of order 4 are possible. Draw them. ***(O.U., MCA, 1994)***

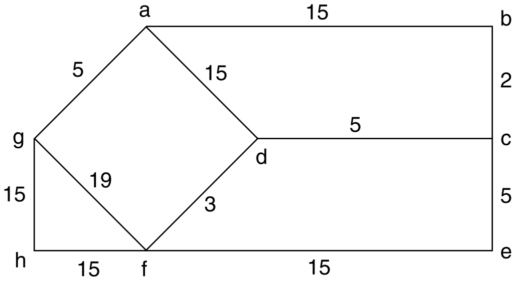
22. Prove that if a connected graph *G* has only are spanning tree, them *G* itself is a tree. ***(O.U., MCA, 1995)***

23. Draw a balanced binary tree of height 4 with minimum number of vertices. ***(O.U., MCA, 1996)***

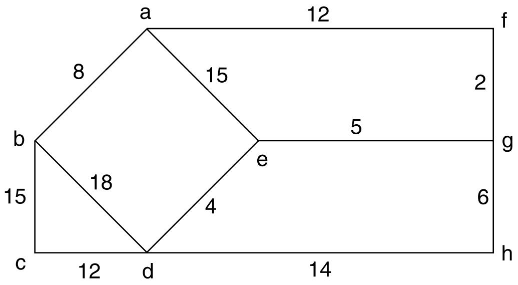
24. Show that a simple non-directed graph *G* is a tree if and only if it is connected and has no cycles. ***(O.U., MCA, 1998)***

25. Let H be a subgraph of a connected graph *G*. Show that *H* is a subgraph of some spanning tree *T* if *H* contains no cycles. ***(O.U., MCA, 1999)***

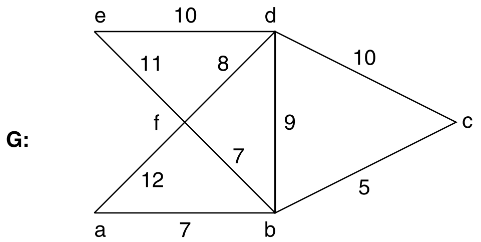
26. Determine a railway network of minimal cost for the cities in the Figure given below:



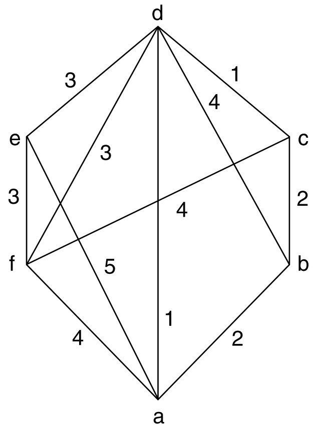
27. Find the minimal spanning tree for the following graph:



28. Find the minimal spanning tree for the graph *G*.



29. Find a minimal spanning tree for the graph.



8.48 PLANAR GRAPHS

In this section, we discuss about graphs which can be drawn on a plane such that no two edges of the graph intersect. The points of intersection of edges in a graph are called cross-overs. The edges in a graph *G*, which intersect are said to cross-over each other. A graph *G* is said to be embedded in a surface *S*, when it can be drawn on *S*, such that no two edges intersect.

Definition 8.82: A graph *G* is said to be planar if it can be drawn on a plane without cross-overs.

From the definition it is clear that a graph is planar if it can be embedded in a plane. A graph which cannot be drawn a plane without cross-over between its edges is called non-planar graph.

8.48.1 Plane Graph

Definition 8.83: An embedding of a planar graph is called a plane graph.

A plane graph partitions the plane into several regions. These are called faces (also called windows or meshes). Each region is characterised by the set of edges forming its boundary. Each plane graph determines a region of infinite area called the exterior region of *G*. If *G* is a connected graph, then the boundary of a region *R* is a closed path in which each cut edge is travelled twice. The boundary of a region *R* is a cycle if the boundary of *R* contains no cut edges of *G*.

8.48.2 Degree of a Face

Definition 8.84: Let *G* be a plane graph and *f* be a face of *G*. The degree of the face *f* is defined as the number of edges in the boundary of *f*, with cut edges counted twice.

8.48.3 Critical Planar Graph

Definition 8.85: A graph G is said to be critical planar if G is non-planar but any subgraph obtained by removing a vertex of G is planar.

For $n \leq 3$, $K_{n,3}$ is critical planar.

The graphs shown in Fig. 8.118 are planar

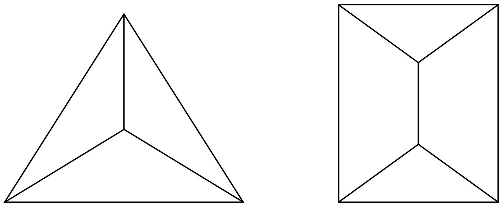


Fig. 8.118 Planar graphs

The graphs shown in Fig. 8.119 are non-planar

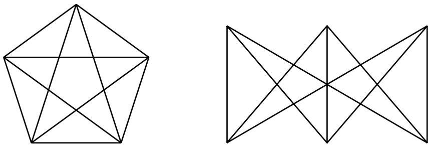


Fig. 8.119 Non-planar graphs

If G is a graph, then we denote the embedding of G on a surface S by $S(G)$. The vertices, edges and faces of $S(G)$ constitute a map on the surface S. If S is the plane $\prod$ then the vertices edges, and faces of $S(G)$ constitute a planar map. It is denoted by $\prod(G)$. In a planar embedding of $\prod(G)$, all faces except one are bounded. The unbound face is called the exterior face (infinite face or outer face). Region in a map which have atleast one common edge are called adjacent regions.

8.48.4 Polyhedral Graph

Definition 8.86: A plane connected graph in which each region has degree equal to or grater than 3 and each vertex has degree equal to or greater than 3 is called a polyhedral graph.

A planar graph may have different planar representations. The number of regions resulting from each embedding is always the same. If G is a planar graph, then the number of vertices, number of edges and the number of regions in G are inter-connected. The number of regions in G can be computed by Euler's formula.

8.48.5 Euler's Formula

Theorem 9.26: If G is a connected plane graph then

$$|V| - |E| + |R| = 2$$

Where $|V|$ denotes the number of vertices in G

$|E|$ denotes the number of edges and

$|R|$ denotes the number of regions in G

Proof: We prove the theorem by mathematical induction on number K of regions determined by G. We first prove the theorem for a tree (i.e., for $K = 1$). A tree determined only one region.

we have $|E| = |V| - 1$, $|R| = 1$ for a tree

$$\therefore \qquad |V| - |E| + |R| = |V| - \{|V| - 1\} + 1 = 2$$

$\therefore$ The result holds for $K = 1$

Assume that the holds for $K \geq 1$. Let G be a connected plane graph determining $(K + 1)$ regions.

Deleting an edge common to the boundary of two regions. We get a graph G^1. If V^1, E^1, and R^1 are the number of vertices, the number of regions and the number of regions respectively of G^1 then $|V^1| - |E^1| + |R^1| = 2$

Also we have

$$|V'| = |V|, |E'| = |E| - 1 \text{ and } |R'| = |R| - 1$$

$$\begin{aligned} \therefore \qquad |V| - |E| + |R| &= |V'| - \{|E'| - 1\} + |R'| - 1 \\ &= |V^1| - |E'| + 1 + |R'| - 1 \\ &= |V'| - |E'| + |R'| = 2 \end{aligned}$$

By mathematical induction the result holds for all connected graphs.

Corollary: If G is a simple connected planar graph with $|E| > 1$, then

(*i*) $|E| \leq 3\,|V| - 6$

(*ii*) There is a vertex v of G such that , deg $(v) \leq 5$.

Proof: of (*i*) G is a simple connected planar graph.

Therefore, each region of G is bounded by atleast three edges and each edge belongs exactly to two regions.

i.e., $$2\,|E| \geq 3\,|R|$$

or $$|R| \leq \frac{2}{3}|E|$$

or $$|V| + |R| \leq + \frac{2}{3}|E|$$

by Euler's formula

$$|V| - |E| + |R| = 2$$

or $$|V| + |R| = |E| + 2$$

substituting in L.H.S. of (1) we get

$$|E| + 2 \leq |V| + \frac{2}{3}|E|$$

or $$3\,|E| + 6 \leq |V| + 2\,|E|$$

or $$|E| \leq |V| - 6$$

Proof: of (*ii*) let each vertex of G have degree ≥ 6

Then $$\sum_{v \in V} \deg(v) = 2\,|E|$$

i.e., $$6\,|V| \leq 2\,|E|$$

or $$|V| \leq \frac{2}{6}\,|E|$$

or $$|V| \leq \frac{1}{3}\,|E|$$

but $$|R| \leq \frac{2}{3}\,|E|$$

Therefore $$|V| + |R| \leq \frac{1}{3}\,|E| + \frac{2}{3}\,|E|$$

or $$|V| + |R| \leq |E|$$

by Euler's formula $|V| + |R| = |E| + 2$

Hence $$|E| + 2 \leq |E|$$

$\Rightarrow$ $2 \leq 0$, a contradiction

Each vertex of G cannot have a vertex degree ≥ 6.

$\Rightarrow$ each vertex of G is of degree ≤ 5

Example 1: Prove that K_5 is non-planar.

Solution: Number of vertices in $K_5 = |V| = 5$

Number of edges in $K_5 = |E| = 10$

If G is planar then $|E| \leq 3\,|V| - 6$

$\therefore \Rightarrow 10 \leq 3.5 - 6$

$\Rightarrow 10 \leq 9$ a contradiction

$\therefore$ K_5 is non-planar

Example 2: Show that $K_{3,\,3}$ satisfies in equality $|E| \leq 3\,|V| - 6$, but it is non-planar.

Solution: For the graph $K_{3,\,3}$ we have

$$|E| = 9,\ |V| = 6$$

and $$3\,|V| - 6 = 3.6 - 6 = 12$$

We have $$|E| = 9 \leq 12 \text{ i.e., } |E| \leq 3\,|V| - 6$$

Hence $K_{3,\,3}$ satisfies the inequality $|E| \leq 3\,|V| - 6$

If the graph is planar then we must have $2\,|E| \geq 4\,|R|$ substituting for $|R|$. From Euler's formula, we get

$$2\,|E| \geq 4\,[|E| - |V| + 2]$$

or $$2.9 \geq 4\,[9 - 6 + 2]$$

or $18 \geq 20$, a contradiction

Hence $K_{3,3}$ in non-planar

Note: The graph K_5 is called Kuratowski's first graph and $K_{3,3}$ is called Kuratowski's second graph (*see* Fig. 8.120(*a*) and (*b*)).

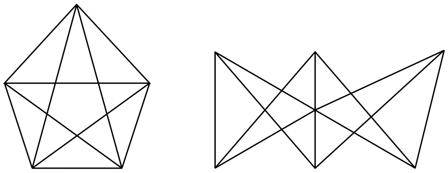


Fig. 8.120 Kuratowski's graphs

Example 3: Show that a complete graph of 4 vertices is planar.

Solution: K_4 can be drawn as shown in Fig. 8.121:

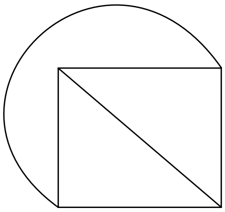


Fig. 8.121

From the Fig. 8.119 it is clear that K_4 be drawn without cross-overs.

Hence, K_4 is planar.

Example 4: Show that the graphs $K_{2,2}$, $K_{2,3}$ and $K_{2,4}$ are planar.

Solution: The graphs of $K_{2,2}$, $K_{2,3}$ and $K_{2,4}$ are shown in Fig. 8.122(*a*), (*b*) and (*c*) respectively.

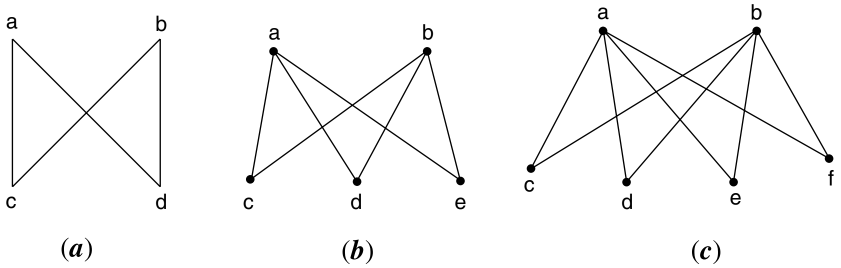


Fig. 8.122

The planar embeddings of $K_{2,2}$, $K_{2,3}$ and $K_{2,4}$ are shown in Fig. 8.123 in which can set that the edges of the graphs can be drawn without crosso-vers.

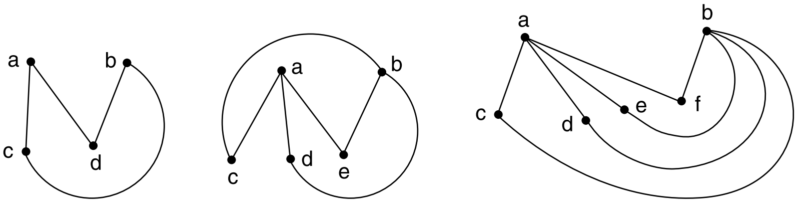


Fig. 8.123 Planer embeddings of $K_{2,\,2,}$ $K_{2,\,3}$ and $K_{2,\,4}$

Example 5: Show that the graph *G* shown in Fig. 8.124 is planar:

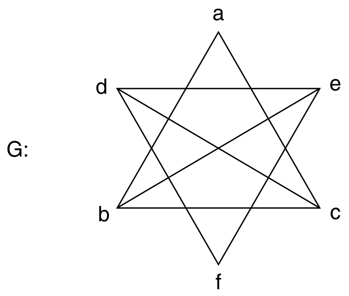


Fig. 8.124

Solution: The edges of *G* shown in Fig. 8.124 can be drawn without cross-overs. The planar embedding of *G* is shown in Fig. 8.125:

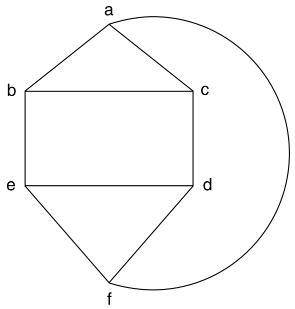


Fig. 8.125

Example 6: Prove that no polyhedral graph with exactly 30 edges and 11 regions exists.

Solution: We have $|E| = 30$, $|R| = 11$

From Euler's formula

$$|V| - |E| + |R| = 2$$

$$\Rightarrow |V| = |E| - |R| + 2 = 30 - 11 + 2 = 21$$

If the graph is polyhedral,

Each vertex has degree equal to or greater then 3 and we must have $3\,|V| \leq 2\,|E|$.

i.e., $3.21 \leq 2.30$

i.e., $63 \leq 60$, a contradiction.

Hence there cannot be a polyhedral graph with exactly 30 edges and 11 regions.

Example 7: Find the minimum number of vertices necessary for a simple connected graph with 7 edges to be planar.

Solution: We have $|E| = 7$.

Substituting in $|E| \leq 3\,|V| - 6$

we get

$$7 \leq 3\,|V| - 6 \Rightarrow 3\,|V| - 6 \geq 7$$

or $$3\,|V| \geq 7 + 6$$

or $$|V| \geq 13/4$$

Therefore, the minimum number vertices necessary for a single graph with 7 edges to be planer is 5.

Example 8: Find the maximum number of edges possible in a simple connected planar graph with 4 vertices.

Solution: We $|V| = n = 4$

$$3\,|V| - 6 = 3 \cdot 4 - 6 = 6$$

Therefore $|E| \leq 3\,|V| - 6$

or $$|E| \leq 6$$

The maximum number of edges possible in a simple connected planar graph with 4 vertices is 6.

8.49 HOMEOMORPHIC GRAPHS

Definition 8.87: Two graphs are said to be homeomorphic if one graph can be obtained from the other by the creation of edges in series or by the merger of edges in series.

A graph G is planar if and only if every graph that is homeomorphic to G is planar.

We now state the following theorem without proof:

Theorem 8 (Kuratowski): A graph is planar and only it has no sub-graph homeomorphic to K_5 or $K_{3,\,3}$.

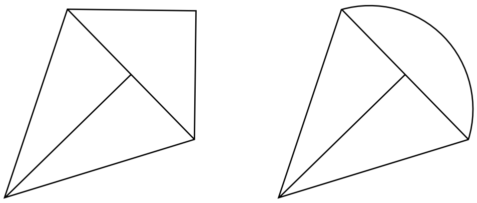


Fig. 8.126 Homeomorphic graphs

8.50 DUAL OF A GRAPH

8.50.1 Geometric Dual

Let G be a planar graph and $F_1, F_2, ..., F_k$ denote the faces or regions of G. Place vertices $V_1, V_2, ... V_k$ one in each of the regions. If two regions F_i and F_j are adjacent draw an edge joining the vertices V_i and V_j that intersects the common edge between F_i and F_j exactly once. If the number of edges between F_i and F_j is more than one, then draw one edge between V_i and V_j for each of the common edges. If an edge e lies entirely in one region say F_i draw a self-loop at the vertex V_i lying in F_i intersecting e exactly once. We denote the new graph obtained by this procedure by G^*. The graph G^* is called a dual of G. We make the following observation:

(*i*) G and G^* have the same number of edges.

(*ii*) The number of vertices in G^* is equal to the number of regions in G and the number of regions in G^* is equal to the number of vertices in G.

(*iii*) An edge forming a self-loop in G yields a pendant edge in G^*.

(*iv*) A pendant edge in G yields a self-loop in G^*.

(*v*) Edges that are in series in G produce parallel edges in G^* and parallel edges in G produce edge in series in G^*.

(*vi*) G^* is planar.

(*vii*) If G^* is a dual of G than G is dual of G^*.

Remarks: If G is a planar graph and G^* is the dual of G, then the number of vertices in G is equal to the number of vertices G^*. G and G^* have the same number of edges and same number regions.

Example: Find the dual of the graph G shown in Fig. 8.127.

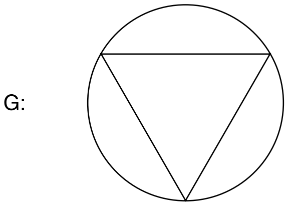


Fig. 8.127

Solution: The dual of G is shown in Fig. 8.128 if the edges of G^* are shown by dashed edges:

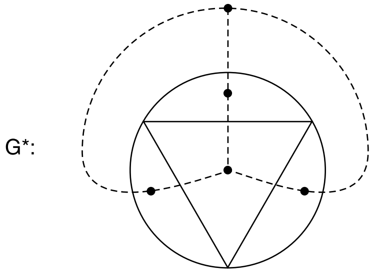


Fig. 8.128 Dual of a graph

The dual of a graph depends on the embedding of the graph in the plane and the same graph may have different geometric duals for different embeddings. All duals of a planar graph are 2-isomorphic. Now we state the following theorem (without proof) which gives a criterion for a graph to be a planar graph.

Theorem 8.27: A graph is planar if and only if it has a dual.

Let G be a planar graph and G^* denote the dual of G. If G and G^* are isomorphic to each other then G is called a self-dual.

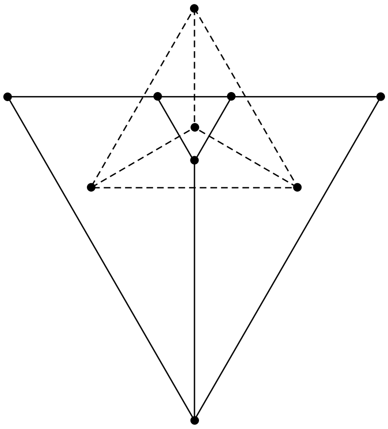


Fig. 8.129 Self-dual graph

The tetrahedron is self-dual. The following graphs are self-dual:

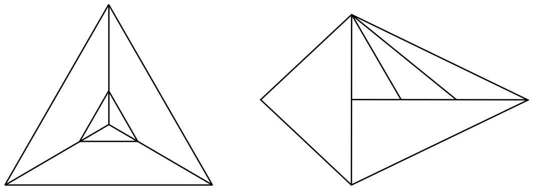


Fig. 8.130 Self-duals

8.50.2 Combinatorial Dual

Definition 8.88: To planar graphs G and G^* are said to be combinatorial duals of each other if there is a one-to-one correspondence between the edges of G and G^* such that if G_1 is any subgraph of G and G^*_1 is the corresponding subgraph G^*, then

Rank of $(G^* - G^*_1)$ = rank of G^* – nullity of G_1.

The above definition in an abstract formulation of the concept of geometrical dual and was given by Whitney. He proved that a graph G is planar if and only if it has a combinatorial.

8.50.3 Thickness of a Graph

Definition 8.89: The minimum number of planar subgraphs whose union is the given graph *G* is called the thickness of *G* and is denoted by *O* (*G*).

The thickness of a planar graph is one.

8.50.4 Crossing Number

Definition 8.90: Let *G* be a graph. The minimum number of pairwise intersection of its edges when *G* is drawn in the plane is called the crossing number of *G*.

The crossing number of each of the Kuratowskis' graphs is one. The crossing number of a planar graph is zero.

8.50.5 Outer Planar Graph

Definition 8.91: A planar graph is outer planar if it can be embedded in the plane so that all its vertices lie on the boundary of a region of *G*.

The graphs shown in Fig. 8.131 is outer planar.

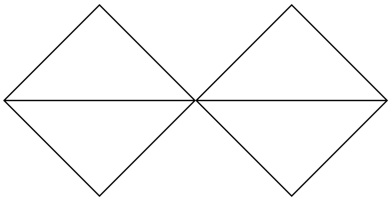


Fig. 8.131

8.50.6 Self-Dual Graph

Definition 8.92: Let *G* be a graph and *G** be the dual of G. If *G* and *G** are isomorphic to each other then *G* is called a self-dual.

8.51 SOLVED EXAMPLES

Example 1: Show that a graph *G* is self-dual if $|E| = 2n - 2$ where *n* is the number of vertices in *G*.

Solution: Let *G** denote the dual of *G*. Since *G* and *G** are isomorphic, we have

$$|E| = |E^*|, |R^*| = n, |V| = |V^*| = n$$

Hence by Euler's formula, we have

$$|E^*| = |V^*| + |R^*| - 2$$

or $$|E| = n + n - 2$$

or $$|E| = 2n - 2$$

Example 2: If *f* denotes the number of regions in a graphs *G*, then show that $n \geq 2 + f/2$.

Solution: We know that

$$3f \leq 2\,|E|$$

i.e.,

$$|E| \geq \frac{3}{2}f$$

By, Euler's formula

$$|V| = |E| - |R| + 2 \geq 3f/2 - f + 2$$

or

$$n \geq f/2 + 2$$

We now state following theorems without proof:

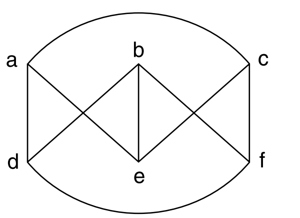
Theorem 8.28: Two planar graphs G and G^1 are duals of each other if there exists a one-to-one correspondence between the edges of G and G^1 such that circuits in G correspond to cut sets in G^1.

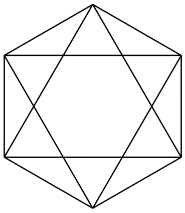
Theorem 8.29: The graph $K_{3,\,3}$ cannot have a dual.

Theorem 8.30: The graph K_5 cannot a dual.

EXERCISE 8.6

1. Draw a planar representation of the following graphs:





2. Show that K_5 is non-planar.

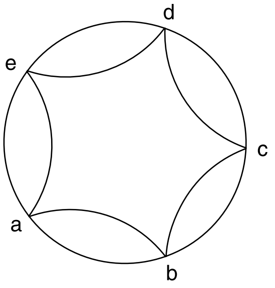
3. Show that a complete bipartite graph $K_{m,\,n}$ is planar if and only if m or n is less than or equal to 2.

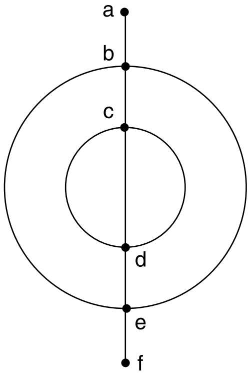
4. Show that a plane connected graphs with less than 30 edges has a vertex of degree $\leq$ 4.

(O.U., MCA, 1997)

5. If the minimum degree of any vertex is 5 show that there are atleast 12 vertices of degree equal to 5.

6. Count the number of vertices, number of edges and number of region of each of the following maps:





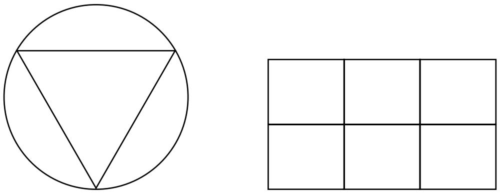
7. Show that there is no map of five regions in the plane such that every pair of regions are adjacent.

8. Give an example for a self-dual graph other than K_4. ***(MKU, MCA, May 2002)***

9. Give an example of a plane connected graph such that $|E| = 3\,|V| - 6$.

10. Show that $K_{3,\,3}$ satisfies the inequality $|E| \leq 3\,|V| - 6$, but it is non-planar.

11. Count the number of vertices, the number of edges and the number of regions of each map and verify Euler's formula.



8.52 EULERS GRAPHS

In this section, we shall study graphs known as Eulers graphs. Euler is called the father of graph theory. He solved a long-standing. Problem called the Konigs Berg Bridge problem.

Konigs Berg Bridge problem: There were two Islands linked to each other and to the banks of Pregal River in Konigs Berg by seven bridges as shown in Fig. 8.132.

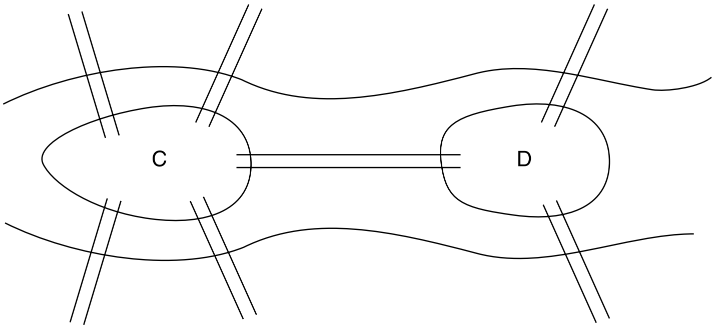


Fig. 8.132

The problem was to begin at any one of the four land areas (A, B, C, D in Fig. 8.132) walk across each bridge exactly once and return the starting point. Many attempts were made to solve this problem. Euler proved that a solution to this problem does not exists.

Euler represented, each land area by a point and joined two such points by a line. If a bridge existed connecting the land areas. Fig. 8.133 shows this representation.

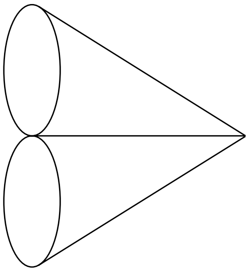


Fig. 8.133 The graph of Konigs Berg Bridge problem

Each point in the graph represents a land area and each line in the graph represents a bridge.

Euler generalised the problem and developed a criterion for a given graph to be traversable satisfying the given conditions.

8.52.1 Euler Path

Definition 8.93: Let G be a multigraph. An Euler path is G is a path that includes each edge of G exactly once and intersects each vertex of G atleast once.

8.52.2 Traversable Graph

Definition 8.94: A graph G is said to be traversable, if it has a path.

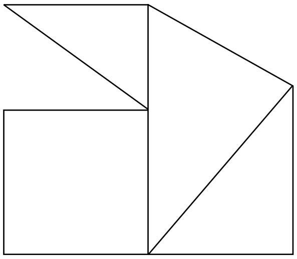


Fig. 8.134 Traversable graph

8.52.3 Eulerian Circuit

Definition 8.95: An Eulerian circuit in G is an Eulerian path in G whose end points are identical.

8.52.4 Eulerian Graph

Definition 8.96: A graph G is said to be Eulerian if it has an Eulerian circuit.

From the definition, it is clear that a trial in a graph is Eulerian if it contains all the edges of the graphs G and if a graph G contains a closed Euleria trial then it Eulerian. In the graph shown in Fig. 8.135, the sequence $v_1 - v_2 - v_3 - v_4 - v_2 - v_5 - v_1$ is a closed Eulerian trial. It contains all the vertices and edge of G.

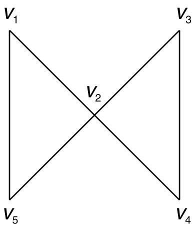


Fig. 8.135

Note: An Euler graph need not connected. If G is connected Euler graph, then starting from any vertex say V_0 of G, entire graph G can be drawn without lifting the pen, ending at V_0 and vice versa.

The graph shown in Fig. 8.136 is Eulerian. It has an Eulerian circuit.

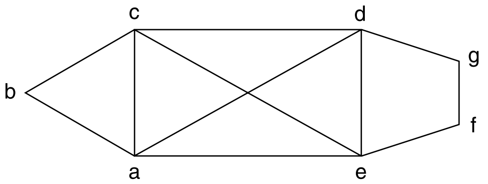


Fig. 8.136 Eulerian graph

Theorem 8.31: The following statements are equivalent for a connected multigraph G.

(1) G is Eulerian.

(2) Every point of G has even degree.

(3) The set of edges of G can be partitioned into cycles.

Proof:

(1) $\Rightarrow$ (2) Let p be an Eulerian path in G. Each occurrence of a given vertex in P contributes two to the degree of that vertex and since each of G appears exactly once in p, every vertex of G must be of even degree.

(2) $\Rightarrow$ G is connected and non-trivial, therefore degree of every vertex in G is atleast two and G contains a cycle say Z_1. The removal of the edges of Z_1 results in a spanning subgraphs G_1, in which every vertex has even degree. If G_1 has no edges, then all the edges of G form a cycle and (3) holds otherwise the argument can be repeated until we obtain a totally disconnected graph G_n.

G_1, G_2, G_3, ... G_n contain the set of edges of G, which partition G into n cycles. Hence proved.

(3) $\Rightarrow$ (1). Let G be partitioned into cycles and Z_1 be are of the cycles. If Z_1 is the only cycle graph, G is Eulerian otherwise, let Z_2 be another cycle in G and V be a common vertex of Z_1 and Z_2. The walk beginning at V and consisting of cycles Z_1 and Z_2 in succession is a closed trial containing all the edges of Z_1 and Z_2. Continuing this process we obtain a closed trial which contains all the edges of G. Hence G is Eulerian.

Theorem 8.32: If a graph G has more than

(*i*) Two vertices of odd degree, then there can be no Euler path in G.

(*ii*) If G is connected graph and has exactly two vertices of odd degree, there is an Euler path in G. Any Euler path in graph G must begin at vertex of odd degree and end at the other.

Proof:

(*i*) Let G be a graph having more than two vertices of odd degree and let v_1, v_2 and v_3 be the vertices of odd degree in G. If there is an Euler path in G, then it must leave (arrive) each of the vertices. Let one of the vertices say v_1, be the beginning of the Euler path in G and another vertex say v_2 be the end of the path. But this leaves the vertex v_3 at one end of an untravelled edge. Thus, there can be no Euler path in G.

(*ii*) Let u and V be two vertices of odd degree in G. By adding the edge $\{u, v\}$ to G we can produce a connected graph say G^1, all of whose vertices are of even degree.

Since G' is a connected graph and every vertex of G' is of even degree, we can find an Euler circuit C in G'. Deleting the edge $\{u, v\}$ from C, we get an Euler path that begins at u (or v) ends at v (or u).

If G is a graph in which there are 0 two vertices of odd degree then G has Euler path and G is traversable. If all the vertices are of even degree, then G has an Euler circuit and G is traversable. The graphs shown in Fig. 8.137 are Eulerian.

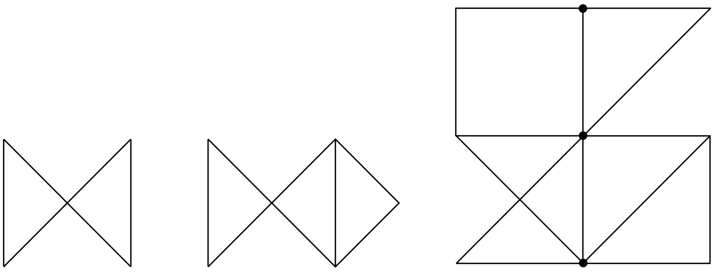


Fig. 8.137 Eulerian graphs

Solved Examples

Example 1: Show that graph G (Fig. 8.138) is Eulerian and find an Eulerian circuit in G.

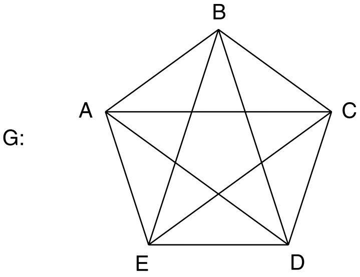


Fig. 8.138

Solution: Each vertex is of even degree in G (there 0 vertices of odd degree). Therefore, G is Eulerian.

$A\ B\ C\ D\ E\ A\ C\ E\ B\ D\ A$ is an Eulerian circuit in G.

Example 2: Show that the graph G. Shown in Fig. 8.139 is not Eulerian.

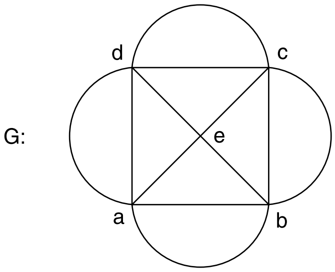
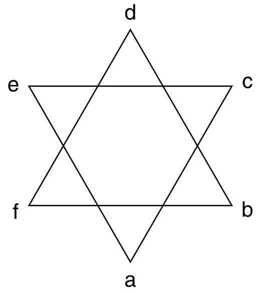


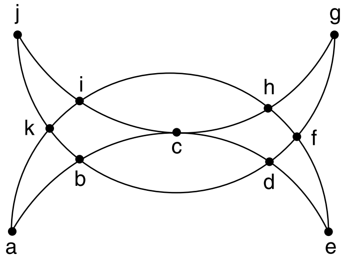
Fig. 8.139

Solution: There are four vertices of degree 5 in the graph, a, b, c, d are the vertices degree 5 in G. Therefore, G is not Eulerian.

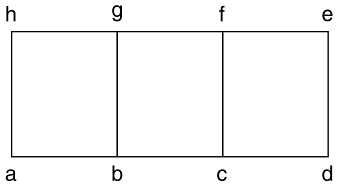
EXERCISE 8.7

1. Show that the graphs are Euler graphs:

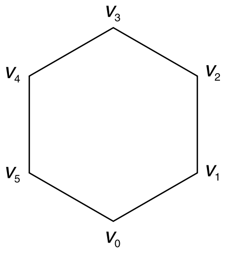




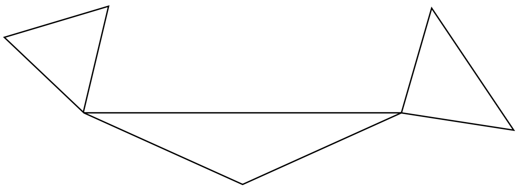
2. Find a closed Eulerian trial in the following graph:



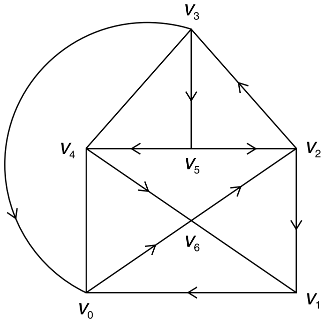
3. Show the graph G is Eulerian:



4. Show the graph given below is Eulerian:



5. Find an Eulerian path in the graphs G:



8.52.5 Fleury's Algorithm

Fleury's algorithm is useful in constructing an Eulerian trial in a connected multigraph G.
Algorithm: Fluery's algorithm to construct a closed Eulerian in a connected even graph.
Input: A connected multigraph G in which every vertex is of even degree.
Output: A closed Eulerian trail in G.

Step 1: Select any vertex $v_0 \in V$ and let $W_0 = V_0$.

Step 2: Suppose that the trail

$W = v_0\, e_0\, v_1\, e_1\, ...\, e_{i-1}\, v_i$ has been chosen. Then choose an edge e_i from $E\,(G) - \{e_0\, e_1\, ...\, e_{i-1}\}$ such that

(*i*) e_i is incident with v_i.

(*ii*) Unless there is no alternative, e_i is not a cut edge of

$$G_i = G - \{\, e_0\, e_1\, ...\, e_{i-1}\}.$$

(*iii*) Stop, when step 2 can no longer be implemented.

8.53 HAMILTONIAN GRAPHS

In Section 9.49, we have seen that an Eulerian path in a connected graph traverses every edge of the graph. Now we discuss about the graphs called the Hamiltonian graphs which contain a closed walk that traverses every vertex of the graph exactly once except the starting vertex at which the walk terminates. While studying non-commutative algebra. Sir William Rowan Hamilton has invented a game called 'Icosian game'. The same in its simplest form asks to find a cycle containing all the vertices of the graph of Dodecahedran.

Definition 8.97: A path in a graph G is called a Hamiltonian path if it contains every vertex of G.

Definition 8.98: A cycle in G is said to be a Hamiltonian cycle if it contains every vertex of G.

Definition 8.99: A graph is said to be a Hamiltonian graph if it contains Hamiltonian cycle i.e. A graph G is Hamiltonian if there exist a cycle containing every vertex of G.

From the above definition, it is clear that a Hamiltonian path in graph G is always a subgraph of a Hamiltonian cycle in G. Hamiltonian path in G may be obtained by deleting an edge from a Hamiltonian cycle in G. Every graph which has a Hamiltonian cycle (circuit) contains a Hamiltonian path, but a graph containing a Hamiltonian path may not have a Hamiltonian cycle and there are many graphs with Hamiltonian paths that have no Hamiltonian cycle. The graphs shown in Fig. 8.140 are Hamiltonian.

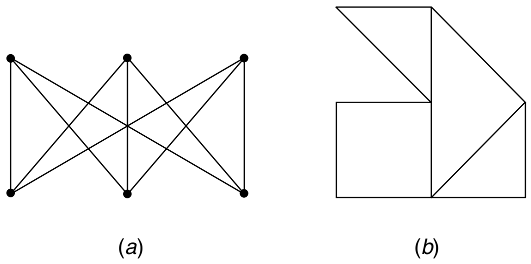


Fig. 8.140 Hamiltonian graphs

A Hamiltonian cycle in a graph of *n* vertices consists of exactly *n* edges usually we consider only simple graphs which do not include self-loops of parallel edges. A given graph may contain more than are Hamiltonian cycle.

Rules for constructing Hamiltonian paths, and cycles in a graph *G*.

Rule 1: If *G* is a graph with *n* vertices, then a Hamiltonian cycle in *G* will contain exactly *n* edges.

Rule 2: There cannot be more than three are more edges incident with one vertex in a Hamiltonian cycle in *G*. Every vertex *v* in a Hamiltonian cycle (circuit) of *G* will contain exactly 2 edges incident on *v*. If *v* is a vertex in *G* then a Hamiltonian path in *G* must contain atleast one edge incident on *v* at most 2 edges incident on *v*.

Rule 3: A Hamiltonian path or cycle constructed in *G* must contain all the vertices of *G*.

Rule 4: Let *V* be a vertex of *G*. Once a Hamiltonian circuit (cycle) we are constructing has passed through *v*, then all the other unused edges incident on *v* can be deleted.

Example 1: Consider the graph *G* in Fig. 8.141

$\{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, g\}$ is a Hamiltonian path in *G*.

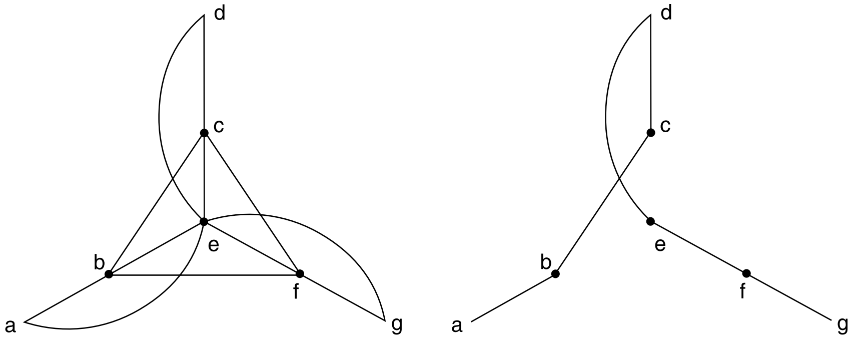


Fig. 8.141

The graph shown Fig. 8.141 has no Hamiltonian circuit in *G*.

Number Hamiltonian circuit in a graph.

A given graph *G* may contain more than are Hamiltonian circuit. In general the determination of number of Hamiltonian cycles (circuits) in a graph is an unsolved problem. However, the number of edge disjoint Hamiltonian circuits in a complete graph with *n* vertices where *n* is odd (and $n \geq 3$) is given by the following theorem:

Theorem 8.33: In a complete graph with n vertices there are $(n - 1)/2$ edge-disjoint Hamiltonian cycles, if n is an odd number ≥ 3.

Proof: Let G be a complete graph with n vertices where n is odd and $n \geq 3$. Then G has $\frac{n(n-1)}{2}$ edges. A Hamiltonian cycle in G contains n edges. Therefore, the number of edge-disjoint Hamiltonian cycle in G cannot exceed $(n - 1)/2$. We show that there cycles in G as follows.

The subgraph of G, shown in Fig. 8.142 is a Hamiltonian cycle.

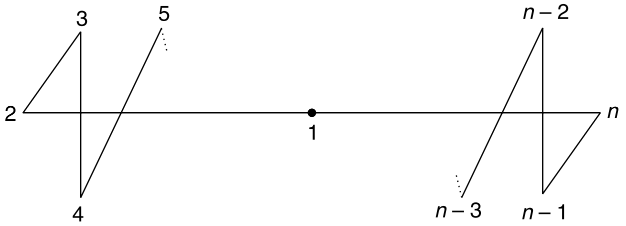


Fig. 8.142

Keeping the vertices fixed on a circle, rotate the polygonal pattern clockwise by

$$\frac{360}{n-1}, \frac{2 \cdot 360}{n-1}, \frac{(n-3)}{2} \cdot \frac{360}{n-1} \text{ degrees.}$$

Observe that each rotation produces a Hamiltonian circuit that has no edge in common with any of the previous ones. Thus, we have $(n - 3)/2$, new Hamiltonian cycles all edges disjoint from the one in Fig. 8.141 and also edge disjoint among themselves. Therefore, the number of edge-disjoint Hamiltonian cycles in G is

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

Hence proved.

Example 1: If G is a complete graph with 7 vertices (i.e., k_n), then the number of edge disjoint Hamiltonian cycles is $\frac{7-1}{2} = 3$.

Example 2: Show that the graph G in Fig. 8.143 is not Hamiltonian.

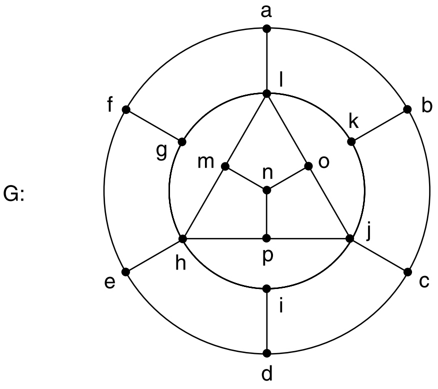


Fig. 8.143

Solution: G has 21 edges and 10 vertices. Therefore any Hamiltonian cycle in G should have 16 edges and Hamiltonian path in G must contain exactly 15 edges. In the graph G we have

$$\deg(l) = \deg(h) = \deg(j) = 5$$

i.e., there an three vertices of degree, therefore atleast three edges on l cannot be included in any Hamiltonian path. The same is true for the vertices h and j. There are 13 vertices of degree 3 in three consider the vertices b, d, f and n. Each of there vertices is of degree three. Atleast one of the three edges incident in each of there vertices cannot be included in any Hamiltonian path. Thus atleast 3 + 3 + 3 + 4 = 13 edges cannot be included in any Hamiltonian path. The number of remaining edges is 27 – 13 = 14. But any Hamiltonian path it is not possible to construct a Hamiltonian with the remaining 14 edges. Thus G has no Hamiltonian path in G and G is not Hamiltonian.

Example 3: Show that are graph shown in Fig. 8.144 has no Hamiltonian cycle. But the graph has a Hamiltonian path.

Solution: G has 9 vertices

$\therefore\ n = 9$

number of edge in any Hamiltonian cycle in G is 9. There are 3 vertices of degree two in G. Therefore all the edges incident on the vertices d, e and f must be included in any Hamiltonian cycle. The edges $\{a, d\}$, $\{d, g\}$, $\{b, e\}$, $\{c, f\}$, $\{f, i\}$ must be included in constructing a Hamiltonian cycle. The degree of b is 3 when the edges given above are included and we include the edge $\{a, b\}$ in the Hamiltonian cycle, we delete the edge $\{b, c\}$. Then we must include $\{a, c\}$ in the Hamiltonian cycle. Thus the degree of a would be 3. Hence no Hamiltonian cycle exists in G. However, the exists a Hamiltonian path in G the edges.

$\{a, d\}$, $\{d, g\}$, $\{g, h\}$, $\{e, b\}$, $\{b, c\}$, $\{c, f\}$, $\{f, i\}$ when included will give us a Hamiltonian path in G. i.e., $a - d - g - h - e - b - c - f - i$ is a Hamiltonian path in G. It is shown in the Fig. 8.145.

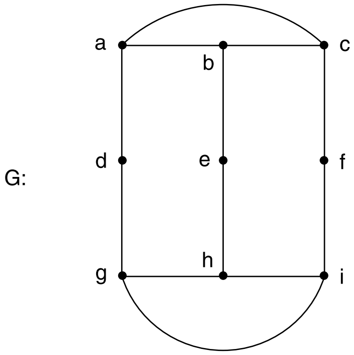


Fig. 8.144

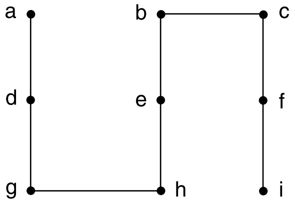


Fig. 8.145 A Hamiltonian path in the graph of Fig. 8.143

8.53.1 Diagonal

Definition 8.100: Let G be a plane Hamiltonian graph and C be a fixed Hamiltonian cycle in G. A diagonal with respect to C is an edge of G that does not lie on G.

Theorem 8.34: Let G be a simple plane graph with n vertices and C be a Hamiltonian cycle in G. If r_i denotes the number of regions of G in the interior of C whose boundary contains exactly i edges and r_i denotes the number of regions of degree i in the exterior of C, then

$$\sum_{i=3}^{n}(i-2)(r_i - r_i^1) = 0$$

Proof: G is a simple planar graph, therefore none of the edges of G intersect. We first consider the interior of C. Suppose that exactly d diagonal occur in the interior of C. A diagonal splits the region through which it passes into two parts. Each time a diagonal is inserted in the interior of C, the number of regions in C is increased by 1. Hence

$$\sum_{i=3}^{n} r_i = d+1 \Rightarrow d = \sum_{i=3}^{n} r_i - 1$$

If N denotes the sum of the degrees of all regions interior to C, then

$$N = \sum_{i=3}^{n} i\ r_i$$

N counts each diagonal twice and each edge of C exactly once, therefore

$$N = \sum_{i=3}^{n} i\ r_i = 2d + n$$

Substituting for d we get

$$\sum_{i=3}^{n} i\ r_i = 2\left[\sum_{i=3}^{n} r_i - 1\right] + n$$

$$= 2\sum_{i=3}^{n} r_i - 2 + n$$

Hence $$\sum_{i=3}^{n}(i-2)\,r_i = n-2 \qquad \text{...(1)}$$

Similarly, by considering the regions external to C we get

$$\sum_{i=3}^{n}(i-2)\,r_i' = n-2 \qquad \text{...(2)}$$

Subtracting (2) from (1) we get

$$\sum_{i=3}^{n}(i-2)(r_i - r_i') = 0$$

Example 1: Show that there are no Hamiltonian planar graphs with regions of degree 5, 8, 9 and 11 with exactly one region of degree 9.

Solution: From Grinberg's theorem we have

$$(5 - 3)\,(r_5 - r_5') = 0,\ (8 - 2)\,(r_8 - r_8') = 0$$

$$(9 - 2)\,(r_9 - r_9') = 0,\ (11 - 2)\,(r_{11} - r_{11}') = 0$$

Adding we get

$$2(r_5 - r_5') + 6(r_8 - r_8') + 7(r_9 - r_9') + 9(r_{11} - r_{11}') = 0$$

There is exactly one region of degree 9, therefore, we get

$$3(r_5 - r_5') + 6(r_8 - r_8') + 7(\pm 1) + 9(r_{11} - r_{11}') = 0$$

or
$$3(r_5 - r_5') + 6(r_8 - r_8') + 9(r_{11} - r_{11}') = \pm 7$$

or
$$3[(r_5 - r_5') + 2(r_8 - r_8') + 3(r_{11} - r_{11}')] = \pm 7$$

i.e., 3 is divisor of ± 7 a contradiction.

Hence there cannot be Hamiltonian planar graphs with regions of degree 5, 8, 9 and 11 with exactly one region of degree 9.

Example 2: Show that the graph *G* in Fig. 8.146 is not Hamiltonian.

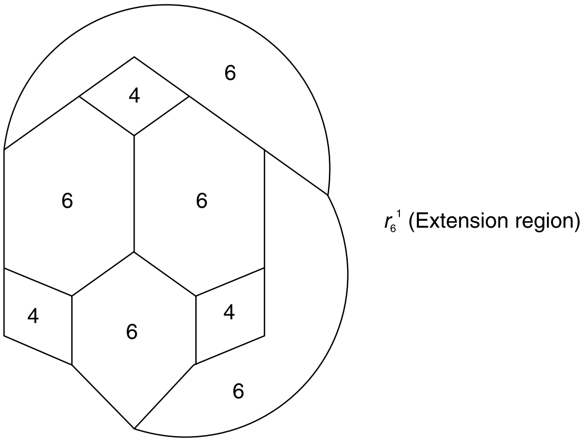


Fig. 8.146

Solution: Number of regions of degree 4 = 3

$\therefore\ r_4 + r_4' = 3$

Number of regions of degree 6 = 6

$\therefore\ r_6 + r_6^1 = 6$

applying Grinberg's theorem

$$(4 - 2)\,(r_4 - r_4') + (6 - 2)\,(r_6 - r_6') = 0$$

or
$$2(r_4 - r_4') + 4(r_6 - r_6') = 0$$

or $$(r_4 - r_4') + 2(r_6 - r_6') = 0$$

or $$(r_4 - r_4') = -2(r_6 - r_6')$$

Hence the difference between r_4 and r_4' must be a multiple of 2 (i.e., even)

But $(r_4 - r_4') = 3$

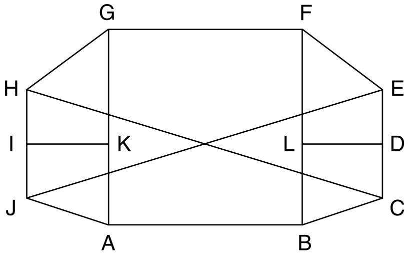
The possibilities are 0, 3, and 1, 2. The difference between 0 and 3 is not even. Similarly, the difference between 1 and 2 is also not even.

Hence there cannot be a Hamiltonian cycle in the graph.

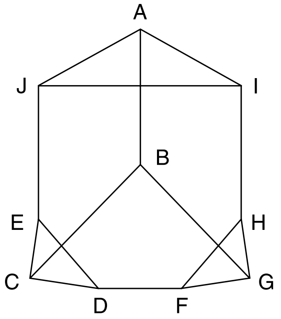
EXERCISE 8.8

1. Show that the following graphs are Hamiltonian:

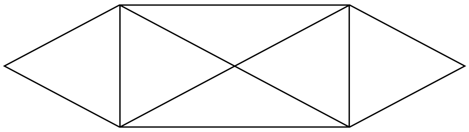
(*a*)



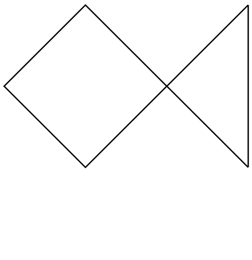
(*b*)



(*c*)

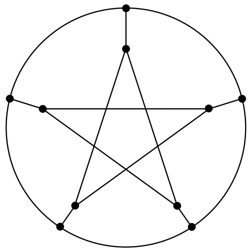


2. Show that graph *G* is Eulerian but not Hamiltonian:

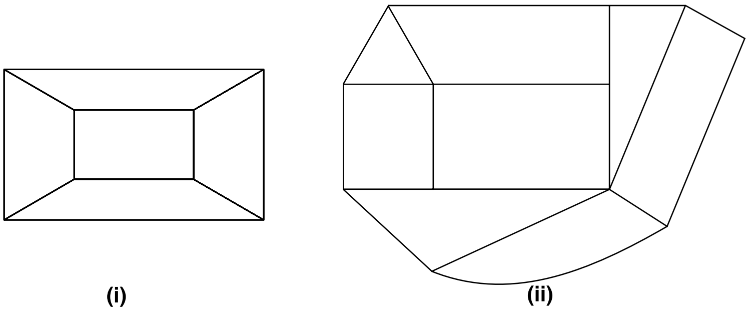


3. Show that Peterson's graphs is non-Hamiltonian.

4. In the graph given below find a Hamiltonian cycle or show that it does not exist: ***(O.U., MCA, 1998)***

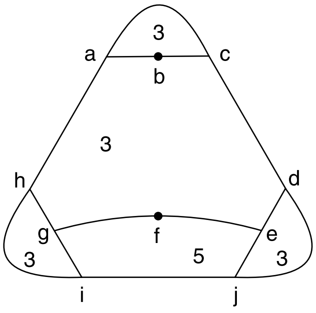


5. Are the graphs given below in Figures (*i*) and (*ii*) are Hamiltonian. If yes find the Hamiltonian circuits. ***(O.U., MCA, 1991)***



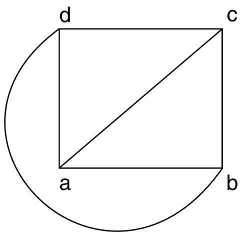
6. Show that there are no planar Hamiltonian graphs of degree 4, 5 and 8 with only one region of degree 4.

7. In the graph shown below, prove that any H-cycle can include exactly two of the edges $\{a, h\}$, $\{c, d\}$, $\{i, j\}$. Further, if H-cycle includes $\{d, e\}$, $\{e, j\}$ the H-cycle cannot include $(a, h\}$.

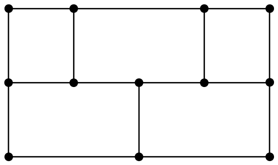


8. Define Hamiltonian circuit and a Hamiltonian path. ***(MKU, MCA, May 2002)***

9. Show that the graph *G* given below has a Hamiltonian cycle but no Euler circuit:



10. Show that the following graph is Hamiltonian:



8.54 GRAPH COLOURING

In this section, we describe the colouring of a graph and its chromatic number. Question related to colouring of vertices, edges and regions are considered.

Definition 8.101: A colouring of a graph *G* is an assignment of colours to its vertices so that no two adjacent vertices have the same colour.

Definition 8.102: A *K*-vertex colouring of a graph *G* is an assignment of *K*-colours to the vertices of *G* such that no two adjacent vertices receive the same colour.

Every graph with *n*-vertices is *n*-colourable. The set of all points with any one colour is independent and is called a colour class. If a graph is *n*-colourable, then the vertex set *V* (G) can be partitioned into *n*-colour classes. The colouring a graph is called proper colouring.

The graph shown in Fig. 8.147 is a properly coloured graph:

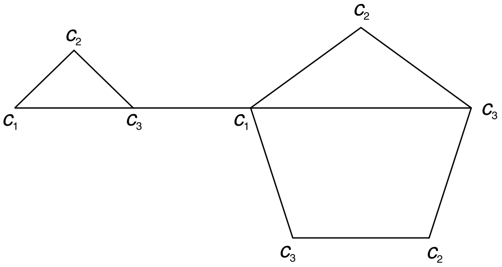


Fig. 8.147

Colours are usually represented by positive integers. Thus *n*-colouring of a graph *G* is a function *f*: *V* (*G*) → (1, 2, ..., *n*)

Such that $f(V_1) \neq f(V_2)$ whenever $\{V_1, V_2\}$ $E(G)$

The vertex colouring of two different graphs are shown in the graphs of Fig. 8.146.

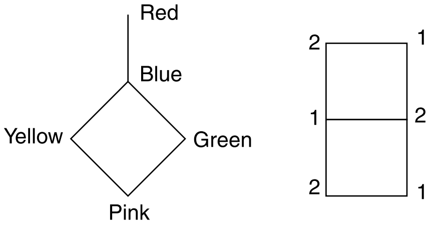


Fig. 8.148

8.54.1 Chromatic Number

Definition 8.103: The Chromatic number of a graph G, is the minimum number of colours required to colour the vertices of G_i. Such that no two adjacent vertices receive the same colour.

The chromatic number of a graph G is denoted by $X(G)$. We observe the following:

1. The Chromatic number of an isolated vertex is one.
2. The Chromatic number of a graph having atleast one edge is atleast two.
3. The Chromatic number of a path P_n, $(n \geq 2)$ is two.
4. The Chromatic number of a wheel graphs is 3 if it has odd number of vertices and u if it has even number of vertices.
5. If G is graph consisting of simply are circuit, with $n \geq 3$, is 2 Chromatic if n is even and 3 Chromatic if n is odd.

We can also define the Chromatic number of a graph as follows.

Definition 8.104: The Chromatic number of a graph G is the least position integer K, such that G has K-colouring.

Theorem 8.35: There exists a K-colouring of a graph G if and only $V(G)$ can be partitioned into K subsets $V_1, V_2, \ldots V_k$ such that no two vertices in V_{i} $(i = 1, 2, \ldots, k)$ are adjacent.

Proof: Let f: $V(G) \rightarrow (1, 2, \ldots k)$ be a colouring of G and let $V_i = \{\in \; f(v) = i, 1 \leq i \leq k\}$.

Therefore, V_i denotes the set of vertices coloured i. Then $V = V_1 \cup V_2 \cup \ldots \cup V_k$ forms a portion of V, such that no two vertices in $V_i = (1 \leq i \leq k)$ are adjacent.

Conversely, let $V = V_1 \cup V_2 \cup \ldots \cup V_k$ be a portion of $V(G)$ such that no two vertices in $V_i = (1 \leq i \leq k)$ are adjacent. Then the function

f: $V(G) \rightarrow (1, 2, \ldots, k)$ defined by

$f(v) = i$ if $v \in V_i$ is a K-colouring of G.

Theorem 8.36: If H is a subgraph of G, then $X(H) \leq X(G)$.

Proof: Let $X(G) = K$ and f denote a K-colouring of G. Then f restricted to $V(H)$ is a K-colouring of H.

Hence $X(H) \leq K \Rightarrow X(H) \leq X(G)$.

Corollary: If $G \geq K_n$; Then $X(G) \geq n$; i.e., a graph G containing complete graph of K-vertices is atleast K-Chromatic.

Theorem 8.37: A graph G is 2-Chromatic if and only if G is bipartite.

Proof: Let G be 2-Chromatic. Then the vertex set V (G) can be partitioned into two-colour classes which are in pendant sets. Hence the two-colour classes form a partition of G. Therefore G is bipartite.

Conversely, let G be a bipartite graph. The vertex set V (G); can be partitioned into two independent set V_1 and V_2. We can use colour C_1 to paint the vertices of V_1 and use colour C_2 to paint the vertices of V_2. Hence V is 2-Chromatic.

Note: If a graph G is bipartite; then it does not imply than X $(G) = 2$. For example $\overline{K}_2$ is bipartite but $X(\bar{k}_2) = 1$. If G contains an edge then G contains atleast one pair of vertices which are adjacent. Hence we require two colours of the edge and X $(G) \geq 2$.

Theorem 8.38: Every tree with two or more vertices is 2-Chromatic.

Proof: Let T denote a given tree and v be any vertex in T. Assign colour 1 to the vertex v. Assign all the p vertices adjacent to v with colour 2 and assign colour 1 to all vertices adjacent to the vertices of colour 2. Continue this process till every vertex in T is coloured. Now we find that, all the vertices at odd distances from v have colour 2 and the vertices.

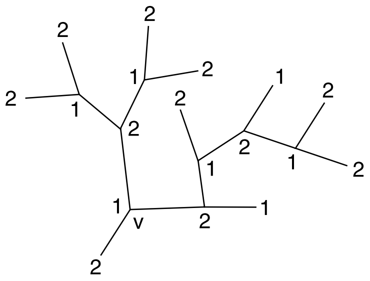


Fig. 8.149

Which are at even distance from v have colour 1. Since T is connected and has atleast two vertices it contains atleast are edge (and there is one and only one path between two vertices in T) T is not 1-colourable. Hence T can be property coloured with 2 colours. Therefore, chromatic number T is 2.

Theorem 8.39: It $\Delta(G)$ denoted Max {deg G (V): $u \in V$ }for any graphs G, then X $(G) \leq \Delta(G) + 1$.

8.54.2 Edge Colouring

Definition 8.105: Assignment of colours to the edges of a graph G. So that no two adjacent edges receive the same colour is called an edge colouring of G.

K-edge colouring of a graph G is an assignment of K-colours to the edges of G such that no two edges of G receive the same colour.

Definition 8.106: A graph G is said to be K-edge colourable; if there exist K-edge colouring of G.

Definition 8.107: The minimum number K, such that a graph G has K-edge colouring is said to be the edge-Chromatic number of G. The edge chromatic number of a graphs G is denoted by $X'(G)$. Thus $X'(G)$ denotes the minimum number of colours required to colour the edges of the graph G. Such that no two adjacent edges of G receive the same colour.

Theorem 8.40: A graph G containing atleast one edge is 2-chromatic if and it contains no odd cycles.

Proof: Let G be a connected graph with cycles of only even lengths. Consider a spanning tree T of G. We know that T can be properly coloured with two colours. Now add edges (of G which are not in T) one by one. Since G has no cycle of odd length the end vertices of every edge being replaced are differently coloured in T. Thus G is properly coloured with two colours i.e., G is 2-chromatic.

Conversely, let G be a 2-coloured graph with atleast one edge. If G has a cycle of odd length, we would need atleast three colours just for that cycle. But G is 2-chromatic, hence G contains no odd cycles.

8.54.3 Five-Colour Theorem

We shall now show that every planar graph can be properly coloured with five colours.

Theorem 8.41: Every planar graph is 5-colourable.

Proof: We shall prove the theorem by induction on the number n of vertices. Since any planar graph with 1, 2, 3, 4 or 5 vertices can be properly coloured with five colours, we assume that vertices of every planar graph with $n - 1$ vertices can be properly coloured with five colours, and then prove that any planar graph G with n vertices requires five colours for proper colouring.

Let G be a planar graph with n vertices. Since G is planar, it must have atleast one vertex of degree five or less. Let v denote the vertex.

Let $G' = G - v$, then G' has $n - 1$ vertices and G' requires no more than 5 colours. Suppose that the vertices of G' have been properly coloured and now we add the vertex v and all the edges incident of v to G'. If the degree of is 1, 2, 3 or 4, we can assign a colour to v so that the vertices of G are properly coloured. We now consider the case in which the degree of v is 5 and all the five colours are used for colouring the vertices of G adjacent to v. Let v_1, v_2, v_3, v_4 and v_5 denote the vertices of adjacent to v in G coloured with C_1, C_2, C_3, C_4 and C_5 respectively.

Let H_1 denote the subgraph of G generated by the vertices coloured C_1 and C_3. If v_1 and v_2 belong to the different components of H_1 interchange the colours C_1 and C_3 in the component containing v_1 and assign ten colour C_3 to the vertices v_1 and v_3. We get the proper colouring of G by assigning colour C_1 to the vertex v.

If v_1 and v_3 are in the same component of H, then there exists a $v_1 - v_3$ path in G all of whose points are coloured alternatively with the colours C_1 and C_3. (*see* Fig. 8.146). Since G is planar a similar path between the vertices v_2 and v_4 coloured alternatively with colours C_2 and C_4 cannot exist. Let H_2 denote the subgraph generated by the vertices coloured C_3 and C_4 *i* then v_2 and v_4 belong to different components of K. We can interchange the colours C_2 and C_4 in the component containing v_2. When the vertices v_2 and v_4 are assigned the colour C_4, we can choose the colour C_2 to paint the vertex v and obtain a proper colouring of G. This completes the proof.

8.54.4 Four-Colour Conjecture

So far we have discussed proper colouring of vertices and proper colouring of vertices of edges of a graph. Now, briefly consider the proper colouring of regions in planar graphs such that no two adjacent region receive the same colour.

The four-colour problem states that every plane map however complex, can be coloured with four colours in such a way that two adjacent regions get different colours, fascinated mathematicians. This problem was solved by Appel and Hanken in 1976. However, this problem is infact equivalent to the statement of conjecture.

Four-colour conjecture: Every planar graph is 4-colourable.

Example: The graph K_4 is a planar graph and K_4 is 4-colourable (Fig. 8.150)

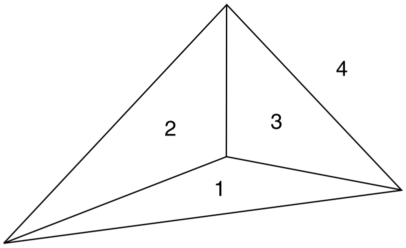


Fig. 8.150

8.54.5 Welch-Powell Algorithm

We give an algorithm by Welch and Powell for a colouring of a graph G.

Algorithm: (Welch-Powell)

Input: A graph G.

Step 1: Order the vertices of G according to decreasing degrees.

Step 2: Assign the first colour to C_1, to the first vertex and then in sequential order assign C_1 to each vertex which is not adjacent to a previous vertex which was assigned the colour C_1.

Step 3: Repeat the Step 2, with a second-colour C_2 and the subsequence of non-coloured vertices.

Step 4: Repeat Step 3, with a third-colour C_3, then a fourth-colour C_4 and so an until all the vertices are coloured.

Step 5: Exit.

Note: Welch-Powell algorithm does not always yield a minimum colouring of a graph G.

Example: Use Welch-Powell algorithm to colour the graph G, and find the chromatic number of the graph.

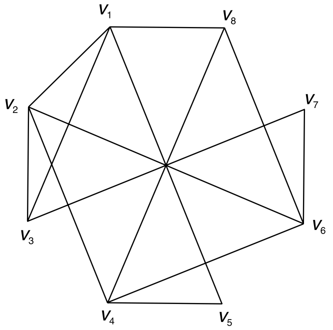


Fig. 8.151

Solution: We have deg $(v_1) = d(v_1) = 4$,

$$d(v_2) = 3, d(v_3) = 3, d(v_4) = 4, d(v_5) = 3, d(v_6) = 4, d(v_7) = 2, d(v_8) = 5$$

we first order, the vertices to decreasing degree to obtain the following sequence v_8, v_1, v_4, v_6, v_2, v_3, v_5, v_7 . C_1 denoted the first-colour, C_2 denotes the second-colour, C_3 denotes the third-colour ....

Which are used to paint the vertices of the graphs *G*.

We first use colour C_1 to paint the vertices v_8, v_2 and v_7 (since v_1, v_4, v_6 are adjacent to v_8, and each of the vertices v_3 and v_5 is connected to either v_8 or v_2. We cannot paint colour C_1 to v_1, v_3, v_4, v_5, v_6 and v_7).

We use the colour C_2 to paint the vertices v_1 and v_4 and the remaining vertices v_6, v_3 and v_5 can be painted with the third-colour.

All the vertices are properly coloured.

Hence $X(G) = 3$.

8.54.6 Independent Sets, Chromatic Partition and Chromatic Polynomials

Let *G* be a properly coloured graph. The vertex set of *G* can be partitioned into different subsets. The proper colouring of *G* induces a partition of the vertices of *G*. Such that no vertices of the same subset are adjacent. Such sets are called Independent sets.

Definition 8.108: A set of vertices in a graph *G* is said to be an independent set of vertices if no two vertices in the set are adjacent.

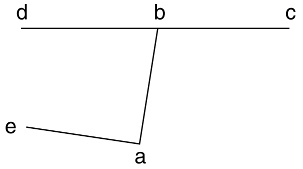


Fig. 8.152

In the graphs of Fig. 8.152. $\{a, c, d\}$ and $\{b, e\}$ are independent sets.

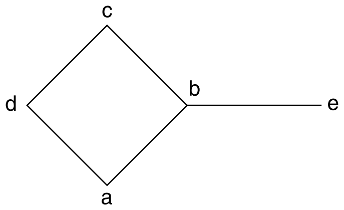


Fig. 8.153

In the graph of Fig. 8.153 $\{a, c, e\}$ is an independent set.

Note: A single vertex in any graph constitutes an independent set and every subset of an independent set is independent.

Definition 8.109: Let *G* be any graph. A subset V' of the vertex set $V(G)$ is called a maximally independent set of *G* if (*i*) V' is an independent set of G.

and (*ii*) If V'' is any other independent set of G, then V' is not a proper subset of G.

$\{V_1, V_3, V_4\}$ and $\{V_2\}$ are maximally independent sets of graph shown in Fig. 8.154.

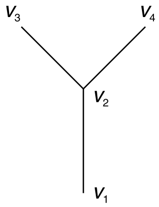


Fig. 8.154

8.54.7 Chromatic Polynomials

Birchoff and Lewis have introduced chromatic polynomials of graphs. Let G be a coloured graph. A colouring of G from λ colours is a colouring of graph G which uses λ or fewer colours. If atleast one of the vertices of G is assigned different colours, then two colourings of graph G from λ colours are said to be different. A graphs G with n vertices can be coloured in many different ways using a sufficiently large number of colours. We use chromatic polynomials to find the number of ways of different proper colouring of a graph on n vertices with a maximum of λ colours.

Definition 8.110: The number of different colourings of a graph on n vertices that can be obtained using λ colours or fewer colours can be expressed as a polynomial of G.

The chromatic polynomial of G is denoted by $P_n(\lambda_i)$.

Let G be a graph on n vertices. If c_i denotes the different ways of properly colouring of G. Using exactly i distinct colours, then these i colours can be chosen out of λ colours in (λ_i) distinct ways.

There are $C_i(\lambda_i)$ distinct ways of properly colouring the graph G using exactly i colours out of λ colours since i can be any positive integer from 1 to n the chromatic polynomial is

$$\sum_{i=1}^{n} \binom{\lambda}{i} C_i$$

where each C_i has to evaluated individually for the given graph. If G is a graph with atleast one edge, then G requires atleast two colours for proper colouring of G, therefore $C_1 = 0$. If G has n vertices, then can be properly coloured using in $n!$ ways, therefore $C_l = 0$.

If G has n vertices; then can be properly coloured using n colours in $n!$ ways. Therefore $c_n = n!$

If G is a complete graph (K_n) on vertices, we have $e_i = 0$ for $i = 1, 2, 3, ..., n - 1$ and $c_n = n!$ Therefore,

$$P_n(\lambda) = \sum_{i=1}^{n} \binom{\lambda}{i} C_i = \frac{\lambda(\lambda-1)(\lambda-2)\ldots(\lambda-n+1)}{n!} \cdot n!$$

$$= \lambda(\lambda-1)(\lambda-2)\ldots(\lambda-n+1)$$

If $G = K_4$ (i.e., complete graph on 4 vertices)

We have $C_1 = C_2 = C_3 = 0$ and $C_4 = 4!$

Hence the chromatic polynomial of G is

$$P_4(\lambda) = \frac{\lambda(\lambda-1)(\lambda-2)(\lambda-3)}{4!} \cdot 4!$$
$$= \lambda(\lambda-1)(\lambda-2)(\lambda-3)$$

Solved Examples

Example 1: Show that the chromatic polynomial of a graph G is

$$\lambda(\lambda-1)(\lambda-2)\ldots(\lambda-n+1)$$

if and only if G is a complete graph on n vertices.

Solution: With λ colours, the first vertex of a G can be coloured in λ ways. A second vertex can be coloured in $(\lambda - 1)$ ways, the third vertex can be coloured in $\lambda - 3$ ways if and only if the third vertex is adjacent to first-two vertices.... and the nth vertex can be coloured in $\lambda - n + 1$ ways if and only if every vertex is adjacent to every other, that is if and only if G is complete.

Example 2: Find the chromatic polynomials of the graph shown in Fig. 8.155.

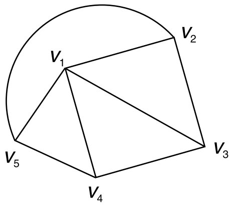


Fig. 8.155

Solution: G has a triangle therefore G requires minimum 3 colours for proper colouring.

We have $C_1 = 0$, $C_2 = 0$

When we have three colours the vertices of the triangle formed by 3 points for example say V_1, V_2, V_3 can be properly coloured in 3! ways. The vertex V_4 can be assigned the colour of V_2 and V_5 can be assigned of the vertex V_3. Thus $C_3 = 3! = 6$.

When we have 4 colours, we can take any four vertices say V_1, V_2, V_3 and V_4 of G and properly be coloured with the 4 colours in 4! ways. The fifth vertex can be assigned the colour the vertex V_2 or of V_3. Thus $C_4 = 2.4! = 48$ and we have $C_5 = 5!$

Hence, the chromatic polynomial of G is

$$P_5(\lambda) = 3!\frac{\lambda(\lambda-1)(\lambda-2)}{3!} + 2 \cdot 4!\frac{\lambda(\lambda-1)(\lambda-2)(\lambda-3)}{4!} +$$
$$5!\frac{\lambda(\lambda-1)(\lambda-2)(\lambda-3)(\lambda-4)}{5!}$$
$$= \lambda(\lambda-1)(\lambda-2) + 2\,\lambda(\lambda-1)(\lambda-2)(\lambda-3) +$$
$$\lambda(\lambda-1)(\lambda-2)(\lambda-3)(\lambda-4)$$

$$= \lambda(\lambda - 1)(\lambda - 2)\left[1 + 2(\lambda - 3) + (\lambda - 3)(\lambda - 4)\right]$$
$$= \lambda(\lambda - 1)(\lambda - 2)[\lambda^2 - 5\lambda + 7]$$

Theorem 8.42: Let u and v be two non-adjacent vertices of a graph G and G' be a graph obtained by adding an edge between u and v. (i.e. $G' = G + u\ v$). Let $G'' = G - u\ v$. i.e., G'' be the simple graph obtained from G by fusing the vertices u and v together and replacing sets of parallel edges with single edges. Then

$$P_n(\lambda) \text{ of } G = P_n(\lambda) \text{ of } G' + P_{n-1}(\lambda) \text{ of } G''$$

Proof: The λ colouring of G is of two types:

(*i*) λ colouring if G assigning different colours to the vertices of u and v.

and (*ii*) λ colouring assigning the same colour to u and v.

Hence the number of ways of properly colouring G such that u and v have different colours.

= Number of ways of properly colouring G' and the number of ways of properly colouring G such that u and v have same colour.

= Number of ways of properly colouring G''.

$$P_n(\lambda) \text{ of } G = P_n(\lambda) \text{ of } G' + P_{n-1}(\lambda) \text{ of } G''$$

Theorem 8.43: Is often used in evaluating the chromatic polynomial of a graph. For example, Fig. 8.156 illustrates how the chromatic polynomials of a graph G is expressed a sum of chromatic polynomials of 5 complete graphs.

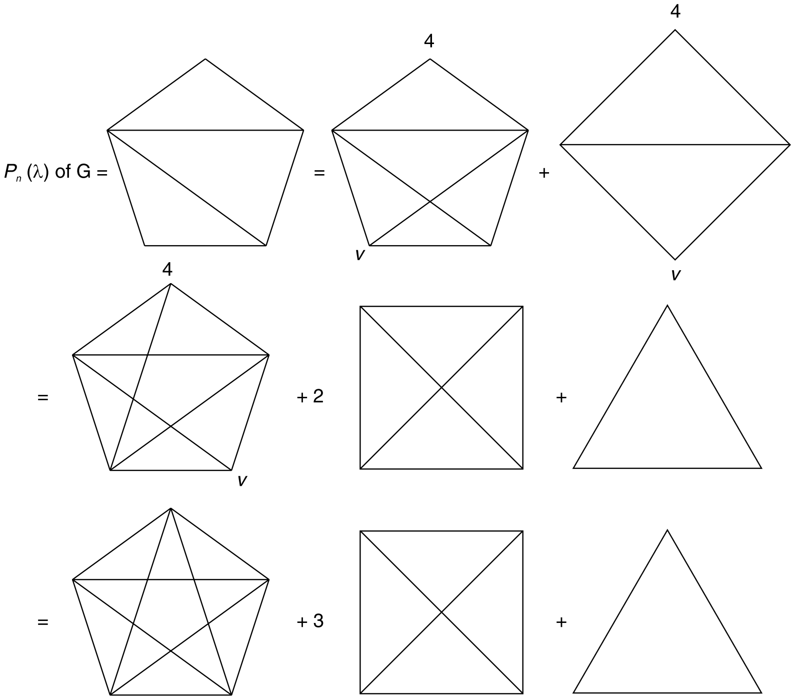


Fig. 8.156

$$= P_n(\lambda) \text{ of } K_5 = 3P_n(\lambda) \text{ of } K_4 + P_n(\lambda) \text{ of } K_3$$

$$P_5(\lambda) \text{ of } G = P_5(\lambda) \text{ of } K_5 + 3P_4(\lambda) \text{ of } K_4 + P_3(\lambda) \text{ of } K_3$$

Example 3: Sketch two non-isomorphic graphs which have the same chromatic polynomial.

Solution: Consider the groups G, and G_2 as shown in Fig. 8.157.

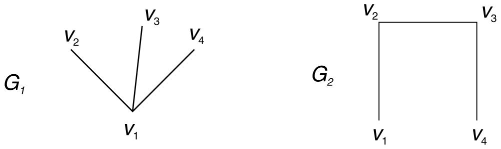


Fig. 8.157

G_1 is a tree with v_1 as to its root

G_2 is a non-directed tree.

we have $X(G_1) = 2 = X(G_2)$

The graph G_1 has a vertex whose degree is 3. There is no vertex of degree 3 in G_2.

The degree sequence of G_1 is (1, 1, 1, 3) and the degree sequence of G_2 is (1, 1, 2, 2). Therefore, the degree sequences of G_1 and G_2 are not the same. Hence G_1 and G_2 are 2-chromatic but not isomorphic.

EXERCISE 8.9

1. Define the terms:

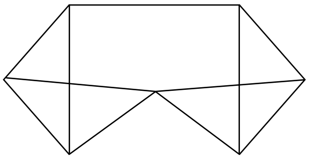
(*i*) Vertex colouring of a graph.

(*ii*) Chromatic number of a graph.

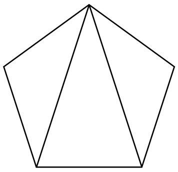
(*iii*) K-critical graph.

2. Find the chromatic number of the following graphs:

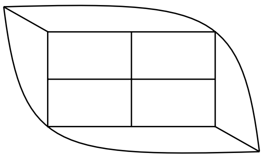
(*i*)



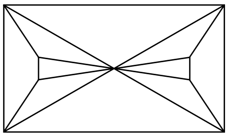
(*ii*)



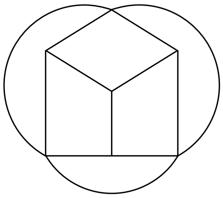
(*iii*)



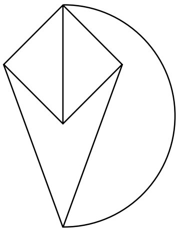
(*iv*)



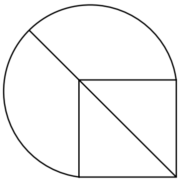
(*v*)



(*vi*)

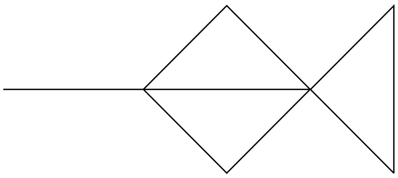


(*vii*)

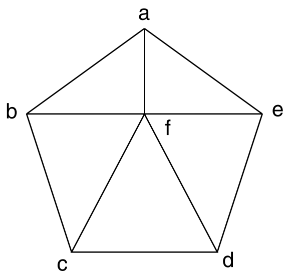


3. Write down all possible independent sets of the following graphs:

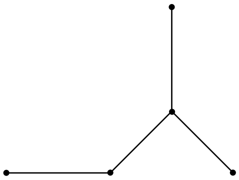
(*i*)



(*ii*)



(*iii*)



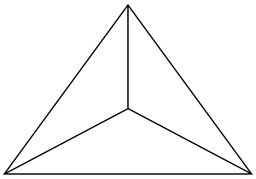
4. Show that the vertices of a planar graph with less than 30 edges is 4-colourable.

5. Show that a simple connected planar graph with 17 edges and 10 vertices cannot be 2-colourable.

6. Show that simple graph with 7 vertices each 4 is non-planar.

7. Show that a graph is dichromatic if and only if it has no odd circuits.

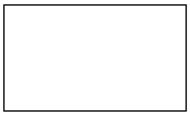
8. Find all maximal independent sets of the following graph:



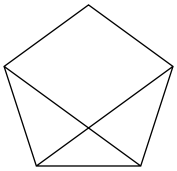
9. Show that the regions of a planar graphs can be 2-coloured if each vertex has degree which is even.

10. Find the chromatic polynomials of the following graphs:

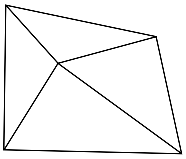
(*i*)



(*ii*)

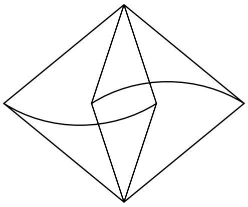


(*iii*)

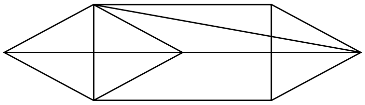


11. Find the chromatic numbers of the following graphs.

(*a*)

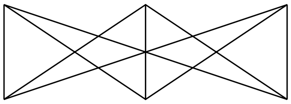


(*b*)

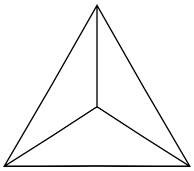


12. Find the edge chromatic number for the graphs given below:

(*a*)



(*b*)



8.55 DIGRAPHS

In this section, we consider digraphs (directed graphs), graphs in which edges have direction. Digraphs are used to represent models of programmes. A city map showing only one-way street is an example of digraph and there are many situations which require digraphs. The definition of a digraph was given in 8.2.3.

Example 1: Let $V = \{a, b, c, d\}$, and

$$E = \{(a, c), (a, d), (b, c), (d, b), (d, d)\}$$

Then $D = (V, E)$ is a digraph (*see* Fig. 8.158).

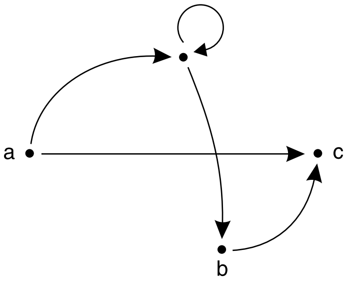


Fig. 8.158

If (u, v) an edge (*arc*) joining u to v in a digraph G_1 the vertex u is called the initial vertex (Tail) and v is called the terminal vertex (Head). We also say that u is adjacent to v and v is adjacent from u. The out degree of a vertex v in a directed graph G is the number of points (vertices) adjacent from it, and the degree of v is the number of points adjacent to v.

Two edges in a directed graph D are said to be parallel if they have same initial and same terminal vertices. An edge with same initial and terminal vertices is called self-loop. If v is an isolated vertex of D then in-degree of v is zero and the out degree of v is also zero. If the degree of v is one, then is called a pendant vertex in G. An alternating sequence of points and edge $v_0\ e_1\ v_1\ e_2\ ...,\ e_n\ v_n$ in which the $e_i = (v_{i-1,}\ v_i)$ is called a walk (directed walk). The number of edge occurring in the walk is called the length of the walk. If the initial and terminal vertices of the walk coincide then the walk is called a closed walk. If $v_0, e_1, v_1, e_2, ..., e_n, v_n$ is a walk then $v_1, v_2, ..., v_{n-1}$ are called the internal vertices of the walk ($v_0 - v_n$ walk).

If all the vertices of a walk in a directed graph D are distinct then the walk is called a path (directed path). A cycle is a non-trivial closed path write all vertices distinct (except the first and last). A directed graph that has no self-loop or parallel edges is called a simple digraph (*see* Fig. 8.159)

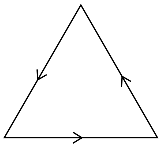


Fig. 8.159

If there is a path from a vertex u to another vertex v in a digraph D, then v is said to be reachable from u, and the distance $d(u, v)$ from u to v is the length of any shortest such path. A digraph is said to be strongly connected if and only if every pair of vertices of it is reachable from one another. If for every pair of points in a digraph D, atleast one is reachable from the other then D is said to be unilaterally connected.

A semi-path in a digraph D is defined as a path in the underlying graph G is D.

A digraph D is said to be weakly connected if its corresponding undirected graph G is connected but D is not strongly connected. If D is weakly connected then every two points of D are joined by a semi-path.

A digraph is that is not even weak is called a disconnected graph.

Example 2: The graph shown in Fig. 8.160 (*a*) is strongly connected, the graph shown in Fig. 8.160 (*b*) is unilateral and the graph shown in Fig. 8.160 (*c*) is a simple digraph.

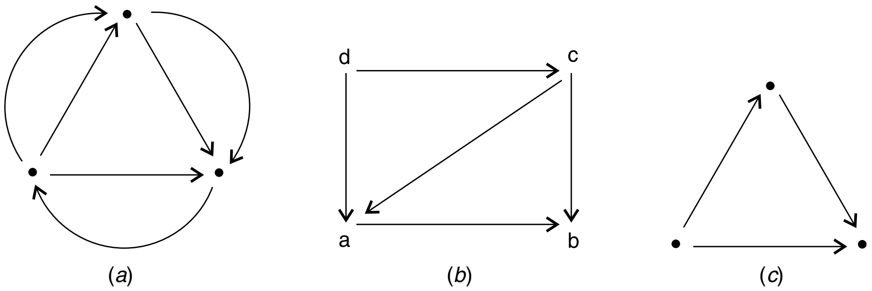


Fig. 8.160

(*a*) Strongly connected graph.
(*b*) Unilaterally connected graph.
(*c*) Simple digraph.

8.56 RELATIONS AND DIGRAPHS

Let *R* be a relation defined on a set *A* and let digraph *D* represent the relation *R*. Each ordered pair (*u, v*) in *R* is represented by a directed edge drawn from *u* to *v* in *D*. If *R* is a reflexive relation the directed graph *D* of *R* will have a self-loop at every vertex. Such a digraph of reflexive (binary) relation on a set *A* is called a reflexive digraph. If *R* is a symmetric relation on a set *A*, then for every directed edge from a vertex *u* to *v*, there is a directed edge from *v* to *u* in the digraph *D* of *R*. The directed graph *D* of a symmetric relation *R* is called a symmetric digraph.

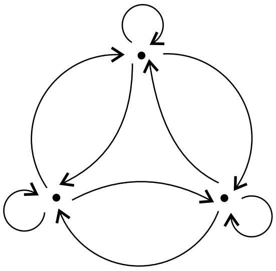


Fig. 8.161 Digraph of a symmetric relation

A digraph representing a transitive relation *R* on a set *A* is called a transitive digraph.

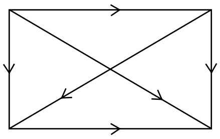


Fig. 8.162 Transitive digraph

A digraph representing an equivalence relation on a set *A* is called equivalence digraph.

Example 1: Given an example of a digraph which is strongly connected.

Solution: The graph shown figure is strongly connected.

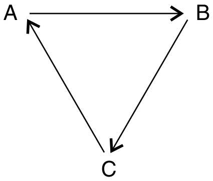


Fig. 8.163

Example 2: Find the shortest spanning path in graph shown in Fig. 8.164:

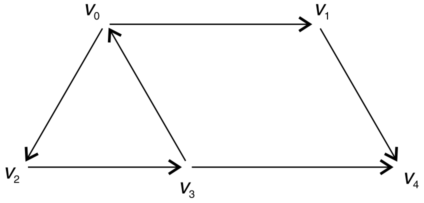


Fig. 8.164

Solution: A spanning path in a graph contains all the vertices of *G*.

$$v_2 - v_3 - v_0 - v_1 - v_4$$

is a simple i.e., shortest spanning path in *G*.

Example 3: Construct the matrix corresponding to the digraph shown in Fig. 8.165

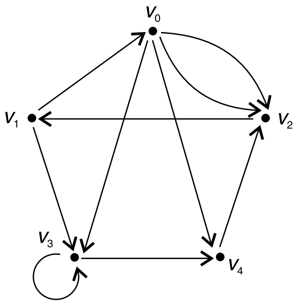


Fig. 8.165

Solution: Let *M* denote the matrix corresponding to the digraph *G*. The matrix *M* is given below:

$$\mathrm{M} = \begin{pmatrix} 0 & 0 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Fig. 8.166

Example 4: Construct digraph corresponding to the matrix *M*. Where *M* is given as

$$\mathrm{M} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{pmatrix}$$

Fig. 8.167

Solution: The matrix M is a 4×4 matrix hence the digraph G has 4 vertices. Let v_0, v_1, v_2 and v_3 denote the vertices of G. The digraph G can be drawn as shown in Fig. 8.168:

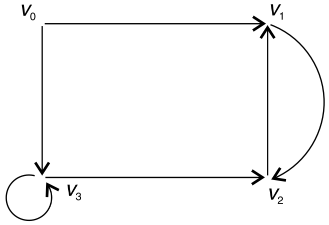


Fig. 8.168

8.57 ARBORESCENCE

Definition 8.111: Let G be a directed graph. G is said to be an arboresence if:

(*i*) G contains no circuit—neither directed nor semi-circuit; and

(*ii*) G has exactly one vertex v of zero in-degree.

The vertex v of zero degree in G is called the root of the arboresence.

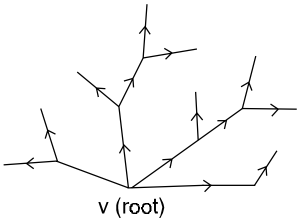


Fig. 8.169

From the definition, it is clear that on arborescence is a directed tree in which there is exactly one vertex of in-degree zero. If G is an arborescence then every vertex of T is reachable, from the root, and the root is not accessible from any other vertex of G. If v is a vertex of out-degree zero, in G then v is necessarily a pendant vertex. An arborescence is sometimes referred to as an out-tree.

Theorem 8.44: An arborescence is a tree in which every vertex other than the root has an in-degree of exactly one.

Proof: Let G be an arborescence with n vertices. G can have at most $n - 1$, edges, because of condition (*i*) If v_1, v_2, ..., v_n denote the vertices of G, then the sum of in degree of all vertices in G, i.e.,

$$d^-(v_1) + d^-(v_2) + \cdots + d^-(v_n) \cdot \leq n - 1$$

exactly one of the terms on the left-hand side of the above equation is zero (by conditions (*ii*)) and the remaining terms must all be positive integers, therefore each of the remaining terms must be 1. Now, since there are exactly $n - 1$, vertices of in-degree one and one vertex of in-degree zero, G has exactly $n - 1$ edges. Since G is without circuits, G must be connected. Hence G must be a tree, in which every vertex other than the root has an in-degree of exactly one.

8.58 WARSHALL'S ALGORITHM

We know that, digraph is just a relation on set and adjacency matrices can be used to represent relations on sets. The methods of finding transitive closure of a given relation (digraph) was discussed in Section 3.16 of Chapter 3. Through there are many methods to find the transitive closure of a relation (digraph) Warshall's method is considered to be the best-known methods describe the methods as follows:

Let $A = \{a_1, a_2, \ldots, a_n\}$ and R be a relation on A. If $v_1, v_2, \ldots, v_n$ is a path in R, then the vertices $v_2, v_3, \ldots, v_{m-1}$ are called internal vertices of the path. For $1 \le r \le n$ we define a Boolean matrix, w_r as follows:

w_r has a 1 in position i, j if and only if there is a path from a_i to a_j in R whose internal vertices if any are the members of the set $\{a_1, a_2, \ldots, a_r\}$. Since all the vertices of the diagram are the elements of A, it follows that w_n has a 1 is position i, j if and only if some path in R connects a_i with a_j. If we define w_0 to be m_r (matrix of R) then we will have a sequence $w_0, w_1, \ldots, w_n$ where $w_0 = m_R$ and $w_n = w_n$.

Suppose $w_r = [p_{ij}]$ and $w_{r-1} = [q_{ij}]$.

If $p_{ij} = 1$, then there must be a path from a_i to a_j whose interior vertices belong to the set $\{a_1, a_2, \ldots, a_r\}$. If a_r is not an interior vertex of this path, then all the interior vertices must come from the set $\{a_1, a_2, \ldots, a_{r-1}\}$ such that $q_{ij} = 1$.

Hence $p_{ij} = 1$ if and only if

(*i*) $q_{ij} = 1$ or
(*ii*) $q_{ir} = 1$ and $q_{rj} = 1$

If w_{r-1} has a 1 in position i_{ij} then by (*i*) so will the matrix w_r and by (*ii*) a new 1 can be added in position i_{ij} of w_r if and only if rth column of $w_r - 1$ has a 1 in position i. The following steps are involved in computing w_r from w_{r-1}.

Step 1: Transfer all 1's in w_{r-1} to w_r.

Step 2: List the locations $s_1, s_2, \ldots$ in column r of w_{r-1} where the entry is 1 and the locations $t_1, t_2, \ldots$, in row r of w_{r-1} where the entry is 1.

Step 3: Put 1's in all the positions s_i, t_j of w_r (if there are 1's in such positions).

Example: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 3), (3, 4), (2, 1)\}$ be a relation on A. The transitive closure of R may be computed as follows:

The matrix of the relation R is

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

M_R is 4 × 4 matrix.

Then $$W_0 = M_n = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Consider the column 1 of w_0. The second location (position) of the column 1 (c_1) has we next consider row 1 of w_0. The second locations row 1 (R_1) has 1.

Therefore, we put 1 in the position 2, 2 of w_0, to form the matrix w_1.

The matrix obtained can be written as follows:

$$W_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

in column 2 of w_1, we find the locations 1 and 2 have 1's. in row 2 the matrix w_1 has 1's in the position 1, 2 and 3. To obtain the matrix w_2 we put 1's in the position (1, 1), (1, 2), (1, 3), (2, 1) (2, 2) and (2, 3) of w_1. It can written as

$$W_2 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The locations 1 and 2 of column 3 of w_2 has 1's and location 4 of row 3 of w_2 has a 1. We put 1 in the position (1, 4) and (2, 4) of w_2 to form w_3.

$$W_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

w_3 has 1's in the locations 1, 2, 3 of column 4 and no 1's in row 4. Therefore no new 1's are added to w_3. While forming w_4.

$$W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

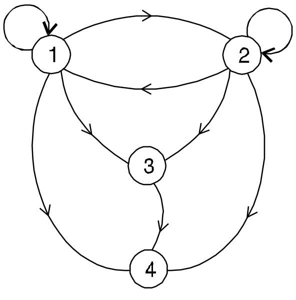
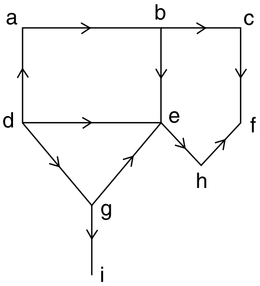


Fig. 8.170 Transitive closure of *R*

EXERCISE 8.10

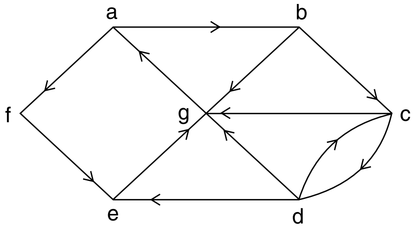
1. Define the terms:
   (*a*) Directed graph
   (*b*) Simple digraph
   (*c*) Walk in a digraph
   (*d*) A symmetric digraph
   (*e*) Symmetric digraph
   (*f*) Strongly connected digraph.
   Give examples.
2. Define the terms:
   (*i*) In degree of a vertex.
   (*ii*) Out degree of a vertex.
   Show that in a digraph *G*, the sum of the degrees in equals the sum of the out degree.
3. Write the adjacency matrix of the graph *G*.



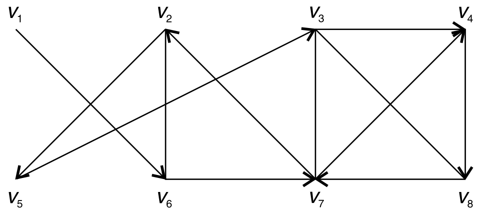
4. Draw the digraph *G* corresponding to the matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{pmatrix}$$

5. Find the out degree of each vertex in the digraph given below:



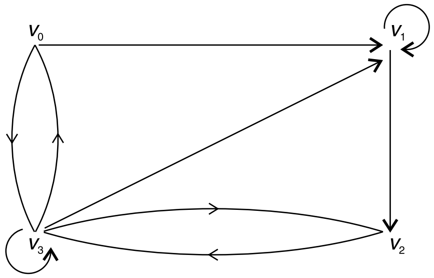
6. Find a simple path in the graph *G*.



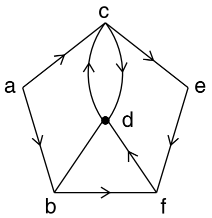
7. Draw the digraph corresponding to the matrix *M*, where *M*

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}$$

8. Construct the matrix corresponding to the digraph *G* (given below):



9. Let R be the relation whose digraph is given below. List all the paths of lengths 3 starting from vertex *a*.



9

Algebraic Structures

9.1 INTRODUCTION

In this chapter, we shall deal with some important algebraic structures—groups, rings, internal domains and fields. We begin with one operational structure (system).

9.2 BINARY OPERATION

Definition 9.1: A binary operation * in a set A is a function from $A \times A$ to A.

Note: The word binary is used in the above definition because we are associating an element of the set A with a pair of elements of A. We can also use symbols like 0, +, ×, etc.

Notation: If * is a binary operation (*b*inary composition) in a Set A then than for the * image of the ordered pair $(a, b) \in A \times A$, we write $a * b$ (or $*\ (a, b)$).

Example 1: Addition (+) is a binary operation in the set of natural number N. Set of integers Z and set of real numbers R.

Example 2: Multiplication (×) is a binary operation in N, Z, Q, R and C.

Example 3: Union, intersection and difference are binary operations in $P(A)$, the power set of A.

9.3 GENERAL PROPERTIES

We now discuss some general properties of binary operations.

Definition 9.2: Let A be any set. A binary operation $*\ A \times A \rightarrow A$ is said to be commutative if for every $a,\ a, b \in A.$

$$a * b = b * a$$

Example 1: Addition is commutative in the set of natural numbers.

Definition 9.3: Let A be a non-empty set. A binary operation $*;\ A \times A \rightarrow A$ is said to be associative if

$$(a * b) * c = a * (b * c) \text{ for every } a, b, c \in A.$$

Example 2: The operations of addition and multiplication over the natural numbers are associative.

Definition 9.4: Let * be a binary operation on a set A. If there exists an element $e_l \in A$ such that $e_l * a = a$ for every $a \in A$, then the element e_l is called the left identity with respect to *. Similarly, if there exists an element $e_r \in A$ such that $a * e_r = a$ for every $a \in A$, the element e_r is called the right identity in A with respect to *.

Definition 9.5: Let * be a binary operation on a non-empty set A. If there exists an element $e \in A$ such that $e * a = a * e = a$ for every $a \in A$, then the element e is called identity with respect to * in A.

Example 3: Zero is the identity element in the set integers with respect to the binary operation addition (i.e., +).

Definition 9.6: Let * be a binary operation on a non-empty set A and e be the identity element in A with respect the operation *. An element $a \in A$ is said to be invertible if there exists an element $b \in A$ such that

$$a * b = b * a = e$$

In which case a and b are inverses of each other. For the operation * if b is the inverses of $a \in A$ then we can write $b = a^{-1}$.

9.3.1 Cancellation Laws

Definition 9.7: A binary operation denoted by * in a set A, is said to satisfy.

(*i*) Left cancellation law if for all a, b, $c \in A$,

$$a * b = a * c \Rightarrow b = c$$

(*ii*) Right cancellation law if for all a, b, $c \in A$

$$b * a = c * a \Rightarrow b = c$$

Definition 9.8: Let * and o be two binary operations inset A; if for all a, b, $c \in A$.

(*i*) $(boc) * a = (b * a)\ o\ (c * a)$
then we say that * is left distributive over o.

(*ii*) $a * (boc) = (a * b)\ o\ (a * c)$
then * is right distributive over o.

(*iii*) and distributive * is both left distributive and right distributive over o.

Example: In P (A), the power set of A, union is distributive over intersection and intersection is distributive of union of sets.

Theorem 9.1: The identity elements of a binary operation * in a set A, if it exists and is unique.

Proof: If possible, let e' and e'' be two identity elements in A with respect to the binary operation $*e'$ is an identity element in A

$$\Rightarrow e' * e'' = e'' * e' = e''$$

and e'' is an identity element in A

$$\Rightarrow e''e' = e' * e'' = e'$$

which together show that

$$e' = e''$$

Theorem 9.2: If * is an associative binary operation in A, then the inverse of every invertible element is unique.

Proof: Let $a \in A$, be an invertible element with respect to *. If possible let b and c be two distinct inverses of the element a in A.

Let e be the identity elements in A with respect to *.

Then we have

$$b * a = a * b = e$$

and $$c * a = a * c = e$$

now $(b *a) * c = b * (a * c)$ $(\because *$ is associative in $A)$

$$\Rightarrow e * c = b * e$$

$$\Rightarrow c = b$$

This completes the proof of the theorem.

Theorem 9.3: If * is an associative binary operation in a set A, such every element is invertible, then * satisfies the left as well as the right cancellation laws i.e.,

$$a * b = a * c \Rightarrow b = c$$

$$b * a = c * a \Rightarrow b = c \ \forall \ a, b, c \in A$$

Proof: Let e be the identity element of A with respect to *. Every element in A is invertible $\Rightarrow a \in A$ is invertible.

Let a' denote the inverse of a in A then

$$a * b = a * c$$

$$\Rightarrow a' * (a * b) = a' * (a * c)$$

$$\Rightarrow (a' * a) * b = (a' * a) * c \ (\because * \text{ is associative})$$

$$\Rightarrow e * b = e * c \ (\because a' \text{ is the inverse of } a)$$

$$\Rightarrow b = c$$

Similarly, we can prove that

$$b * a = c * a \Rightarrow b = c \ \forall \ a, b, c \in A$$

EXERCISE 9.1

1. Show that division is a binary operation on $R - \{0\}$ and $C - \{0\}$.
2. Show that addition is a binary operation in the set M of all $m \times n$ matrices.
3. Show that the least common multiple of two natural is a binary operation in the set of natural numbers N.

4. If * is a binary operation in R defined by $a * a = a + b - ab \; \forall \; a, b \in R,$ then

Show that the inverse of $a \neq 1$ is $\dfrac{a}{a-1}$.

5. Define a 'binary operation'. Mention the various properties binary composition and give examples of each.

9.4 n-ARY OPERATION

Definition 9.9: Let A be a non-empty set. A mapping f: $A^n \rightarrow A$ is called an n-ary operation on the set A and n is called the order of the operation.

For $n = 1, f$: $A \rightarrow A$ is called a unary operation.

For $n = 2, f$: $A^2 \rightarrow A$ is called a binary operation.

It an operation (or composition) on the elements of a set produces images which are also the elements of the same set, the set is said to be closed under that operation and this property is called closure property.

9.5 ALGEBRAIC STRUCTURES (ALGEBRAIC SYSTEMS)

A system consisting of a non-empty set S and one or more n-ary operations on the set S is called an algebraic system. If A is a non-empty set and $f_1, f_2, f_3, \ldots$ are n-ary operations on A, then $(S, f_1, f_2, f_3, \ldots)$ is an algebraic systems (or structure).

The operations on a set S, define a structure on the elements of S, therefore S is called an algebraic structure. Our purpose in this chapter is to study the elementary aspects of some of the most fundamental algebraic structures—groupoids, semi-groups, monoids, groups and rings. We begin with the following definition of an algebraic structure.

Definition 9.10: If A is a set and * is a binary operation on A, then (A, *) is called an algebraic structure.

Example 1: Let R be the set of real numbers, then (R, +) is an algebraic structure.

Example 2: Let Z be the set of integers. Addition (+) and multiplication (×), are binary operations on Z. The system (Z, +) is an algebraic structure and $(Z, \cdot)$ is also an algebraic structure.

Example 3: If N denotes the set of natural numbers then (N, +) is an algebraic structure.

9.5.1 Groupoid

We have defined an algebraic structure. If * is a binary operation on a non-empty set A. Such that $a * b \in A$ for all $a, b \in A$ then we say that A is closed under the operation.

Example 1: If $A = \{0, 1\}$, then A is closed under multiplication.

We have $0 \times 0 = 0$, $0 \times 1 = 0$, $1 \times 0 = 0$, and $1 \times 1 = 1$

But A is not closed under the binary operation addition. Since $1 + 1 = 2$ does not belong to A.

Now we define the following algebraic structure:

Definition 9.11: A groupoid is an algebraic structure consisting of non-empty set A and a binary operation *, which is such that A is closed under *.

Example 2: The set of real numbers is closed under addition, therefore (R, +) is a groupoid.

Example 3: If E denotes the set of even numbers then E is closed under addition. And (E, +) is a groupoid.

Example 4: Let Z^+ denotes the set of positive integers and * be a binary operation on Z^+ defined as follows

$$a * b = 3a + 4b \ \forall \ a, b \in Z^+$$

Clearly (Z^+, *) is a groupoid.

9.6 SEMI-GROUP

Definition 9.12: Let S be a non-empty set and * be a binary operation on S. The algebraic (S, *) is called a semi-group if the operation * is associative. In other words, the groupoid is a semi-group if

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

Thus, a semi-group requires the following:

(*i*) A sets.

(*ii*) A binary operation * defined on the elements of S.

(*iii*) Closure, $a * b$ whenever $a, b \in S$.

(*iv*) Associativity i $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Example 1: Let N be the set of natural numbers. Then (N, +) and (N, *) are semi-groups.

Example 2: X be a non-empty set and P (X) denote the power set of X. Then $(P(x), \cup)$ and $(P(x), \cap)$ are semi-groups.

Example 3: Let Z be the set of integers and Z_m be the set equivalence classes generated by the equivalence relation "congruent modulo M" for any positive integers m. Then $+_m$ be defined integers of + on Z as follows:

For any $[i], [j] \in Z_m$

$$[i], +_m [j] = [(i + j) \bmod m]$$

The algebraic system (Z_m, + m) is a semi-group.

9.7 HOMOMORPHISM OF SEMI-GROUPS

Definition 9.13: Let (S, *) and (T, 0) be any two semi-groups. A mapping f: $S \rightarrow T$ such that for any two elements $a, b \in S$

$$f(a * b) = f(a) \text{ o } f(b)$$

is called a semi-group homomorphism.

Definition 9.14: A homomorphism of a semi-group into itself is called a semi-group endomorphism.

9.8 ISOMORPHISM OF SEMI-GROUPS

Definition 9.15: Let $(S, *)$ and $(T, 0)$ be any two semi-groups. A homomorphism f: $S \rightarrow T$ is called a semi-group isomorphism if f is one-to-one and onto.

If f: $S \rightarrow T$ is an isomorphism then $(S, *)$ and $(T, 0)$ are said to be isomorphic.

Definition 9.16: An isomorphism of a semi-group onto itself is called a semi-group automorphism.

Theorem 9.4: Let $(S, *)$, $(T, 0)$ and (V, Δ) be semi-grouops f: $S \rightarrow T$, and $T \rightarrow V$ be semi-group homomorphism. Then gof: $S \rightarrow V$ is a semi-groups homomorphism from $(S, *)$ to $(\vee, \Delta)$.

Proof: Let $a, b \in S$ then

$$\begin{aligned}(gof)\,(a * b) &= g\,[f\,(a * b)\\ &= g\,[f\,(a)\;o\,f\,(b)]\\ &= (g\,f\,(a))\;\Delta\;(gf\,(b))\\ &= (gof)\,(a)\;\Delta\;(gof)\,(b)\end{aligned}$$

Hence $gof: S \rightarrow V$ is a semi-group homomorphism.

We state the following theorem without proof.

Theorem 9.5: The set of all endomorphisms of a semi-group is a semi-group under the operation of (left) composition.

Theorem 9.6: The set of all semi-group automorphisms of a semi-group is a semi-group under the operation of (left) composition.

Theorem 9.7: Let $(S, *)$ be a semi-group and $(S^s, 0)$ be the semi-group of functions from S to S, then there exists a homomorphism $\varnothing : S \rightarrow S^s$ under the operation of left composition.

Proof: Let $a \in A$ and let

$\varnothing : (a) = f_a$ where $f_a \in S^s$ and f_a is defined by $f_a\,(b) = a * b$ for any $b \in S$.

$$\begin{aligned}f_{a*b}(c) &= (a * b) * c\\ &= a * (b * c)\\ &= f_a\,(f_b\,(c))\\ &= (f_a\,o\,f_b)\;(c) \text{ for all } c \in S\end{aligned}$$

and $\varnothing(a * b) = f_{a*b} = f_a\,o\,f_b = \varnothing(a)\;o\;\varnothing(b)$ for all $a, b \in S$.

Thus $S \rightarrow S^s$ is a homomorphism form $(S, *)$ into $(S^s, 0)$.

9.9 MONOID

Definition 9.17: A semi-group $(M, *)$ with an identity element with respect to the binary operation * is called a monoid. In other words, an algebraic system $(M, *)$ is called a monoid if:

(*i*) $(a * b) * c = a * (b * c) \ \forall \ a, b, c \in M$.

(*ii*) There exists an element $e \in M$ such that $e * a = a * e = a \ \forall \ a \in M$.

Example 1: Let Z be the set of integers (Z, +) is a monoid 0 is the identity element in Z with respect to +.

Example 2: Let N be the set of natural numbers (N, X) is a monoid. 1 e_i the identity element in N with respect to the composition X.

Let (M, *) be a monoid. If the operation * is commutative then (M, *) is said to be commutative. If $a^i, a^j \in M$, we have $a^{i+j} = a^i * a^j = a^j * a^i$ for all $i, j \in M$.

A monoid (M, *) is said to be cyclic if there exists an element $a \in M$. Such that every element of M can be expressed as some power of a. If M is a cyclic monoid such that every element is some power of $a \in M$, then a is called the generator of M. A cyclic monoid is commutative and a cyclic monoid is commutative and a cyclic monoid may have more than one generator.

Example 3: The algebraic system (N, +) is a cyclic monoid generated by 1.

Example 4: If $M = \{-1, 1, i, -i\}$, where $i = \sqrt{-1}$, then (M, *) is a cyclic monoid: The elements i and $-i$ are its generators.

9.10 MONOID HOMOMORPHISM

Definition 9.18: Let (M, *) and (T, 0) be any two monoids e_m and e_t denote the identity elements of (M, *) and (T, 0) respectively. A mapping

$$f: M \to T$$

such that for any two elements $a, b \in M$

$$f(a * b) = f(a) \circ f(b)$$

and

$$f(e_m) = e_t$$

is called a monoid homomorphism.

Monoid homomorphism presents the associativity and identity. It also preserves commutative. If $a \in M$ is invertible and $a^{-1} \in M$ is the inverse of a in M, then $f(a^{-1})$ is the inverse of $f(a)$, i.e., $f(a^{-1}) = [f(a)]^{-1}$.

9.11 GROUPS

Definition 9.19: A group is an algebraic structure (G, *) in which the binary operation * on G satisfies the following conditions:

$G - 1$ for all $a, b, c, \in G$

$$a * (b * c) = (a * b) * c \text{ (associativity)}$$

$G - 2$ there exists an elements $e \in G$ such that for any $a \in G$

$$a * e = e * a = a \text{ (existence of identity)}$$

G –3 for every $a \in G$, there exists an element denoted by a^{-1} in G such that

$$a * a^{-1} = a^{-1} * a = e$$

a^{-1} is called the inverse of a in G.

Example 1: $(Z, +)$ is a group
where Z denote the set of integers.

Example 2: $(R, +)$ is a group
where R denote the set of real numbers.

9.11.1 Abelian Group (or Commutative Group)

Definition 9.20: Let $(G, *)$ be a group. If $*$ is commutative that is

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

then $(G, *)$ is called an Abelian group.

Example: $(Z, +)$ is an Abelian group.

9.11.2 Finite Group

A group G is said to be a finite group if the set G is a finite set.

Example: $G = \{-1, 1\}$ is a group with respect to the operation multiplication. Where G is a finite set having 2 elements. Therefore G is a finite group.

9.11.3 Infinite Group

A group G, which is not finite is called an infinite group.

9.11.4 Order of a Finite Group

Definition 9.21: The order of a finite group $(G, *)$ is the number of distinct element in G. The order of G is denoted by $O(G)$ or by $|G|$.

Example: Let $G = \{-1, 1\}$

The set G is a group with respect to the binary operation multiplication and $O(G) = 2$.

9.12 SOLVED EXAMPLES

Example 1: Show that the set $G = \{1, -1, i, -i\}$ where $i = \sqrt{-1}$ is an abelian group with respect to multiplication as a binary operation.

Solution: Let us construct the composition table.

Table 9.1

•	1	–1	i	$-i$
1	1	–1	i	$-i$
–1	–1	1	$-i$	i
$-i$	i	$-i$	–1	1
$-i$	$-i$	i	1	–1

From the above composition, it is clear that the algebraic structure $(G, \cdot)$ is closed and satisfies the following axioms:

Associativity: For any three elements $a, b, c \in G$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Since

$$1 \cdot (-1 \cdot i) = 1 \cdot -i = -i$$

$$(1 \cdot -1) \cdot i = -1 \cdot i = -i$$

$$\Rightarrow 1 \cdot (-1 \cdot i) = (1 \cdot -1)\, i$$

Similarly with any other three elements of G the properties holds.

$\therefore$ Associative law holds in $(G, \cdot)$

Existence of identity: 1 is the identity element $(G, \cdot)$ such that $1 \cdot a = a = a \cdot 1\ \forall\ a \in G$

Existence of inverse: $1 \cdot 1 = 1 = 1 \cdot 1 \Rightarrow$ 1 is inverse of 1

$(-1) \cdot (-1) = 1 = (-1) \cdot (-1) \Rightarrow -1$ is the inverse of (-1)

$i \cdot (-i) = 1 = -i \cdot i \Rightarrow -i$ is the inverse of i in G.

$-i \cdot i = 1 = i \cdot (-i) \Rightarrow i$ is the inverse of $-i$ in G.

Hence inverse of every element in G exists.

Thus all the axioms of a group are satisfied.

Commutativity: $a \cdot b = b \cdot a\ \forall\ a, b \in G$ hold in G

$$1 \cdot 1 = 1 = 1 \cdot 1, -1 \cdot 1 = -1 = 1 \cdot -1$$

$$i \cdot 1 = i = 1 \cdot i;\ i \cdot -i = -i \cdot i = 1\ = 1 \text{ etc.}$$

commutative law is satisfied

Hence $(G, \cdot)$ is an abelian group.

Example 2: Prove that $G = \{1, \omega, \omega^2\}$ is a group with respect to multiplication where $1, \omega, \omega^2$ are cube roots of unity.

Solution: We construct the composition table as follows:

Table 9.2

•	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

The algebraic system is $(G, \cdot)$ where $\omega^3 = 1$ and multiplication '·' is the binary operation on G.

From the composition table; it is clear that $(G, \cdot)$ is closed with respect to the operation multiplication and the operation '·' is associative.

1 is the identity element in G such that

$$1 \cdot a = a = a \cdot 1 \;\forall\; a \in G$$

Each element of G is invertible

$1 \cdot 1 = 1 \Rightarrow$ 1 is its own inverse.

$\omega \cdot \omega^2 = \omega^3 = 1 \Rightarrow \omega^2$ is the inverse of ω and ω is the inverse of ω^2 in G.

$\therefore$ $(G, \cdot)$ is a group and $a \cdot b = b \cdot a \;\forall\; a, b \in G$ that is commutative law holds in G with respect to multiplication.

$\therefore$ $(G, \cdot)$ is an abelian group.

Example 3: Prove that the set Z of all integers with binary operation * defined by $a * b = a + b + 1$ $\forall\; a, b \in G$ is an abelian group.

Solution: Sum of two integers is again an integer; therefore $a+b \in Z \;\forall\; a, b \in Z$

$$\Rightarrow\; a+b+1 \cdot \in Z \;\forall\; a, b \in Z$$

$\Rightarrow$ Z is called with respect to *

Associative law for all $a, b,\; a, b \in G$ we have $(a * b) * c = a * (b * c)$ as

$$\begin{aligned}(a * b) * c &= (a + b + 1) * c\\ &= a + b + 1 + c + 1\\ &= a + b + c + 2\end{aligned}$$

also

$$\begin{aligned}a * (b * c) &= a * (b + c + 1)\\ &= a + b + c + 1 + 1\\ &= a + b + c + 2\end{aligned}$$

Hence $(a * b) * c = a * (b * c) \in a, b \in Z$.

Example 4: Let S be non-empty set and $P(S)$ be the collection of all subsets of S. Let the binary operation Δ called the symmetric difference of sets be defined as

$$A \,\Delta\, B = (A - B) \cup (B - A) \;\forall\; A, B \in P(S)$$

then show that $(P(S), \Delta)$ is an abelian group.

Solution: If A and B are any two subsets of S, then $A \,\Delta\, B$ is also a subset of S, therefore $(P(S), \Delta)$ is closed with respect to Δ.

Associativity: $\forall\; A, B, C \in P(S)$

$(A \,\Delta\, B) \,\Delta\, C = A \,\Delta (B \,\Delta\, C)$ can easily be verified.

Existence of identity

$\varnothing \in P(S)$ such that

$A \,\Delta\, \varnothing = A = \varnothing \,\Delta\, A$

$\Rightarrow \varnothing$ is the identity in $(P\,(S),\ \Delta)$

Existence of inverse: $\forall\ A \in P(S)$

$A \,\Delta\, A = \varnothing \Rightarrow A$ is the inverse of A.

Commutative law $\forall\ A, B \in P(S)$

$$\begin{aligned} A \,\Delta\, B &= (A - B) \cup (B - A) \\ &= (B - A) \cup (A - B) \\ &= B \,\Delta\, A \end{aligned}$$

Hence $(P\,(S),\ \Delta)$ is an abelian group.

Example 5: Show that the set of four transformations f_1, f_2, f_3 and f_4 on the set of complex numbers be defined by

$$f_1(z) = z,\ f_2(z) = -z$$

$$f_3(z) = \frac{1}{z},\ f_4(z) = \frac{-1}{z}$$

Forms a finite abelian group with respect to the binary operation as the composition of product of two functions.

Solution: Let $G = \{f_1, f_2, f_3, f_4\}$ and '.' denote the composition as the composite of two functions.

We have

$$f_1, f_1 = f_1, f_1, f_2, = f_2, f_1, = f_2$$

$$f_1, f_3, = f_3, f_I = f_1, f_4 = f_4, f_1 = f_4$$

$$f_2\ f_2(z) = -\ f_2(-z) = (-z) = z = f_1(z)$$

$$\Rightarrow f_2\ f_2 = f_1$$

$$f_2\ f_3(z) = f_2(f_3(z)) = f_2\left(\frac{1}{z}\right) = -\frac{1}{z} = f_4(z)$$

$$\Rightarrow f_2\ f_3 = f_4$$

Similarly, we can show that

$$f_2 \cdot f_4 = f_3,\ f_3 \cdot f_2 = f_4$$

$$f_3 \cdot f_3 = f_1,\ f_3 \cdot f_4 = f_2$$

$$f_4 \cdot f_2 = f_3,\ f_4 \cdot f_3 = f_2 \text{ and } f_4 \cdot f_4 = f_1$$

we have the following table:

Table 9.3

$\bullet$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

From the Table 9.3 , it is clear that all the entries are the elements of G and therefore closure property holds good. The composite of functions is associative. f_1 is the identity element of G with respect to the given operation. The inverses of f_1, f_2, f_3 and f_4 are f_1, f_2, f_3 and f_4 respectively i.e., each element in G is its own inverse.

Also, commutative law holds good in G. Therefore $(G, \cdot)$ is an abelian group.

9.13 ADDITION MODULO *m*

We shall now define a composite known as "addition modulo m" where m is fixed integer.

If a and b are any two integers, and r is the least non-negative reminder obtained by dividing the ordinary. Sum of a and b by m, then the addition modulo m of a and b is r symbolically.

$$a +_m b = r, 0 \leq r < m$$

Example: $7 +_5 9 = 1$

since $7 + 9 = 16 = 5 \cdot 3 + 1$

also $-15 +_5 3 = 2$

since $-15 + 3 = -12 = -5 \cdot 2 + (-2)$

The numbers 13 and –23 are identical under addition modulo 4, as their difference is divisible by 4. We therefore write.

$$13 \equiv 1 \pmod 4$$

which is read as 13 is congruent to 1 mod 4.

Also $-23 \equiv 1 \pmod 4$

Which is read as –23 is congruent to 1 mod 4.

$\therefore$ In general, if the difference $a - b$ is divisible by m we write.

$$a \equiv b \pmod m$$

i.e., "a is congruent to b mod m."

9.14 MULTIPLICATION MODULO *P*

The multiplication modulo p, where p is a positive integer of any two integers a and b is defined as r, where r is the least non-negative remainder when the product of a and b is divided by p. Symbolically we write

$$a \times_p b = r, 0 \leq r < p$$

Example 1: Show that the set $G = \{0, 1, 2, 3, 4\}$ is an abelian group with respect to addition modulo 5.

Solution: We form the composition table as follows:

Table 9.4

+5	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Since all the entries in the composition table are elements of G, the set G is closed with respect to addition modulo 5.

Associativity: For any three element $a, b, c \in G$ $(a + b) + c$ and $a + (b + c)$ leave the same remainder when divided by 5.

i.e., $$(a +_5 b) +_5 c = a +_5 (b +_5 c)$$

We have $$(1 +_5 3) +_5 4 = 3 = 1 +_5 (3 +_5 4) \text{ etc.}$$

Existence of identity: Clearly $0 \in G$ is the identity element we have $0 +_5 9 = 9 = 9 +_5 0 \; \forall \; a \in G$.

Existence of inverse: Each element in G is invertible with respect to addition modulo 5.

0 is its own inverse

4 is the inverse of 1 and 1 is the inverse of 4

2 is the inverse of 3 and 3 is the inverse of 2 with respect to addition modulo 5 in G.

Commutativity: From the composition table it is clear that

$$a +_5 b = b +_5 a \; \forall \; a, b \in G$$

Hence $(G, +_5)$ is an abelian group.

Example 2: Show that the set $G = \{1, 2, 3, 4\}$ is an abelian with respect to multiplication modulo 5.

Solution: The composition table for multiplication modulo 5 is

Table 9.5

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the above table, it is clear that G is closed with respect to the operation × 5 and the binary composition $\times_5$ is associative 1 is the identity element.

Each element in G has a inverse.

1 is its own inverse

2 is the inverse of 3

3 is the inverse of 2

4 is the inverse of 4, with respect to the binary operation $\times_5$. Commutative law holds good in $(G, \times_5)$. Therefore $(G, \times_5)$ is an abelian group.

9.15 ADDITIVE GROUP OF INTEGERS MODULO *m*

In general, we can define a binary composition denoted by $+_m$, in the set $G = \{0, 1, 2, \ldots, m - 1\}$.

As follows:

for $$a, b \in G$$

$a +_m b$ = remainder obtained by dividing $a + b$ (the ordinary sum of a and b) by m.

$(G, +_m)$ is a commutative group of order m. The group $(G, +_m)$ is called additive group of integers modulo m. The set G.

9.15.1 Multiplicative Group of Integers

consider the set $G_0 = \{1, 2, 3, \ldots, p - 1\}$, where p is a prime.

Let us define a binary operation in G_0 to be denoted by $\cdot p$ (or $\times_p$) and called multiplication modulo p as follows.

For a, $a, b \in G_0$, we define

$a \cdot_p b = r$, where r is the remainder obtained on dividing the ordinary product ab by p.

$(G_0, \cdot_p)$ is a commutative group of order $p - 1$.

9.16 CONGRUENCES

Consider the relation "Congruence modulo m" defined in 9.12. The relation congruence modulo 'm' is an equivalence relation in the set of integers. The operation 'Congruence modulo m' Partitions Z into disjoint equivalence classes called residue classes modulo m or congruence classes modulo m.

If $a \in Z$, then the residue class of a is denoted by $\bar{a}$ or $[\bar{a}]$ where $\bar{a} = [\bar{a}] = \{x : x \in Z$, and $x - a$ is divisible by $m\}$.

$\{0, 1, 2, \ldots, m - 1\}$ is called the set of residue modulo m.

Definition 9.22: Let $m \in N$ and $n \in Z$, and $\bar{r} = \{x : x \in Z, x \equiv r$ (mod m).

Then the set

$Z_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m} - 1\}$ is called the complete set of residue classes modulo m where $\bar{r} = \{\ldots, -2m + r, -m + r, r, m, m + r, 2m + r, \ldots\}$ and $\bar{0}, \bar{1}, \bar{2}, ..., \overline{m} - 1$ are all distinct.

Example: If $m = 6$, then $Z_m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Where

$$\bar{0} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$

$$\bar{1} = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$$

$$\bar{2} = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$$

$$\bar{3} = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$$

$$\bar{4} = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$$

$$\bar{5} = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$$

$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ are all disjoint.

Addition of residue classes we define addition of residue classes denoted by + as $\bar{a} + \bar{b} = \overline{a + b}$ $\forall\ a, b \in Z_m$, where + on R.H.S. is ordinary addition. If r is the remainder when $a + b$ is divided by m then $\overline{a + b} = \bar{a} + \bar{b} = r$.

The set $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m} - 1\}$ is an abelian group of order m with respect to addition of residue classes. If P is a prime, then set of non-zero residue classes modulo p forms a group of order $(p - 1)$, with respect to multiplication of residue classes where $=p = \{\bar{0}, \bar{1}, \bar{2}, ..., \bar{p} - 1\}$

$$= \{\bar{r} : r \in Z, \text{ and } 1 \leq r \leq p - 1\}$$

and $\bar{a} \cdot \bar{b} = \overline{ab}$ for all $a, b \in Z_p$

EXERCISE 9.2

1. Define (*i*) group (*ii*) abelian group.

2. Show that the following algebraic structures are groups.

(*a*) The set of real numbers under multiplication.

(*b*) The set of rational numbers under addition.

(*c*) The set of non-zero real numbers under multiplication.

(*d*) The set of complex numbers under addition.

(*e*) The set of non-zero complex numbers under multiplication.

(*f*) The set R in which $a * b = \dfrac{ab}{2}$ $\forall\ a, b \in R$.

3. Show that the set of all vectors in R^2 is an infinite group with victor addition as the composition.
4. Prove that the set $G = \{a + \sqrt{2}\,b: a, b \in Q\}$ is a group with respect to addition.
5. Show that the set of all victors in R^3 with victor addition as binary composition is an infinite abelian group.
6. Show that the set of non-signed matrices of order n by m (n is fixed) with elements are rational numbers with matrix multiplication as binary composition is a group.
7. Prove that the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

form a multiplicative group
8. On the set of integers Z, we introduce a binary operation * defined as follows. $a * b = a + b + 1$, where + is ordinary addition. Show that $(Z, *)$ is a group.
9. Show that the set $G = \{-1, 1\}$, is a finite abelian group of order 2, under multiplication.
10. Prove that the set {1, 2, 3, 4,5, 6} of order 6 is a finite abelian group of order 6 under multiplication modulo 7.
11. Show that $n * y = x^y$ in a binary operation on the set of natural numbers. *Is* the operation commutative and associative.

9.17 ELEMENTARY PROPERTIES OF GROUPS

Theorem 9.8: If $(G, *)$ is a group, then the identity element in G is unique.

Proof: Let e_1 and e_2 be identity elements in G.

e_1 is the identity element and $e_2 \in G$

$$\Rightarrow e_1 * e_2 = e_2 = e_2 * e \qquad \dots (i)$$

e_2 is the identity and $e_1 \in G$

$$\Rightarrow e_2 * e_1 = e_1 = e_1 * e_2 \qquad \dots (ii)$$

from (*i*) and (*ii*), we get $e_1 = e_2$

Theorem 9.9: The inverse of each element in a group $(G, *)$ is unique.

Proof: Let $a \in G$ and e be the identity element in G.

Let $b \in G$ be an inverse of a in G also let $c \in G$ be an inverse of a in G since b is the inverse of a, we have

$$a * b = b * a = e$$

Also c is an inverse of a in $G \Rightarrow a * c = c * a = e$

Now
$$\begin{aligned} b &= b * e \\ &= b * (a * c) \ (e \text{ is the identity}) \\ &= (b * a) * c \\ &= e * c \text{ (by associative law)} \\ &= c \end{aligned}$$

Note: The identity element is its own inverse.

Theorem 9.10: In a group $(G, \times)$

$$(a^{-1})^{-1} = a \ \forall \ a \in G$$

(a^{-1} is the inverse of a in G)

Proof: G is a group

$\therefore \ a \in G \Rightarrow a^{-1} \in G$ such that

$$a^{-1} * a = e = a * a^{-1}$$

now $a^{-1} \in G \Rightarrow (a^{-1})^{-1} \in G$ such that

$$(a^{-1})\,(a^{-1})^{-1} = e\,(a^{-1})^{-1} * (a^{-1})$$

consider $a^{-1} * a = e$

$$\Rightarrow (a^{-1})^{-1} *(a^{-1} * a) = (a^{-1})^{-1} * e$$
$$\Rightarrow \{(a^{-1})^{-1} * a^{-1}) * a = (a^{-1})^{-1}$$
$$\Rightarrow e * a = (a^{-1})^{-1}$$
$$\Rightarrow a = (a^{-1})^{-1}$$

Therefore $(a^{-1})^{-1} = a \ \forall \ a \in G$

Theorem 9.11: If $(G, *)$ is a group then $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$ (Reversal law).

Proof: Let $a, b \in G$ and e be the identity element in G.

$$a \in G \Rightarrow a^{-1} \in G \text{ such that } a * a^{-1} = a^{-1} * a = e$$

and $b \in G \Rightarrow b^{-1} \in G$ such that $b^{-1} = b^{-1} * b = e$

now $a, b \in G \Rightarrow a{*}b \in G$ and $(ab)^{-1} \in G$

Consider $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ (by associative law)
$= b^{-1} * e * b \ (a^{-1} * a = e)$
$= b^{-1} * b$ (e is the identity)
$= e \ (b^{-1} * b = e)$

and $(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * b^{-1}) * a^{-1}$ (by associative law)
$= a * e * a^{-1}$
$= a * a^{-1}$ (e is the identity)
$= e$

Therefore $(b^{-1} * a^{-1})\,(a * b) = (a * b) * (b^{-1} * a^{-1}) = e$

$\Rightarrow$ $(a * b)^{-1} = b^{-1} * a^{-1} \ \forall \ a, b \in G$ (by the definition of inverse)

Theorem 9.12: Cancellation laws hold good in G, i.e., for all $a, b, \ a, b, c \in G$

$$a * b = a * c \ \Rightarrow \ b = c \text{ (left cancellation law)}$$

$b * a = c * a \Rightarrow b = c$ (right cancellation law)

Proof: $a \in G \Rightarrow a^{-1} \in G$ such that

$a * a^{-1} = a^{-1} * a = e$, where e is the identity element in G.

Consider

$$a * b = a * c$$
$$\Rightarrow a^{-1} * (a * b) = a^{-1} (a * c)$$
$$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c \text{ (by associative law)}$$
$$\Rightarrow e * b = e * c \; (a^{-1} \text{ is the inverse of } a \text{ in } G)$$
$$\Rightarrow b = c \; (e \text{ is the identity element in } G)$$

now

$$b * a = c * a$$
$$\Rightarrow (b * a)\, a^{-1} = (c * a) * a^{-1}$$
$$\Rightarrow b * (a * a^{-1}) = c * (a * a^{-1}) \text{ (by associative law)}$$
$$\Rightarrow b * e = c * e \; (a\, a^{-1} = e)$$
$$\Rightarrow b = c \; (e \text{ is the identity element in } G)$$

Hence cancellation laws hold good in G.

Theorem 9.13: If a and b are any two elements of group $(G, *)$ then the equations. $a * x = b$ and $y * a = b$ have unique solution in G.

Proof: Let $a \in G$, then $a^{-1} \in G$

Such that $a * a^{-1} = a^{-1} * a = e$

Now $a^{-1} \in G, b \in G \Rightarrow a^{-1} * b \in G$ (closure property)

Consider

$$a * x = b$$
$$\Rightarrow a^{-1} * (a * x) = a^{-1} * b$$
$$\Rightarrow (a^{-1} * a) * n = a^{-1} * b$$
$$\Rightarrow e * x = a^{-1} * b$$
$$\Rightarrow x = a^{-1} * b$$

Hence $x = a^{-1} * b$ is a solution in G of the equation $a * x = b$.

Now we shall show that, the solution is unique:

If possible let there be two solutions:

Say $x_1 * x_2$ of $a * x = b$ in G, then

$$a * x_1 = b \text{ and } a * x_2 = b$$
$$\Rightarrow a * x_1 = a * x_2$$
$$\Rightarrow x_1 = x_2 \text{ (by left cancellation law)}$$

Therefore $a * x = b$, has unique solution in G.

Similarly, we can show that
$y * a = b$, has unique solution in G.

9.18 ALTERNATIVE POSTULATES FOR A GROUP

We state the following theorem (without proof). Which helps us to think of the alternative postulates for a group.

Theorem 9.14: If $(G, *)$ is a semi-group such that

$$x * a = b \text{ and } a * y = b$$

have a solution for $a, b \in G$ then $(G, *)$ is a group.

Theorem 9.15: If $(G, *)$ is a finite semi-group

Such that $\forall\ a, b, c \in G$

$$a * b = a * c \Rightarrow b = c$$

and $$b * a = c * a \Rightarrow b = c$$

then $(G, *)$ is a group.

Theorem 9.16: If $(G, *)$ is a semi-group, such that

(*i*) There exists an element $e \in G$, such that

$$a * e = a\ \forall\ a \in G$$

(*ii*) $a \in G \Rightarrow$ There exists an element, $a_1 \in G$ such that

$$a * a_1 = e$$

then $(G, *)$ is a group.

Theorem 9.17: If $(G, *)$ is a finite group of orders n, then for each $a \in G$, there exists a positive integer $m \leq n$ such that $a^m = e$, e being the identity of G.

Proof: Let $a \in G$, then

$$a * a = a^2 \in G$$
$$a^2 * a = a * a * a = a^3 \in G$$
$$a^{n-1} * a = a^n \in G$$

$\therefore\ e, a, a^2, a^3, \ldots, a^n$ are all elements of G.

These elements are $(n + 1)$ in numbers, therefore they cannot all be distinct. If some $a^r = e$ then the theorem is proved. In the other case, we must have

$$a^r = a^s,\ 1 \leq r \leq s \leq n$$

because all the elements are not distinct

now

$$a^r = a^s$$
$$\Rightarrow a^r, a^{-r} = a^s, a^{-r}$$

$$\Rightarrow a^0 = a^{s-r}$$
$$\Rightarrow e = a^{s-r}$$

from our choice of r and

$$1 \leq r \leq s \leq n$$
$$\Rightarrow 1 \leq s - r \leq n.$$

9.19 ORDER OF AN ELEMENT

Definition 9.23: Let $(G, *)$ be a group and $a \in G$, then the least positive integers, n if it exists such that $a^n = e$ is called the order of $a \in G$.

The order of an element $a \in G$ is be denoted by $O\,(a)$.

Example 1: $G = \{1, -1, i, -i\}$, is a group with respect to multiplication 1 is the identity in G.

$$1^1 = 1^2 = 1^3 = \ldots = 1 \Rightarrow O\,(1) = 1$$
$$(-1)^2 = (-1)^4 = (-1)^6 = \ldots = 1 \Rightarrow O\,(-1) = 2$$
$$i^4 = i^8 = i^{12} = \ldots = 1 \Rightarrow O\,(i) = 4$$
$$(-i)^4 = (-i)^8 = \ldots = 1 \Rightarrow O\,(-i) = 4$$

Example 2: $G = \{1, \omega, \omega^2\}$ is a group $w.\,r.$ to multiplication in which we have $O\,(1) = 1$, $O\,(\omega) = 3$, $O\,(\omega^2) = 3$

Example 3: In $\{Q, -\{0\}, x\}$,

The order of 1 is 1 i.e., $O\,(a) = 1$ and $O\,(-1) = 2$

Note: The identity of group has order 1 i.e., $O\,(e) = 1$.

We now prove certain properties of an element of a group.

Theorem 9.18: The order of every element of a finite group is finite.

Proof: Let $a \in G$, then there exists a positive integer $m \leq n$, such that

$$a^m = e$$

This proves that, the order of a, cannot be more than; since m is finite, $O\,(a)$ is finite.

Theorem 9.19: If $(G, *)$, $O\,(a) = n$, and m is a positive integer then $a^m = e$, if and only if m is multiple of n, i.e., $m = nq$ for some $q \in N$.

Proof: Since $O\,(a) = n$

There cannot be another positive integer $x < n$ such that $a^x = e$

Thus, if $a^m = e$, then $m = n$

Let us assume

$$a^m = e$$

we can find integers, q and r such that

$$m = nq + r, 0 \leq r < n$$

we first prove that

$$\begin{aligned} & a^m = e \Rightarrow m = nq,\ q \in N \\ & \Rightarrow e - t \Rightarrow e = a^{nq} * a^r \ (\therefore\ a^m = e) \\ & \Rightarrow e = (a^n)^q * a^r \\ & \Rightarrow e = e * a^2 \\ & \Rightarrow e = a^r \\ & \Rightarrow r = 0\ (\ \therefore\ O\ (a) = n \text{ and } 0 \leq r \leq n) \end{aligned}$$

Thus, we get $m = nq$

Now, we prove that

$$m = nq \Rightarrow a^m = e$$

Consider

$$\begin{aligned} & m = nq \Rightarrow a^m = a^n\ q \\ & \Rightarrow a^m = (a^n)^q \\ & \Rightarrow a^m = e^q \\ & \Rightarrow a^m = e \end{aligned}$$

This completes the proof.

Theorem 9.20: If $(G, *)$ is a group and then

$$O\ (a^p) = O\ (a),\ \forall\ a \in G \text{ and } \forall\ p \in Z$$

i.e., the order of any integral power of any element of an group is less then or equal to the order of the element.

Proof: Let $O\ (a) = m$ and $O\ (a^p) = n$, where P is an integers

Since $O\ (a) = m$, we have $a^m = e$ and $(a^p)^m = a^{pm} = a^{mp} = (a^m)^p = e$

$$\begin{aligned} & \Rightarrow O\ (a^p) \leq m \\ & \Rightarrow O\ (a^p) \leq O\ (a) \end{aligned}$$

This completes the proof of the theorem.

Theorem 9.21: If $(G, *)$ is a group then $O\ (a) = O\ (a^{-1})$

i.e., the order of an element of a group is always equal to the order of its inverse.

Proof: By previous theorem

$$O\ (a^{-1}) \leq O\ (a) \qquad \ldots (1)$$

Also

$$a = (a^{-1})^{-1}$$

again by same property

$$O\ (a) \leq O\ (a^{-1}) \qquad \ldots (2)$$

From (1) and (2)

$$O\ (a) = O\ (a^{-1}).$$

9.20 SUB-GROUP

We now introduce the concept of a sub-group.

Definition 9.24: Let $(G, *)$ be a group and H, be a non-empty subset of G. If $(H, *)$ is itself is a group, then $(H, *)$ is called sub-group of $(G, *)$.

Example 1: Let $a = \{1, -1, i, -i\}$ and $H = \{1, -1\}$

G and H are groups with respect to the binary operation, multiplication.

H is a subset of G, therefore (H, X) is a sub-group (G, X).

Example 2: Consider $(Z_6, +_6)$, the group of integers modulo 6.

$H = \{0, 2, 4\}$ is a subset of Z_6 and $\{H, +_6\}$ is a group.

$\therefore$ $\{H, +_6\}$ is a sub-group.

Theorem 9.22: If $(G, *)$ is a group and $H \leq G$, then $(H, *)$ is a sub-group of $(G, *)$ if and only if

(*i*) $a, b \in H \Rightarrow a * b \in H$;

(*ii*) $a \in H \Rightarrow a^{-1} \in H$

Proof: If $(H, *)$ is a sub-group of $(G, *)$, then conditions (*i*) and (*ii*) are obviously satisfied.

We, therefore prove now that if conditions (*i*) and (*ii*) are satisfied then $(H, *)$ is a sub-group of $(G, *)$.

To prove that $(H, *)$ is a sub-group of $(G, *)$ all that we are required to prove is : $*$ is associative in H and identity $e \in H$.

That $*$ is associative in H follows from the fact that $*$ is associative in G.

Also,

$$a \in H \Rightarrow a^{-1} \in H \text{ by } (ii)$$

and
$$e \in H \text{ and } a^{-1} \in H \Rightarrow a * a^{-1} = e \in H \text{ by } (i)$$

Hence, H is a sub-group of G.

Theorem 9.23: Let $(G, *)$ be a group and $\varnothing \neq H \subseteq G$.

Then $(H, *)$ is a sub-group of $(G, *)$ if and only if $a, b \in H \Rightarrow a*b^{-1} \in H$.

Proof: If $(H, *)$ is a sub-group and $a, b \in H$ then $b^{-1} \in H$ and so $a*b^{-1} \in H$ by closure axioms.

Conversely, suppose H is a non-empty subset of G which contains the element $a*b^{-1} \in H$, whenever $a, b \in H$ since $a \in H$.

Then $a, a \in H \Rightarrow a * a^{-1} = e \in H$ by the hypothesis. Again $e, a \in H \Rightarrow e * a^{-1} = a^{-1} \in H$.

Finally, $a, b \in H \Rightarrow a * b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} = a*b \in H$.

The set H "inherits" the associative law as a subject of G, so that all the group axioms are satisfied, and $(H, *)$ is therefore a sub-group of $(G, *)$.

Theorem 9.24: Let $(G, *)$ be a finite group and $\varnothing \neq H \subseteq G$. Then $(H, *)$ is a sub-group $(G, *)$ if and only if $a, b \in H \Rightarrow a * b \in H$.

Proof: If (H, *) is a sub-group and $a, b \in H$ then $a * b \in H$ by closure axiom.

Conversely, suppose H is a non-empty subset of G and contains the element $a * b \in H$.

Whenever $a = b \in H$.

If $a \in H$, $a^2, a^3, a^4, \ldots$ all belong to H. Since H is finite, the elements $a^2, a^3, a^4, \ldots$ cannot be all different that is only finite numbers of elements can be different. Therefore, some elements repeat. Let

$$a^i = a^i,\ i > j > 0$$

Now

$$\begin{aligned} a^i = a^j &\Rightarrow a^i * a^{-j} = a^j * a^{-j} \\ &\Rightarrow a^{i-j} = e \\ &\Rightarrow a^{i-j} * a^{-1} = e * a^{-1} \\ &\Rightarrow a^{i-j-1} = a^{-1} \end{aligned}$$

But $i - j - 1 \geq 0$. Hence $a^{i-j-1} = a^{-1} \in H$. Here $i > j \Rightarrow i - j > 0$ and $a^{i-j} = e \in H$. The set "H" "inherits" the associative law as a subset of G, so that all group axioms are satisfied and (H, *) is a sub-group of (G, *).

Theorem 9.25: If (H_1, *) and (H_2, *) are both sub-groups of the group (G, *), then $(H_1 \cap H_2, *)$ is also a sub-group.

Proof: The set $H, \cap H_2 \neq \varnothing$, since $e \in H_1, \cap H_2$. Suppose that $a, b \in H_1 \cap H_2$, then $a, b \in H_1$ and $a, b \in H_2$, since (H_1, *) and (H_2, *) are sub-groups.

$$a, b \in H_1 \Rightarrow a * b^{-1} \in H_1$$

and

$$a, b \in H_2 \Rightarrow a * b^{-1} \in H_2$$

That is $a * b^{-1} \in H_1 \cap H_2$ which implies $(H_1 \cap H_2)$ is a sub-group of (G, *).

Theorem 9.26: If (G, *) is a group and (H, *) is a sub-group of (G, *) and (K, *) is a sub-group of (G, *) then (HK, *) is a sub-group of (G, *) if and only if $HK = KH$

Where

$$HK = \{h * k \,/\, h \in H, k \in K\} \text{ and } KH = \{k * h \,/\, h \in H, k \in K\}$$

Proof: Left as an exercise to the student.

Example 3: ({0, 2, 4} + 1) is a sub-group of (6, +) because, if H = {0, 2, 4} then

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 2 &= 2 \\ 0 + 4 &= 4 \\ 2 + 2 &= 4 \\ 2 + 4 &= 0 \\ 4 + 4 &= 2 \end{aligned}$$

i.e., $a, b \in H \Rightarrow a + b \in H$.

Example 4: Let $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ and let

$$H_1 = \{0, \pm 2, \pm 4, \pm 6, ...\}$$

and $$H_2 = \{0, \pm 3, \pm 6, \pm 9, ...\}$$

$$H_1 \cap H_2 = \{0, \pm 6, \pm 12, ...\}$$

Here $(H_1, +)$ and $(H_2, +)$ are sub-groups of $(Z_1, +)$ and $(H_1 \cap H_2, +)$ is also a sub-group of $(Z_1, +)$ ….

But $(H_1 \cup H_2, +)$ is not a sub-group since

$$H_1 \cup H_2 = \{0, \pm 2, \pm 3, \pm 4, ...\}$$

and $$2, 3 \in H_1 \cup H_2 \text{ but } 2 + 3 = 5 \notin H_1 \cup H_2$$

Hence $H_1 \cup H_2$ is not closed under +.

9.21 CENTRE OF A GROUP

Definition 9.25: Let $(a, *)$ be a group, then centre of the group G is the set of those elements of G which commute with every element of G. The centre of G is denoted by $Z(G)$.

Thus $$Z(G) = \{a \in G / a * x = x * a \ \forall \ x \in G\}$$

9.22 COSETS

Let $(H, *)$ be a sub-group $(G, *)$ and $a \in G$

Then the sub-set:

$$a * H = \{a * h : h \in H\}$$

is called a left coset of H in G, and the subset

$$H * G = \{h * a : h \in H\}$$

is called a right coset of H in G.

Note: In general $a * H \neq H * a$, however if G is abelian then

$$a * H = H * a \ \forall \ a \in G$$

Example 1: Let $H = \{1, -1\}$ and $G = \{1, -1, i, -i\}$

there $(H, *)$ is a sub-group $(G, *)$

The various left cosets and right cosets of H in G are given below:

Left cosets of H in G	Right cosets of H in G
$1 \times H = \{1, -1\} = H$	$H \times 1 = \{1, -1\} = H$
$-1 \times H = \{-1, 1\} = H$	$H \times -1 = \{-1, 1\} = H$
$i \times H = \{i, -i\}$	$H \times i = \{i, -i\}$
$-i \times H = \{-i, i\}$	$H \times -i = \{-i, i\}$

There are only two distinct left cosets of H in G and two distinct right cosets of H in G.

Also we have

$$\begin{aligned} G &= H \cup H \times i \\ &= H \cup i \times H \\ &= H \cup H \times (-i) \\ &= H \cup (-i) \times H \end{aligned}$$

If e is the identity element of G, then

$$e * H = \{e * h: L \in H\} = \{h: h \in H\} = H$$

Similarly, $H * e = H$

Moreover, since $e \in H$, we have

$$a = a * e \in a * H \quad \text{and} \quad a = e * a \in a * H$$

i.e., every element of G belongs to some left (right) coset of H in G.

Example 2: Consider the group $(Z, +)$

Let $$H_n = \{0, \pm n, \pm 2n, \pm 3n, ...\}$$

then the left cosets of H in Z are

$$H_n, 1 + H_n, 2 + H_n, 3 + H_n, ..., (n-1) + H_n$$

and $$Z = H_n \cup 1 + H_n + 2 + H_n + ... + (n-1) + H_n$$

Theorem 9.27: If $(H, *)$ is a sub-group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Proof: Let $a * H = H$

Since $e \in H$ then $a = a * e \in a * H$

Hence $a \in H$

Conversely

Let $a \in H$

then $a * H \subseteq H$

$(H, *)$ is a sub-group.

$\therefore$ $$a \in H, h \in H \Rightarrow a^{-1} * h \in H.$$

Now $h \in H$

$$\Rightarrow h = a * (a^{-1} * h) \in a * H$$

$\therefore$ $$\begin{aligned} &h \in H \Rightarrow h \in a * H \\ &\Rightarrow H \subseteq a * H \end{aligned}$$

Hence $a * H = H$

We now state the following theorem without proof:

Theorem 9.28: If $(H, *)$ is a sub-group of $(G, *)$, then $a * H = b * H$ if and only if $a^{-1} * b \in H$.

Theorem 9.29: If $(H, *)$ is a sub-group of $(G, *)$, then any two left cosets of H in a are either identical or disjoint.

Proof: Let $a * H$ and $b * H$ be two left cosets of H in G. If $a * H$ and $b * H$ have no common element, then $a * H$ and $b * H$ are disjoint.

If $\qquad a * H \cap b * H \neq \varnothing$

Let $\qquad c \in a * H \cap b * H$

Then $c = a * h_1$ and $c = a * h_2$

For some $h_1, h_2 \in H$

It follows that

$$a * h_1 = b * h_2$$
$$\Rightarrow a^{-1} * b = h_1 * h_2^{-1}$$
$$\Rightarrow a^{-1} * b \in H \; (\therefore h_1 * h_2^{-1} \in H)$$
$$\Rightarrow a * H = b * H.$$

Theorem 9.30: There exists a one-to-one correspondence between the elements of sub-group H and those of any coset of H in G.

Proof: Define a mapping

$$f\colon H \to a * H$$

by $f(h) = a * h$ for all $h \in H$

Let $h_1, h_2 \in H$ such that

$$f(h_1) = f(h_2)$$

now

$$f(h_1) = f(h_2)$$
$$\Rightarrow a * h_1 = a * h_2$$
$$\Rightarrow h_1 = h_2 \text{ (by left cancellation law)}$$

$\therefore f$ is one-one.

Every element of $a * H$ is of the form $a * H$ for same $h \in H$.

$\therefore f$ is onto.

This completes the proof of the theorem.

Note: If $(G, *)$ in a finite group, and $(H, *)$ is a sub-group of G, then any two left cosets of H in G have the same number of elements.

Theorem 9.31: If $a * H$ and $b * H$ are two distinct left cosets of H in G, then exists a one-to-one correspondence between $a * H$ and $b * H$.

Proof: Consider the mapping

$$f\colon a * H \to b * H$$

defined by

$$f(a * h) = b * h \text{ where } h \in H.$$

The mapping *f* is one-one, since

$$f(a * h_1) = f(\ a * h_2) \text{ where } h_1, h_2 \in H$$
$$\Rightarrow b * h_1 = b * h_2$$
$$\Rightarrow h_1 = h_2 \text{ (by left cancellation law).}$$

Thus *f* is one-one

f is onto mapping, since

$$b * h \in b * H \text{ is the } f\text{-image of}$$
$$a * h \in a * H$$

Thus *f* as defined above is a objective mapping from $a * H$ to $b * H$.

This completes the proof of the theorem.

Lagrange's Theorem: The theorem stated above indicate that each element of the group *G* belongs to one and only one left coset of *H*. Thus *G* can be partitioned by *G* into disjoint sets each of which has exactly as many elements as *H*. When the theorems are interpreted in the context of finite groups only we obtain the following theorem known as Lagrange's theorem.

Theorem 9.32: (Lagrange's Theorem)

The order of any sub-group of a finite group divides the order of the group.

Proof: Let (*G*, *) we a finite group of order *h*, and (*H*, *) be a sub-group of *G* of order *m*.

We can decompose the set *G* into a union of a finite number of distinct left cosets of *H* say *K*.

Let $a_1 H, a_2 H, \ldots a_k H$ denote the *k* distinct left cosets of *H* in *G* such that

$$G = a_1 * H \cup a_2 * H \cup a_3 * H \cup \ldots \cup a_k * H.$$

Where all the *K* left coset appearing on the right hand side are disjoint.

Therefore,

$$O(G) = O(a_1 * H) + O(a_2 * H) + \ldots O(q_k * H)$$
$$\Rightarrow n = m + m + \ldots k \text{ terms}$$
$$\Rightarrow n = km$$
$$\Rightarrow m/n$$
$$\Rightarrow O(H) / O(G).$$

This completes the proof of the theorem.

9.23 INDEX OF A SUB-GROUP

Definition 9.26: The number of distinct left (or right) cosets of *H* in *G* is called index of *H* in *G*.

The index of *H* in *G* is denoted by $I_G(H)$. Lagrange's theorem proved above can also be stated as follows:

If (*G*, *) is a finite group and (*H*, *) is a sub-group of *G*, then

$$I_G(H) = \frac{O(G)}{O(H)}$$

Lagrange's theorem is of fundamental importance and is used to prove many other important results.

Theorem 9.33: The order of every element of a finite group is a divisor of the order of the group.

Proof: Let $(G, *)$ be a finite group and $a \in G$ and let $O(a) = m$

Consider the set

$$H = \{a, a^2, a^3, \ldots a^m = e\}$$

Obviously $(H, +)$ is a sub-group of $(G, *)$ and $O(H) = m$ Lagrange's theorem ensures that

$$O(H) / O(G) \Rightarrow m / O(G)$$
$$\Rightarrow O(a) / O(G)$$

This completes the proof of the theorem,

We know that if H and K are two sub-groups of a group G, then HK is a sub-group of G if and only if $H * K = K * H$.

If H and K are finite sub-groups of a group G, then we can find the $O(H * K)$ by making use of following theorem.

Theorem 9.34: Let $(G, *)$ be a group $(H, *)$ and $(K, *)$ be two finite sub-groups of G such that $H * K = K * H$ then

$$O(H * K) = \frac{O(H) * O(K)}{O(H \cap K)}.$$

EXERCISE 9.3

1. Show that the system $(\{1, -1\}, \times)$ is an abelian group.

2. Show that the set of complex numbers is a group under multiplication is a group.

3. Show that the set of even integers is a group under addition.

4. If Q denotes the set of rational numbers, then show that $Q - \{1\}$ is a group with respect to the operation $*$ defined by $a * b = a + b + ab$.

5. Show that the set $G = \{6^n : n \in Z\}$ is a group with respect to multiplication.

6. Show that the pair $\{(0, 4, 8, 12), + 16\}$ is a group.

7. Prove that a group $(G, *)$ is commutative if and only if

$$(a * b)^{-1} = a^{-1} * b^{-1} \ \forall \ a, b \in G.$$

8. Let $(G, *)$ be a group since that $(a * b^2) = a^2 + b^2$ for every $a, b \in G.$ Prove that G is commutative.

9. Given $a^2 = e$ for every element a of the group $(G, *)$ show that G is commutative.

10. If $(G, *)$ is a group of even order prove that it has an element $a \neq e$ satisfying $a^2 = e$.

11. In a group $(Z, +)$ show that every element except o is of infinite order.

12. In any element, prove that the identity element is the only element whose order is 1.

13. Find the order of all elements of a group $(Z_4, +_4)$.

14. Give can example to show that the union of two groups may not be a sub-group.

15. If K is a sub-group of H and H is a sub-group of G, show that K is a sub-group of G.

16. If G is a group and $z\,a = 0\ \forall\ a \in G,$ then show that G is abelian.

9.24 ISOMORPHISM

Let $(G, *)$ and (G', Δ) be two groups.

A objective mapping

$$f\colon G \to G'$$

satisfying

$$f(a * b) = f(a)\ \Delta\ f(b),\ \forall\ a, b \in G$$

is called an isomorphism of G to G'.

If there exists an isomorphism between two groups $(G, *)$ and (G', Δ) then G and G' are said to isomorphic to each other.

If $(G, *)$ is isomorphic to $(G', \Delta),$ we use the symbol

$$(G, *) \cong (G', \Delta)$$

for the statement G is isomorphic to G'.

Example 1: Consider the group $(R, +)$ and $(R^+, \times)$ where R^+ denoted the set of positive real numbers. Consider the mapping.

$$f_a\colon R \to R^+,\ a \in R^+$$

defined by

$$f_a\,(x) = a^n$$

the mapping f_a is structure preserving:
we have

$$f_a\,(x + y) = a^{x+y} = a^x \times a^y$$

$\Rightarrow f_a$ is structure preserving

Also
$$\begin{aligned} f_a\,(x) &= f_a\,(y) \\ \Rightarrow a^x &= a^y \\ \Rightarrow a^{x-y} &= 1 \\ \Rightarrow x - y &= 0 \\ \Rightarrow x &= y \end{aligned}$$
$\Rightarrow f_a$ is one-one.

From the definition

$y \in R^+ \Rightarrow$ There exists a real number
x such that $y = a^x$

$$\therefore \quad y \in R^+ \Rightarrow y = a^x \text{ for some } x \in k.$$
$$\Rightarrow y = f_a(x)$$
$$\Rightarrow f_a \text{ is onto}$$

$\therefore$ Thus $(R, +) \cong (R^+, x)$

Example 2: The groups $(Z, +)$ and $(nZ, +)$, $n \in Z$ are isomorphic to each other.

9.25 PROPERTIES OF ISOMORPHISM

We now that some properties of isomorphic groups. Let $(G, *)$ and (G', Δ) be two groups such that $(G, *) \cong (G', \Delta)$. Also let e, e' be the identity elements of G and G' respectively then.

(*i*) $f(e) = e'$

(*ii*) $f(a^{-1}) = [f(a)]^{-1} \ \forall \ a \in G$

(*iii*) $O(a) = O[f(a)] \ \forall \ a \in G$

(*iv*) $f^{-1}: G' \to G$ is an isomorphism.

(*v*) The composite of two isomorphisms is an isomorphism.

We shall prove the following theorem, by introducing a relation in the set of all groups.

Theorem 9.35: The relation '$\cong$' in the set of all groups is an equivalence relation.

Proof: (*a*) $\cong$ is reflexive

If $(G, *)$ is a group then

$$(G, *) \cong (G', *)$$

since the identity mapping

$$I_G : G \to G'$$

is an isomorphism from $(G, *)$ to $(G', *)$

(*b*) $\cong$ is symmetric

Let $(G, *) \cong (G', \Delta)$

Then $(G', \Delta) \cong (G, *)$

Therefore $\cong$ is symmetric

(*c*) $\cong$ is transitive

Let $(G, *) \cong (G', \Delta)$ and $(G', \Delta) \cong (G'', \square)$

Then $(G, *) \cong (G'', \square)$

Therefore $\cong$ is transitive.

$\therefore$ $\cong$ is reflexive, symmetric and transitive therefore $\cong$ is an equivalence relation in the set of all groups.

9.26 CYCLIC GROUPS

Let $(G, *)$ be a group. If there exists an element $a \in G$ such that

$G = \{a^m: m \text{ is an integer}\}$

i.e., $(G, *)$ is cyclic, if there exists an element $a \in G$ such that every element of G is a power of a and a is called the generator of the cyclic group.

If a is a generator of $(G, *)$, then we write $G = <a>$.

Note: If $(G, +)$ is a cyclic group then each element of G can be expressed in the form $n\,a$ where n is an integer.

Example 1: Let Z denote the set of integers $(Z, +)$ is an infinite cyclic group 1 and -1 are the generators of the group $(Z, +)$.

Example 2: $G = \{1, -1, i, -i\}$is a group with respect to the binary operation '×'. $(G, \times)$ is a cyclic group.

i is a generator of G.

Since
$$(i)^4 = 1$$
$$(i)^3 = -i$$
$$i^2 = -i$$
$$(i^0)^1 = i$$

and
$$G = \{i^4, i^2, i, i^3\}$$
$$= < i >$$

Similarly $(-i)$ is a generator

$i, -i$ are the only generators of G.

If $(G, *)$ is an infinite group generated by an element a, then we can write,

$$G = \{\ldots a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3,\ldots\}.$$

And if $(G, *)$ is a finite cyclic group generated by a, then we can write,

$$G = \{a, a^2, a^3, \ldots, a^n = e\}$$

If $(G, *)$ is a finite cyclic group of order n then

$$a^i * a^j = a^{i+j} \text{ if } i + j < n$$
$$= a^0 \text{ if } i + j = 0$$
$$= a^{i+j-n} \text{ if } i + j > n$$

where a is the generator of G.

We now state and prove the following theorems:

Theorem 9.36: Every cyclic group is abelian

Proof: Let $(G, *)$ be a cyclic group

Generated by a

$$x, y \in G$$

$\Rightarrow x = a^m$ and $y = a^n$ for some integers

m and n

$$\begin{aligned} x * y &= a^m * a^n \\ &= a^{m+n} \\ &= a^{n+m} \\ &= a^n * a^m \\ &= y * x \end{aligned}$$

This completes the proof of the theorem.

Note: The converse of the theorem may not hold.

Theorem 9.37: Every group of prime order is cyclic.

Proof: Let $O(G) = p$ where p is a prime number and

let $$a \neq e \in G$$

consider the sub-group of G, generated by a

Let $H = <a>$

$$\Rightarrow O(H) > 1$$

H is a sub-group of G

By Lagrange's theorem

$$\begin{aligned} & O(H) / O(G) \Rightarrow O(H) / p \\ & \Rightarrow O(H) = 1 \text{ or } p \\ & \Rightarrow O(H) = p \text{ since } O(H) \neq 1 \\ & O(H) = O(G) \end{aligned}$$

But H is cyclic $\Rightarrow$ G is cyclic

Hence the theorem.

Theorem 9.38: Every infinite cyclic group is isomorphic to $(Z, +)$.

Proof: Let $(G, *)$ be an infinite cyclic group generator by $\varnothing$.

Define a mapping

$$\varnothing : Z \to G$$

by the rule

$$\varnothing(x) = a^x, \ n \in Z$$

$\varnothing$ is one-one, since

$$a^x = a^y \Rightarrow x = y$$

The mapping $\varnothing$ is obviously onto.

Also, we have

$$\begin{aligned} \varnothing(x + y) &= a^{x+y} \\ &= a^x * a^y \\ &= \varnothing(x) * \varnothing(y) \end{aligned}$$

$\Rightarrow \varnothing$ is structure preserving

$\therefore \varnothing$ is an isomorphism

$$\varnothing\ (G, *) \cong (I, +).$$

Theorem 9.39: Every finite cyclic group of order n is isomorphic to $(Z_n, +)$. We leave the proof to the reader and state the following theorem without proof.

"Every proper sub-group of an infinite cyclic group is isomorphic to the group itself."

Theorem 9.40: Every proper sub-group of finite cyclic group is a finite cyclic group.

Theorem 9.41: The only groups which do not possess proper sub-group are the prime order finite sub-groups.

Example 3: $(G, *)$ is a group order 60, find all the sub-groups of G.

Solution: We can write

$$60 = 1 \times 2 \times 2 \times 3 \times 5$$
$$= 1 \times 2^2 \times 3 \times 5$$

Therefore, the factors of 60 are:

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$$

Let a be a generator of $(G, *)$ then the sub-groups of $(G, *)$ are

$$\{e\}, <a>, <a^2>, <a^3>, <a^4>, <a^5>, <a^6>, <a^{10}>, <a^{12}>, <a^{15}>, <a^{20}>, <a^{30}>.$$

EXERCISE 9.4

1. Show that every group of order 2 is isomorphic to every other group of order 2.
2. Show that every group of order 3 is isomorphic to every other group of order 3.
3. Show that $(I, +)$ is isomorphic to $\{a^m : a \in Z\}, +_5 \;\; m \in Z$ is fixed.
4. Let $G = Z_6$, then show that $O(\bar{3}) = 2$.
5. Let $(G, *)$ be an infinite cyclic group then prove that G has exactly the generators.
6. If $G = <a>$ is cyclic group of order n then show that $O(a) = n$.
7. Let G be a group, H be a sub-group of G such that $[G: H] = 2$ show that every left coset of H in G is also.
8. Show that any two cyclic groups of the same order are isomorphic.
9. Prove that any non-cyclic group of order 4 is isomorphic to Klein 4 – groups.
10. If $(G, *)$ is a group of order 4, then show that G is abelian.
11. Show that the additive group Z_4 is isomorphic to the multiplicative group of non-zero elements of Z_5.
12. Find all sub-groups of a cyclic group of orders 10 and 12.
13. Let $(Z_{12}, +_{12})$ be the group of integers modulo 12 then show that the subset generated by 3.

$$<3> = \{3n\ (\text{mod}_{12}) = n \in Z\}$$
$$= \{0, 3, 6, 9\}.$$

14. Consider ($G_1 + 1_5$) the group of integers modulo 15 and the sub-group $H = \{0, 3, 6, 9, 12\}$ of G. Find all left cosets of H in G.

9.27 NORMAL SUB-GROUPS

Definition 9.27: A sub-group (H, *) of (G, *) is called a normal sub-group of G if for all $h \in H,\ g \in G$ and $ghg^{-1} \in H$.

If H is normal in G then we write $H \not\subset G$.

Example 1: Let (G, *) be a group, then ({e}, *) is a normal sub-group in G. It is called the trivial normal sub-group.

Example 2: (G, *) is normal in (G, *). It is called the improper normal sub-graph of G.

9.27.1 Simple Group

Definition 9.28: A group (G, *) is called simple group if its only normal sub-groups are G and $\{e\}$.

Example 1: A group of prime order has no proper sub-groups.

Therefore, every group of prime order is simple.

We now give an equivalent definition for the sub-group to be normal.

Definition 9.29: A sub-group (H, *) of a group (G, *) is said to be normal sub-group of (G, *) is for every $s \in G,\ ghg^{-1} \subseteq H.$

Theorem 9.42: Every sub-group of an abelian group is normal sub-group.

Proof: Let (G, *) be an abelian group and (H, *) be a sub-group of G.

Now $s \in G, h \in H$

$$\begin{aligned} \Rightarrow g * h * g^{-1} &= h * g * g^{-1} \ \therefore \ (G \text{ is abelian and } H \leq G) \\ &= h * e \\ &= h \end{aligned}$$

$$\therefore \qquad g * h * g^{-1} = h \in H \ \forall \ g \in G, h \in H$$

(H, *) is normal in G.

Theorem 9.43: A sub-group (H, *) is normal in (G, *), if and only if $gh = Hg$ for each $g \in G$.

Proof: Suppose (H, *) is normal in (G, *)

Therefore, each $g \in G,\ g * h * g^{-1} \subseteq H$ i.e., $g\,H \subseteq Hg$.

By replacing g by g^{-1} we have $g^{-1} * H$

$$\begin{aligned} g * (g^{-1} * H) * gH &= Hg, \ \forall g \in G \\ (g * g^{-1}) * H * g &\subseteq g * H * (g^{-1} * g) \\ \Rightarrow e * H * g &\subseteq g * H * e \\ \Rightarrow H * g &\subseteq g * H \end{aligned}$$

Thus $Hg = gh$

Conversely assume that $gH = Hg, \ \forall g \in G$

Then $gh\, g^{-1} = H \ \forall \ g \in G$

Showing that $(H, *)$ is normal in $(G, *)$.

Example 2: Show that every sub-group of an abelian group is normal.

Solution: Let $(G, *)$ be an abelian group and $(H, *)$ be a sub-group of G.

Let g be any element of G and $h \in H$

Then we have

$$\begin{aligned} g * h * g^{-1} &= g * g^{-1} * h \\ &= e * h \\ &= h \in H \end{aligned}$$

$\therefore$ Hence, H is normal in G.

9.27.2 Quotient Group

Let $(H, *)$ be a normal sub-group of a group $(G, *)$. The set of all cosets of H in G is known as the quotient G/H;

$$G/H = \{a * H\colon \ a \in G\}$$

Here $a * H = H * a \quad \forall \ a \in G$

Now $(a * H) * (b * H)$

$$\begin{aligned} &= (a * b * H) * H \\ &= ((a * b) * H) * H \\ &= (a * b) * H * H \\ &= (a * b) * H. \end{aligned}$$

i.e., product of two left cosets of H in G is again a left coset in G. Similarly, we can show that, the product of two right cosets is again a right coset in G.

Theorem 9.44: If $(H, *)$ is a normal sub-group of the group $(G, *)$, then the system $(G/H, *)$, forms a group, known as quotient group of G be H (or factor group).

Proof: We observe the following in G/H.

(*i*) The operation $*$ is associative in G/H for $\{(a * H) * (b * H)\} * (c * H)$

$$\begin{aligned} &= [(a * b) * H) (c * H) \\ &= ((a * b) * c) * H \\ &= a * (b * c) * H \\ &= (a * H) * (b * c) * H \\ &= (a * H) * \{(b * H) * (c * H)\} \end{aligned}$$

(*ii*) G/H has an identity element $H = e * H$ for $*$.

For $(a * H) * (e * H) = (a * e) * H = a * H$

and $(e * H) * (a * H) = (e * a) * H = a * H$

(*iii*) For each $a * H$ there exists $a^{-1} * 1 +$ such that

$$\begin{aligned}(a * H) * (a^{-1} * H) &= (a * a^{-1}) * H \\ &= e * H \\ &= (a^{-1} * a) * H \\ &= (a^{-1} * H) * (a * H)\end{aligned}$$

$\therefore$ $a^{-1} * H$ is the inverse of $a * H$.

Corollary: If $(G, *)$ is a finite group and $(H, *)$ is a normal sub-group of $(G, *)$, then

$$O\,(G/H) = O\,(G)/O\,(H)$$

Example: If $H_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

Then $(H_3, +)$ is a normal sub-group of $(Z, +)$ of all integers. The cosets of H in Z are

$$\begin{aligned}H_3 &= \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} \\ 1 + H_3 &= \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} \\ 2 + H_3 &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}\end{aligned}$$

$\therefore$ $G/H = \{H_3, 1 + H_3, 2 + H_3,\}$

Now

Table 9.6

$+$	H_3	$1 + H_3$	$2 + H_3$
H_3	H_3	$1 + H_3$	$2 + H_3$
$1 + H_3$	H_3	$2 + H_3$	H_3
$2 + H_3$	$2 + H_3$	H_3	$1 + H_3$

It is clear from the Table 9.6, that $(Z/H_3, +)$ is a group.

9.28 PERMUTATION GROUPS

A permutation is a one-one mapping of a non-empty set onto itself.

When a set S is a finite, with n elements in it, we speaking a permutation of n symbols. It is not necessary to limit our discussion with same definitions.

9.28.1 Equal Permutations

Let S be a non-empty set. The permutation f and G defined on S, are said to be equal if $f(a) = g(a)$ for all $a \in S$.

Example 1: Let $S = \{1, 2, 3, 4\}$

and let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ $g = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

we have $f(1) = g(1) = 3$

$$f(2) = g(2) = 1$$
$$f(3) = g(3) = 2$$
$$f(4) = g(4) = 4$$

i.e., $f(a) = g(a)\ \forall\ a \in S$, therefore

$$f = g$$

Let $S = (a_1, a_2, \ldots, a_n)$ be a finite set. The number of permutations on S contains is $n!$. The set of all permutations on S is denoted by S_n. Where $|S_n| = n!$ If $f \in S_n$ then f is of the form

$$f = \{(a, f(a), (a_2), f(a_2))\}, \ldots, (a_n, f(a_n))\}$$

It can also be written as

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \ldots & f(a_n) \end{pmatrix}$$

the images $f(a_1), f(a_2), \ldots\ , f(a_n)$ are the elements of S arranged in some order. The order of symbols in the first row of a permutation is immaterial but columns should not be affected and every permutation of S_n may be written in $n!$ ways.

Example 2: Let $S = \{1, 2, 3\}$ and $f = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}$

We can write
$$f = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix} = \begin{pmatrix} 2\,3\,1 \\ 3\,1\,2 \end{pmatrix} = \begin{pmatrix} 3\,1\,2 \\ 1\,2\,3 \end{pmatrix}$$

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

Hence, there are $3! = 6$ ways of writing f.

9.28.2 Identity Permutation

Let S be a finite non-empty set. An identity permutation on S denoted by I is defined $I(a) = a$ for all $a \in S$.

Example 1: Let $S = \{a_1, a_2, \ldots, a_n\}$

Then $I = \begin{pmatrix} a_1\ a_2\ \ldots\ a_n \\ a_1\ a_2\ \ldots\ a_n \end{pmatrix}$ is the identity permutation on S.

Example 2: Let $S = \{1, 2, 3, 4\}$, then

$f = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,2\,3\,4 \end{pmatrix}$ is the identity permutation on S.

9.28.3 Product of Permutations (or Composition of Permutations)

Let $S = (a_1, a_2, \ldots, a_n)$, and let

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{pmatrix} \; g = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \ldots & g(a_n) \end{pmatrix}$$

be two arbitrary on S. We can find the composite of f and g as follows:

$$fog = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \ldots & f(a_n) \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \ldots & g(a_n) \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(g(a_1)) & f(g(a_2)) & \ldots & f(g(a_n)) \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ g(a_1) & g(a_2) & \ldots & g(a_n) \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(g(a_1)) & f(g(a_2)) & \ldots & f(g(a_n)) \end{pmatrix}$$

Clearly fog is a permutation and $fog \in S_n$.

Note: In general $fog \neq gof$

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

and $$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \; g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

be two permutations on S, we complete fog as follows:

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

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

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

9.28.4 Inverse of a Permutation

If f is a permutation on $S = (a_1, a_2, \ldots, a_n)$ such that

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

then there exists a permutation called the inverse f, denoted f^{-1} such that $fof^{-1} = f^{-1}of = I$ (the identity permutation on S)

where $$f^{-1} = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

Theorem 9.45: If S a set of n symbols, then the set S_n of all permutations on S in a group with respect to the operation product of two permutations.

Proof: We have already seen that the product (composite) of two permutations on n symbols is again a permutation. The product of permutations is associative. The identity permutation I defined on S acts as the identity element of the group. If f is a permutation on S, then f^{-1} is also a one-one mapping on S onto itself. Hence f^{-1} is also a permutation in S such that

$$f\, o\, f^{-1} = f^{-1} o\, f = I$$

Thus S_n is a group.

Definition 9.30: The group S_n is called the symmetric group (or permutation group).

Note:

(*i*) The order of S_n is $n!$.

(*ii*) For $n \leq 2$, the group S_n is abelian and for $n \geq 3$, the group S_n is non-abelian.

If f is a permutation a finite set S we define $f^2 = f\, o\, f$, $f^3 = f\, o\, f\, o\, f$, … order of a permutation.

Let S be a finite non-empty set with n symbols and S_n denote the set of all permutations on S. And let I denote the identity permutation on S. If $f \in S_n$, then the least positive integer k such that $f^k = I$ is called the order of f in S_n.

Example:

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

Then $$f^2 = f\, o\, f = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,2\,3\,4\,5\,6\,7\,8 \end{pmatrix}$$

$$= I$$

$\therefore$ order of f is 2.

9.29 CYCLIC PERMUTATION

Let $S = \{a_1, a_2, \ldots, a_n\}$ be a finite set of n symbols. A permutation f defined or S is said to be cyclic permutation if f is defined such that

$$f(a_1) = a_2, f(a_2) = a_3, \ldots, f(a_{n-1}) = a_n \text{ and } f(a_n) = (a_1)$$

Example: Let $S = \{1, 2, 3, 4\}$

Then $\begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$ is a cyclic permutation.

If $S = \{a_1, a_2, \ldots, a_n\}$ and f is a cyclic permutation on S, then we can write

$f = (a_1\, a_2 \ldots a_n)$

9.29.1 Transposition

A cyclic of length 2 is called a transposition.

Let $S = \{a_1, a_2, a_3, \ldots, a_n\}$ f, g and h be cyclic permutations on S.

Then we have:

(*i*) $(f \, o \, g)^{-1} = g^{-1} \, o \, f^{-1}$

(*ii*) $(f \, o \, g \, o \, h)^{-1} = h^{-1} \, o \, g^{-1} \, o \, f^{-1}$

If S_n is a permutation group on n symbols, then of the $n!$ permutation in S_n, 1/2 n! are even permutations and 1/2 n! are odd permutations. The set of all even permutations of degree n form a group under the composition of permutations. The group of even permutations is called alternating group.

We state the following theorem without proof.

Theorem 9.46: Every permutation may be expressed as the product of transpositions in many ways.

Note: If f is a cycle of length n, then f can be expressed as a product of $(n - 1)$ transpositions. Even and odd permutations.

Definition 9.31: A permutation f is said to be an even permutation if f can be expressed as the product of even number of transpositions.

Definition 9.32: A permutation f is said to be an odd permutation if f is expressed as the product of odd number of transpositions.

Note:

(*i*) An identity permutation is considered as an even permutation.

(*ii*) A transposition is always odd.

(*iii*) The product of two even permutations is even, and also the product of two odd permutations is even.

(*iv*) The product of an even and an odd permutation is odd. Similarly the product of an odd permutation and an even permutations is odd.

Let $S = \{a_1, a_2, a_3, \ldots, a_k, a_{k+1}, \ldots, a_n\}$

$$\text{If } f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_k & a_{k+1} & a_{k+2} & \ldots & a_n \\ a_2 & a_3 & a_4 & \ldots & a_1 & a_{k+1} & a_{k+2} & \ldots & a_n \end{pmatrix}$$

then f is S cyclic permutation. The length of f is k and degree of f is n. We can ignore the elements a_{k+1}, $a_{k+2}, \ldots, a_n$ which are mapped onto themselves and write

$f = (a_1 \, a_2 \, a_3 \ldots a_k)$

A cyclic permutation does not change by changing the places of its elements, provided their order is not changed.

9.29.2 Disjoint Cycles

Definition 9.33: Let $S = (a_1, a_2, \ldots, a_n)$. If f and g are two cycles on S such that they have no common elements, then f and g are said to be disjoint cycles.

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

If $f = (1 \; 4 \; 5)$ and $f = (2, 3, 6)$

then f and g are disjoint cyclic permutations on S.

Note: The product of two disjoint cycles is commutative.

Every permutation can be written as a product of disjoint cycles and transpositions.

For example: Consider the permutation

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

the above permutation f can be written as $f = (1\ 2\ 3\ 4\ 5)\ (6\ 7)$. Which is a product of two cycles. We now state, the following theorem:

Theorem 9.47: Every permutation of n symbols can be expressed a product of disjoint cycles.

Proof: Let f be an element of S_n.

Consider the cycle

$$(1\, f(1)\, f^2\, (1), \ldots)$$

Since $O\,(f)$ is finite, $f^k = 1$ for some k, i.e., $f^k\,(1) = 1$ for some k

Choose smallest $k > 0$ such that $f^k\,(1) = 1$.

Then the cycle $(1\, f(1)\ \ f^2\ (1), \ldots, f^{k-1}\,(1))$ and the permutation f will have the same effect on the symbols

$$1\, f(1)\, f^2\,(1), \ldots, f^{k-1}\,(1)$$

If f, fixes all the remaining symbols then

$$f = (1\, f(1)\, f^2\,(1), \ldots, f^{k-1}\,(1))$$

and the theorem is otherwise, choose a symbol i, such that $f\,(i) \neq i$ and consider the cycle.

$(i\, f\,(i)\, f^2\,(i), \ldots, f^{m-1}\,(i))$ where m is the least positive integer such that $f^m(i) = i$.

If $1\, f(1)\, f^2\,(1), \ldots, f^{k-1}\,(1), i\, f\,(i), \ldots, f^{m-1}\,(i)$ do not exhaust all the symbols and there is stole another symbol not fixed number of steps, the procedure must terminate as there are only a finite number of symbols. Thus

$$f = (1\, f(1)\, f^2\,(1), \ldots, f^{k-1}\,(1)), (i)\, f\,(i), \ldots, f^{m-1}\,(i))$$

is a product of disjoint cycles.

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

Compute $(5\ 6\ 3)\ o\ (4\ 1\ 3\ 5)$

Solution:

$$(4\ 1\ 3\ 5) = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,2\,5\,1\,4\,6 \end{pmatrix}$$

and

$$(\ 5\ 6\ 3) = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,2\,5\,4\,6\,3 \end{pmatrix}$$

$$\therefore \qquad (5\ 6\ 3)\ o\ (4\ 1\ 3\ 5) = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,2\,5\,4\,6\,3 \end{pmatrix} o \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,2\,5\,1\,4\,6 \end{pmatrix}$$

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

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

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

Find (1 3) *o* (2 4 5) *o* (2 3)

Solution: (1 3) *o* (2 4 5) *o* (2 3)

$$= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 2\ 1\ 4\ 5 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 4\ 3\ 5\ 2 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 4\ 3\ 5\ 2 \\ 3\ 4\ 1\ 5\ 2 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 4\ 3\ 5\ 2 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 1\ 5\ 2 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 3\ 2\ 4\ 5 \\ 3\ 1\ 4\ 5\ 2 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

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

= (1 3 4 5 2)

or (1 3) *o* (2 4 5) *o* (2 3)

= (1 3 2 4 5) *o* (2 3)

$$= \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 2\ 5\ 1 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1\ 3\ 2\ 4\ 5 \\ 3\ 2\ 4\ 5\ 1 \end{pmatrix} o \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 1\ 3\ 2\ 4\ 5 \end{pmatrix}$$

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

= (1 3 4 5 2)

Example 3: Express $f = (a_1\ a_2\ a_3\ \ldots\ a_n)$ as a product of transpositions.

Solution: $f = (a_1\ a_2\ a_3\ \ldots\ a_n)$

$$= (a_1\, a_2)\ o\ (a_1\, a_{n-1})\ o\ \ldots\ o\ (a_1\, a_3)\ o\ (a_1\, a_2)$$

(i.e., a cycle of length can be expressed as a product of $n - 1$ transpositions.)

Example 4: Show that $f = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 7\ 3\ 1\ 8\ 5\ 6\ 2\ 4 \end{pmatrix}$ is even.

Solution:

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

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

$$= (1\ 7\ 2\ 3)\ o\ (4\ 8)\ o\ (5)\ o\ (6)$$

$$= (1\ 3)\ o\ (1\ 2)\ o\ (1\ 7)\ o\ (4\ 8)$$

f is expressed as a product of 4 transpositions, therefore *f* is even.

Example 5: Show that $f = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 1\ 4\ 3\ 6\ 5\ 8\ 7\ 2 \end{pmatrix}$ is odd

Solution:

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

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

$$= (1)\ o\ (2\ 4\ 6\ 8)\ o\ (3)\ o\ (5)\ o\ (7)$$

$$= (2\ 4\ 6\ 8)$$

$$= (2\ 8)\ o\ (2\ 6)\ o\ (2\ 4)$$

f is expressed as a product of 3 transpositions 3 is an odd number.

$\therefore$ *f* is odd.

9.30 GROUP HOMOMORPHISM

The concept of group isomorphism was already introduced. A more general concept is that of group homorphism with which we concern ourselves in this section.

Definition 9.34: Let $(G, *)$ and $(\overline{G}, \Delta)$ be any two groups. A mapping $f\colon G \to \overline{G}$ is called a homomorphism of G to $\overline{G}$ if.

$$f(a * b) = f(a)\ \Delta\ f(b)\ \ \forall\ \ a, b \in G$$

Example 1: Let $G = R$, $\overline{G} = R - \{0\}$

$(G, \cdot)$ and $(\overline{G}, \cdot)$ are groups and G and $\overline{G}$ are groups with respect to multiplication. Then the mapping f: $G \to \overline{G}$, defined by $f(a) = \mathrm{a}^n \ \forall \ a \in G$, where $n \in Z$ fixed, is a homomorphism.

Since $f(ab) = (ab)^n = a^n \cdot b^n = f(a) f(b)$.

Example 2: Let $G = R$, the set of real numbers and $\overline{G} = R - \{u)$

$(G, +)$ and $(\overline{G}, \cdot)$ are groups. Define a mapping f: $G \to \overline{G}$ by

$$f(a) = 2^a \ \forall \ a \in G$$

clearly $f(a + b) = 2^{a+b} = 2^a \, 2^b = f(a) \cdot f(b)$

$\Rightarrow f$ is a homomorphism of G into $\overline{G}$.

Definition 9.35: Let $(G, *)$ and $(\overline{G}, \Delta)$ be two groups. A mapping f: $G \to \overline{G}$ defined by $f(a * b) = f(a) \ \Delta \ f(b)$ is called isomorphism, if f is a one-one, onto mapping.

From the above definition, it is clear that, a one-one, onto homomorphism is an isomorphism. Thus every isomorphism is necessarily a homomorphism, whereas the converse need not be true. If f: $G \to \overline{G}$ is onto homomorphism, then $\overline{G}$ is called homomorphism image of G. Every quotient group of group is a homomorphic image of the group.

Definition 9.36: Let $(G, *)$ be a group. A mapping f: $G \to \overline{G}$ is called, endomorphism if $f(a * b) = f(a) * f(b)$.

Definition 9.37: Let $(G, *)$ be a group. A mapping f: $G \to G$ defined by $f(a * b) = f(a) * f(b)$ is called an automorphism if f is a objective mapping.

9.31 KERNEL OF A HOMOMORPHISM

Let G and $\overline{G}$ be any two groups and f: $G \to \overline{G}$ be a homomorphism. Then Kernel of f denoted by Ker f the set $K = (a \in G\text{: } f(a) = \overline{e})$.

Where $\overline{e}$ is the identity of $\overline{G}$.

Ker f is called the Kernel of the homomorphism f. Thus the Kernel of f is the set of all those elements of the domain set which are mapped onto the identity of the range set.

Theorem 9.48: Let $(G, *)$ and $(\overline{G}, \cdot)$ be two groups and f be a homomorphism then

(*i*) $f(e) = \overline{e}$, where e is the identity of G and $\overline{e}$ is the identity in $\overline{G}$.

(*ii*) $f(a^{-1}) = [f(a)]^{-1} \ \forall \ a \in G$

(*iii*) $f(a^n) = [f(a)]^n \ \forall \ a \in G$ and $n \in Z$

Proof: (*i*) $a \in G \Rightarrow a = a * e$

$$\Rightarrow f(a) = f(a * e)$$

$$= f(a) \, o \, f(e) \quad (\because f \text{ is a homomorphism})$$

Now $f(a) \in \overline{G}$ and $\overline{e}$ in the identity of $\overline{G}$

$$\Rightarrow f(a) \, o \, \overline{e} = f(a)$$

$\therefore$ $$f(a) \, o \, f(e) = f(a) = f(a) \, o \, \overline{e}$$

$$\Rightarrow f(a) \cdot f(e) = f(a) \, o \, \overline{e}$$

$$\Rightarrow f(e) = \overline{e} \quad \text{(by left cancellation law)}$$

(*ii*) $$a \in G \Rightarrow a^{-1} \; \forall \; a \in G$$

$$\Rightarrow a * a^{-1} \in G$$

$$\Rightarrow e \in G$$

$\therefore$ $$\Rightarrow f(a * a^{-1}) = f(e)$$

$$\Rightarrow f(a) \, o \, f(a^{-1}) = f(e) = \overline{e}$$

$$\Rightarrow [f(a)]^{-1} = f(a^{-1}) \; \forall \; a \in G$$

(*iii*) Left as an exercise to the student.

Theorem 9.49: Let f be a homomorphism of $(G, *)$ into $(\overline{G}, \cdot)$ with Kernel K, then K is a normal sub-group of G.

Proof: We know that

$$f(e) = \Rightarrow \overline{e} \; e \in K$$

Thus $ker f = K$ is a non-empty.

Subset of G.

K is a sub-group of G

$$a, \; a, b \in K \; \Rightarrow f(a) = \overline{e}, \text{ and } f(b) = \overline{e}$$

now $$f(a * b) = f(a) \, o \, f(b)$$

$$= \overline{e} \; o \; \overline{e} \quad (\therefore f \text{ is a homomorphism})$$

$$= \overline{e}$$

$\therefore$ $$a \in K, b \in K \Rightarrow a * b \in K$$

Now $$a \in K \Rightarrow a \in G \Rightarrow a^{-1} \in G$$

Also $$f(a^{-1}) = [f(a)]^{-1}$$

$$= (\overline{e})^{-1}$$

$$= \overline{e}$$

$$\Rightarrow a^{-1} \in K \; \forall \; a \in K$$

Thus K is a sub-group of G.

We now prove that K is a normal sub-group G.

$$\begin{aligned}
& K \in K,\ a \in G \\
& \Rightarrow f(a * K * a^{-1}) \\
& = f(a * K)\ o\ f(a^{-1}) \\
& = f(a)\ o f(K)\ o f(a^{-1}) \\
& = f(a)\ o\ \bar{e}\ \ o f(a^{-1}) \\
& = f(a)\ o f(a^{-1}) \\
& = f(a * a^{-1}) \\
& = f(e) = \bar{e} \\
& \Rightarrow a * K * a^{-1} \in K \quad \forall\ K \in K, a \in G
\end{aligned}$$

Hence, K is a normal sub-group of G.

Now we state the following theorem without proof.

Theorem 9.50: Let f be a homomorphism of $(G, *)$ into $(\overline{G}, \cdot)$ with Kernel K, then $G/K \cong \overline{G}$

9.32 SOLVED EXAMPLES

Example 1: Let G be $(Z, +)$ i.e., the group of integers under addition and let f: $G \rightarrow G$ defined by $\varnothing\ (x) = 3x\ \forall\ x \in G$. Prove that f is homomorphism, determine its Kernel.

Solution: We have $\varnothing\ (x) = 3x\ \forall\ x \in G$

$$\forall\ x, y \in G \Rightarrow x + y \in G \quad (\because\ G \text{ is a group under addition})$$

Now
$$\begin{aligned}
f(x + y) &= 3\ (x + y) \\
&= 3x + 3y \\
&= f(x) + f(y)
\end{aligned}$$

Hence f is homomorphism.

Kernel of homomorphism consists of half of zero i.e., the integers whose double is zero.

Thus $K = \{0\}$

Example 2: Let $\varnothing\ G \rightarrow \overline{G}$ defined by $\varnothing(a) = \bar{e}$. Prove that $\forall\ a \in G$ is homomorphism.

Solution: $\forall\ a, b \in G \Rightarrow b \in G$ $(\because$ G is a group)

Now
$$\begin{aligned}
\varnothing\ (a * b) &= \bar{e} \\
&= \bar{e} * \bar{e} = \varnothing(a) \cdot \varnothing(b)
\end{aligned}$$

Hence $\varnothing$ is homomorphism.

Example 3: Consider two groups G and $\overline{G}$ where $G = (Z, +)$ and $\overline{G} = \{Z^m/m = 0, \ldots, x\}$.

Let $\varnothing = Z \rightarrow \{Z^m/m$ is an integer$\}$. Defined by $f(m) = 2^m$ where $m \in Z$. Prove that $\varnothing$ is homomorphism.

Solution: We have $\varnothing\ (m) = 2^m$ where $m \in Z$.

$$\therefore \qquad \varnothing\ (m + r) = 2^{m+r} = 2^m\, 2^r = \varnothing\ (m)\ \varnothing\ (r)$$

Hence $\varnothing$ is homomorphism.

Example 4: Prove that the mapping $\varnothing$ is an automorphism. Where

(*a*) G, the group of integers under addition $\varnothing\ (x) = -x$

(*b*) G, the group of positive reals under multiplication $\varnothing\ (x) = x^2$.

Solution:

(*a*) Let $x, y \in G$, then $x + y \in G$ (Since G is a group under addition)

Now $\varnothing\ (x + y) = -(x + y) = -\text{x} - y = \varnothing\ (x) + \varnothing\ (y)$.

$\therefore \varnothing$ is homomorphism.

Now $y \in G \Rightarrow y \in G$ [Since G is a group under addition].

Now $\varnothing\ (-y) = -(-y) = y \in G$

$\therefore \varnothing$ is onto.

$\varnothing\ (x) = \varnothing\ (y) = -x = -y = x = y$

$\therefore \varnothing$ is one-one.

Hence $\varnothing$ is an automorphism.

(*b*) Let $x, y \in G$. Then $x * y \in G$ ($\therefore$ G is a group under multiplication)

Now $\varnothing\ (x * y) = (x\,y)^2 = x^2 * y^2 = \varnothing\ (x) * \varnothing\ (y)$.

$\therefore \varnothing$ is homomorphism.

Now $y \in G$, there exists $y^{1/2} \in G$ such that

$\varnothing\ (y^{1/2}) = (y^{1/2})^2 = y$

$\therefore \varnothing$ is onto

$\varnothing\ (x) = \varnothing\ (y) = x^2 = y^2 \Rightarrow x = y$

$\therefore \varnothing$ is one-one.

Example 5: If for a group $G, f\colon G \rightarrow G$ is given by $f(x) = x^2,\ x \in G$ is a homomorphism, prove that G is abelian.

Solution: $a, b \in G \Rightarrow a\,b \in G$

$f\colon G \rightarrow G$ is a homomorphism

$$\therefore \qquad f(a) = a^2, f(b) = b^2 \text{ and } f(ab) = (ab)^2$$

Now $f(ab) = (ab)^2$

$\Rightarrow f(a) = f(b) = (ab)\,(ab)$

$\Rightarrow a^2\, b^2 = (ab)\,(ab)$

$\Rightarrow (aa)\,(bb) = (ab)\,(ab)$

$\Rightarrow a\,(ab)\,b = a\,(ba)\,b$

$\Rightarrow (ab)\,b = (ba)\,b$

$\Rightarrow ab = ba$ (Cancellation law hold good in G)

$\Rightarrow G$ is abelian.

EXERCISE 9.5

1. Define:
   (*a*) Sub-group
   (*b*) Order of a group
   (*c*) Finite group
   (*d*) Order of an element.
2. Show that the set of all elements a of an abelian group G which satisfy $a^2 = e$, forms a sub-groups of G.
3. If G is a group and $N(a) = n \in G \;\; (ax = xa)$ for $a \in G$, then prove that $N(a)$ is a sub-group of G.
4. If $G = \{1, -1, i, -i\}$ is a group under multiplication then write all sub-groups of G.
5. Let $(G, 0)$ be a group and $a \in G$. If $N(G)$ denotes the normalizer of a in G, then show that $(N(G), 0)$ is a sub-group of $(G, 0)$.
6. Define a cyclic group and give examples.
7. Show that the group $\{a, a^2, a^3, = e, 0\}$ is a cyclic group.
8. Let P be the collection of sub-groups of $(G, *)$ prove that the intersection of sub-groups in P is a sub-group of $(G, *)$.
9. Find all the sub-groups of a cyclic group of order 60.
10. Find all the sub-groups of a cyclic group of order 10.
11. Show that every sub-group of a cyclic group is cyclic.
12. List all sub-groups of a cyclic group of order 12.
13. Show that the group $(\{0, 6\}, +_{12})$ is a sub-group of $(Z_{12}, +_{12})$ of integers modulo 12.
14. Show that every cyclic group is commutative.
15. State and prove Lagrange's theorem.
16. If $(G, *)$ is a finite group of composite order then show that $(G, *)$ has non-trivial sub-groups.
17. Show that every group of Prime order is cyclic.
18. Prove that every sub-group of an abelian group is normal.
19. Prove that every quotient group of an abelian group is abelian.

20. If $(G, *)$ is a finite group of order n, with generator a. Then show that a^m is also a generator of G if and only if $m < n$, and $(m, n) = 1$.

21. If $(H_1,)$ and $(H_2,)$ are two normal sub-group of $(G,)$ then show that is also a normal sub-group of G.

22. Show that the intersection of any collection of normal sub-groups itself a normal sub-group.

23. Prove that every sub-group of index 2 is a normal sub-group.

24. Prove that the symmetric group of two symbols $(S_2, 0)$ is commutative.

25. Determine whether the following permutations are odd or even:

(*a*) $\begin{pmatrix} a\ b\ c \\ c\ a\ b \end{pmatrix}$

(*b*) $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7 \\ 3\ 2\ 4\ 5\ 6\ 7\ 1 \end{pmatrix}$

(*c*) $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9 \\ 6\ 1\ 4\ 3\ 2\ 5\ 7\ 9\ 8 \end{pmatrix}$

(*d*) $\begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 2\ 4\ 1\ 5 \end{pmatrix}$

26. Express the following permutations as the product of transpositions.

(*a*) $\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7 \\ 5\ 7\ 6\ 2\ 1\ 3\ 4 \end{pmatrix}$

(*b*) $(1\ 2\ 3)\ o\ (4\ 5)\ o\ (6\ 7\ 8)$

27. $G = (f_1, f_2, f_3, f_4)$ where

$$f_1 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 2\ 3\ 4 \end{pmatrix},\ f_2 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 1\ 4\ 3 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 1\ 2 \end{pmatrix},\ f_4 = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 2\ 1 \end{pmatrix}$$

Show that $(G, \cdot)$ is an abelian group.

9.33 ALGEBRAIC SYSTEM WITH TWO BINARY OPERATIONS

In the previous section, we studied, some of the elementary aspects of groups, which are algebraic systems with one suitably restricted binary operation. We now proceed to study rings, which are algebraic systems with two binary operations. We will also study some particular types of rings, notably, integral domains and fields. We use the symbols '+' and '·' for any two binary operation and refer to these as 'addition' and 'multiplication' respectively as against their usage in the concept of numbers. In this section, we use R to denotes an arbitrary set. (In this section, the symbol R will no longer denote the set of real numbers, unless specified).

The identity elements $(R, +)$ and $(R, \cdot)$ are denoted by '0' and '1' respectively. The inverse of a with respect to '+' is denoted by $-a$. We now define ring as follows.

9.33.1 Ring

Definition 9.38: An algebraic system $(R, +, \cdot)$ is called a ring if the binary operations '+' and '$\cdot$' R satisfy the following properties:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is a semi-group.
3. The operation '.' is distributive over +, that is for any $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and}$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Example 1: The set of all matrices of the form $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ a and b being real numbers, with matrix addition and matrix multiplication is a ring.

Example 2: The set of integers Z, with respect to the operations + and × is a ring.

9.34 SPECIAL TYPES OF RINGS

9.34.1 Commutative Ring or Abelian Ring

A ring R is said to be a commutative ring or an abelian ring if it satisfies the commutative law, $\forall\ a, b \in R$, $a \cdot b = b \cdot a$.

9.34.2 Ring with Unity

A ring R which contains the multiplicative identity (called unity) is called a ring with unity.

Thus if $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a \ \ \forall\ a \in R$, then the ring is called a ring with unity.

9.34.3 Ring without Unity

A ring R, which does not contain multiplicative identity is called a ring without unity.

9.34.4 Finite and Infinite Ring

If the number of elements in the ring R. Is finite, then $<R, +, \cdot>$ is called a finite ring, otherwise. It is called an infinite ring.

9.34.5 Order of Ring

The number of elements in a finite ring R is called the order of ring R.

This is denoted by $|R|$.

Definition 9.39: Let $(R, +, \cdot)$ be a ring with unity. An element $a \in R$ is said to be invertible, if there exists an element $a^{-1} \in R,$ called the inverse of a such that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

9.35 PROPERTIES OF RINGS

Theorem 9.51: If R is a ring then:

(*i*) $a \cdot 0 = 0 = 0 \cdot a \;\; \forall \;\; a \in R$

(*ii*) $a\,(-b) = (-a)\,b = -(ab) \;\; \forall \;\; a, b \in R$

(*iii*) $(-a)\,(-b) = ab, \;\; \forall \;\; a, b \in R$

Proof:

(*i*) We know that

$$a + 0 = a \;\; \forall \;\; a \in R$$

$$\Rightarrow \;\; a \cdot (a + 0) = a \cdot a$$

$$\Rightarrow \;\; a \cdot a + a \cdot 0 = a \cdot a + 0$$

$$\Rightarrow \;\; a \cdot 0 = 0 \;\; \text{(by left cancellation under addition)}$$

Similarly, we can prove

$$0 \cdot a = 0$$

(*ii*) $b \in R \Rightarrow -b \in R$ such that $b + (-b) = 0$

$$\Rightarrow \;\; a \cdot (b + (-b)) = a \cdot 0$$

$$\Rightarrow \;\; a \cdot b + a \cdot (-b) = 0$$

$$\Rightarrow \;\; a \cdot (-b) = -\,(a \cdot b)$$

Similarly, we can prove

$$(-a) \cdot b = -\,(a \cdot b)$$

(*iii*) We have

$$\begin{aligned} & a \cdot (-b) + (-a) \cdot (-b) \\ &= (a + (-a)) \cdot (-b) \\ &= 0 \cdot (-b) \\ &= 0 \\ &= a \cdot ((-b) + b) \\ &= a \cdot (-b) + a \cdot b \end{aligned}$$

By left cancellation law

$$(-a) \cdot (-b) = a \cdot b$$

Second method

$$(-a)\cdot(-b) = -((-a)\cdot b) = -(-(a\cdot b)) = ab$$

Corollary 1: Let $(R, +, \cdot)$ be a ring, then

$$a\cdot(b-c) = a\cdot b - a\cdot c$$

$$(b-c)\cdot a = b\cdot a - c\cdot a \text{ for all } a, b, c \in R$$

Proof:

$$\begin{aligned} a\cdot(b-c) &= a\cdot(b+(-c)) \\ &= a\cdot b + a\cdot(-c) \\ &= a\cdot b - a\cdot c \end{aligned}$$

Hence $a\cdot(b-c) = a\cdot b - a\cdot c$

Similarly, we can prove that

$$(b-c)\cdot a = b\cdot a - c\cdot a$$

Corollary 2: If $(R, +, \cdot)$ is a ring with unity then for all $a \in R$

(*i*) $(-1)\cdot a = -a$

(*ii*) $(-1)\cdot(-1) = 1$

Proof:

(*i*) $(-1)\cdot a = -(1\cdot a) = -a$

(*ii*) R is a ring with unity element, then $1\cdot a = a \ \forall \ a \in R$

We have

$$\begin{aligned} (1)a + (-1)\cdot a &= 1\cdot a + (-1)\cdot a \\ &= (1+(-1))\cdot a \\ &= 0\cdot a \\ &= 0 \end{aligned}$$

$$\Rightarrow a + (-1)a = 0$$

$$\Rightarrow (-1)\cdot a = -a$$

if $a = -1$, then $(-1)\cdot(-1) = -(-1)$

$$\Rightarrow (-1)\cdot(-1) = 1$$

Definition 9.40: Let $(R, +, \cdot)$ be a ring. R is said to be with zero divisors if there exists two non-zero elements, $a, b \in R$ such that $a\cdot b = 0$.

Note: If $a \neq 0$, $b \neq 0 \Rightarrow ab = 0$ in R, a is called the left zero divisor and b is called the right zero divisor.

Definition 9.41: Let $(R, + \cdot)$ be a ring. R is said to be without zero divisors if $ab = 0 = \Rightarrow$ either $a = 0$ or $b = 0$ for all a, $a, b \in R$.

Example: Let R denote the set of ordered pairs of real number i.e.

Let $R = \{(a, b): a, b \text{ are real}\}$ and addition and multiplication on R be defined as follows:

$$(a, b) + (c, d) = (a + c, b + d)$$
$$(a, b)\ (c, d) = (ac, bd)$$

Clearly $(R, +, \cdot)$ is a commutative ring with unity (1, 1)

We observe that

$$(1, 0)\ (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$$

where (0, 0) is the additive identity in R also $(1, 0) \neq (0, 0), (0, 1) \neq (0, 0)$

Thus (1, 0) and (0, 1) are zero divisors of the ring R.

9.36 SUB-RINGS

Definition 9.42: Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. If $(S, +, \cdot)$ is a ring then $(S, +, \cdot)$ is called a sub-ring of R.

Example: Let E denote the set of even integers. $(E, +, \cdot)$ is a sub-ring of $(Z, +, \cdot)$, where Z denotes the set of integers.

Note: Every ring $(R, +, \cdot)$ has two trivial sub-rings $(\{0\}, +, \cdot)$ and $(R, +, \cdot)$ where 0 is the additive identity of $(R, +, \cdot)$.

Definition 9.43: Let $(S, +, \cdot)$ be a sub-ring of $(R, +, \cdot)$ where R is a ring with identity element 1. If $1 \in S$, then S is called a unitary sub-ring of R and the ring is said to be unitary over ring $(S, +, \cdot)$.

9.37 COEFFICIENTS AND EXPONENTS

Let $(R, +, \cdot)$ is ring and $a \in R$. If m is a positive integer then we can write.

$$ma = a + a + \ldots + a \ (m \text{ times}) \text{ and } a^m = a \cdot a \ldots a \ (m \text{ times})$$

moreover, for all positive integers m and n, we have

$$a^m\, a^n = a^{m+n} \text{ and } (a^m)^n = a^{mn}$$

Definition 9.44: Let $(R, +, \cdot)$ be a ring. If there exists a positive integer n such that $na = 0$ for all $a \in R$, then such a least positive integer n is called the characteristic of the ring R. If no such integer exists, then $(R, +, \cdot)$ is said to be characteristic zero.

Example 1: The ring $(Z, +, \cdot)$ is characteristic zero.

Example 2: In the ring $(Z_6, +_6, \times_6)$ of integers, we have

$$a +_6 a +_6 a +_6 a +_6 a +_6 a = 0 \ \forall \ a \in Z_6$$

$(Z_6, +_6, \times_6)$ is of characteristic zero.

Definition 9.45: Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is said to be idempotent if $a \cdot a = a^2 = a$.

Example 3: In the ring $(Z_6, +_6, \times_6)$ the elements 0, 1, 3 and 4 are idempotent.

Definition 9.46: Let $(R, +, \cdot)$ be a ring. An element $a \in R$ is said to be nilpotent if there exists a positive integer n such that $a^n = 0$

Example 4: Zero element of a ring is nilpotent.

Definition 9.47: Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. Then the system $(S, +, \cdot)$ is a subring of $(R, +, \cdot)$ if and only if.

(*i*) $a - b \in S$ for all $a, b \in S$

(*ii*) $a \, . \, b \in S$ for all $a, b \in S$

Theorem 9.52: Let $(S_1, +, \cdot)$ and $(S_2, +, \cdot)$ be two sub-rings of a ring $(R, +, \cdot)$. Then $(S_1 \cap S_2, +, \cdot)$ is also a sub-ring of $(R, +, \cdot)$.

Definition 9.48: Let $(R, +, \cdot)$ be a ring. If $a \, . \, a = a \; \forall \; a \in R$ then $(R, +, \cdot)$ is said to be Boolean ring.

Example 5: Let S be non-empty set. Then $(P\,(S), \Delta, \cap)$ is a ring where $P\,(S)$, is the power set of S

$P\,(S, \Delta, \cap)$ is a Boolean ring, since

$$A \cap A = A \; = A \text{ for all } A \in P(S)$$

Theorem 9.53: If $(R, +, \cdot)$ is a Boolean ring, then $a + a = 0 \; \forall \; a \in R$.

Proof: $a \in R \Rightarrow a + a \in R$

since $(R, +, \cdot)$ is Boolean ring,

then $(a + b) + 0 = (a + a)$

$$\Rightarrow (a + a) + 0 = (a + a) \cdot (a + a)$$

$$= (a \cdot a + a \cdot a) + (a \cdot a + a \cdot a)$$

$$= (a + a) + (a + a)$$

by left cancellation we have $a + a = 0$.

Definition 9.49: A commutative ring $(R, +, \cdot)$ with unity is an integral domain if it has no zero divisors.

Example 6: Ring of integers is an integral domain.

Definition 9.50: A ring $(R, +, \cdot)$ is said to be a division ring (or Skew field) if its non-zero elements form a group under multiplication.

Example 7: The ring of rational numbers $(Q, +, \cdot)$ is a division ring, since $1 \in Q$ and the non-zero elements of Q are invertible.

Example 8: Show that a division ring has no zero divisors.

Solution : Let $(R, +, \cdot)$ be a division ring

Let $a, b \in R$ and $a \neq 0$. Let $ab = 0$

R is a division ring, therefore $a \in R \Rightarrow a^{-1} \in R$ such that $aa^{-1} = a^{-1}\, a = 1$

Now $ab = 0$

$$\Rightarrow a^{-1}\,(ab) = a^{-1}\,0$$

$$\Rightarrow (a^{-1}\,a)\,b = 0$$

$$\Rightarrow 1b = 0$$

$$\Rightarrow b = 0$$

Thus $a, b \in R, a \neq 0$ and $ab = 0 \Rightarrow b = 0$

Similarly, we can show that $a, b \in R, b \neq 0$ and $ab = 0 \Rightarrow a = 0$

Hence $ab \in R, ab = 0 \Rightarrow a = 0$ or $b = 0$

Therefore a division ring has no zero divisors.

Definition 9.51: A commutative division ring is called a field.

Example 9: Let Q be the set of rational numbers and '+' and '.' be two binary operation, then $(Q, +, \cdot)$ is a ring.

Also Q is field.

Theorem 9.54: A finite integral domain is a field.

Definition 9.52: Let $(D, +, \cdot)$ be an integral domain. D is said to be of characteristic p, if p is the smallest positive integer such that $pa = 0 \;\forall\; a \in D$

Example 10: The characteristic of the ring of integers $(Z, +, \cdot)$ is zero

Example 11: $R = \{0, 1, 2, 3, 4, 5, 6\}$ is a ring under addition and multiplication modulo 7.

Since 7 is the least positive integer so that

$7a = 0$ for all $a \in R,$ the characteristic of R is 7.

Example 12: If R is a non-zero ring so that $a^2 = a \;\forall\; a \in R,$ prove that the characteristic of R is 2.

Solution: Since $a^2 = a \;\forall\; a \in R$

We have $(a + a)^2 = (a + a)$

i.e.

$$(a + a)\,(a + a) = (a + a)$$

$$\Rightarrow a(a + a) + a(a + a) = a + a$$

$$\Rightarrow (aa + aa) + (aa + aa) = a + a$$

$$\Rightarrow (a^2 + a^2) + (a^2 + a^2) = a + a$$

$$\Rightarrow (a + a) + (a + a) = (a + a) + 0$$

$$\Rightarrow a + a = 0$$

$$\Rightarrow 2a = 0$$

2 is the least positive integer so that

$$2a = 0 \;\forall\; a \in R$$

Hence, the characteristic of R is 2.

Theorem 9.55: The characteristic of an integral domain is either a prime or zero.

Theorem 9.56: The characteristic of a field is either a prime or zero.

Definition 9.53: A mapping f from a ring R into the ring R' is said to be homomorphism if

(*i*) $f(a + b) = f(a) + f(b)$

(*ii*) $f(ab) = f(a)f(b)$

for all $a, b \in R$.

Theorem 9.57: If f is a homomorphism of R into R', then

(*i*) $f(0) = 0'$ (0 is the additive identity of R').

(*ii*) $f(-a) = -f(a)$ for every $a \in R$

Definition 9.54: Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R is said to be an ideal of R if.

(*i*) S is a sub-group of R under addition.

(*ii*) For every $s \in S$ and $r \in R$, both sr and rs are in S.

Example 13: In any ring $(R, +, \cdot)$, the trivial sub-rings $(R, +, \cdot)$ and $(\{0\}, +, \cdot)$ are both ideals.

Example 14: $(\{0, 3, 6, 9\}, +_{12}, \times_{12})$ is an ideal of the ring $(Z_{12}, +_{12}, \times_{12})$.

Definition 9.55: The center of a ring R is the set of all elements $a \in R$ such that

$$xa = ax \text{ for all } x \in R$$

If R is a commutative ring then the center of R is trivially, the ring R itself . The center of any ring R is a subring of R.

EXERCISE 9.6

1. Define:

(*a*) Ring

(*b*) Commutative ring

(*c*) Ring with unity

(*d*) Integral domain

(*e*) Field

give examples

2. Show that the system $(E, +, \cdot)$ of even integers is a ring under ordinary addition and multiplication.
3. Define sub-ring and give an example.
4. Show that a ring $(R, +, \cdot)$ is without zero divisors if and only if cancellation law holds for multiplication.
5. If $(R, +, \cdot)$ is a ring and $a, b \in R$ show that equation $a + n = b$ has unique solution in R.
6. If R is a ring commutative with characteristic 2. Show that $(a + b)^2 = a^2 + b^2 \ \forall \ a, b \in R$.
7. If R is a Boolean ring, then show that $a + a = 0 \ \forall \ a \in R$.
8. Show that every Boolean ring is commutative.
9. Show that a finite integral domain is a field.
10. If $D = \{a + b\sqrt{5} : a, b \in Z\}$, show that $(D, +, \cdot)$ is an integral domain.

10

Finite State Machines

10.1 INTRODUCTION

In this chapter, we study finite state machines. A finite state machine is a mathematical system with discrete inputs and outputs. Each internal configuration of the system is called a state. A table lamp is a finite state machine. A switching circuit is a finite state machine. In computer science, we find many examples of finite state systems.

Finite state machines have many applications. A finite state machine can be used to model a physical system and is similar to finite state automation. Lexical scanners, parity check machines, shift registers, vending machines, etc., are some examples of finite state machines. A device that receives a set of input signals and produces corresponding output signals is called an information—processing machine.

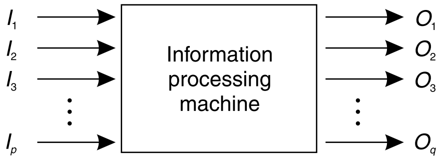


Fig. 10.1 Information—Processing machine

Machines can be divided into two classes.

(*a*) Machines with memory.

(*b*) Machines without memory.

A vending machine is a machine with memory. Table lamp and adder are examples of machines that have no memory. A summary of post events of the machine is represented by a state and a machine may have a certain number of states corresponding to a certain number of distinct classes of past history. A machine with finite number of states is called a finite state machine.

Definition 10.1: A finite state machine is a system $M = (S, I, O, \delta, \lambda)$ where the sets S, I and O are alphabets that represent the state, input and output symbols of the machine respectively. δ is a mapping of $S \times I$ into S, which denotes the next state function and λ is a mapping of $S \times I$ into O, which denotes the output function. The alphabets I and O are not necessarily disjoint but $I \cap S = O \cap S = \varnothing$, we shall denote the alphabets by

$$S = \{s_0, s_1, s_2, \ldots, s_m\}$$
$$I = \{a_0, a_1, a_2, \ldots, a_n\}$$
$$O = \{o_0, o_1, o_2, \ldots, o_r\}$$

And we shall assume that the finite state machine is in an initial state S_0.

The function $\delta : S \times I \rightarrow S$, is also referred to as the transition function. At any state, a finite state machine produces an output letter according to the output function λ. The figure shown in Fig 10.2 is an abstract representation of a finite state machine.

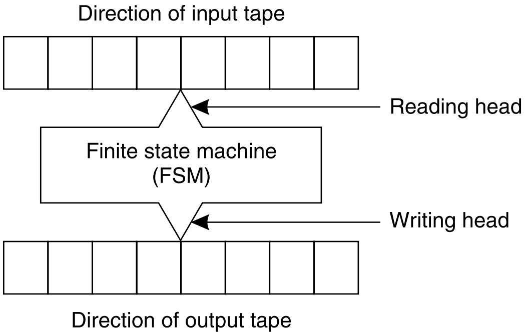


Fig. 10.2

The input tape is divided into squares and input symbols are stored on the input tape. The output symbols are stored in output tape. The machine reads a sequence of symbols that are stored on an input tape and stores sequence of output symbols on an output tape. The input and output tapes are allowed to move only in one direction.

Example 1: Let $S = \{s_0, s_1, s_2\}$

$I = \{a, b\}$

$O = \{p, q, r\}$

Initial state s_0

Next state function $\delta : S \times I \rightarrow S$, be defined by

$$\delta\ (s_0, a) = s_1,\ \delta\ (s_1, a) = s_2,\ \delta\ (s_2, a) = s_0,$$
$$\delta\ (s_0, b) = s_1,\ \delta\ (s_1, b) = s_2,\ \delta\ (s_2, b) = s_1,$$

output function $\lambda : S \times I \rightarrow O$, be defined by

$$\lambda\ (s_0, a) = p,\ \lambda\ (s_1, a) = p,\ \lambda\ (s_2, a) = r,$$
$$\lambda\ (s_0, b) = q,\ \lambda\ (s_1, b) = r,\ \lambda\ (s_q, b) = q,$$

then $M = (S, I, O, \delta, \lambda)$ defines a finite state machine, with three internal states two input symbols and three output symbols.

10.2 TRANSITION TABLE

A finite state machine M can be represented by a table, called the transition table (or state table) in which the functions δ and λ can be described.

Example 1: Let $S = \{s_0, s_1\}$, $I = \{a, b\}$, $O = \{0, 1\}$

Initial state is s_0.

Next state function $\delta : S \times I \to S$, be defined by

$$\delta\ (s_0, a) = s_1,\ \delta\ (s_1, a) = s_0,$$

$$\delta\ (s_0, b) = s_1,\ \delta\ (s_1, b) = s_1,$$

output function $\lambda : S \times I \to O$, be defined by

$$\lambda\ (s_0, a) = 1,\ \lambda\ (s_1, a) = 0,$$

$$\lambda\ (s_0, b) = 1,\ \lambda\ (s_1, b) = 1,$$

then $M = (S, I, O\ \delta, \lambda)$ is a finite state machine with s_0 as the initial state.

The state table of M is given in Table 10.1.

Table 10.1

I	δ		λ	
S	a	b	a	b
S_0	S_1	S_1	1	1
S_1	S_0	S_1	0	1

10.3 TRANSITION DIAGRAM (STATE DIAGRAM)

Definition 10.2: The state diagram of a finite state machine M is a directed graph, in which there is a node for each state symbol in S, and each node is labelled by the state symbol with which it is associated. Furthermore for each ordered pair (s_i, s_j) there exists such that 3-tuples (s_i, q_p, s_j) and (s_i, a_p, o_k) there is a branch originating at s_i and terminating at s_j where each such branch is labelled by a_p/o_k (or a_p, o_k).

Thus, the transition diagram of a finite state machine is digraph. The vertices are the states, the initial state is indicated by an arrow (as shown in Fig. 10.1) for example: If we are in state s_0 and inputting a_p causes output o and moves to state s_1. We draw a directed line (edge) from vertex s_0 to s_1 and label it $a_{p/o}$. The transition diagram of the finite state machine M given by Table 10.1 is shown in Fig. 10.3.

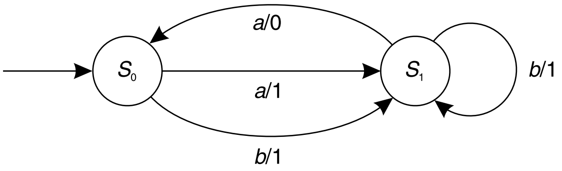


Fig. 10.3 A Transition diagram

Example: Draw the transition diagram of the finite State machine describe the Table 10.2.

Table 10.2

$S \backslash I$	δ		λ	
	a	b	a	b
S_0	S_1	S_1	x	y
S_1	S_0	S_1	x	y
S_2	S_0	S_1	x	y

Solution: The graphical representation i.e., transition diagram of the finite state machine is pictured in Fig. 10.4.

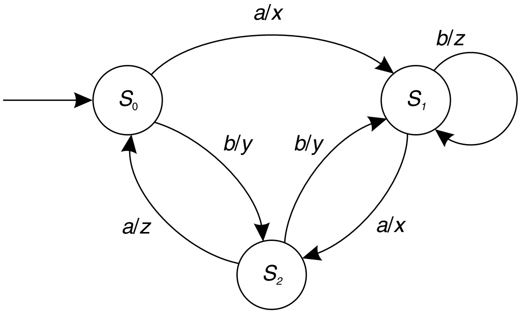


Fig. 10.4

10.4 FINITE STATE MACHINE (ALTERNATIVE DEFINITION)

A finite state machine is always associated with a initial state. It consists of

1. A finite set of states.
2. A finite set I of input symbols.
3. A finite set O of output symbols.
4. A next state function δ from $S \times I$ into S.
5. An output function $S \times I$ into O.
6. An initial state $S_0 \in S$.

Thus, we can define a finite state machine M as a 6-tuple

$M = (S, I, O, \delta, \lambda, S_0)$

Example 1: Draw the transition diagram state diagram of the finite state machine $M = (S, I, O, \delta, \lambda, S_0)$ given in the Table 10.3.

Table 10.3

I S	δ			λ		
	a	*b*	*c*	*a*	*b*	*c*
S_0	S_0	S_1	S_2	0	1	0
S_1	S_0	S_1	S_0	1	1	1
S_2	S_2	S_1	S_0	1	0	0

Solution: We have $S = \{s_0, s_1, s_2\}$

$I = \{a, b, c\}$

$O = \{0, 1\}$

S_0 is the initial state

The state diagram can be drawn as shown in Fig. 10.5.

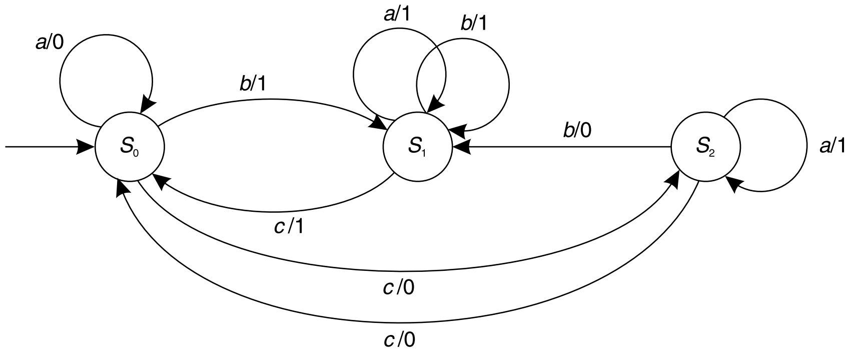


Fig. 10.5

Example 2: Find the sets *S*, *I* and *O*, the initial state, and transition table defining the next state and output function for the finite state machine given in Fig. 10.6.

Solution: We have $S = \{s_0, s_1, s_2, s_3\}$

$I = \{a, b\}$

$O = \{0, 1\}$

S_0 is the initial state

$\delta : S \times I \to S$ is the next function defined by

$\delta\ (s_0, a) = s_1,\ \delta\ (s_1, a) = s_0,\ \delta\ (s_2, a) = s_3,\ \delta\ (s_3, a) = s_1,$

$\delta\ (s_0, b) = s_2,\ \delta\ (s_1, b) = s_2,\ \delta\ (s_2, b) = s_0,\ \delta\ (s_3, b) = s_3$

output function

$\lambda : S \times I\ \lambda\ O$ is defined by

$\lambda\ (s_0, a) = 0,\ \lambda\ (s_1, a) = 1,\ \lambda\ (s_2, a) = 0,\ \lambda\ (s_3, a) = 0,$

$\lambda\ (s_0, b) = 0,\ \lambda\ (s_1, b) = 0,\ \lambda\ (s_2, b) = 1,\ \lambda\ (s_3, b) = 0$

The state table is given in Table 10.4.

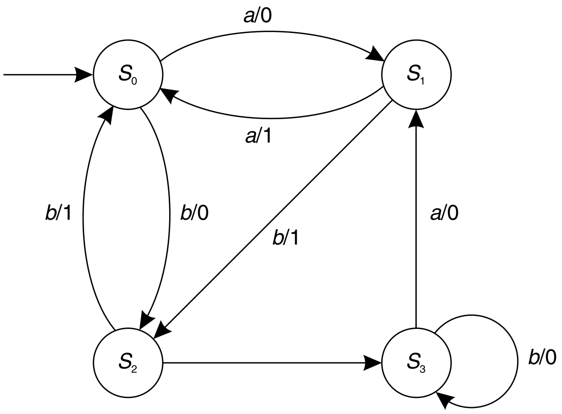


Fig. 10.6

Table 10.4

I / S	δ		λ	
	a	*b*	*a*	*b*
S_0	S_1	S_2	0	0
S_1	S_0	S_2	1	0
S_2	S_3	S_0	0	1
S_3	S_1	S_3	0	0

Example 3: Binary adder:

A serial adder operates in a sequential manner to perform an indicated operation. The block diagram of an adder in given in Fig. 10.7.

The sequence of bits for *x*, *y* and *z* are represented by

$$x_{n-1}\ x_{n-2}\ \ldots x_1\ x_0$$

$$y_{n-1}\ y_{n-2}\ \ldots y_1\ y_0$$

and $z_{n-1}\ z_{n-2}\ \ldots z_1\ z_0$ respectively.

Where *x* and *y* denote the inputs and *z* denotes the output. The number of bits in *n*.

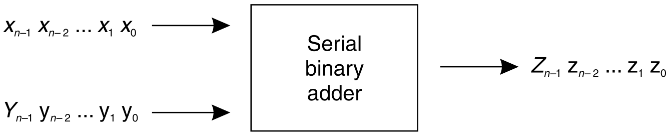

$x_{n-1}\ x_{n-2}\ \ldots\ x_1\ x_0$
$Y_{n-1}\ y_{n-2}\ \ldots\ y_1\ y_0$
Serial binary adder
$Z_{n-1}\ z_{n-2}\ \ldots\ z_1\ z_0$

Fig. 10.7 Serial binary adder

The least significant digits $x_1\ y_0$ of the inputs arrive simultaneously at the input terminals at time f_o.

If $M = (S, I, O, \delta, \lambda, S_0)$ is a finite state machine, a string γ over *I* is called an input string and corresponding there exists a string $P \in O$ called the output string.

A finite state machine transforms words into words. If I^* and O^* denote the sets of words on the input and output alphabets I and O respectively. We can describe an operation of the machine by the function

$$g: I^* \to O^*$$

Where the domain and range of g are infinite sets.

Consider the sequence $a = a_0, a_1, a_2, \ldots a_n \ldots$ of the input symbols, we can define a function δ_n as follows

$$\delta_n : S \times I^n \to S, \text{ such that}$$
$$S_n = \delta_n\ (s_0, a_0, a_1, \ldots a_{n-1})$$
$$= \delta\ (s_{n-1}\ (s_0, a_0, a_1, \ldots a_{n-1}), a_{n-1})$$

for the output symbols $O_0, O_1, O_2, \ldots$. We define the function for the output sequence as follows.

$$\lambda_n : S \times I^n \to S, \text{ such that}$$
$$O_{n-1} = \lambda_n\ (s_0, a_0, a_1, \ldots a_{n-1})$$

10.5 EQUIVALENCE OF FINITE STATE MACHINES

Finite state machines which produce, the same output sequence, when they are given the same input sequence are said to be equivalent. The internal structures of two equivalent machines may differ.

Definition 10.3: Let $\alpha = a_0, a_1, \ldots a_{n-1}$ be any input sequence containing n symbols and let β be any output symbol. Then mapping δ and λ can be extended as follows.

(*i*) $\delta\ (s_i, \alpha\beta) = \delta\ (\delta(s_i, \alpha)\beta)$

(*ii*) $\lambda\ (s_i, \alpha\beta) = \lambda\ (\delta(s_i, \alpha)\beta)$

(*iii*) $\delta\ (s_i, a_0, a_1, \ldots a_{n-1}) = \lambda\ (s_i, a_0)\ \lambda\ (s_i, a_0, a_1) \ldots \lambda\ (s_i, a_0, a_1, \ldots a_{n-1})$

We now introduce the notion of equivalent states.

Definition 10.4: Let $M = (S, I, O, \delta, \lambda)$ be a finite state machine. Two states $s_i, s_j \in S$ are said to be equivalent, written $s_i \equiv s_j$ and only if $\lambda\ (s_i, a) = \lambda\ (s_j, a)$ for every word $a \in I^*$.

The relation $\equiv$ is an equivalence relation.

Definition 10.5: Let $M = (S, I, O, \delta, \lambda)$ be a finite state machine. Then for some positive integer k, s_i is said to be k-equivalent to s_j, if $s_i \overset{k}{\equiv} s_j \Leftrightarrow \lambda\ (s_i, a) = \lambda\ (s_j, a)$ for all $|a| \le k$.

From the above definition it is clear that two states s_i and s_j are equivalent if they have the same output and if, for every input letter, their successors are $(k-1)$ equivalent only if $s_i \equiv s_j$, but not the converse. If s_i and s_j are k-equivalent and if s_j and s_h are k-equivalent, then s_i and s_h are also k-equivalent. The k-equivalence relation is also an equivalence relation and corresponding we can find a partition P_k, which is a k-partition in the set of states S whose k-equivalence is defined as follows.

$$[s_i]_k = \left\{ s_j : s_i \overset{k}{\equiv} s_j \right\} \text{ and } P_k = \bigcup_{s \in s} [s]_k$$

10.6 COVERING

Let $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ and $M = (S, I, O, \delta, \lambda)$ be two finite state machines.

If (*i*) M and $\overline{M}$ have the same input and output alphabet, and

(*ii*) There exists a function f: $S \to \overline{S}$ such that for every positive integer r,

$$\delta_r\ (s, a) = \overline{\delta}_r\ (f(s), a)$$

and $$\lambda_r\ (s, a) = \overline{\lambda}_r\ (f(s), a)\ \ \forall\ a \in I$$

then we say that $\overline{M}$ covers M.

Note: *If $\overline{M}$ covers M; then M covers $\overline{M}$.*

Lemma 10.1: The relation covering is reflexive and transitive.

Proof: Consider the finite state machine $M = (S, I, O, \delta, I)$ and the identity mapping f: $S \to S$.

We have $$\overline{S} = S, \overline{I} = I, \overline{O} = O, \overline{\delta} = \delta, \overline{\lambda} = \lambda$$

and $$\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$$

By definition $\overline{M}$ and M have the same input and output alphabet, also we have

$$\delta_r\ (s, a) = \delta_r\ (f(s), a) = \delta_r\ (f(s), a)\ \forall\ a \in I$$

$\therefore\ \overline{M}$ covers M i.e., M covers M, thus the relation covering is reflexive.

To prove that the relation covering is transitive, we suppose that $\overline{\overline{M}}$ covers $\overline{M}$ and $\overline{M}$ covers M where $\overline{\overline{M}} = (\overline{\overline{S}}, \overline{\overline{I}}, \overline{\overline{O}}, \overline{\overline{\delta}}, \overline{\overline{\lambda}})$, $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ and $M = (S, I, O, \delta, \lambda)$.

Now $\overline{\overline{M}}$ covers $\overline{M}$ $\Rightarrow \overline{\overline{I}} = \overline{I}, \overline{\overline{O}} = \overline{O}$ … (*i*)

and there exists a mapping β such that $\overline{\delta}_r\ (s, a) = \overline{\overline{\delta}}_r\ (\overline{f}(\overline{s}), a)$ ... (*ii*)

since $\overline{M}$ covers N, we have

$$\overline{I} = I, \overline{O} = O \qquad \text{… (}iii\text{)}$$

and there exists a mapping $f: S \to \overline{S}$ such that

$$\delta_r\ (s, a) = \overline{\delta}_r\ (f(s), a) \qquad \text{… (}iv\text{)}$$

from (*i*) and (*ii*)

$$\overline{\overline{I}} = \overline{I} = I \text{ and } \overline{\overline{O}} = \overline{O} = O \qquad \text{… (}v\text{)}$$

consider the mapping

$$\varnothing = \overline{f}\ o\ f : s \to \overline{s}$$

Now $$\begin{aligned}\delta_r\ (s, a) &= \overline{\delta}_r\ (f(s), a) \text{ (by (}iv\text{))}\\ &= \overline{\overline{\delta}}_r\ (\overline{f}\ (f(s), a)) \text{ (by (}ii\text{))}\\ &= \overline{\overline{\delta}}_r\ (\varnothing\ (s), a)\ \ (\varnothing = \overline{f}\ o\ f)\end{aligned}$$

$\therefore$ $$\delta_r\ (s, a) = \overline{\overline{\delta}}_r\ (\varnothing\ (s), a) \qquad \text{… (}vi\text{)}$$

from (*v*) and (*vi*)

$\overline{\overline{M}}$ covers M.

Hence the relation covering is transitive.

Theorem 10.1: Let M be a finite state machine and S be any state in M. if a and b are any words, then

(*i*) $\delta\ (s, ab) = \delta\ (\delta\ \ (s, a), b)$

(*ii*) $\lambda\ (s, ab) = \lambda\ (\delta\ \ (s, a), b)$

Proof: We prove the theorem by induction on the length of b.

Let $b = \alpha$

Then $\delta\ (s, a\alpha) = \delta(\delta(s, a), \alpha)$

Let us assume that the equation is true for any length n i.e.,

$$\delta\ (s, ab) = \delta(\delta(s, a), b)$$

We prove that it is true for $(n + 10)$ symbols also we can write $\delta\ (s, ab\alpha) = \delta(\delta(s, ab), \alpha)$. The right hand side of the above identity can be written as

$$\delta\ (\delta(s, ab)\alpha) = \delta(\delta(\delta(s, a), b), \alpha) \text{ (by induction)}$$

Taking $\overline{s} = \delta\ (s, a)$ we can write the right side of the equation as:

$$\begin{aligned}\delta(\delta(\delta(s, a), b), \alpha) &= \delta\ (\delta(\overline{s}, b)\alpha)\\ &= \delta\ (\overline{s}, b\alpha)\\ &= \delta\ (\delta(s, a), b\alpha)\end{aligned}$$

Hence the equation is true when length of b is $n + 1$. This completes proof of (*i*) similarly we can prove that

$$(\lambda, ab) = \lambda(\delta(s, a), b)$$

we shall now state the following theorem without proof.

Theorem 10.2: Let $M = (S, I, O, \delta, \lambda)$ be a finite state machine and $S_i, S_j \in S$. If $S_i \equiv S_j$, then for any input sequence a.

$$\delta(S_i, a) = \delta(S_j, a)$$

Theorem 10.3: Let P denote the partition generated by the equivalence relation $\equiv$ and corresponding to the k-equivalence relation $\overset{k}{\equiv}$, let p_k denote the k-partition on the set of states S. If for some positive integer k, $P_{k+1} = P_k$, then $P_k = P$ and conversely.

Theorem 10.4: Let $S_i, S_j \in S$ then $S_i \overset{k+1}{\equiv} S_j$ if and only if $S_i \overset{k}{\equiv} S_j$ and for all $a \in I$, $\delta(S_i, a) \overset{k}{\equiv} \delta(S_j, a)$.

We now define equivalent machines.

Definition 10.6: Two finite state machines $M = (S, I, O, \delta, \lambda)$ and $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ are said to be equivalent, if and only if for all $S_i \in S$, there exists an $S_j \in \overline{S}$ such that $S_i \equiv S_j$, and for all $S_j \in \overline{S}$, there exists an $S_i \in S$ such that $S_i \equiv S_j$.

If M and $\overline{M}$ are equivalent we write $M \equiv \overline{M}$.

Example 1: The finite state machines given in the two tables. Table 10.5 (*a*) and Table 10.5 (*b*) are equivalent.

Table 10.5 *Equivalent Machines*

(*a*)

I	δ		λ	
S	0	1	0	1
S_0	S_5	S_3	0	1
S_1	S_1	S_4	0	0
S_2	S_1	S_3	0	0
S_3	S_1	S_2	0	0
S_4	S_5	S_2	0	1
S_5	S_4	S_1	0	1

(*b*)

I	δ		λ	
S	0	1	0	1
S_0	S_5	S_3	0	1
S_1	S_1	S_4	0	0
S_2	S_1	S_3	0	0
S_3	S_1	S_2	0	0

Definition 10.7: A finite state machine $M = (S, I, O, \delta, \lambda)$ is said to be reduced if any only if $S_i \equiv S_j$ $\Rightarrow S_j \equiv S_i$ for all states $S_i, S_j \in S$.

Let the set of states S be partitioned in a set of equivalence classes $[s]$, such that $P = \cup\, [s]$. Let f be a function defined on P such that $f\,[s] = \overline{S}$, where $\overline{S}$ is an arbitrary fixed element of $[s]$.

Clearly $[s] = [\overline{s}]$.

We construct a reduced finite state machine $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ by taking

$$\overline{S} = \{\overline{s} : \lambda\ s\ (s \in S \text{ and } f\,([s])) = \overline{s}\},\quad \overline{O} = o \text{ and } \overline{I} = o.$$

The function $\overline{\delta}$ and $\overline{\lambda}$ are defined as follows:

$$\overline{\delta}\,(\overline{s}, a) = f\ [\delta\,(\overline{s}, a)]$$

and $\overline{\lambda}\,(\overline{s}, a) = \lambda\,(\overline{s}, a)$ where $\overline{s} \in s$ and also $\overline{s} \in \overline{S}$

10.7 FINITE STATE HOMOMORPHISM

Definition 10.8: Let $M = (S, I, O, \delta, \lambda)$ and $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ be two finite state machines. Let *f* be a mapping from *s* into $\overline{S}$ defined such that

$$f(\delta\ (s, a) = \overline{\delta}\ (f(s), a)$$

$\lambda\ (s, a) = \overline{\lambda}\ (f(s), a)$, for all $a \in I$ then *f* is called a finite state homomorphism.

Example: Let $M = (S, I, O, \delta, \lambda)$ and $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ be two finite state machines. Where $S = (a, b, c)$ and $\overline{S} = \{1, 2\}$. A mapping $f: S \to \overline{S}$ defined by $f(a) = 1, f(b) = 2, f(c) = 2$, is a homomorphism from *M* to $\overline{M}$.

Definition 10.9: Let $M = (S, I, O, \delta, \lambda)$ and $\overline{M} = (\overline{S}, \overline{I}, \overline{O}, \overline{\delta}, \overline{\lambda})$ denote two finite state machines and $f: S \to \overline{S}$ be a homomorphism. If *f* is one-one and into (a bijection), then *M* is said to be isomorphic to $\overline{M}$.

Solved Examples

Example 1: Let $M = (S, I, O, \delta, \lambda)$ be finite state machine with transition table appearing in Table 10.6. Find the set *S*, *I*, *O* and initial state S_0. Draw the state diagram. If $\alpha = a\ a\ b\ a\ b\ a\ a\ b\ b\ a\ b$ is an input word. Find the corresponding sequence of state and the output word.

Table 10.6

S \ I	δ		λ	
	a	b	a	b
S_0	S_1	S_2	x	y
S_1	S_3	S_1	y	z
S_2	S_1	S_0	z	x
S_3	S_0	S_2	z	x

Solution: We have $S = \{s_0, s_1, s_2, s_3\}$

$I = \{a, b\}$

$O = \{x, y, z\}$

and s_0 the initial state.

The transition diagram of *M* can be drawn as shown in Fig. 10.8.

Let β denote the sequence of states and *r* denote the output word, corresponding to $\alpha = a\ a\ b\ a\ b\ a\ a\ b\ b\ a\ b$.

S_0 is the initial state.

Starting with S_0, we move state to state by the arrows which are labelled and obtain the following sequence:

$$S_0 \xrightarrow{a/x} S_1 \xrightarrow{a/y} S_3 \xrightarrow{b/x} S_2 \xrightarrow{a/z} S_1 \xrightarrow{b/z} S_1 \xrightarrow{a/y} S_3 \xrightarrow{a/z} S_0 \xrightarrow{b/y} S_2 \xrightarrow{b/x} S_0 \xrightarrow{a/x} S_1 \xrightarrow{b/z} S_1$$

$\therefore\ \beta = s_0, s_1, s_3, s_2, s_1, s_1, s_3, s_0, s_2, s_0, s_1, s_1$ is the sequence of states and $r = x\,y\,x\,z\,z\,y\,z\,y\,x\,x\,z$ is the corresponding output word.

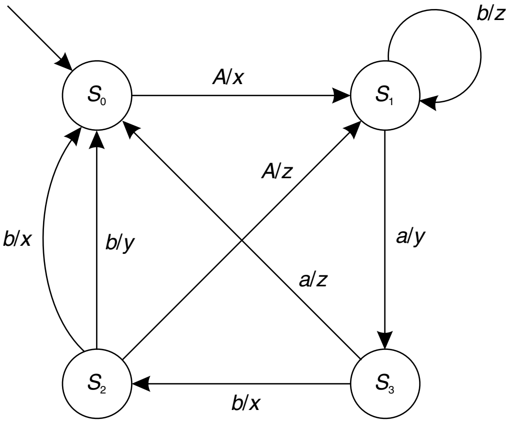


Fig. 10.8

Example 2: Let $I = \{a, b\}$, $O = \{0, 1\}$ and $S = \{s_0, s_1\}$. Define the functions $\delta : S \times I \to S$, and $\lambda : S \times I \to O$ by the rules given in Table 10.7 representing the finite state machine $M = (S, I, O, \delta, \lambda)$

Table 10.7

I / S	δ		λ	
	a	b	a	b
S_0	S_0	S_1	0	1
S_1	S_1	S_1	1	0

We can interpret Table 10.7 as follows:

$\delta\ (s_0, a) = s_0,\ \delta\ (s_1, a) = s_1,$

$\delta\ (s_0, b) = s_1,\ \delta\ (s_1, b) = s_1$

and $\lambda\ (s_0, a) = 0,\ \lambda\ (s_0, b) = 1,$

$\lambda\ (s_0, b) = 1,\ \lambda\ (s_0, b) = 0$

EXERCISE 10.1

1. Draw the state diagram for the finite state machine given by the Table on page 410.

I	*Input*		*Output*	
S	0	1	0	1
S_1	S_2	S_2	0	1
S_2	S_2	S_3	1	1
S_3	S_5	S_5	0	1
S_4	S_4	S_1	1	1
S_5	S_5	S_4	1	1

2. Draw the state diagram for the following finite state machine:

I	*Input* δ		*Output* λ	
S	0	1	0	1
a	*b*	*c*	0	0
b	*b*	*c*	0	0
c	*b*	*c*	0	1

3. A finite state machine is given by the following table. Draw its state diagram:

States	*Input* δ		*Output* λ	
S	0	1	0	1
a	*b*	*c*	0	1
b	*a*	*c*	0	1
c	*c*	*a*	1	0

4. Draw finite state diagram for the finite state machine given by the following table:

States	*Input*			*Output*
	0	1	2	
A	*A*	*B*	*C*	
B	*B*	*C*	*A*	
C	*C*	*A*	*B*	

5. A finite machine is given by the following table:

(*i*) Draw the transition diagram

(*ii*) Find the sequence of states (q)

(*iii*) Find the output word (r) for the input word $p = a\ b\ a\ a\ b$.

6. Show that there is no finite state machine which can do binary multiplication.

7. Draw a transition diagram for the finite state machine.

$$M = (S, I, O, \delta, \lambda), \text{ where}$$
$$I = (a, b), O = (0, 1), S = (s_0, s_1).$$

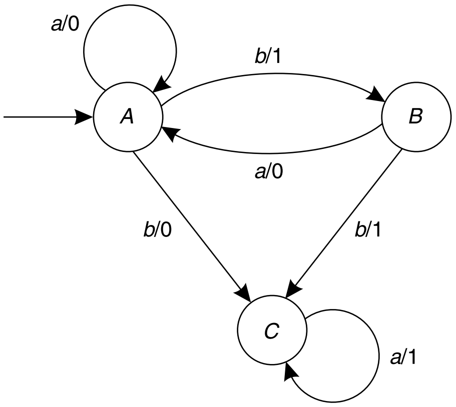
I / *S*	δ		λ	
	a	*b*	*a*	*b*
S_0	S_1	S_1	1	1
S_1	S_0	S_1	0	1

8.

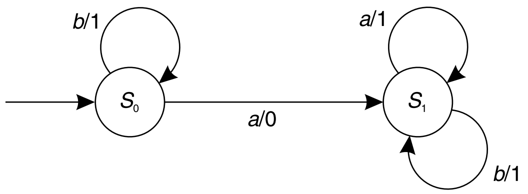
I / S	δ			λ		
	a	*b*	*c*	*a*	*b*	*c*
S_0	S_0	S_1	S_2	0	1	0
S_1	S_1	S_1	S_0	1	1	1
S_2	S_2	S_1	S_0	1	0	0

9. Find the sets S, I and O. Also find the initial state. Find the next state function. (δ) and the output function (λ) for each of the finite state machine.

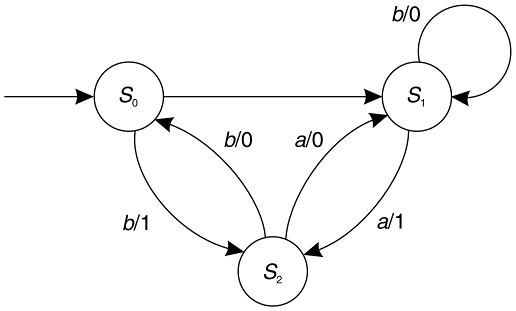
(*a*)



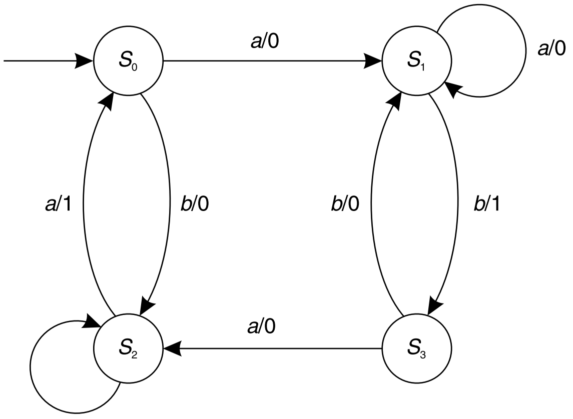
(*b*)


b/1
a/1
S_0
S_1
a/0
b/1

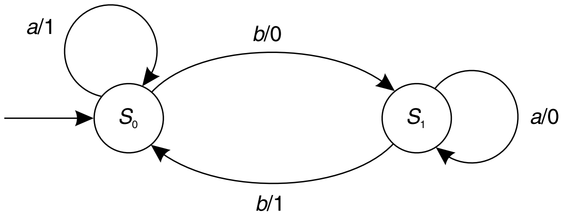
(*c*)


b/0
S_0
S_1
b/0
a/0
b/1
a/1
S_2

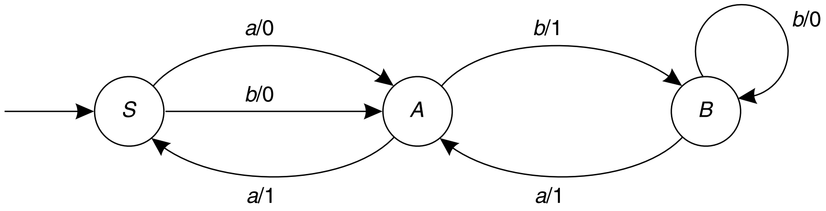
(*d*)


a/0
S_0
S_1
a/0
a/1
b/0
b/0
b/1
a/0
S_2
S_3

(*e*)


a/1
b/0
S_0
S_1
a/0
b/1

(*f*)


a/0
b/1
b/0
b/0
S
A
B
a/1
a/1

10. Let $M = (S, I, O, \delta, \lambda)$ be the finite state machine appearing in the table given below:

I	δ		λ	
S	*a*	*b*	*a*	*b*
S_0	S_2	S_1	*y*	*z*
S_1	S_2	S_3	*x*	*y*
S_2	S_2	S_1	*y*	*z*
S_3	S_3	S_0	*z*	*x*

Find *S*, *I* and *O*…. Draw the state diagram also find the output word *r* if the input word is α = *a a b b a b b a a b*.

10.8 FORMAL LANGUAGE, GRAMMAR

Formal languages one used to model natural languages and to communicate with computers. We begin with basic definitions.

10.8.1 Alphabet

Definition 10.10: A finite non-empty set of symbols that can be used to construct words is called an alphabet. It is denoted by *A*.

Each element of *A* is called a letter.

10.8.2 Word

Definition 10.11: A word (String) from an alphabet *A* is a finite sequence elements of *A* (i.e., letters of *A*)

Example 1: $w = a\ a\ b\ b\ a\ c$ is a word from the alphabet $A = (a, b, c)$

Example 2: $a_1\ a_2\ a_3\ a_4\ a_2\ a_2$ is string (word) on the alphabet (a_1, a_2, a_3, a_4)

Example 3: 2 7 3 0 1 7 8 is a string on the alphabet (0, 1, 2, 3, …, 9)

An empty word is an empty sequence from the alphabet *A*. It is denoted by λ.

If $a_1\ a_2\ a_3\ \ldots\ a_n$ is a string then the length of the string is *n*. If $1 \le i \le j \le n$, the string $a_{i+1}\ a_{i+2}\ \ldots\ a_j$ is called a segment of the string $a_1\ a_2\ a_3\ \ldots\ a_n$ length of a word.

Definition 10.12: The length of a word α is defined as the number of letters in its sequence of letters. It is denoted by $l(\alpha)$.

10.8.3 Subword

Definition 10.13: A word α is called a subword of the word *w* if $w = \alpha_0\ \alpha\ \alpha_1$ λ itself is a subword of *w*.

If $\alpha_0 = \lambda$ (the empty word), then α is called an initial segment of the word *w*.

Example: If $w = a\ b\ c$, then λ, a, b, c, ab, ac, bc, abc and are subwords of w.

10.8.4 Concatenation

Let $a_1\ a_2\ a_3 \ldots a_p$ and $b_1\ b_2\ b_3 \ldots b_q$ be strings. Then their concatenation is the string $a_1\ a_2\ a_3 \ldots a_p\ \ b_1\ b_2\ b_3 \ldots b_q$. It is of length $p \times q$.

The Concatenation is also called the join or product of strings.

Example 1: The Concatenation of 3215 and 7281 is 32157281.

Example 2: The concatenation of 'place' and 'ment' is 'placement'.

If α and β are strings, the concatenation of α and β is $\alpha\ \beta$. In general, it is not communicative i.e., $\alpha\ \beta \neq \beta\ \alpha$.

Example 3: If $\alpha = aabbac$ and $\beta = cabbca$ then $\alpha\beta = aabbaccabbca$ and $\beta\alpha = cabbcaaabbac$.

If A is an alphabet, then the finite set of all strings on A is denoted by A^*.

Formal Language

Definition 10.14: Let A be an alphabet A formal language L over A is a subset of A^*, the set of all strings over A.

Example: Let $A = (a, b)$ then $L = (a^m\ b^m : m > 0)$ is a language over A. It consists of all words beginning with one or more a's followed by the same number of b's.

Definition 10.15: It L_1 and L_2 are language over an alphabet A, then the language $L_1\ L_2$ over A is set of all words over A formed by concatenating words in L_1 with in L_2.

$$\therefore \qquad L_1\ L_2 = \{w{:}\alpha\,\beta \ \ where\ \ \alpha \in L_1,\ \beta \in L_2\}$$

Example 1: If $L_1 = (a, ab, a^2)$, $L_2 = (b, b^2, aba)$ then $L_1\ L_2 = (ab, ab^2, a^2ba, ab^2, ab^3, ababa, a^2b, a^2b^2, a^3ba)$

Let L be a language over A. We can write $L^0 = \{\lambda\}$, $L^1 = L$ and $L^{n+1} = L^n\ L$ (for $n > 0$)

Example 2: If $L\ (a, bc)$ then $L^3 = (aaa, aabc, abca, bcaa, bcbcbc, bcbca, bcabc, abcbc)$.

10.8.5 Grammar

Definition 10.16: A phase-structure grammar G (or simply a grammar) is (N, T, P, S) where

(*i*) N is a finite non-empty set whose elements are called variables (or non-terminals).

(*ii*) T is a finite non-empty set whose elements are called terminals where $N \cap T = \varnothing$.

(*iii*) A finite set P whose elements are $\alpha \to \beta$. When α and β are strings on $N\ U\ T$ (where α has atleast are symbol form N). The elements of P are called productions or production rules.

(*iv*) S is a special variable (non-terminal) called the start symbol. It is an element of N.

Example: Let $N = (S, A)$

$T = (a, b)$

$P = \{S \to bS,\ S \to aA,\ A \to bA,\ A \to b\}.$

Then $G = (N, T, P, S)$ is a grammar.

Language generated by a grammar.

Definition 10.17: If G is a grammar, then the set of all strings over T (set of terminals) derivable from S (start symbol). It is denoted by $L\,(G)$.

The elements of $L\,(G)$ are called sentences.

If $\alpha \to \beta$ is a production and $a\,\alpha\,b \in (N U T)^*$, we say that $a\,\beta\,b$ is directly from $a\,\alpha\,b$ and write.

$$a\,\alpha\,b \Rightarrow a\,\beta\,b \text{ or } a\,\alpha\,b \underset{G}{\Rightarrow} a\,\beta\,b \text{ or } \alpha \underset{G}{\Rightarrow} \beta$$

Example: Consider the grammar $G\,(N, T, P, S)$, where $N = (S, A)$, $T = (a, b)$,

$$P = (S \to bS,\ S \to aA,\ A \to bA,\ A \to b).$$

The string *ab A bb* can be derivable directly from *a A bb* by using the production $A \to bA$. It is written as $aAbb \Rightarrow abAbb$

Definition 10.18: If α and β are strings on $N\,U\,T$ then we say that α derive β if $\alpha \overset{*}{\underset{G}{\Rightarrow}} \beta$, where $\overset{*}{\underset{G}{\Rightarrow}}$ denotes the reflexive-transitive closure of the relation $\underset{G}{\Rightarrow}$ in $(N\,U\,T)^*$

Example 1: Consider the grammar $G = (N, T, P, S)$, where $N = (S, A, a, b)$ $T = (a, b)$, and $P = (S \to aA,\ S \to b,\ A \to aa)$ with S as the start symbol.

Solution: $L\,(G)$ can be derived as follows:

We start with S.

$$\begin{aligned} S &\Rightarrow aA \\ &\Rightarrow aaa \end{aligned}$$

we can also use $S \to b$ to derive b

$$\therefore \qquad L(G) = \{b,\ aaa\}$$

Example 2: Show that the language $L(G) = \{a^n\ b^n\ c^n : n \geq 1\}$ can be generated by $G = (N, T, P, S)$ where $N = (S, B, C)$, $T = (a, b, c)$

$P = (S \to asBc,\ S \to aBc,\ cb \to Bc,\ aB \to ab,\ bB \to bb,\ bc \to bc,\ cc \to cc)$ and S is the starting symbol.

Solution: We derive the string *abc* as follows.

$$\begin{aligned} S &\Rightarrow aBc \\ &\Rightarrow abc \\ &\Rightarrow abc \end{aligned}$$

And the string a^2 b^2 c^2 can be derived from S as follows.

$$\begin{aligned} S &\Rightarrow aSbc \\ &\Rightarrow aaBcBc \\ &\Rightarrow aaBBcc \\ &\Rightarrow aabBcc \\ &\Rightarrow aabbcc \\ &\Rightarrow aabbcc \\ &\Rightarrow aabbcc \end{aligned}$$

For n = 1 and n = 2, we have proved that a^n b^n c^n can be derived from S, which shows that $L(G) = \{a^n\, b^n\, c^n : n \geq 1\}$ is generated by G.

Example 3: Consider the grammar G = (N, T, P, S), where N = (A, B, S), T = (a, b), $P = \{S \rightarrow aB,\ B \rightarrow b,\ B \rightarrow bA,\ A \rightarrow aB\}$ and S is the starting symbol.

Solution: We prove by giving example. We derive ab, (n = 1) and $(ab)^2$, (n = 2)

$$\begin{aligned} S &\Rightarrow aB \\ &\Rightarrow ab \end{aligned}$$

$\therefore$ $$S \Rightarrow (ab)^1$$

and $$\begin{aligned} S &\Rightarrow aB \\ &\Rightarrow abA \\ &\Rightarrow abaB \\ &\Rightarrow abab \\ &\Rightarrow (ab)(ab) \end{aligned}$$

$\therefore$ L (G) can be generated by G.

10.8.6 Types of Grammars

Definition 10.19: A grammar G which has no restriction on its production is called type zero grammar. It is denoted by the symbol T_0.

Definition 10.20: A grammar G is said to be of Type 1, every production $\alpha \rightarrow \beta$ has the property that $l(\alpha) \leq l(\beta)$. It is denoted by T_1.

Definition 10.21: A grammar G is said to be of Type 2, if every production is of the form $A \rightarrow \beta$, where $\beta \in N$.

It is denoted by T_2 and is called contex-free grammar.

Definition 10.22: A grammar G is said to be of the Type 3, if $l(\alpha) \leq l(\beta)$, $\alpha \in N$ and β was the form $a\ b$ or a where $a \in T$ and $B \in N$. It is denoted by T_3 and is called regular grammar.

10.8.7 Derivation Trees

Derivations can be displayed as trees. The pictures representing derivations are called derivation tree (or generation trees). It is also called a parse tree. The vertices of a derivation tree are labeled with terminal or variable symbols of the grammar. If an interior vertex v is labeled A and the children are labeled $v_1, v_2, \ldots, v_p$ from the left then $A \rightarrow v_1\ v_2 \ldots v_p$ must be a production.

Figure 10.9 given below is a Parse Tree.

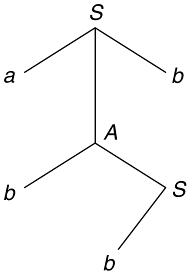


Fig. 10.9 Parse Tree

Example: Draw a derivation tree for the string $a^2\ b^2\ c$ in the grammar.

$$G = (N, T, P, S) \text{ where}$$
$$N = (\ v_0, v_1), T = (a, b, c), S = v_0$$
$$P = \{v_0 \rightarrow a\,v_0 \,/\, bv_1,\ v_1 \rightarrow b\,v_1 \,/\, c\}$$

Solution: For the derivation $a^2\ b^2\ c$

$$v_0 \Rightarrow a\,v_0 \Rightarrow a\,a\,v_0 \Rightarrow a\,a\,b\,v_1$$
$$\Rightarrow a\,a\,b\,b\,v_1$$
$$\Rightarrow a\,a\,b\,b\,c$$

The corresponding derivation is as shown in figure below (Fig. 10.10)

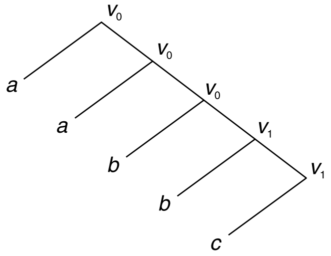


Fig. 10.10 Derivation tree

10.9 FINITE AUTOMATA

A mathematical model of system, with discrete inputs and outputs is called finite automation. It can transform, energy, material and information and is used for performing certain functions without the direct participation of a human being automatic packing machine is an example of a finite automatic.

Definition 10.23: A finite automation $A = (S, I, \delta, S_0, F)$ is a finite-state machine in which

(*i*) S is a finite set of states.

(*ii*) I is a finite set of inputs called input alphabet.

(*iii*) δ is a function which maps $S \times I$ into S and is usually called transition function.

(*iv*) $S_0 \in S$ is the initial state.

(*v*) $F \subseteq S$ is set of final states.

Note: The finite automation defined above is also called discrete finite automation (DFA).

The state diagram of a finite automation (FA) is a directed graph in which the nodes (vertices) correspond to the states of finite automation. The directed edge of the graph indicate the transition of a state. The edges in the diagram are labeled with input/output.

The initial state in the transition diagram is indicated by the arrow labeled 'start' and final state is indicated by a 'double circle'.

The block diagram of a finite automation is shown in Fig. 10.11.

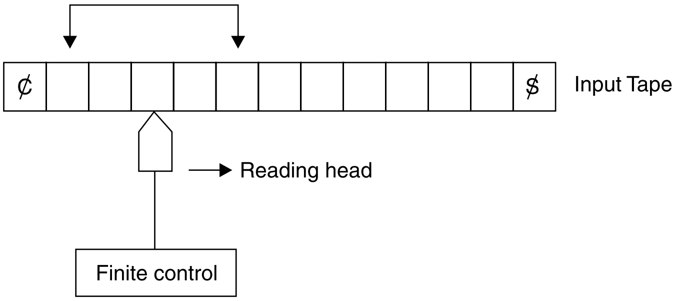


Fig. 10.11 Block diagram of a finite automation

The various components of a finite automation (FA) are explained as follows:

(*i*) *Input Tape:* It is divided into square, each square containing a single symbol from the input alphabet *I*. The end squares of the input tape contain end-markers ⊄ at the left end and $ at the right end to show that the tape is of finite length.

(*ii*) *Reading Head:* The reading head examines only one square (one symbol) at a time and can move one square either to the left or to the right.

(*iii*) *Finite Control:* It is some states from *S*, reading a sequence of symbols from *I* written on a tape.

Properties of Transition Functions

1. The state of a system can be changed only by an input symbol.
2. $\delta(s, a, \alpha) = \delta(\delta(s, a), \delta)$ and $\delta(s, \alpha, a) = \delta(\delta(s, \alpha), a)$ for all strings α and input symbols a.

Acceptability by a Finite Automation

A string α is said be accepted by a finite automation $A = (S, I, \delta, S_0, F)$ if $\delta(S_0, \alpha) = \beta$ for some $\beta \in F$. The language accepted by A is the set $\{\alpha : \delta(S_0, \alpha) \in F\}$. It is denoted by $L(A)$.

A language is a regular set if it is the set accepted by some finite automation.

Example 1: Draw the transition diagram of the finite state machine defined by the table given below:

Table 10.8

I / S	δ		λ	
	a	b	a	b
S_0	S_1	S_0	1	0
S_1	S_2	S_0	1	0
S_2	S_2	S_0	1	0

The finite state machine has S_1 and S_2 as the accepting starts. The lost output is 1. Hence, it is finite automation. The transition diagram of the automation can be drawn as shown in Fig. 10.12 (note that output symbols are omitted in the diagram).

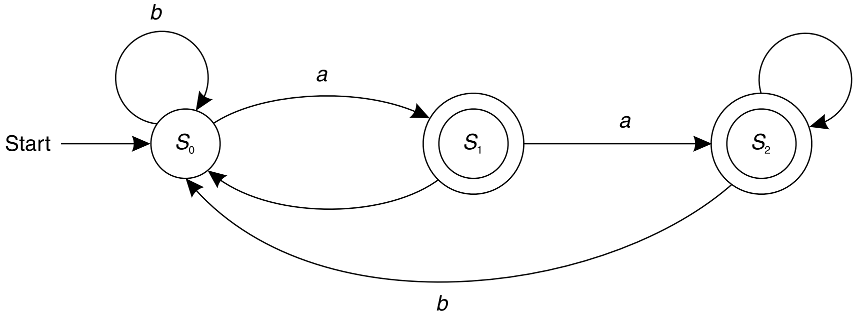


Fig. 10.12 Transition diagram

Example 2: Consider the transition diagram of Fig. 10.13. Construct the state table and give the entire sequence of states for the input string 110101.

Solution: The finite automation (FA) shown in Fig. 10.13 is $A = (S, I, \delta, S_0, F)$

Where $S = (S_0, S_1, S_2, S_3)$

$I = (0, 1)$

$F = (S_0)$

and δ is defined by

$$\delta(q_1, 0) = q_3, \quad \delta(q_1, 1) = q_0$$
$$\delta(q_2, 0) = q_0, \quad \delta(q_2, 1) = q_3$$
$$\delta(q_3, 0) = q_1, \quad \delta(q_3, 1) = q_2$$

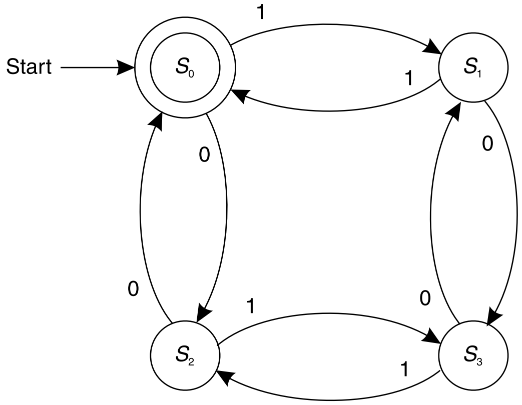


Fig. 10.13

The transition table can be constructed as shown in table:

Table 10.9

States	*Inputs*	
	0	*1*
S_0	S_2	S_1
S_1	S_3	S_0
S_2	S_0	S_3
S_3	S_1	S_2

Consider the string 110101

We have

$$\delta(S_0, 11) = \delta(\delta(S_0, 1), 1) = \delta(S_1, 1) = S_0$$

$$\delta(S_0, 0) = S_2$$

$$\Rightarrow \delta(S_0, 110) = \delta(\delta(S_0, 11), 0) = \delta(S_0, 0) = S_2$$

$$\Rightarrow \delta(S_0, 1101) = \delta(\delta(S_0, 110), 1)$$

$$= \delta(S_2, 1)$$

$$= S_3$$

$$\Rightarrow \delta(S_0, 11010) = \delta(\delta(S_0, 1101), 0)$$

$$= \delta(S_3, 0)$$

$$= S_1$$

$$\begin{aligned}\Rightarrow \delta(S_0, 110101) &= \delta(\delta(S_0, 11010), 1)\\ &= \delta(S_1, 1)\\ &= S_0\end{aligned}$$

The entire sequence of states is

$$S_0^1 \to S_1^1 \to S_0^0 \to S_2^1 \to S_3^0 \to S_1^1 \to S_0$$

Thus ten string 110101 is in A.

Example 3: Consider the finite automation $A = (S, I, \delta, S_0, F)$

where $S = (S_0, S_1, S_2)$

$I = (a, b)$

$F = (S_0, S_1)$

and $\delta(S_0, a) = S_0, \quad \delta(S_1, a) = S_0, \quad \delta(S_2, a) = S_2$

$\delta(S_0, b) = S_1, \quad \delta(S_1, b) = S_2, \quad \delta(S_2, b) = S_2$

Show that the word $\alpha = ababba$ is not accepted by A.

Solution:

$$\begin{aligned}\delta(S_0, a) &= S_0\\ \Rightarrow \delta(S_0, ab) &= \delta(\delta(S_0, a), b)\\ &= \delta(S_0, b) = S_1\\ \Rightarrow \delta(S_0, aba) &= \delta(\delta(S_0, ab), a)\\ &= \delta(S_1, a)\\ &= S_0\\ \Rightarrow \delta(S_0, abab) &= \delta(\delta(S_0, aba), b)\\ &= \delta(S_0, b)\\ &= S_1\\ \Rightarrow \delta(S_0, ababb) &= \delta(\delta(S_0, abab), b)\\ &= \delta(S_1, b)\\ &= S_2\\ \Rightarrow \delta(S_0, ababba) &= \delta(\delta(S_0, ababba), a)\\ &= \delta(S_2, a)\\ &= S_2\end{aligned}$$

The find state (accepting state) is not in F.

The word α is not accepted by A.

Example 4: Draw the transition diagram to represent the finite automation $A = (S, I, \delta, S_0, F)$, where $S = (S_0, S_1, S_2, S_3)$, $I = (a, b)$, $F = (S_0)$, and F is defined by

$$\delta(S_0, a) = S_2, \quad \delta(S_3, a) = S_1,$$

$$\delta(S_1, a) = S_3, \quad \delta(S_0, b) = S_1, \quad \delta(S_2, b) = S_3$$

$$\delta(S_2, a) = S_0, \quad \delta(S_1, b) = S_0, \quad \delta(S_3, b) = S_2$$

Solution: The transition diagram representing the finite automation is a shown in Fig. 10.14.

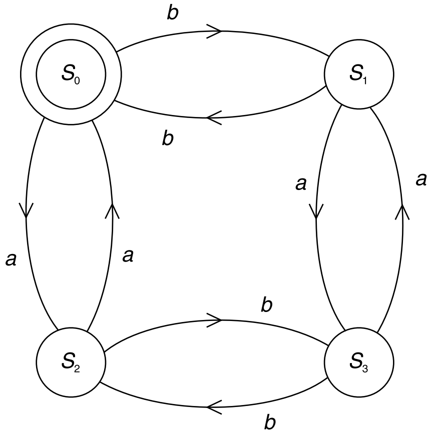
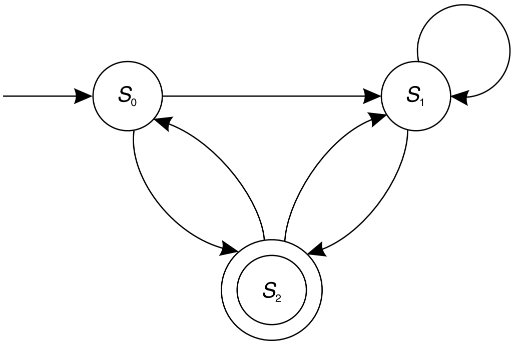


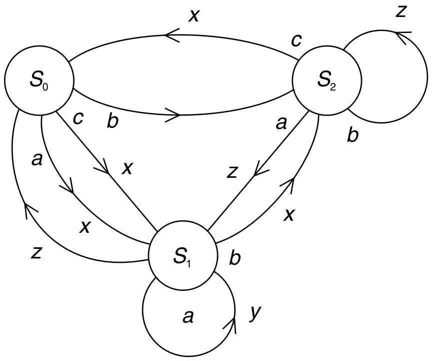
Fig. 10.14

EXERCISE 10.2

1. Define finite automation.
2. Design a finite automation that accepts precisely those strings over (a, b) that contain an odd number of a's.
3. Draw the transition diagram of the finite automation of the figure given below as a transition diagram of finite state machine.



4. Find the finite state automation A with the input symbols a, b, c and output symbols x, y, z and state diagram is given below:



10.10 NON-DETERMINISTIC FINITE AUTOMATION (NDFA)

A non-deterministic finite automation (NDFA) is a 5-tuple $A^1 = (S, I, \delta^1, S_0^1, F^1)$ where

(*i*) S is a finite set of states.

(*ii*) I is a finite set of inputs.

(*iii*) δ^1 is a transition function mapping from $S \times I$ into 2^s (i.e., P (S), power set of S).

(*iv*) $S_0^1 \in S$ is the initial state.

(*v*) $F^1 \subseteq S$ is the set of find states.

Note: The out come for a non-deterministic finite automation is a subset of S.

Example 1: Consider the NDFA shown in table below with S_2 and S_3 as the find states. Draw the state diagram for the NDFA.

Table 10.10

States	*Inputs*	
	0	*1*
S_0	(S_0, S_3)	(S_0, S_1)
S_1	$\varnothing$	(S_2)
S_2	(S_2)	(S_2)
S_3	(S_4)	$\varnothing$
S_4	(S_4)	(S_4)

Solution: The transition diagram for the NDFA is given below:

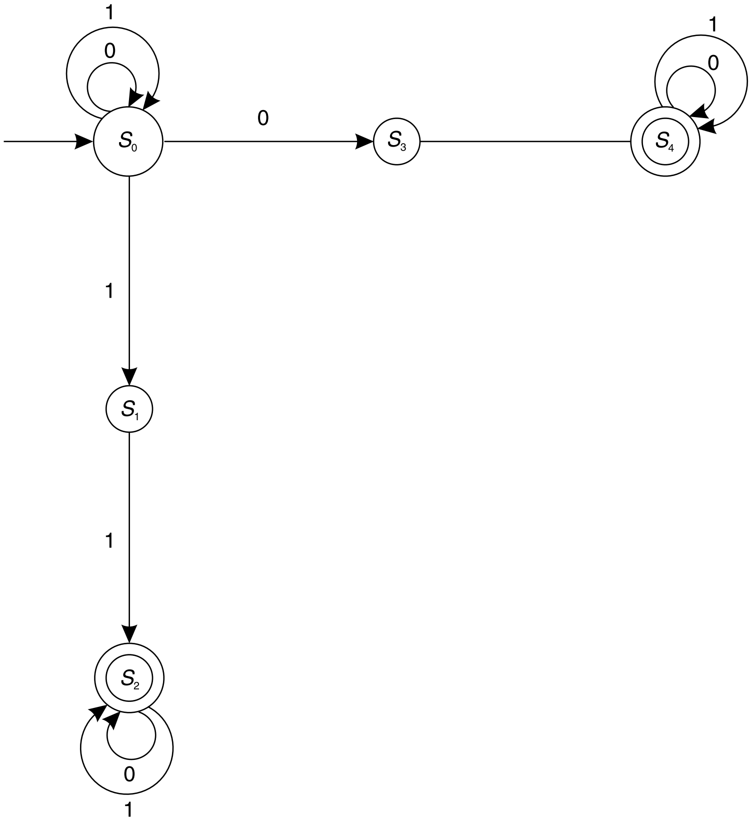


Fig. 10.15 The transition diagram for a NDFA

Equivalence of DFA and NDFA

Let $A = (S, I, \delta, S_0, F)$ denote a DFA and

$A^1 = (S, I, \delta^1, S_0, F^1)$ denote a NDFA.

By defining $\delta^1 (S, \alpha) = \{\delta (S, \alpha)\}$, we can make DFA, and the NDFA equivalent finite state machines that is, for every NDFA we can construct an equivalent DFA.

Example 2: Construct a DFA equivalent to $A^1 = (\{S_0, S_1, S_2, S_3\}, \{0, 1\}, \{S_3\})$, where the transition function is given by the table below.

Table 10.11

States	*Inputs*	
	a	*b*
S_0	S_0, S_1	S_0
S_1	S_2	S_1
S_2	S_3	S_3
$\textcircled{S_3}$		S_2

Solution: We have $S = (S_0, S_1, S_2, S_3)$

The DFA equivalent to A^1 is given in table below:

Table 10.12

States	*Inputs*	
	a	*b*
(S_0)	(S_0, S_1)	(S_0)
(S_0, S_1)	(S_0, S_1, S_2)	(S_0, S_1)
(S_0, S_1, S_2)	(S_0, S_1, S_2, S_3)	(S_0, S_1, S_3)
(S_0, S_1, S_3)	(S_0, S_1, S_2)	(S_0, S_1, S_2)
(S_0, S_1, S_2, S_3)	(S_0, S_1, S_2, S_3)	(S_0, S_1, S_2, S_3)

Example 3: Construct a deterministic automation equivalent to:

$$A = (\{S_0, S_1\}, \{0, 1\}, \delta, S_0, \{S_0\})$$

where the transition function δ is given by the table below:

Table 10.13

States	*Inputs*	
	0	*1*
S_0	S_0	S_1
S_1	S_1	S_0, S_1

Solution: Let $S = (S_0, S_1)$ then $2^s = P(S) = \{\varnothing, \{S_0\}, \{S_1\}, \{S_0, S_1\}\}$ for the DFA equivalent to A^1 we have (S_0) as the initial state and (S_0), (S_0, S_1) as the final states.

The equivalent can be constructed as shown in Table 10.14.

Table 10.14

States	*Inputs*	
	a	*b*
∅	∅	∅
(S_0)	(S_0)	(S_1)
(S_1)	(S_1)	(S_0, S_1)
(S_0, S_1)	(S_0, S_1)	(S_0, S_1)

Example 4: Construct a DFA from the NDFA $A^1 = (\{S_0, S_1, S_2\}, \{a, b\}, \delta^1, S_0, F^1)$, where $F = (S_1)$ and the transition function is given by the following table:

Table 10.15

	Inputs	
δ'	*a*	*b*
S_0	(S_1, S_2)	ϕ
S_1	ϕ	(S_2)
S_2	ϕ	(S_2)

Solution: We have $S = \{S_0, S_1, S_2\}$

$$\therefore \qquad P(S) = 2^S = \{\phi \{S_0\}, \{S_1\}, \{S_2\}, \{S_0, S_2\}, \{S_1, S_2\}, \{S_0, S_1, S_2\}\}$$

$$S_0^1 = \{S_0\}$$

$$F^1 = \{(S_1), (S_0, S_1), (S_1, S_2), (S_0, S_1, S_2)\}$$

The equivalent transition function is defined as follows:

Table 10.16

δ^1	*a*	*b*
ϕ	ϕ	ϕ
(S_0)	(S, S_2)	ϕ
(S_1)	ϕ	(S_2)
(S_2)	ϕ	(S_2)
(S_0, S_1)	(S_1, S_0)	(S_2)
(S_0, S_2)	(S_1, S_2)	(S_2)
(S_1, S_2)	ϕ	(S_2)
(S_0, S_1, S_2)	(S_1, S_2)	(S_2)

10.11 FINITE AUTOMATA WITH OUTPUTS

In this section, we discuss, two different models namely, (1) The Moore machine, and (2) The Mealy machine the Moore machine is restricted model and is associated with the state and in the case of Mealy machine, the output is associated with the transition. The machines are defined as follows.

10.11.1 Moore Machine

A Moore machine is a six tuple $(S, I, \Delta, \delta, \lambda, S_0)$, where

(*i*) S is the finite set of states.

(*ii*) I is the input alphabet.

(*iii*) Δ is the output alphabet.

(*iv*) δ is the transition function from $I \times S$ into S.

(*v*) λ is the output function mapping S into Δ.

(*vi*) S_0 is the initial state.

If $\alpha_1\ \alpha_2\ \alpha_3 \ldots \alpha_n,\ n \geq 0$ denotes an input, then the output of the machine is given by $\lambda(S_0)\ \lambda(S_1)\ \lambda(S_2) \ldots \lambda(S_n)$, where $S_0, S_1, S_2, \ldots S_n$ is the sequence of states such that

$$\delta(S_{i-1}, \alpha_i) = S_i \text{ for } 1 \leq i \leq n$$

For a Moore machine if the input string is of length n, the output string is of the length $n + 1$.

Example: The table given below is a Moore machine:

Table 10.17

Present state	*Next state* δ		*Output* λ
	0	1	
S_0	S_3	S_1	0
S_1	S_1	S_2	1
S_2	S_2	S_3	0
S_3	S_3	S_2	0

If α is the input string, then the transition states is given by

$$S_0 \rightarrow S_1 \rightarrow S_1 \rightarrow S_2 \rightarrow S_3$$

The output string is 01100 and the output is $\lambda(S_0) = 0$

10.11.2 Mealy Machine

A Mealy machine is a six-tuple $(S, I, \Delta, \delta, \lambda^1, S_0)$, where (*i*) S is a finite set of states.

(*ii*) I is the input alphabet.

(*iii*) Δ is the output alphabet.

(*iv*) δ is the transition function $I \times S$ into S.

(*v*) λ^1 is the output function mapping S into Δ.

(*vi*) S_0 is the initial state.

For a Mealy machine if the input string is of length n, the output string is also of the length n. The table given below is an example of Mealy machine:

Table 10.18

	Next State			
Present	$\alpha = 0$		$\alpha = 1$	
state	*State*	*Output*	*State*	*Output*
S_0	S_3	0	S_1	1
S_1	S_1	1	S_2	0
S_2	S_2	0	S_3	0
S_3	S_3	0	S_0	0

We can construct a Mealy machine which is equivalent to the Moore machine

(*i*) By defining $\lambda^1 (S, \alpha) = \lambda (\bar{\delta} (S, \alpha))$ for all states S and input symbols α.

(*ii*) By taking the transition function the same as that of the Moore machine.

Bibliography

Allenby R. B. J. T. (1991), *Rings, Fields and Graphs*.

Appel K. and W. Hanken, “Every planar map is four-colourable” Illinois, *J. Maths*, 21 (1977).

Barker S. F., *The Elements of Logic*, 5th edition, McGraw-Hill, New York, 1989.

Birshoff G. and Maclane, S., “A Survey of Modern Algebra”, 3rd edition, MacMillan.

Brualdi R. A., *Introductory Combinations*, Prentice-Hall, 1999.

Chartrand G. and L. Lesniak, *Graphs and Digraphs*, Woods Worth Behnont Calif, 1986.

Copi I. M. and C. Cohen, *Introduction to Logic*, 10th edition, Prentice-Hall. 1998.

Deo N., *Graph Theory and Application to Engineering and Computer Science*, Prentice-Hall, Englewood Cliffs N. J., 1974.

Edgar W. J., *The Elements of Logic*, SRA Chicago, 1989.

Even S., *Graph Algorithm*, Computer Science Press, Rockville. Md., 1979.

Gallier J. H., *Logic for Computer Science*, Harper & Row, New York, 1986.

Gould R., *Graph Theory*, Benjamim, 1988.

Halmos P. R., *Lectures on Boolean Algebras*, Springer-Verlog, 1970.

Harary F., *Graphs Theory*, Addition–Wesley Reading, Mass., 1969.

Liu C. L., *Elements of Discrete Mathematics*, 2nd edition, McGraw-Hill, 1985.

Mendelson E., *Boolean Algebra and Switching Circuits*, Schawn, New York, 1970.

ORE O., *Graphs and their Uses*, Mathematical Association of America, Washington, D. C., 1963.

Roberts F. S., *Applied Combinations*, Prentice-Hall, Englewood Cliffs, N. J., 1984.

Stoll R. E., *Set Theory and Logic*, Dover, New York, 1979.

Tucker A., *Applied Combinations*, 3rd edition, Wiley, New York, 1995.

West D., *Introduction to Graph Theory*, 2nd edition, Prentice-Hall, Upper Saddle River, N. J., 2000.

Wilson R. J., *Introduction to Graph Theory*, 4th edition, Addison–Wesley Reading, Mass, 1996.

Index

Absorption laws 140
Ackermann function 105
Acyclic graph 274
Adder 173
Adjacency matrix 238
Algorithm:
  Kruskals 288
  prims 291
Ancestor 297
AND gate 166
Anti-symmetric relation 70
Arborescence 342
Axiom of choice 128

Balanced binary tree 238
Bijection 82
Biconditional 9
Binary operation 347
Binary relation 69, 75
B-Tree 299
Binary tree: 294
  balanced 298
  left child in 297
  right child in 297
Binomial theorem 209
Bipartite graph 263
Bit 138
Boolean algebra 137
  absorption laws for 140
  associative laws for 137
  commutative laws for 137
  complement laws for 138
  De Morgan's laws for 141
  distributive laws for 138
  involution law 140
Boolean expression 143
Boolean functions: 143
  conjunctive normal form of 144
  disjunctive normal form of 144
Bounded lattice 130

Cardinality 63
Cartesian product 65
Centre of a group 370
Chain 118
Child 297
  left 297
  right 297
Circuit:
  decorder 175
  full-adder 174
  half-adder 174
  switching 163
Circular permutations 191
Closed path 250
Combinations 195
Commutative laws:
  for Boolean algebra 137
  for sets 52
Comparable sets 64
Complement of a set 54
Complement of a graph 257

Composition
 of functions 82
Concatenation 420
Connectivity 258
Conjunction 2
Conjunctive normal form 21
Connected graph 258
Connectives 2
Connectivity 277
Contingency 12
Contradiction 12
Comparability 118
Cosets 370
Cover of an element 122
Cut edge 275
Cut vertex 275
Cycle
 Hamiltonian 319

Decoder 175
Degree of a vertex 222
Derivation tree 423
Difference of sets 54
Digraph 219
Directed graph 219
Direct proof 31
Disjoint sets 47
Disjunction 3
Disjunctive normal form 20
Distance between vertices 282
Distributive laws:
 for Boolean algebra 138
 for sets 53
Double negation 6
Dual graph 310
Dual order 119
Duality principle 15

Edge: 218
 connectivity 277
 directed 219
 series 237

Empty set 46
Encoder 177
Equal sets 46
Equivalence relation 70
Equivalence classes 73
Euler 218
Euler's formula for graphs
Exclusive OR 168
Existential quantifier 29
Expression tree 294

Factorial function 187
Finite automata 423
Finite set 47
Finite state machines 404
Forest 274
Formal language 420
Function 90
 absolute value 103
 Ackermann's 105
 bijection 82
 Boolean 143
 ceiling 102
 constant 83
 characteristic 86
 floor 102
 generating 108
 logarithmic 103
 one-to-one 85
 onto 82
 primitive recursive 103

Girth 279
Grammar 420
Graph 218
 acyclic 274
 adjacency matrix 238
 bipartite 263
 colouring of 327
 complement 257
 complete 225
 complete bipartite 263

connected 258
cycle 262
directed 219
dual 310
Euler 314
Euler's formula 304
finite 221
hamiltonian 319
Homeomorphic 309
incidence matrix of
isomorphic 265
multi 220
path 262
planar 303
polyhedral 304
self loop 219
separable 276
simple 220
simple path 250
star 263
subgraph of 252
thickness of 312
weighted 221
wheel 262
Group
Abelian 354
cyclic group 377
semigroup 351
subgroup of 368
finite 354
normal subgroup 380
quotient 381
Groupoid 351

Hashing function 106
Hasse diagram 118

Incidence matrix 240
Indegree 221
Infimum 225
Intersection of sets 54
Isolated vertex 223
Isomorphism 265, 374

Karnaugh map 150
K-regular graph 224
Kruskals algorithm 228
Kuratowski's graphs 307

Labelled graph 223
Lattice 128
Least element 122
Level of a vertex 293
Lexicographic order 121
Linked representation 240
Literal 144
Logically equivalent 12
Loop 219
Lower bound 124

Mappng inverse 83
Matrix
adjacency 238
incidence 240
Maxterm 144
Maximum degree 223
Minimum degree 223
Minterm 144
Multigraph 220
Mux 177

NAND-gate 167
Negation 3
NOR-gate 167
Normal forms 20
NOT-gate 167
Null graph 220
Null set 46

Order of an element 366
Order of a graph 225
OR gate 166
Out degree of a vertex 222

Partial function 103
Partial order 118
Partitions 200

Path 249
- closed 250
- length 250
- simple 250

Pendant vertex 224
Permutation 187
Permutation groups 382
Pigeonhole principle 206
- extended 207

Planar graph 303
Power set 47
Prims algorithm 291
Primitive recursion 104
Proof: by cases 34
- by contradition 32
- by contraposition 31
- by counter example 34

Proposition 4
- biconditional 9
- compound 2
- conditional 9
- conjunction of 2
- contradiction 12
- contrapositive 10
- negation of 3

Pseudo graph 221
Power set 47

Quantifier:
- existential 29
- universal 29

Quotient group 381

r-arrangement 187
Range
- of a function 90
- of a relation 69

r-combination 195
Recurrence relation 100
Recursion 100
Relation 69
- asymmetric 72
- anti-symmetric 70
- compatible 72
- complementary 73
- composition of 84
- digraph of 80
- domain of 70
- equivalence 70
- inverse 71
- irreflexive 72
- partial order 118
- recurrence 100, 110
- reflexive 70
- symmetric 70
- total order 118
- transitive 70
- transitive closure of
- universal 72

Set 44
- cartesian product
- complement of 54
- difference of 54
- disjoint 47
- finite 47
- intersection of 51
- null 46
- power 47
- proper subset of 45
- singleton 46
- subset of 45
- super 46
- union of 48
- universal 42
- Venn diagram 58

Simple path 251
Size of a graph 225
Spanning tree: 285
- minimal 287

String 101
Subgroup 368
- Superset 46

Symmetric difference 57
Symmetric relation 70

Tautology 12
Terminal vertex 250
Total order 118
Transposition 386
Transitive extension 77
    closure 77
Tree 280
    binary 294
    centre 284
    directed 281
    expression 294
    height balanced 298
    radius 283
    rooted 292
    spanning 285

Union of graphs 254
Union of sets 48
Universal set 47
Upper bound 124

Vertex
    adjacent 219
    degree of 222
    indegree of 221
    outdegree of 222
    eccentricity 284

Walk 250
Well formed formula 11
Well-ordered set 127
Weighted graph 221
Wheel graph 262