PG Sc IT S3 01
Exam. Code:M3 IDM

Introduction to Discrete Mathematics and Formal Languages and Automata

SEMESTER-III

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

BLOCK-1

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Prof. Anjana Kakati Mahanta, Gauhati University

Prof. (Retd.) Pranhari Talukdar, Gauhati University

Dr. Jyotiprakash Goswami, Assam Engineering College

Prof. Sikhar Kumar Sarma, Gauhati University

Programme Coordinator

Dr. Ridip Dev Choudhury, KKHSOU

Course Coordinator

Mr. Harekrishna Deka, KKHSOU

Dr.Nabankur Pathak,KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
1, 2, 4, 6, 7, 8	Dr. Dilip Kumar Sarma,Cotton University
3, 5	Mr.Harekrishna Deka, KKHSOU

Editorial Team

Content : Dr. Parag Kumar Dev, Cotton University

Structue, Format & Graphics: Harekrishna Deka, KKHSOU

January, 2022 **ISBN NO :**

This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 License (international): http://creativecommons.org/licenses/by-nc-sa/4.0/

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

Headquarters : Patgaon, Rani Gate, Guwahati - 781017
City Office : NH 37,Resham Nagar,Khanapara,Guwahati-781022; Web: www.kkhsou.in

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

Introduction to Discrete Mathematics and Formal Languages and Automata

Block-1

DETAILED SYLLABUS

		Pages
UNIT 1 :	**SETS, RELATIONS AND FUNCTIONS** Sets, Set Operations, Concept of Relations, Identity Relation, Inverse Relation, Types of Relation, Equivalence Relation, Concept of Function,Identity Function, Constant Function, Types of Function.	**7-53**
UNIT 2 :	**LATTICES** Partially Ordered Sets (Posets), Partial Order Relation,Partially Ordered Set,Dual of the partially Ordered Set (A, $\leq$), Covering Relation and Hasse Diagram, Upper Bound and Lower Bound, Lattices as Posets, Propertices of Lattices, Lattices as Algebraic Structures, Sublattices, Direct Product of Lattices, Homomorphism of Lattices, Some Special Lattices, Bounded Lattice, Distributive Lattice, Complemented Lattice.	**54-106**
UNIT 3 :	**PROPOSITIONAL LOGIC** Statements, Examples of Statement,Truth Tables, Logical Connectives, Negation, Conjunction, Disjunction, Conditional Statements, Biconditional Statements, Statement Formula, Tautology, Contradiction, Logical Equivalence, Equivalent Formulas.	**107-138**
UNIT 4 :	**BOOLEAN ALGEBRA** Definition of Boolean Algebra and Examples, Duality, Basic Theorems on Boolean Algebra, Boolean Algebra as Lattice, Boolean Algebra of Propositions Two-Element Boolean Algebra.	**139-165**

UNIT 5 : COMBINATORICS **166-184**

The Pigeonhole Principle, Counting principle,The Rule of Sum, The Rule of product, Permutation, Combination, Principle of Inclusion-Exclusion.

UNIT 6 : BASIC ALGEBRAIC STRUCTURE **185-239**

Binary Operation, Commutative Binary Operation, Associative Binary Operation, Identity Element, Inverse of an Element, Group, Subgroup, Coset, Cyclic Group, Normal Subgroup, Quotient Group, Ring, Integral Domain and Field.

UNIT 7 : GRAPH THEORY **240-301**

Definition of a Graph, Loop and Parallel Edges; Simple Graph, Incidence and Degree, Different Types of Graphs, Finite Graph, Infinite Graph, Null Graph, Complete Graph, Regular Graph, Bipartite Graph, Complete Bipartite Graph, Directed Graph, Walk, Path and Cycles, Subgraph of a Graph, Connected and Disconnected Graphs, Graph Isomorphis, Eulerian Graph and Hamiltanian Graph, Eulerian Graph, Hamiltonian Graph.

UNIT 8 : TREES **302-346**

Trees, Properties of a Tree, Distance and Centres in a Tree, Rooted and Binary Trees, Counting Trees, Spanning Trees, Fundamental Circuits, Spanning Trees in a Weighted Graph, Connectivity and Separability, Cutset, Edge-Connectivity, Cut Vertex-Set, Vertex-Connectivity, Separable Graph, Cut-Vertex, Flow Network, Matrix Representation of Graphs: Adjacency Matrix, Incidence Matrix, Path Matrix, Cutset Matrix, Circuit Matrix.

COURSE INTRODUCTION

The course **Introduction to Discrete Mathematics and Formal Languages and Automata** is designed with an aim to acquaint the learners with discrete mathematics and the theory of computer science.The course is divided into two blocks. The first block comprises of eight units covering the concepts of discrete mathematics. The second block comprises of seven units covering some concepts of formal language and automata.

The course is divided into two blocks :

Block 1 discusses the various mathematical concepts of discrete mathematics. The block begins with the concepts of sets, relations and functions. Thereafter, there is a discussion on the lattices, propositional logic and Boolean Algerbra. The block also explains basic algebraic structure and counting principles. An introduction to graph theory along with the concept of tree and its properties are also included at the end of this block.

Block 2 deals with some basic concepts of theoritical computer science, namely formal language and automata. The basic aim of studying automata theory is to identify a boundary between what is computable and what is not. It also includes the study of abstract machines that can perform computing.Therefore, it is necessary that the computing machine understands the instruction given by human beings and those instructions are to be written in some language. Before a computing machine can perform any task, it must understand the task and therefore the language recognition is one of the critical issues in the theory of computer science.

Each unit of this course includes some along-side boxes to help you know some of the difficult, unfamiliar terms. Some “EXERCISES” have been included to help you apply your mind to some of the points in the units. You may find some boxes marked with: “LET US KNOW”. These boxes will provide you with some additional interesting and relevant information. Again, you will get “CHECK YOUR PROGRESS” questions. These have been designed to enable you to self-check your progress of study. It will be helpful for you if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with “ANSWERS TO CHECK YOUR PROGRESS” given at the end of each unit.

BLOCK INTRODUCTION

This is the *First Block* of the course '***Introduction to Discrete Mathematics and Formal Languages and Automata***'.This block is on ***Discrete Mathematics***.Discrete Mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous.From the computer science perspective,Discrete Mathematics plays a vital role.Discrete mathematics is like a bridge connecting the mathematical concepts with various branches of computer science.The units of this blocks are provided with various examples that illustrate the basic concepts.

This block comprises the following eight units :

Unit - 1 gives general overview of the concepts on sets,relations and functions.

Unit - 2 concerned with partial ordered sets and lattices.This unit also covers a detailed discussion on properties of lattices and its types along with a number of solved examples.

Unit - 3 deals with the concepts of propositional logic.

Unit - 4 concentrates on Boolean algebra.

Unit - 5 introduces concepts on Combinatorics.

Unit - 6 includes the basic concepts of Basic algebraic structures.In this unit,we emphasized the algebraic structure where a thorough discussion of groups,rings and fields are presented.

Unit - 7 introduces the concepts on graph theory.

Unit - 8 includes the basic concepts of trees.A tree is a special type of graph and has several applications.

The structure of Block 1 is as follows :

UNIT 1 : SETS, RELATIONS AND FUNCTIONS

UNIT 2 : LATTICES

UNIT 3 : PROPOSITIONAL LOGIC

UNIT 4 : BOOLEAN ALGEBRA

UNIT 5 : COMBINATORICS

UNIT 6 : BASIC ALGEBRAIC STRUCTURE

UNIT 7 : GRAPH THEORY

UNIT 8 : TREES

UNIT 1 : SETS, RELATIONS AND FUNCTIONS

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Sets

1.4 Set Operations

1.5 Concept of Relations

- 1.5.1 Identity Relation
- 1.5.2 Inverse Relation

1.6 Types of Relation

1.7 Equivalence Relation

1.8 Concept of Function

- 1.8.1 Identity Function
- 1.8.2 Constant Function

1.9 Types of Function

1.10 Let Us Sum Up

1.11 Further Readings

1.12 Answers To Check Your Progress

1.13 Model Questions

1.1 LEARNING OBJECTIVES

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

- the notion of set and set operations
- the concept of a relation
- different types of relation
- equivalence relation
- the concept of a function
- different types of function.

1.2 INTRODUCTION

Set theory may be called the language of modern mathematics. The famous German mathematician Georg Cantor (1845-1918) has introduced the notion of set theory. Explaining the importance of set theory in the development of mathematics, the celebrated mathematician David Hilbert (1862-1943) has opined,– 'No one shall expel us from the paradise which cantor has created for us.'

In this unit, we will study sets, relations and functions.

1.3 SETS

A set may be viewed as a well defined collection of objects (elements, points, members) such that given any object, it is possible to determine whether that object belongs to the given collection or not.

Some of the examples of sets are as follows.

1. The set of natural numbers.
2. The set of natural numbers greater than ten.
3. The set of the roots of the equation $x^2–5x+6 = 0$.
4. The set of all points in a plane.

Let us consider the following two collections.

5. The collection of all interesting books in a library.
6. The collection of natural numbers much greater than ten.

The terms 'interesting' and 'much greater than' are not well defined. So, the example collections given in (5) and (6) are not examples of sets.

Generally we use capital letters, A, B, C, ... to denote sets, and lowercase letters, a, b, c, ... to denote elements of sets. If x is an element of a set A, we denote this fact by $x \in A$ (read as 'x belongs to A', or, 'x is in A). If y is not an element of the set A, we denote this fact by $y \notin A$ (read as 'y does not belong to A', or 'y is not in A').

Let A be the set of natural numbers greater than 10. Clearly $15 \in A$, but $5 \notin A$.

The set of natural numbers is denoted by $\underline{\underline{N}}$, the set of integers is denoted by $\underline{\underline{Z}}$, the set of rational numbers is denoted by $\underline{\underline{Q}}$, the set of real

numbers is denoted by $\underline{\underline{R}}$, the set of complex numbers is denoted by $\underline{\underline{C}}$. N is the first letter of the word natural, Z is the first letter of the German word zahl (meaning numbers), Q is the first letter of the word quotient, R is the first letter of the word real, and C is the first letter of the word complex.

A set can be described either by listing the elements or by giving a characterizing property of the elements. The standard way to describe a set by listing all its elements separated by commas and within braces. For example, the set of the roots of the equation $x^2–5x+6=0$ is {2, 3}. If the set is an infinite set, i.e., if the set has infinite number of elements, then the first three or four elements are written, and then dots (generally three) are put, e.g.,

$\underline{\underline{N}}$ = {1, 2, 3, ...}

$\underline{\underline{Z}}$ = {0, $\pm$1, $\pm$2, . . .}

The notation of describing a set by listing its elements is called Tabular notation or Roster notation.

The second way is to state those properties which characterize the elements of a set. For example-

A = {x : x is odd integer, x > 0} ..... (1) which reads ‘A is the set of x such that x is an odd integer, and x is greater than 0.’

The notation of describing a set by giving a characterizing property is called Set-Builder notation or Rule notation. The symbol : or / is read as ‘such that’.

The set given in (1) can also be written in tabular notation, viz.

A = {1, 3, 5, 7, ...}

$\underline{\underline{Q}}$ and $\underline{\underline{R}}$ cannot be written by listing the elements, i.e., in tabular notation, for between any two rational (or real) numbers, there exist infinite number of rational (or real) numbers.

$\underline{\underline{Q}}$ can be written in this way

$\underline{\underline{Q}}$ = {x : x is a rational number}

$$= \left\{ \frac{p}{q} : p, q \in \underline{\underline{Z}}, q \neq 0 \right\}$$

Similarly $\underline{\underline{R}}$ can be written as

$\underline{\underline{R}}$ = {x : x is a real number}

Let us consider the set

A = {a, e, i, o, u} consisting of the vowels of the English alphabet. It can be written is set-builder notation as follows.

A = {x : x is a vowel of the English alphabet}

Null Set : The set with no slements is called the null set (or empty set or void set), and is denoted by the sysmbol ϕ. Thus ϕ = { }.

The set of natural numbers less than one is a null set.

$\{x : x \neq x\} = \phi$.

Singleton set : A set containing only one element is called a singleton set.

A = {0} is a singleton set.

Note : ϕ is the null set, whereas $\{\phi\}$ is a singleton set containing one element ϕ.

Finite set : A set is said to be a finite set if it is null or contains a finite number of elements; otherwise it is said to be an infinite set.

A = {a, e, i, o, u} is a finite set

$\underline{\underline{N}}$, $\underline{\underline{Z}}$, $\underline{\underline{Q}}$, $\underline{\underline{R}}$ are infinite sets.

Subset of a set : If every element of a set A is also an element of a set B, then A is called a subset of B. Symbolically, we write $A \subseteq B$.

If at least on element of A is not in B, i.e., if A is not a subset of B, we write $A \not\subseteq B$, or $B \not\supseteq A$.

Note : 1. The null set is taken to be a subset of every set.

2. Every set A is a subset of itself.

3. If A is any set, then A is the improper subset of A. Any other subset of A is a proper subset of A. [A First Course In Abstract Algebra (2003) by John B Fraleigh]

Theorem 1 : Let A be a finite set having n elements, i.e., n(A) = n. Then the number of subsets of A is 2^n.

[n(A) denotes the number of elements of a finite set A].

Proof : Let A be a finite set, and n(A) = n. Number of subsets containing no element = ${}^nC_0$.

Number of subsets containing one element = ${}^nC_1$.

Number of subsets containing 2 elements = ${}^nC_2$.

In this way, number of subsets containing n elements = ${}^nC_n$.

$\therefore$ total number of subsets = ${}^nC_0 + {}^nC_1 + {}^nC_2 + \ldots . + {}^nC_n = 2^n$.



LET US KNOW

If n is a positive integer,

$(1+x)^n = {}^nC_0 + {}^nC_1 x + {}^nC_2 x^2 + \ldots . + {}^nC_n x^n$

putting x = 1, we get $2^n = {}^nC_0 + {}^nC_1 + {}^nC_2 + \ldots . + {}^nC_n$.

Example 1 : Write down all the subsets of A = {1, 2, 3}

Solution : n(A) = 3

$\therefore$ number of subsets of A = $2^3 = 8$

The subsets of A are

ϕ , {1, 2, 3}, {1}, {2}, {3}, {1, 2}, {2, 3}, {3, 1}

Comparable sets : Two sets A and B are said to be comparable if $A \subseteq B$ or $B \supseteq A$.

A and B are not comparable if $A \not\subseteq B$ and $B \not\subseteq A$.

Example 2 : Let A = {1, 2}, B = {1, 2, 3}. Are A and B comparable?

Solution : Every element in A is an element in B, i.e., $A \subseteq B$.

$\therefore$ A and B are comparable.

Example 3 : Let A = {1, 3, 5}, B = {2, 3, 5}. Are A and B comparable?

Solution : Clearly $A \not\subseteq B$, $B \not\subseteq A$.

$\therefore$ A and B are not comparable.

Note : If $x \in A \Rightarrow x \in B$

Or

$x \notin B \Rightarrow x \notin A$

Then $A \subseteq B$

Conversely, if $A \subseteq B$, then $x \in A \Rightarrow x \in B$ or $x \notin B \Rightarrow x \notin A$

Theorem 2 : Let A, B, C be three sets. If $A \subseteq B$, $B \subseteq C$, then $A \subseteq C$.

Proof : Let $x \in A$

$\because A \subseteq B$, $\therefore x \in A \Rightarrow x \in B$

$\because B \subseteq C$, $\therefore x \in B \Rightarrow x \in C$.

Thus $x \in A \Rightarrow x \in C$

$\therefore A \subseteq C$.

Power set : The collection of all subsets of a set A is called the power set A, Generally it is denoted by P(A).

Note : 1. Every element of a power set is a set. Thus, a power set is a set of sets.

2. If A is a finite set, and n(A) = n, then $n\{P(A)\} = 2^n$.

Example 4 : Let A = {1, 2}. Write down the power set of A.

Solution : A = {1, 2}, n(A) = 2

$\therefore n\{P(A)\} = 2^2 = 4$

P (A) = { ϕ , {1, 2}, {1}, {2}}

Note : P(A) is a set of sets. Every element of P(A) is a set.

Example 5 : Let A = {1, 2, 3, 4}. Write down the power set of A.

Solution : A = {1, 2, 3, 4}, n(A) = 4

$\therefore n\{P(A)\} = 2^4 = 16$

P (A) = { ϕ , {1, 2, 3, 4}, {1, 2, 3}, {1, 2, 4}, {1, 3, 4}, {2, 3, 4}, {1, 2}, {1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}, {1}, {2}, {3,}, {4}}.

Equality of sets : Two sets A and B are said to be equal if $A \subseteq B$ and $B \subseteq A$. Symbolically we write A=B. If the sets A and B are not equal, we write $A \neq B$.

Example 6 : Let A be the set of odd positive integers, and

B = {2n+1 : n = 0, 1, 2, 3, . . . }

Clearly A = B

Note : If we are to prove that the sets A and B are equal, we will prove that $A \subseteq B$ and $B \subseteq A$.

If $A \subseteq B$ and $B \subseteq A$, Then A and B have the same elements, i.e., A=B.



LET US KNOW

A set remains the same if its elements are rearranged or repeated.

{1, 2, 3} and {3, 2, 1} are the same

{ w, o, l, f } and {f, o, l, l, o, w} are the same.

Universal set : In any discussion of set theory, the members of all sets under investigation usually belong to a fixed large set. It is called the universal set. Generally it is denoted by U.

Let us suppose that we are discussing the following sets.

E = {2, 4, 6, 8, . . .}

O = {1, 3, 5, 7, . . .}

P = {2, 3, 5, 7, 11, . . .}

In this case, the set of natural numbers N can be taken as the universal set.

In plane geometry, the set consisting of all the points in the plane is taken as the universal set.

Venn diagrams : A venn diagram, after the name of the British logician John Venn (1834-1883), is a pictorial representation of sets in which sets are presented by enclosed areas in the plane. The universal set U is represented by the interior of a rectangle, whereas the other sets are represented by circles lying within the rectange.

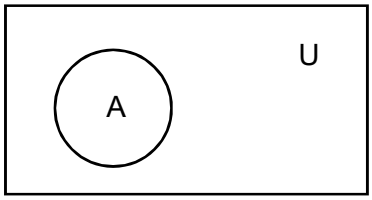


Fig 1.1

1.4 SET OPERATIONS

Let U be the universal set, and $A \subseteq U$, $B \subseteq U$.

Union : The union of A and B, denoted by $A \cup B$, is the set of all elements which belong to A or to B. Thus,

$A \cup B = \{x : x \in A \text{ or } x \in B\}$

Fig 1.2 (a) is Venn diagram in which $A \cup B$ is shaded.

Note : 1. $x \in A \cup B$ means x is in A or x is in B or x is in A and B. Here 'or' is used in the inclusive sense.

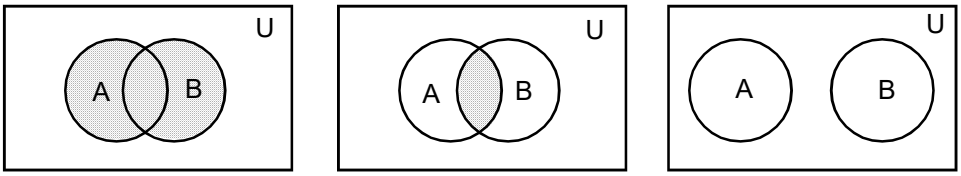
2. $x \in A \cup B \Rightarrow x \in A$ or $x \in B$

$x \notin A \cup B \Rightarrow x \notin A$ and $x \notin B$.

Example 7 : Let A = {20, 21, 22}

B = {21, 23, 25}

Then $A \cup B$ = {20, 21,22, 23, 25}



$A \cup B$ (a) $A \cap B$ (b) A, B are disjoint (c)

Fig 1.2

Intersection : The intersection of A and B, denoted by $A \cap B$, is the set of all elements which belong to both A and B. Thus,

$A \cap B = \{x : x \in A \text{ and } x \in B\}$

Fig 1.2 (b) is a Venn diagram in which $A \cap B$ is shaded.

Note : 1. $x \in A \cap B \Rightarrow x \in A$ and $x \in B$

$x \notin A \cap B \Rightarrow x \notin A$ or $x \notin B$

2. If the sets A and B do not have any common elements, i.e., if $A \cap B = \phi$, then A and B are said to be disjoint.

Fig 1.2 (c) is a Venn diagram in which A, B are disjoint.

Example 8 : Let A = {20, 21, 22}

B = {21, 23, 25}

Then $A \cap B$ = {21}

Example 9 : Let E = the set of even positive integers = {2, 4, 6, 8, ...}

P = the set of prime numbers

= {2, 3, 5, 7, 11, ...}

$E \cap P$ = {2}, a singleton set.

Note : 2 is the only even number which is prime.

Example 10 : Let E = the set of even positive integers

= {2, 4, 6, 8, ...}

F = the set of odd positive integers

= {1, 3, 5, 7, ...}

$E \cup F$ = {1, 2, 3, 4, 5, 6, 7, 8, ...}

= the set of positive integers

= $\underline{\underline{N}}$

$E \cap F = \phi$

Theorem 3 : Let A, B be two sets. Then

(a) $(A \cap B) \subseteq A \subseteq (A \cup B)$

(a) $(A \cap B) \subseteq B \subseteq (A \cup B)$

Proof (a) Let $x \in A \cap B$

$x \in A$ and $x \in B$

This $x \in A \cap B \Rightarrow x \in A$

$\therefore A \cap B \subseteq A$ (i)

Again, Let $x \in A$

$\Rightarrow x \in A \cup B$

$\therefore A \subseteq A \cup B$ (ii)

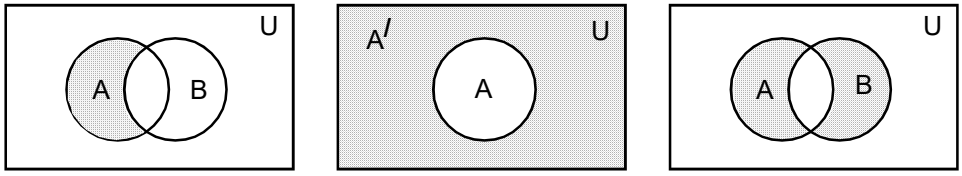
From (1) and (2) $A \cap B \subseteq A \subseteq A \cup B$

(b) Try yourself

Difference : The difference of A and B, denoted by A–B (or A \ B), is the set of elements which belong to A but which do not belong to B. Thus

$A–B = \{x : x \in A, x \notin B\}$

Note : A – B is read as "A minus B". Fig 1.3 (a) is a Venn diagram in which A – B is shaded.



A–B is shaded (a) $A^{/}$ is shaded (b) A–B is shaded (c)

Fig 1.3

The difference of B and A, denoted. by B–A, is the set of elements which belong to B but which do not belong to A. Thus

$B – A = \{x : x \in B, x \notin A\}$

Example 11 : Let $A = \{20, 21, 22\}$

$B = \{21, 23, 25\}$

$A – B = \{20, 22\}$

$B – A = \{23, 25\}$

Clearly $A – B \neq B – A$.

Note : From the above example, it is clear that difference of two sets is not commutative.

Complementation : The complement of a subset A of a universal set U is a subset of U, denoted by A' (or A^c), and is defined by

$A' = \{x : x \in U, x \notin A\}$

Fig 1.3 (b) is a Venn diagram in which A' is shaded.

Example 12 : Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

A = {2, 4, 6, 8, 10}

Then A' = {1, 3, 5, 7, 9}

Symmetric Difference : The sysmmetric difference of A and B, denoted by $A \Delta B$, is defined by

$A \Delta B = (A - B) \cup (B - A)$

Fig 1.3 (c) is a Venn diagram in which $A \Delta B$ is shaded.

Note : 1. $A \Delta B$ is the set of all those elements which belong either to A or to B, but not to both.

2. $A \Delta B$ can also be expressed as $(A \cup B)–(A \cap B)$

Example 13 : Let A = {20, 21, 22}

B = {21, 23, 25}

$A - B = \{20, 22\}$, $B - A = \{23, 25\}$

$A \Delta B = (A - B) \cup (B - A) = \{20, 22, 23, 25\}$

Theorem 4 : (Consistency property) The following three relations are equivalent $A \subseteq B$, $A \cap B = A$, and $A \cup B = B$

Proof : Let $A \subseteq B$.

Let $x \in A$

This $\Rightarrow x \in B$ $(\because A \subseteq B)$

Thus, $x \in A$ and $x \in B$.

$\therefore x \in A \cap B$

$\therefore A \subseteq A \cap B$ (1)

Again, we know that $A \cap B \subseteq A$ (2) [Theorem 3]

$\therefore$ from (1) and (2) $A \cap B = A$.

Again, Let $A \cap B = A$.

Let $x \in A$

This $\Rightarrow x \in A \cap B$ $(\because A \cap B = A)$

$\Rightarrow x \in A$ and $x \in B$

Thus, $x \in A \Rightarrow x \in B$

$\therefore A \subseteq B$

Thus, $A \subseteq B$ is equivalent to $A \cap B = A$

Again, Let $A \subseteq B$

Let $x \in A \cup B$

$\Rightarrow x \in A$ or $x \in B$

If $x \in A$, then $x \in B$ $(\because A \subseteq B)$

In either case, $x \in B$

Thus $x \in A \cup B \Rightarrow x \in B$

$\therefore A \cup B \subseteq B$ (3)

Again, $B \subseteq A \cup B$ (4) [Theorem 3]

$\therefore A \cup B = B$

Again, Let $A \cup B = B$

Let $x \in A$

$\Rightarrow x \in A \cup B$

$\Rightarrow x \in B$ $(\because A \cup B = B)$

$\therefore A \subseteq B$

Thus, $A \subseteq B$ is equivalent to $A \cup B = B$. Thus $A \subseteq B$, $A \cap B = A$, and $A \cup B = B$ are equivalent.

Laws of the algebra of sets

The following laws are related to the operations of union, and intersection. We will prove some of them.

Idempotent laws

1. (a) $A \cup A = A$, 1. (b) $A \cap A = A$

Commutative laws

2. (a) $A \cup B = B \cup A$, 2. (b) $A \cap B = B \cap A$

Associative laws

3. (a) $(A \cup B) \cup C = A \cup (B \cup C)$

3. (b) $(A \cap B) \cap C = A \cap (B \cap C)$

Distributive laws

4. (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

4. (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Absorption laws

5. (a) $A \cup (A \cap B) = A$ 5. (b) $A \cap (A \cup B) = A$

Identity laws

6. (a) $A \cup \phi = A$, 6. (b) $A \cap U = A$

7. (a) $A \cup U = U$ 7. (b) $A \cap U = \phi$

Involution laws

8. $(A')' = A$

Complement laws

9. (a) $A \cup A' = U$ 9. (b) $A \cap A' = \phi$

10. (b) $U' = \phi$ 10. (b) $\phi' = U$

De Morgan's laws

11. (a) $(A \cup B)' = A' \cap B'$

11. (b) $(A \cap B)' = A' \cup B'$

Proof of 1(a)

$x \in A \cup A$

$\Rightarrow x \in A$ or $x \in A$

$\Rightarrow x \in A$

$\therefore A \cup A \subseteq A$ (i)

Again, $y \in A$

$\Rightarrow y \in A$ or $y \in A$

$\Rightarrow y \in A \cup A$

$\therefore A \subseteq A \cup A$ (ii)

From (i) and (ii), $A \cup A = A$

Proof of 1(b)

$x \in A \cap A$

$\Rightarrow x \in A$ and $x \in A$

$\Rightarrow x \in A$

$\therefore A \cap A \subseteq A$ (i)

Again $y \in A$

$\Rightarrow y \in A$ and $y \in A$

$\Rightarrow y \in A \cap A$

$\therefore A \subseteq A \cap A$ (ii)

From (i) and (ii), $A \cap A = A$

Proof of 2(a)

$x \in A \cup B$

$\Rightarrow x \in A$ or $x \in B$

$\Rightarrow x \in B$ or $x \in A$

$\Rightarrow x \in B \cup A$

$\therefore A \cup B \subseteq B \cup A$ (i)

Again $y \in B \cup A$

$\Rightarrow y \in B$ or $y \in A$

$\Rightarrow y \in A$ or $x \in B$

$\Rightarrow y \in A \cup B$

$\therefore B \cup A \subseteq A \cup B$ (ii)

From (i) and (ii), $A \cup B = B \cup A$.

Proof of 2(b)

$x \in A \cap B$

$\Rightarrow x \in A$ and $x \in B$

$\Rightarrow x \in B$ and $x \in A$

$\Rightarrow x \in B \cap A$

$\therefore A \cap B \subseteq B \cap A$ (i)

Again, $y \in B \cap A$

$\Rightarrow y \in B$ and $y \in A$

$\Rightarrow y \in A$ and $x \in B$

$\Rightarrow y \in A \cap B$

$\therefore B \cap A \subseteq A \cap B$ (ii)

From (i) and (ii), $A \cap B = B \cap A$.

Proof of 3(a)

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

$\Rightarrow x \in A$ or $x \in B \cup C$

$\Rightarrow x \in A$ or $(x \in B$ or $x \in C)$

$\Rightarrow (x \in A$ or $x \in B)$ or $x \in C$

$\Rightarrow x \in A \cup B$ or $x \in C$

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

$\therefore A \cup (B \cup C) \subseteq (A \cup B) \cup C$ (i)

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

$\Rightarrow y \in A \cup B$ or $y \in C$

$\Rightarrow (y \in A$ or $y \in B)$ or $y \in C$

$\Rightarrow y \in A$ or $(y \in B$ or $y \in C)$

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

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

$\therefore (A \cup B) \cup C \subseteq A \cup (B \cup C)$ (ii)

From (i) and (ii), $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof of 3(b)

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

$\Rightarrow x \in A$ and $x \in B \cap C$

$\Rightarrow x \in A$ and $(x \in B$ and $x \in C)$

$\Rightarrow (x \in A$ and $x \in B)$ and $x \in C$

$\Rightarrow x \in A \cap B$ and $x \in C$

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

$\therefore A \cap (B \cap C) \subseteq (A \cap B) \cap C$ (i)

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

$\Rightarrow (y \in A$ and $y \in B)$ and $y \in C$

$\Rightarrow y \in A$ and $(y \in B$ and $y \in C)$

$\Rightarrow y \in A$ and $y \in B \cap C$

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

$\therefore (A \cap B) \cap C \subseteq A \cap (B \cap C)$ (ii)

From (i) and (ii), $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof of 4(a)

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

$\Rightarrow x \in A$ or $x \in B \cap C$

$\Rightarrow x \in A$ or $(x \in B$ and $x \in C)$

If $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$ and, therefore, $x \in (A \cup B) \cap (A \cup C)$

If $x \in B$ and $x \in C$, then $x \in A \cup B$ and $x \in A \cup C$ and, therefore, $x \in (A \cup B) \cap (A \cup C)$.

$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ (i)

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

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

$\Rightarrow$ $(x \in A$ or $x \in B)$ and $(x \in A$ or $x \in C)$

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

$\Rightarrow$ $x \in A$ or $x \in B \cap C$

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

$\therefore$ $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ (ii)

From (i) and (ii), $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof of 4(b)

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

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

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

If $x \in B$ then $x \in A \cap B$ (since $x \in A$)

If $x \in C$ then $x \in A \cap C$ (since $x \in A$)

i.e., $x \in A \cap B$ or $x \in A \cap C$

$\therefore$ $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ (i)

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

$\Rightarrow$ $x \in A \cap B$ or $x \in A \cap C$

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

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

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

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

$\therefore$ $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ (ii)

From (i) and (ii), $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof of 5(a)

We know that $A \cap B \subseteq A$ [Theorem 3]

$\therefore$ $(A \cap B) \cup A = A$ [Theorem 4]

i.e. $A \cup (A \cap B) = A$ [by 2(a)]

Proof of 5(b)

We know that $A \subseteq A \cup B$ [Theorem 3]

$\therefore$ $A \cap (A \cup B) = A$ [Theorem 4]

Proof of 11(a)

$x \in (A \cup B)'$

$\Rightarrow x \notin A \cup B$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \in A^/$ and $x \in B^/$

$\Rightarrow x \in A^/ \cap B^/$

$\therefore (A \cup B)^/ \subseteq A^/ \cap B^/$ (i)

Again $x \in A^/ \cap B^/$

$\Rightarrow x \in A^/$ and $x \in B^/$

$\Rightarrow x \notin A$ and $x \notin B$

$\Rightarrow x \notin A \cup B$

$\Rightarrow x \in (A \cup B)^/$

$\therefore A^/ \cap B^/ \subseteq (A \cup B)^/$ (ii)

From (i) and (ii), $(A \cup B)^/ = A^/ \cap B^/$.

Proof of 11(b)

$x \in (A \cap B)^/$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \in A^/$ or $x \in B^/$

$\Rightarrow x \in A^/ \cup B^/$

$\therefore (A \cap B)^/ \subseteq A^/ \cup B^/$ (i)

Again $x \in A^/ \cup B^/$

$\Rightarrow x \in A^/$ or $x \in B^/$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in (A \cap B)^/$

$\therefore A^/ \cup B^/ \subseteq (A \cup B)^/$ (ii)

From (i) and (ii), $(A \cap B)^/ = A^/ \cup B^/$.

Note : The laws 11(a), 11(b) are called De Morgan's laws after the name of the famous mathematician Augustus De Morgan (1806-1871). It may be mentioned that De Morgan was born in Madurai of Tamilnadu.

Theorem 5 : (a) $A–B = A \cap B^/$

(b) $A–B = B^/–A^/$

(c) $A \subseteq B$ if and only if $B^/ \subseteq A^/$.

Proof : (a) $x \in A–B$

$\Rightarrow x \in A$ and $x \notin B$

$\Rightarrow x \in A$ and $x \in B'$

$\Rightarrow x \in A \cap B'$

$\therefore A - B \subseteq A \cap B'$ (i)

Again, $x \in A \cap B'$

$\Rightarrow x \in A$ and $x \in B'$

$\Rightarrow x \in A$ and $x \notin B$

$\Rightarrow x \in A - B$

$\therefore A \cap B' \subseteq A - B$ (ii)

From (i) and (ii), $A - B = A \cap B'$

(b) $x \in A - B$

$\Rightarrow x \in A$ and $x \notin B$

$\Rightarrow x \notin A'$ and $x \in B'$

$\Rightarrow x \in B'$ and $x \notin A'$

$\Rightarrow x \in B' - A'$

$\therefore A - B \subseteq B' - A'$ (i)

Again, $x \in B' - A'$

$\Rightarrow x \in B'$ and $x \notin A'$

$\Rightarrow x \notin A'$ and $x \in B'$

$\Rightarrow x \in A$ and $x \in B'$

$\Rightarrow x \in A - B$

$\therefore B' - A' \subseteq A - B$ (ii)

From (i) and (ii), $A - B = B' - A'$

(c) Let $A \subseteq B$

Let $x \in B' \Rightarrow x \notin B$

$\Rightarrow x \notin A$ ($\because A \subseteq B$)

$\Rightarrow x \in A'$

$\therefore B' \subseteq A'$

Again, Let $B' \subseteq A'$

Let $x \in A \Rightarrow x \notin A'$

$\Rightarrow x \notin B'$ ($\because B' \subseteq A'$)

$\Rightarrow x \in B$

$\therefore A \subseteq B$



CHECK YOUR PROGRESS

Q 1: If A= {1, 2, 3}, B = {–1, 2, 3}; find A ∪ B, A ∩ B, A–B, B–A.

Q 2: Which of the following sets are null sets, and which are singleton sets?

(a) The set of even but prime numbers.

(b) The set of prime numbers less than two.

(c) The set of odd natural numbers divisible by 2.

(d) {ϕ}

(e) {x : x+10 = 10}

(f) {x : x^2 = 9, and x is even}

(g) {x : x ≠ x}

(h) The set of real numbers which are neither positive nor negative.

Q 3: Consider the following three sets.

A = the set consisting of the letters of the word FILE.

B = the set consisting of the letters of the word LIFE.

C = the set consisting of the letters of the word LIEF

Are the three sets equal ?

Q 4: Consider the following three sets.

A = {0, 2}, B = {2}, C = {x : x^2 – 2x = 0}

Are the three sets equal ?

Q 5: Write down all the subsets of the following sets.

(a) {0}, (b) {0, 1}, (c) ϕ , (d) {ϕ}, (e) {{1, 2}, {3, 4}}

Q 6: Are the following sets comparable ? Give reasons.

(a) {1, 2}, {2, 3}, (b) {2, 4, 6}, {1, 2, 3, 4, 5, 6}

Q 7: If A = {1, 2, 3, 4, 5}, what is the number of subsets of A ? Write down any three disjoint subsets of A.

Q 8: Write down three sets A, B, C such that A ∩ B = A ∩ C, but B ≠ C.

Q 9: Write down three sets A, B, C such that A ∪ B = A ∪ C, B ≠ C.

Q 10: Write down three sets A, B, C such that $A \cap B \neq \phi$, $B \cap C \neq \phi$, $C \cap A \neq \phi$, but $A \cap B \cap C = \phi$.

Q 11: Let A, B, C be three sets such that $A \subseteq B$, $B \subseteq C$. Prove that $A \subseteq B \subseteq C$.

Q 12: Let A, B, C be three sets such that $A = B$. Prove that $A \cap C = B \cap C$.

Q 13: Let A, B be two sets. If $B' \subseteq A'$, prove that $A \subseteq B$.

Q 14: Let A, B, C be three sets such that $A \subseteq B$.
Prove that $C–B \subseteq C–A$.

Q 15: Let A, B be two sets such that $A \cup B = A \cap B$. Prove that $A = B$.

Q 16: Let A, B be two sets. Prove that (i) if $A \subseteq B$, $A \cup B = B$,
(ii) $(A–B) \cup A = A$, (iii) $(A–B) \cap B = \phi$.

Q 17: Let A, B, C be three sets such that $A \cup B = B$, $B \cup C = C$.
Prove that $A \subseteq C$.

Q 18: Let A, B be two sets. Prove that $A \cap (A' \cup B) = A \cap B$.

Q 19: If A, B are nonempty sets, prove that A–B, $A \cap B$, B–A are pairwise disjoint.

1.5 CONCEPT OF RELATIONS

Let A, B be two nonempty sets. The cartesian product of A and B, denoted by AXB, is defined by $AXB = \{(a, b) : a \in A, b \in B\}$.

(a, b) is called an ordered pair.

Example 13 :

Let A = {1, 3, 5, 7}

B = {2, 4, 6}

AXB = {(1, 2), (1, 4), (1, 6), (3, 2), (3, 4), (3, 6), (5, 2), (5, 4), (5, 6), (7, 2), (7, 4), (7, 6)}

BXA = {(2, 1), (2, 3), (2, 5), (2, 7), (4, 1), (4, 3), (4, 5), (4, 7), (6, 1), (6, 3), (6, 5), (6, 7)}.

We note that n(A) = 4, n(B) = 3,

n(AXB) = n(BXA) = 12 = 4 x 3

n(A) denotes the number of elements of A.

If A, B are finite sets, and n(A) = x, n(B) = y, then n(AXB) = n(BXA) = xy.

The ordered pair (a, b) is equal to the ordered pair (c, d) if and only if a is equal to c, and b is equal to d. Symbolically, (a, b) = (c, d) $\Rightarrow$ a=c, b=d.

In example, AXB $\neq$ BXA.

If one of the sets is infinite, then AXB and BXA are infinite.

The cartesian product of A and A, i.e. AXA, is often denoted by A^2.

Example 14 :

Let A = {1, 3, 5, 7}. Then

A^2 = AXA = {(1, 1), (1, 3), (1, 5), (1, 7), (3, 1), (3, 3), (3, 5), (3, 7), (5, 1), (5, 3), (5, 5), (5, 7), (7, 1), (7, 3), (7, 5), (7, 7)}

$n(A^2)$ = n(AXA) = 4 x 4 = 16.

Definition : Let A and B be two nonempty sets. A subset R of AXB is said to be **relation** from A to B.

If A = B, then any subset of AXA is said to be a relation on A.

If R $\subseteq$ AXB, and (a, b) $\in$ R; a $\in$ A, b $\in$ B; it is also written as aRb, and is read as “a is related to b”.

Note : 1. The set of the first components of the ordered pairs of R is called the **domain**, and the set of the second components of the ordered pairs of R is called the **range** of R.

2. If A, B are finite sets, and n(A) = x, n(B) = y; then n(A x B) = xy. So the number of subsets of AXB is 2^{xy}.

Therefore, the number of relations from A to B is 2^{xy}.

Example 15 :

Let A = {1, 2, 3}

B = {8, 9}

$\therefore$ AXB = {(1, 8), (1, 9), (2, 8), (2, 9), (3, 8), (3, 9)}

Let R = {(1, 8), (2, 9), (3,9)}

Clearly R $\subseteq$ AXB

$\therefore$ R is a relation from A to B.

Here 1R8, 2R9, 3R9

Domain of R = {1, 2, 3}

Range of R = {8, 9}

Example 16 :

Let $\underline{\underline{R}}$ be the set of real numbers.

Let R = {(x, y) : x, y $\in \underline{\underline{R}}$, x < y} $\subseteq \underline{\underline{R}} X \underline{\underline{R}}$

$\therefore$ R is a relation on $\underline{\underline{R}}$.

$\because$ 3 < 5, $\therefore$ (3, 5) $\in$ R, i.e., 3R5

19 < 27, $\therefore$ (19, 27) $\in$ R, i.e., 19R27

But 5 > 3, $\therefore$ (5, 3) $\notin$ R, i.e., 5$\not R$ 3.

Example 17 :

Let X be the set of odd integers.

Let R = {(x, y) : x $\in$ X, y $\in$ X, and x+y is odd}

We know that the sum of two odd integers is an even integer.

$\therefore$ if x, y are odd, then x+y cannot be odd.

$\therefore$ R = $\phi \subseteq$ X x Y.

In this case R is called a **null relation** on X.

Example 18 :

Let E be the set of even integers.

Let R = {(x, y) : x, y $\in$ E, and x+y is even}

We know that the sum of two even integers is an even integer.

$\therefore$ if x, y are even, then x+y always even.

$\therefore$ R = E x E $\subseteq$ E x E.

In this case R is called a **universal relation** on E.

1.5.1 Identity Relation

Let A be a nonempty set.

The relation I_A = {(a, a): $\in$ A} is called the identity relation on A.

Example 19: Let A = {1, 2, 3, 4}

Then I_A = {(1, 1), (2, 2), (3, 3), (4, 4)} $\subseteq$ AXA

Clearly I_A is the identity relation on A.

1.5.2 Inverse Relation

Let A, B be two nonempty sets. Let R be a relation from A to B, i.e., R $\subseteq$ AXB. The inverse relation of R is denoted by R^{-1}, and is

defined by $R^{-1} = \{(b, a) : (a, b) \in R\} \subseteq BXA$

Clearly, domain of R^{-1} = range of R

range of R^{-1} = domain of R.

Example 20 : Let A = {1, 2, 3}

B = {5, 6}

$R = \{(1, 5), (2, 6), (3, 5)\} \subseteq AXB$

$R^{-1} = \{(5, 1), (6, 2), (5, 3)\} \subseteq BXA$.



CHECK YOUR PROGRESS

Q 20: Let A, B be two finite sets, and n(A) = 4, n(B) = 3. How many relations are there from A to B ?

Q 21: Let A be a finite set such that n(A) = 5. Write down the number of relations on A.

Q 22: Let $\underline{\underline{N}}$ be the set of natural numbers.

Let $R = \{(x, y) : x, y \in \underline{\underline{N}}, x > y\}$.

Examine if the following ordered pairs belong to R.

(7, 4), (23, 32), (5, 5), (72, 27), (18, 19), (25, 21).

Q 23: Let E be the set of even integers.

Let $R = \{(x, y) : x, y \in E$, and x+y is odd$\}$

Is R a null relation on A ? Justify your answer.

Q 24: Let A = {1, 2, 3, 4, 5}

Write down the identity relation on A.

Q 25: Let A = {4, 5, 6}, B = {7, 8, 9}

Let R = {(4, 7), (5, 8), (6, 7), (6, 8), (6, 9)} Write down R^{-1}.

1.6 TYPES OF RELATION

Let A be a nonempty set, and R be a relation on A, i.e., $R \subseteq AXA$.

1. R is called **reflexive** if $(a, a) \in R$, i.e., if aRa, for all $a \in A$.
2. R is called **symmetric** if whenever $(a, b) \in R$, then $(b, a) \in R$, i.e., if whenever aRb, then bRa; $a, b \in A$.
3. R is called **antisymmetric** if $(a, b) \in R$,, $(b, a) \in R \Rightarrow a = b$, i.e., if aRb,

$bRa \Rightarrow a = b$; $a, b \in A$.

4. R is called **transitive** if whenever $(a, b), (b, c) \in R$, then $(a, c) \in R$, i.e., if whenever aRb, bRc, then aRc; $a, b, c \in A$

Example 21: Let $A = \{1, 2, 3\}$

$R = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$

Examine if R is reflexive, symmetric, antisymmetric, transitive.

Solution : Here $(1, 1) \in R$, $(2, 2) \in R$, but $(3, 3) \notin R$.

$\therefore$ R is not reflexive.

Again, $(a, b) \in R \Rightarrow (b, a) \in R$

$\therefore$ R is symmetric.

Again $(1, 2) \in R$, $(2, 1) \in R$, but $1 \neq 2$.

$\therefore$ R is not antisymmetric.

Again if $(a, b) \in R$, $(b, c) \in R$; then $(a, c) \in R$

$\therefore$ R is transitive.

Example 22: Let $\underline{\underline{Z}}$ be the set of integers, and $R = \{(x, y) : x, y \in \underline{\underline{Z}}, x \leq y\}$

Examine if R is reflexive, symmetric, antisymmetric, and transitive.

Solution : We have $a \leq a$, for all $a \in \underline{\underline{Z}}$ i.e., $(a, a) \in R$, for all $a \in \underline{\underline{Z}}$.

$\therefore$ R is reflexive.

We have $2<5$, but $5 \not< 2$

i.e. $(2, 5) \in R$, but $(5, 2) \notin R$.

$\therefore$ R is not symmetric.

Again $a \leq b$, $b \leq a \Rightarrow a = b$

i.e., $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$.

$\therefore$ R is antisymmetric.

Again $a \leq b$, $b \leq c \Rightarrow a \leq c$

i.e., $(a, b), (b, c) \in R \Rightarrow (a, c) \in R$.

$\therefore$ R is transitive.

Example 23: Give an example of a relation which is transitive, but neither reflexive nor symmetric.

Solution : Let $A = \{1, 2\}$.

Let $R = \{(1, 1), (1, 2)\} \subseteq AXA$.

Clearly R is a relation on A.

Here $(2, 2) \notin R$.

$\therefore$ R is not reflexive.

Again $(1, 2) \in R$, but $(2, 1) \notin R$.

$\therefore$ R is not symmetric.

But R is transitive.

1.7 EQUIVALENCE RELATION

Let A be a nonempty set. A relation R on A is called an equivalence relation if it is reflexive, symmetric, and transitive.

Example 24: Let $\underline{\underline{Z}}$ be the set of integers, and R = {(x, y) : x, y $\in \underline{\underline{Z}}$, and x+y is even}

Examine if R is an equivalence relation on $\underline{\underline{Z}}$.

Solution : Let $x \in \underline{\underline{Z}}$.

$\therefore$ x+x is even.

$\Rightarrow (x, x) \in R$, for all $x \in \underline{\underline{Z}}$

$\therefore$ R is reflexive.

$(x, y) \in R \Rightarrow$ x+y is even

$\Rightarrow$ y+x is even

$\Rightarrow (y, x) \in R$

$\therefore$ R is symmetric.

$(x, y) \in R, (y, z) \in R$

$\Rightarrow$ x+y is even, y+z is even.

$\Rightarrow$ (x+y) +(y+z) is even

$\Rightarrow$ (x+z) + 2y is even

$\Rightarrow$ x+z is even

$\therefore (x, z) \in R$

$\therefore$ R is transitive.

Thus, R is an equivalence relation on $\underline{\underline{Z}}$.

Example 25 : Let A be the set of all straight lines in a plane.

Let R ={(x, y) : x, y $\in$ A, and x $\perp$ y}

Examine if R is reflexive, symmetric, and transitive.

Solution : Let $x \in A$, i.e., x is a straight line in a plane.

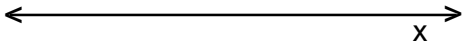


Fig 1.4 (a)

A line cannot be perpendicular to itself, i.e., $x \perp x$.

$\therefore (x, x) \notin R$

$\therefore$ R is not reflexive.

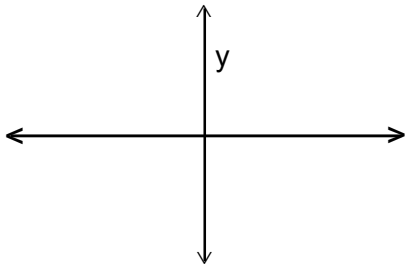


Fig 1.4 (b)

Let $(x, y) \in R$, i.e., $x \perp y$.

We know that if a line x is perpendicular to y, then y is perpendicular to x, i.e.,

$x \perp y \Rightarrow y \perp x$

i.e. $(x, y) \in R \Rightarrow (y, x) \in R$

$\therefore$ R is symmetric.

Let $(x, y) \in R$, $(y, z) \in R$

i.e. $x \perp y$, $y \perp z$

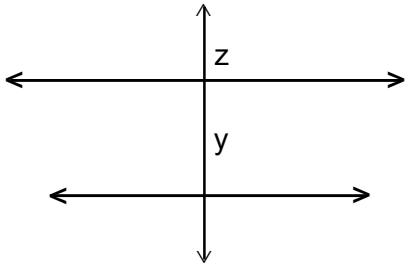


Fig 1.4 (c)

x is perpendicular to y, y is perpendicular to z.

$\therefore$ x||z, i.e., $x \perp z$

i.e. $(x, y) \in R$, $(y, z) \in R \not\Rightarrow (x, z) \in R$.

$\therefore$ R is not transitive.

Example 26: Let A be the set of all triangles in a plane. Let

$R = \{(x, y) : x, y \in A, \text{ and } x \cong y\}$

Examine R is an equivalence relation on A.

Solution : Every triangle is congruent to itself. Let $x \in A$, i.e. x is a triangle in a plane. Then x is congruent to itself, i.e., $x \cong x$, i.e., $(x, x) \in R$.

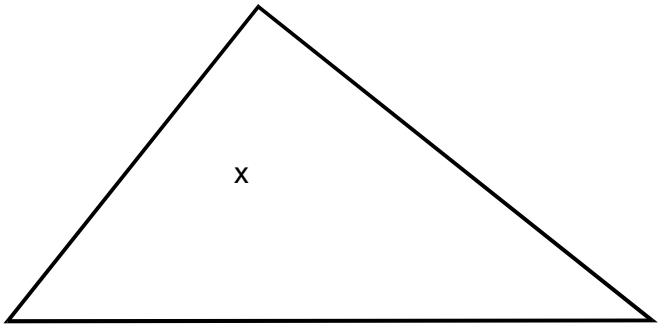


Fig 1.5

$\therefore$ R is reflexive.

Let $(x, y) \in R \Rightarrow x \cong y \Rightarrow y \cong x$,

$\Rightarrow (y, x) \in R$

Let $(x, y) \in R$, and $(y, z) \in R$

$\Rightarrow x \cong y$, and $y \cong z$

$\therefore x \cong z$,

i.e., $(x, z) \in R$.

$\therefore$ R is transitive.

Thus, R is an equivalence relation.

Example 27: Let A be the set of all straight lines in a plane.

Let $R = \{(x, y) : x, y \in A$, and $x||y\}$.

Examine if R is an equivalence relation on A.

Solution : Let $x \in A$, i.e., x is a straight line in a plane.

A line is parallel to itself, i.e., $x||x$,for all $x \in A$,

$\therefore (x, x) \in R$, for all $x \in A$

$\therefore$ R is reflexive.

Let $x, y \in A$, and let $x||y$.

$\therefore y||x$

$\therefore (x, y) \in R \Rightarrow (y, x) \in R$.

$\therefore$ R is symmetric.

Let $x, y, z \in A$ such that $x||y$, $y||z$.

$\therefore x||z$

i.e. $(x, y) \in R$, $(y, z) \in R \Rightarrow (x, z) \in R$.

$\therefore$ R is transitive.

Thus, R is an equivalence relation on A.

Example 28: Let $\underline{\underline{N}}$ be the set of natural numbers. Let a relation R be defined on $\underline{\underline{N}} \times \underline{\underline{N}}$ by (a, b) R (c, d) if and only if ad = bc.

Show that R is an equivalence relation on $\underline{\underline{N}} \times \underline{\underline{N}}$.

Solution : Let a, b $\in \underline{\underline{N}}$

$\therefore$ (a, b) $\in \underline{\underline{N}} \times \underline{\underline{N}}$

We have ab = ba

$\therefore$ (a, b) R (a, b)

$\therefore$ R is reflexive.

Let (a, b), (c, d) $\in \underline{\underline{N}} \times \underline{\underline{N}}$

Now (a, b) R (c, d) $\Rightarrow$ ad = bc

$\Rightarrow$ cb = da

$\Rightarrow$ (c, d) R (a, b)

$\therefore$ R is symmetric.

Let (a, b), (c, d), (e, f) $\in \underline{\underline{N}} \times \underline{\underline{N}}$ such that (a, b) R (c, d), and (c, d) R (e, f).

$\Rightarrow$ ad = bc, and cf = de

$\Rightarrow$ adcf = bcde

$\Rightarrow$ af = be

$\Rightarrow$ (a, b) R (e, f)

$\therefore$ R is transitive.

Thus, R is an equivalence relation on $\underline{\underline{N}} \times \underline{\underline{N}}$.

Example 29: (Congruence modulo n).

Let $\underline{\underline{Z}}$ be the set of integers, and n be a fixed positive integer.

Let a, b $\in \underline{\underline{Z}}$.

a is said to be congruent modulo n if and only if a–b is divisible by n. Symbolically, we write $a \equiv b \pmod{n}$.

Show that the relation 'congruence modulo n' is an equivalence relation on $\underline{\underline{Z}}$.

Solution : We know that a–a is divisible by n, i.e., $a \equiv a \pmod{n}$.

$\therefore$ the relation is reflexive.

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

$\Rightarrow$ a–b is divisible by n

$\Rightarrow$ b–a is divisible by n

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

$\therefore$ the relation is symmetric.

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

$\Rightarrow$ a–b is divisible by n, b–c is divisible by n.

$\Rightarrow$ (a–b) + (b–c) is divisible by n.

$\Rightarrow$ a–c is divisible by n.

$\Rightarrow a \equiv c \pmod{n}$

$\therefore$ the relation is transitive.

Thus, the relation 'congruence modulo n' is an equivalence relation on $\underline{\underline{Z}}$.

> We know 15–3 is divisible by 4.
>
> $\therefore$ 15 is congruent to 3 modulo 4, i.e., $15 \equiv 3$ (modulo 4).
>
> 15–3 is not divisible by 7.
>
> $\therefore$ 15 is not congruent to 3 modulo 7, i.e.,
>
> $15 \not\equiv 3 \pmod{7}$.

Example 30: Let $\underline{\underline{Z}}$ be the set of integers. Let $R = \{(a, b) : a, b \in \underline{\underline{Z}}, ab \geq 0\}$. Examine if R is an equivalence relation on $\underline{\underline{Z}}$.

Solution : We have $aa \geq 0$

$\therefore (a, a) \in R$, for all $a \in \underline{\underline{Z}}$

$\therefore$ R is reflexive.

Let $(a, b) \in R$

$\therefore ab \geq 0$

$\Rightarrow ba \geq 0$

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

$\therefore$ R is symmetric.

We have

(–2) x 0 = 0, 0 x 2 = 0

$\therefore (-2, 0) \in R$, $(0, 2) \in R$

Now (–2) x 2 = –4 < 0

$\therefore (-2, 2) \notin R$

$\therefore$ R is not transitive. Thus, R is not an equivalence relation on $\underline{\underline{Z}}$.

Theorem 6 : The inverse of an equivalence relation is also an equivalence relation.

Proof : Let A be a nonempty set.

Let R be an equivalence relation on A.

R is reflexive.

$\therefore$ $(x, x) \in R$, for all $x \in A$.

$\Rightarrow$ $(x, x) \in R^{-1}$, for all $x \in A$, [by definition of R^{-1}]

$\therefore$ R^{-1} is reflexive.

Let $(x, y) \in R^{-1}$; $x, y \in A$

This $\Rightarrow$ $(y, x) \in R$, [by definition of R^{-1}]

$\Rightarrow$ $(x, y) \in R$, [$\because$ R is symmetric]

$\Rightarrow$ $(y, x) \in R^{-1}$

$\therefore$ R^{-1} is symmetric.

Let $(x, y), (y, z) \in R^{-1}$.

$\Rightarrow$ $(y, x), (z, y) \in R$, [by definition of R^{-1}]

$\Rightarrow$ $(z, y), (y, x) \in R$,

$\Rightarrow$ $(z, x) \in R$, [$\because$ R is transitive]

$\Rightarrow$ $(x, z) \in R^{-1}$

$\therefore$ R^{-1} is transitive.

Thus, R^{-1} is an equivalence relationon A.

Theorem 7 : The intersection of two equivalence relations is also an equivalence relation.

Proof : Let A be a nonempty set. Let R and S be two equivalence relations on A.

R and S are reflexive

$\therefore$ $(x, x) \in R$ and $(x, x) \in S$, for all $x \in A$.

$\Rightarrow$ $(x, x) \in R \cap S$, for all $x \in A$.

$\therefore$ $R \cap S$ is reflexive.

Let $(x, y) \in R \cap S$

This $\Rightarrow$ $(x, y) \in R$ and $(x,y) \in S$

$\Rightarrow$ $(y, x) \in R$ and $(y, x) \in S$, [$\because$ R and S are symmetric]

$\Rightarrow$ $(y, x) \in R \cap S$

$\therefore$ $R \cap S$ is symmetric.

Let $(x, y) \in R \cap S$, $(y, z) \in R \cap S$

$\Rightarrow$ $(x, y) \in R$ and $(x, y) \in S$, $(y, z) \in R$ and $(y, z) \in S$

$\Rightarrow$ $(x, z) \in R$ and $(x, z) \in S$, [$\because$ R and S are transitive]

$\Rightarrow$ $(x, z) \in R \cap S$

$\therefore$ $R \cap S$ is transitive.

Thus, $R \cap S$ is an equivalence relation on A.

Note : The union of two equivalence relations is not necessarily an equivalence relation.

Let us consider A = {1, 2, 3}

Now, R = {(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)}

S = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)}

are two equivalence relations on A.

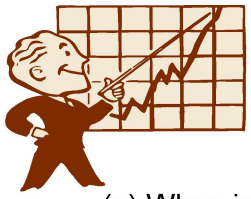
RUS = {(1, 1), (2, 2), (3, 3), (1, 3), (3, 1), (1, 2), (2, 1)}

$(2, 1) \in R \cup S$, $(1, 3) \in R \cup S$

But $(2, 3) \notin R \cup S$

$\therefore$ $R \cup S$ is not transitive.

R



CHECK YOUR PROGRESS

Q 26: Let A be a nonempty set, and R be a relation on A.

(a) When is R not reflexive ?

(b) When is R not symmetric ?

(c) When is R not antisymmetric ?

(d) When is R not transitive ?

Q 27: Let be the set of integers.

Let R = {(a, b) : a, b , a–b is divisible by 5} Examine if R is an equivalence relation on .

Q 28: Let A be the set of all triangles in a plane

Let R = {(x, y) : x, y A, x is similar to y}

Examine if R is an equivalence relation on A.

1.8 CONCEPT OF FUNCTION

Let A and B be two nonempty sets,and f AXB such that

(i) (x, y) f, for all x A and y

(ii) (x, y) ′) f ′.

In this case f is said to be a function (or a mapping) from the set A to the set B. Symbolically, we write f : A

Here A is called the domain and B is called the codomain of f.

Example 31 : Let A = {1, 2}, B = {7, 8, 9}

f = {(1, 8), (2, 7)} AXB

Here each element of A appears as the first component exactly in one of the ordered pairs of f.

f is a function from A to B.

Example 32 : Let A = {1, 2}, B = {7, 8, 9}

g = {(1, 7), (1, 9)}

Here two distinct ordered pairs have the same first component.

f is not a function from A to B.

Example 33 : Let A = {1, 2, 3, 4}, B = {x, y, z, w}. Are the following relations from A to B functions ?

(i) f_1 = {(1, x), (1, w), (2, x), (3, y), (4, w)}

(ii) f_2 = {(1, y), (2, z), (3, x), (4, x)}

Solution : (i) No. Here two distinct ordered pairs (1, x), (1, w) have the same first component.

(ii) Yes. Here each element of A appears as the first component exactly in one of the ordered pairs of f_2.

Thus we see that

Every function is a relation, but every relation is not a function.

The above definition of function can be restated as follows.

If A and B are two nonempty sets and if each element of A is associated with a unique element of B, then the rule by which this associationis made, is called a function from the set A to the set B. The rules are denoted by f, g etc. Here A, B may be identical.

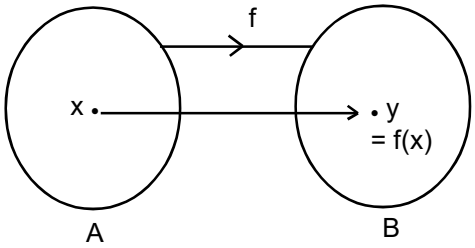


Fig 1.6

Let f be a function from A to B, i.e., f : A

of B that is associated with x of A is called the image of x under f. Symbolically we write it as y = f(x),x is called the pre-image of y.

A is the domain, and B is the codomain of f.

The set of all the images under f is called the range of f.

Example 34 : Let be the set of natural numbers, and integers, and

f : , x

Clearly f is a function from to Domain of f =

Codomain of f =

Now, $f(1) = (-1)^1 = -1$, $f(2) = (-1)^2 = 1$, $f(3) = (-1)^3 = -1$, $f(4) = (-1)^4 = 1$, and so on.

range of f = {–1, 1}.

1.8.1 Identity Function

Let A be a nonempty set, and i : A A, i (x) = x, for all x A.

Then i is called the identity function.

Note : In case of identity function, domain and co-domain are the same.

Example 25 : Let A = {1, 2, 3}.

Let i : A A, such that f(1) = 1, f(2) = 2, f(3) = 3. Then i is the identity function.

1.8.2 Constant Function

Let A, B be two non-empty sets, and f : A

= k, for all x A.

Then f is called a constant function.

Note : The range of a constant function is a singleton set.

Example 36 : Let A = {1, 3, 5, 7, ...} be the set of odd positive integers, and

f : A $x^x + 1$, for all x A.

Now, $f(1) = (-1)^1 + 1 = -1 + 1 = 0$

$f(3) = (-1)^3 + 1 = -1 + 1 = 0$

$f(5) = (-1)^5 + 1 = -1 + 1 = 0$

Thus, $f(x) = (-1)^x + 1 = 0$, for all x A.

f is a constant function.

1.9 TYPES OF FUNCTION

Let A, B be two nonempty sets and f : A

1. If there is at least one element in B which is not the image of any element in A, then f is called an into function.
2. If each element in B is the image of at least one element in A, then f is called an onto function (or a surjective function or a surjective).

Note : In case of onto function, range of f = co-domain of f.

3. If different elements in A have different images in B, then f is called a one-one function (or an injective function or an injection).
4. If two (or more) different elements in A have the same image in B, then f is called a **many-one** function.
5. A function is said to be **bijective** if it is one-one (injective) and onto (surjective).

Note : Identity function is a bijective function.

How to prove that f is one-one ?

If $f(x_1) = f(x_2)$ $_1 = x_2$, then f is one-one

OR

If x_1 x_2 $_1$) $_2$)

How to prove that f is onto ?

Let y

Let y = f(x)

We find x in terms of y.

If x A, then f is onto, otherwise not.

Example 37 : Let

Let f :

Examine if f is a bijective function.

Solution : Let x_1, x_2

Now $f(x_1) = f(x_2)$

$3x_1 + 7 = 3x_2 + 7$

$x_1 = x_2$

f is one-one (injection)

Let y

Let $y = f(x)$

$y = 3x + 7$

x =

If y = 1, x = = –2

f is not onto

f is not a bijective function.

Example 38 : Let X be the set of real numbers excluding 1. Show that the function

f : X X, f(x) =

Solution : Let x_1, x_2 X (domain)

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

(by componendo and dividendo)

$x_1 = x_2$

f is one-one

Let y

Let y = f(x)

y(x–1) = x+1

yx–y = x+1

yx–x = y+1

(y–1) = y+1

(domain)

Thus, for every y X (co-domain), There exists

such that

f is onto.

Example 39 : Let A = {1, 2, 3}. Write down all the bijective functions from A to itself.

Solution :

i : A A, i(1) =1, i(2) = 2, i(3) = 3

f_1 : A A, $f_1(1)=1$, $f_1(2) = 3$, $f_1(3) = 2$

f_2 : A A, $f_2(1)=2$, $f_2(2) = 1$, $f_2(3) = 3$

f_3 : A A, $f_3(1)=2$, $f_3(2) = 3$, $f_3(3) = 1$

f_4 : A A, $f_4(1)=3$, $f_4(2) = 1$, $f_4(3) = 2$

f_5 : A A, $f_5(1)=4$, $f_5(2) = 2$, $f_5(3) = 1$

Note : There are



LET US KNOW

If A is a finite set having n elements, there are n bijective functions from A to itself.

The first element of the domain can be associated in n ways, the second element can be associated in (n–1) ways, the third element can be associated in (n–2) ways. In this way, the (n–1)th element can be associated in 2 ways, the n th element can be associated in 1 way.

Thus, all the n elements can be associated in n(n–1) (n–2) . . . 2.1,

i.e., n

Thus, the number of bijective functions from A to itself is n

Theorem 8 : Let A be a finite set, and f : A A be onto. Then f is one-one.

Proof : Let A be a finite set having n elements.

Let A = $\{a_1, a_2, \ldots, a_n\}$, where a_i's are distinct.

Let f : A A be onto.

range of f = co-domain of f = **A**

A = $\{f(a_1), f(a_2), \ldots, f(a_n)\}$

A has n elements.

$f(a_1)$ $f(a_2)$, . . . , $f(a_n)$ are distinct. Thus, distinct elements in **A** (domain) have distinct images in A (co-domain),

f is one-one.

Note : The result does not hold good if A is an infinite set.

Let be the set of natural numbers.

Let f : ,

Now f(1) = 1, f(2) = 1,

f(3) = 3–1 = 2, f(4) = 4–1 = 3, f(5) = 5–1 = 4, and so on.

Thus, each element in

in

Here f is not one-one, for f(1) = 1, f(2) = 1

Theorem 9 : Let A be a finite set, and f : A A be one-one. Then f is onto.

Proof : Let A be a finite set having n elements.

Let A = $\{a_1, a_2, \ldots, a_n\}$, where a_i's are distinct.

Let f : A A be one-one.

$f(a_1), f(a_2), \ldots, f(a_n)$ are n distinct elements of A (co-domain)

Let u A (co-domain)

Let u = $f(a_i)$, 1 i

Thus, there exists a A (domain) such that $f(a_i) = u$

f is onto.

Note : The result does not hold good if A is an infinite set.

Let

Let f :

Let x_1, x_2

Then $f(x_1) = f(x_2)$ $_1$ $_2$ $_1 = x_2$

f is one-one

f is not onto, for the range of f is {5, 10, 15, 20, . . . }



CHECK YOUR PROGRESS

Q 29: If A = {1, 2}, write down all the bijective functions from A to itself.

Q 30: Let A = {1, 2, 3, 4, 5}. How many bijective functions are there from the set A to itself ?

Q 31: Write down the condition such that a constant function is onto.

Q 32: Write down the condition such that a constant function is one-one.

Q 33: Let be the set of real numbers.

Let f : , f(x) = , x .

Examine if f is a bijective function.

Q 34: Let be the set of natural numbers.

Let f : , $f(x) = x^2 + 1$, x .

Examine if f is (i) one-one, (ii) onto.

Q 35: Let be the set of real numbers.

f : is defined by

Examine if f is (i) one-one, (ii) onto.

Q 36: Let f : be defined by f(x) = |x|.

Examine if f is (i) one-one, (ii) onto.



LET US KNOW

f(x) = |x| = ,

x is a real number

The function is known as the absolute value function or modulus function.



1.10 LET US SUM UP

- A set may be viewed as a well defined collection of objects (elements, point, members) such that given any object, it is possible to determine whether that object belongs to the given collection or not.
- Union, intersection, difference, symmetric difference, complementation are some operations on set.
- If A, B are nonempty sets, a subset of AXB is said to be a relation from A to B.
- A relation R on a nonempty set A is called
  (i) reflexive, if (a, a) R, for all a A
  (ii) symmetric if whenever (a, b) R, (b, a)
  (iii) antisymmetric if (a, b) R, (b, a) R,
  (iv) transitive if whenever (a, b), (b, c) R, then (a, c)
- A relation R on a nonempty set A is called an equivalence relation if it is reflexive, symmetric, and transitive.
- If A, and B are two nonempty sets and if each element of A is associated with a unique element of B, then the rule by which this association is made, is called a function from A to B.
- Every function is relation, but every relation is not a function.

1.11 FURTHER READINGS

1) **A Course in Abstract Algebra** by Vijay K Khanna and SK Bhambri (Vikas Publishing House Private Limited).

2) **Higher Algebra Abstract and Linear** by Sadhan Kumar Mapa (Asoke Prakasan).

3) **Modern Algebra** by AR Vasistha (Krishna Prakashan Media (P) Ltd.

1.12 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: A= {1, 2, 3}, B = {–1, 2, 3};

A B = {–1, 1, 2, 3}, A

A–B = {1} B–A = {–1}

Ans to Q No 2: (a) Singleton set, for 2 is the only even number, which is prime.

(b) null set, for there are no prime numbers less than 2.

(c) null set, for there are no odd natural numbers that are divisible by 2.

(d) singleton set, the only element is

(e) singleton set, zero satisfies x+10 = 10.

(f) null set, for there is no even number whose square is 9.

(g) null set.

(h) singleton set, for 0 is the only number which is neither positive nor negative.

Ans to Q No 3: A = {F, I, L, E}, B = {L, I, F, E}, C = {L, I, E, F} clearly A = B = C.

Ans to Q No 4: A = {0, 2}, B = {2}, C = $\{x : x^2 - 2x = 0\}$ = {0, 2} clearly A

B

Note that A B, B

Ans to Q No 5: (a) The subsets of {0} are

(b) The subsets of {0, 1} are

(c) The subset of is

(d) The subsets of { } are , {

(e) The subsets of {(1, 2), (3, 4)} are

(3, 4)}.

Ans to Q No 6: (a) {1, 2} is not a subset of {2, 3};

{2, 3} is not a subset of {1, 2};

{1, 2}, {2, 3} are not comparable.

(b) {2, 4, 6} is a subset of {1, 2, 3, 4, 5, 6}.

{2, 4, 6}, and {1, 2, 3, 4, 5, 6} are comparable.

Ans to Q No 7: A = {1, 2, 3, 4, 5}, n(A) = 5

Number of subsets of A = $2^5 = 32$.

Any three disjoint subsets of A are {1, 2}, {3, 4}, {5}.

Ans to Q No 8: A = {1, 2, 3, 4, 5}

B = {2, 4, 6, 8, 10}

C = {2, 4, 6, 7, 9}

A B = {2, 4, 4} = A C, but B

Ans to Q No 9: A = {1, 2, 3, 4, 5, 6}

B = {2, 4, 6, 7, 9}

C = {1, 3, 5, 7, 9}

A B = {1, 2, 3, 4, 5, 6, 7,9} = A C, but B

Ans to Q No 10: A = {1, 2}, B = {2, 3}, C = {1, 3}

A B = {2} , B C = {3} , C A = {1} , but A B C =

Ans to Q No 11: Let x A

This x B [A

x C [B

Thus, x A x

A

Ans to Q No 12: Let x A

This x A and x C

x B and x

x B

A C B

Again, Let y B

y B and y

y A and y

y A

B C A

From (1) and (2) A C = B

Ans to Q No 13: Let x A

This x A′

x ′, (′ A′ x A′ x ′)

x

Thus, x A x

A

Ans to Q No 14: Let x

This x C and x B

x C and x A, (A B, x B x A)

x

Thus, x C–B x

C–B

Ans to Q No 15: Let x A

This x A B (A A

x A B (A B, x B = A

x A and x

Thus, x A x

A

Again, Let y

This y A B (B A B)

y A B (A B = A

y A and y

Thus, y B y A

B A (2)

From (1) and (2), A = B.

Ans to Q No 16: (i) Let x A

This x A or x B

x B or x A (A B x A x

x

Thus, x A B x

A B

Again, we know that B A

From (1) and (2), A

(ii) Let x A – B

This x A or x B

x A or x A

A – B A

We know that if A B, A

A – B A (A– B) A = A

(iii) Let x (A – B)

This x A – B and x B

(x A and x B) and x

x A and (x B and x

x B and x

But there cannot be any element x which satisfies x B and x

This implies that (A – B) B must be empty, i.e., (A – B) B =

Ans to Q No 17: Let x A

This x A B

x B (A

x B C

x C (B

Thus, x A x

A

Ans to Q No 18: A ′ B) = (A A′) (A

= A

Ans to Q No 19: (A – B) (A A)

= (A ′) (B A), (A – B = A ′)

= A ∩ B) ∪ A

= A ∪ A

= (A ∪) ∩ A

= ∩ A

=

∴ A – B, and A

Again, (A ∩ B) ∪ A)

= (A ∩ B) ∪ (B ∩ A′), (B – A = B ∩ A′)

= A ∩ (B ∪ B) ∩ A′

= A ∩ (B ∩ A′)

= A ∩ B)

= (A ∪ A′) ∩

= ∩

=

∴ A

Again, (B – A)

= (B ∩ A′) ∩ (A ∪)

= B ∪ A) ∩ ′

= (B ∪) ∩ ′

= ∩ ′

=

∴ B – A, and A – B are disjoint.

Ans to Q No 20: n(A) = 4, n(B) = 3.

number of relations from A to B = $2^{4x3} = 2^{12}$

Ans to Q No 21: n(A) = 5

∴ number of relations on A = $2^{5x5} = 2^{25}$.

Ans to Q No 22:

7 > 4, ∴ (7, 4) ∈ R

23 ∴ (23, 32) ∈

5 ∴ (5, 5) ∈

72 > 27, ∴ (72, 27) ∈ R

18 ∴ (18, 19) ∈

25 > 21, ∴ (25, 21) ∈ R

Ans to Q No 23: The sum of two even integers cannot be odd.

R is a null relation.

Ans to Q No 24: The identity relation I_A

= {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)}

Ans to Q No 25: R^{-1} = {(7, 4), (8, 5), (7, 6), (8, 6), (9, 6)}

Ans to Q No 26: (a) If there exists at least one a A such that (a, a)

(b) If there exist a, b A such that (a, b) R, but (b, a)

(c) If there exist a, b A, a b, such that (a, b) R, but (b, a)

(d) If there exist a, b, c A such that (a, b) R, (b, c) R but (a, c)

Ans to Q No 27: Let a

0 is divisible by 5

i.e. a – a is divisible by 5.

(a, a) R, for all a

R is reflexive.

Let (a, b) R; a, b

This a – b is divisible by 5.

b – a is divisible by 5

(b, a)

R is symmetric.

Again, let (a, b) R, (b, c) R; a, b, c

This a – b is divisible by 5; b – c is divisible by 5.

(a – b) + (b – c) is divisible by 5

a – c is divisible by 5

(a, c)

R is transitive.

Thus, R is an equivalence relation on

Ans to Q No 28: Let x A, i. e., x is a triangle in a plane.

We know that a triangle is similar to itself.

x is similar to x

i.e. (x, x)

R is reflexive.

Let (x, y)

This .

y is similar to x

(y, x)

R is symmetric.

Let (x, y) R, (y, z)

This

x is similar to z

(x, z)

R is transitive

Thus, R is an equivalance relation on A.

Ans to Q No 29: There are 2 bijective functions from

A = {1, 2} to itself.

i : A A, i(1) = 1, i (2) = 2

f : A A, f(1) = 2, f (2) = 1

Ans to Q No 30: A = {1, 2, 3, 4, 5}, n(A) = 5

number of bijective functions from A to A = 5

120.

Ans to Q No 31: A constant function is onto if the co-domain is a singleton set.

Ans to Q No 32: A constant function is one-one if the domain is a singleton set.

Ans to Q No 33: f : , f(x) = , x

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

=

$3x_1 + 7 = 3x_2 + 7$

$3x_1 = 3x_2$

$x_1 = x_2$

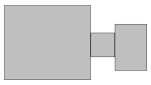
f is one-one.

Let u

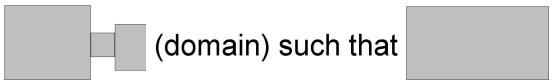
Let f(x) = u

$3x + 7 = 5u$

$3x = 5u - 7$

$x =$ 

Thus, corresponding to every u s

 (domain) such that

f is onto.

Thus, f is a bijective function.

Ans to Q No 34: f : $^2 + 1$

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

$x_1^2 + 1 = x_2^2 + 1$

$x_1^2 = x_2^2$

$x_1 = x_2$

f is one-one

Clearly, f is not onto. 1 (co-domain) is not an image of any element of

Ans to Q No 35: f is neither one-one nor onto.

$f(1) = 1, f(2) = 1, f(3) = 1, \ldots$

f is many-one.

Moreover, the range of $f = \{-1, 0, 1\}$

f is not onto.

Ans to Q No 36: f is neither one-one nor onto

$f(1) = |1| = 1, f(-1) = |-1| = 1$

f is many-one.

Again, the range of f is the set of non-negative real numbers.

f is not onto.

1.13 MODEL QUESTIONS

Q 1: Let A be a finite set having n elements. Prove that the number of subsets of A is 2^n.

Q 2: Let A, B, C be three sets. Prove that (A – C) (C – B) =

Q 3: Let A = {1, 2, 3}, B = {3, 4, 5}

How many relations are there from A to B ?

Q 4: Let A = {3, 4, 5}, B = {5, 6, 7}

Which of the following relations are functions from A to B ? If it is a function, determine whether it is one-one and whether it is onto ?

(i) {(3, 5), (4, 5), (5, 7)}

(ii) {(3, 7), (4, 5), (5, 6)}

(iii) {(3, 6), (4, 6), (5, 6)}

(iv) {(3, 6), (4, 7), (5, 5)}

Q 5: Let A = {1, 2, 3}

R = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)}

Examine if R is (i) reflexive, (ii) symcuetric, (iii) transitive.

Q 6: Let be the set of rational numbers and f :

defined by f(x) = 4x+ 5. Examine if f is bijective.

Q 7: Let be be the set of complex numbers and

numbers.

Let f : , f(z) = |z|, z

Examine if f is (i) one-one, (ii) onto.

[Hints : Neither one-one nor onto.

f(3+4i)=5, f(3–4i) = |3–4i| = 5 f is not one-one, f(z) = |z| 0, but

contains negative numbers so, f is not onto.]

*** ***** ***

UNIT 2 : LATTICES

UNIT STRUCTURE

2.1 Learning Objectives

2.2 Introduction

2.3 Partially Ordered Sets (Posets)

- 2.3.1 Partial Order Relation
- 2.3.2 Partially Ordered Set
- 2.3.3 Dual of the partially Ordered Set (A, $\leq$)
- 2.3.4 Covering Relation and Hasse Diagram
- 2.3.5 Upper Bound and Lower Bound

2.4 Lattices as Posets

2.5 Propertices of Lattices

2.6 Lattices as Algebraic Structures

2.7 Sublattices

2.8 Direct Product of Lattices

2.9 Homomorphism of Lattices

2.10 Some Special Lattices

- 2.10.1 Bounded Lattice
- 2.10.2 Distributive Lattice
- 2.10.3 Complemented Lattice

2.11 Let Us Sum Up

2.12 Further Readings

2.13 Answers To Check Your Progress

2.14 Model Questions

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know-

- lattices as posets, lattices as algebraic structures
- properties of lattices
- sublattices, direct product of lattices, homomorphism of lattices, and some special lattices.

2.2 INTRODUCTION

Lattice (also called Dedekind Structure) is an important branch of abstract mathematics. The concept of a lattice was first studied by Richard Dedekind (1831-1916) in 1879. Later on the subject was developed by Garrett Birkhoff (1911-1996), John Von Neumann (1903-1957), and others in the first half of the twentieth century.

A lattice is a partially ordered set in which every two elements have a unique least upper bound (also called supremum), and a unique greatest lower bound (also called infimum). It can also be viewed as an algebraic structure satisfying certain axioms. In this unit we will study both the views and show that the two definitions are equivalent. Also we will study different properties of lattices, sublattices and some special lattices.

2.3 PARTIALLY ORDERED SETS (POSETS)

2.3.1 Partial Order Relation

The concept of a partially ordered set is based on that of a partial order relation. A generalisation of the familiar '$\leq$' (less than or equal to) relation gives the notion of a partial order relation.

Let A be a nonempty set. A relation R on A is said to be a partial order relation if R is reflexive, antisymmetric, and transitive, i.e., R is a partial order relation on A if

(i) aRa, for every $a \in A$ **(reflexivity)**

(ii) aRb and bRa imply a = b, a, $b \in A$ **(antisymmetry)**

(iii) aRb and bRc imply a = c, a, b, $c \in A$ **(transitivity)**

Note : A partial order relation on a nonempty set A is often denoted by "$\leq$", even if it is not our usual 'less than or equal to'.

$a \leq b$ is read 'a precedes b' or 'b succeeds a'.

Some Examples of Partial Order Relation

1. The most familiar relation $\leq$ (less than or equal to) on the set of natural numbers $\underline{\underline{N}}$ is a partial order relation on $\underline{\underline{N}}$.

(i) We have $a \leq a$, for every $a \in \underline{\underline{N}}$.

$\therefore \leq$ is reflexive.

(ii) If $a \leq b$, $b \leq a$; $a, b \in \underline{\underline{N}}$, than $a = b$

$\therefore \leq$ is antisymmetric

(iii) If $a \leq b$, $b \leq c$; $a, b, c \in \underline{\underline{N}}$, than $a \leq c$

$\therefore \leq$ is transitive

$\therefore \leq$ is a partial order relation on $\underline{\underline{N}}$.

Note : The relation $\leq$ (less than or equal to) is a partial order relation on any nonempty subset of the set of real numbers.

2. Let x = {1, 2, 3}

Let P(x) be the power set of X, i.e., P(x) is the set of all subsets of X, i.e.,

P(x) = [{1, 2, 3}, {1, 2}, {2, 3}, {3, 1}, {1}, {2}, {3}, ϕ]

Let $A, B \in P(x)$

Let $A \leq B$ mean "A is a subset of B", i.e. "$A \subseteq B$"

(i) We have $A \subseteq A$, for any $A \in P(x)$

i.e. $A \leq A$, for any $A \in P(x)$

$\therefore \leq$ is reflexive.

(ii) We know that $A \subseteq B$, $B \subseteq A$ imply A=B, $A, B \in P(x)$

i.e., $A \leq B$, $B \leq A$ imply A=B

$\therefore \leq$ is antisymmetric.

(iii) We know that $A \subseteq B$, $B \subseteq C$ imply A=C, $A, B, C \in P(x)$

i.e. $A \leq B$, $B \leq C$ imply A=C

$\therefore \leq$ is transitive.

$\therefore \leq$ is a partial order relation on P(x).

Note : We note that the above power set P(x) has non-comparable elements, e.g., {1}, {2, 3} under the partial order relation $\subseteq$. (This is the reason behind for using the adjective 'partial'.) If this possibility does not exist, i.e. if for every pair a, b on a nonempty set A, we have either $a \leq b$ or $b \leq a$, then the partial order relation is called a linear order relation.

The partial order relation $\leq$ (less than or equal to) on the set of natural numbers $\underline{\underline{N}}$ is a linear order relation.



LET US KNOW

If "$\leq$" is a partial order relation on a nonempty set A, and we have either $a \leq b$ or $b \leq a$, $a, b \in A$, then a, b are said to be comparable.

3. Let x be a nonempty set and P(x) be the power set of X. Let $A \leq B$ mean "A is a subset of B", $A, B \in P(x)$. Then $\leq$ is a partial order relation on P(x).
4. Let D_{36} be the set of all positive divisors of 36, i.e., D_{36} = {1, 2, 3, 4, 6, 9, 12, 18, 36}

   Let $a \leq b$ mean "a divides b", i.e., "a is a divisor of b", $a, b \in D_{36}$.

   Clearly, (i) a divides a, for every $a \in D_{36}$.

   $\therefore$ i. e., $a \leq a$

   $\therefore$ $\leq$ is reflexive.

   (ii) a divides b, b divides a imply a = b, $a, b \in D_{36}$.

   i.e., $a \leq b$, $b \leq a$ imply a = b

   $\therefore \leq$ is antisymmetric.

   $\therefore \leq$ is a partial order relation on D_{36}.

   (iii) a divides b, b divides c

   imply a divides c : $a, b, c \in D_{36}$

   i.e. $a \leq b$, $b \leq c$ imply $a \leq c$

   $\therefore \leq$ is a transitive

   $\therefore \leq$ is a partial order on D_{36}.
5. Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a, b \in \underline{\underline{N}}$. Let $a \leq b$ mean 'a divides b', i.e., 'a is a divisor of b'.

   'a divides b' means there is a natural number m such that b = ma.

   (i) a divides a, $a \in \underline{\underline{N}}$ (a = 1a)

   i. e., $a \leq a$

   $\therefore$ $\leq$ is reflexive.

   (ii) Let a divide b, and b divide a. Since a divides b, there is a natural number m such that b = ma.

Since b divides a, there is a natural number n such that

$a = nb$.

$\therefore b = ma = m(nb) = mnb$

$\therefore mn = 1$, (b is a natural number, $b \neq 0$)

Since m, n are natural numbers, therefore m = 1, n = 1.

$\therefore a = b$

Thus, a divides b, b divides a imply a = b

i.e., $a \leq b$, $b \leq a$ imply a = b

$\therefore \leq$ is antisymmetric.

(iii) Let a divide b, and b divide c.

Since a divides b, there is a natural number m such that b = ma.

Since b divides c, there is a natural number p such that c = pb.

Now, c = pb = p(ma) = (pm)a, where pm is a natural number.

$\therefore$ a divides c.

Thus, a divides b, b divides c imply a divides c.

i.e., $a \leq b$, $b \leq c$ imply $a \leq c$.

$\therefore \leq$ is transitive.

$\therefore \leq$ is a partial order relation on $\underline{\underline{N}}$.

Note : Let $\underline{\underline{Z}}_0$ be the set of integers excluding zero. Let $a, b \in \underline{\underline{Z}}_0$. Let $a \leq b$ mean 'a divides b'. Then $\leq$ is not a partial order relation on $\underline{\underline{Z}}_0$. Why ?

3 divides – 3, –3 divides 3. But $3 \neq -3$. $\leq$ is not antisymmetric.

2.3.2 Partially Ordered Set

A nonempty set A together with a partial order relation $\leq$ on A is called a partially ordered set (or a poset), and is denoted by $(A, \leq)$.

Some Examples of Partially Ordered Sets

1. Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a, b \in \underline{\underline{N}}$. Then '$\leq$' (less than or equal to) is a partial order relation on $\underline{\underline{N}}$.

   $\therefore (\underline{\underline{N}}, \leq)$ is a partially ordered set.

2. Let X = {1, 2, 3}

   Let P(x) be the power set of X.

Let $A, B \in P(x)$.

Let $A \leq B$ mean 'A is a subset of B'.

Then $\leq$ is a partial order relation on P(x).

$\therefore$ $(P(x), \leq)$ is a poset.

3. Let X be a nonempty set and P(x) be the power set of X. Let $A \leq B$ mean 'A is a subset of B', $A, B \in P(x)$. Then $\leq$ is a partial order relation on P(x).

   $\therefore$ $[P(x), \leq]$ is poset.

4. Let D_{36} be the set of all positive divisors of 36, i.e., $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

   Let $a \leq b$ mean 'a divides b', $a, b \in D_{36}$.

   Then $\leq$ is a partial order relation on D_{36}.

   $\therefore (D_{36}, \leq)$ is a poset.

5. Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a, b \in \underline{\underline{N}}$. Let $a \leq b$ mean 'a divides b'. Then $\leq$ is a partial order relation on $\underline{\underline{N}}$.

   $\therefore (\underline{\underline{N}}, \leq)$ is a poset.



LET US KNOW

A poset $(A, \leq)$ with a linear order relation is called a linearly ordered set or a chain. Thus, in a chain$(A, \leq)$, we have either $a \leq b$ or $b \leq a$, $a, b \in A$.

2.3.3 Dual of the partially Ordered Set $(A, \leq)$

Let $(A, \leq)$ be a poset.

We define a relation $\geq$ on A by '$a \geq b$ if and only if $b \leq a$' for $a, b \in A$.

(i) We have $a \leq a$, for all $a \in A$. since $(A, \leq)$ is a poset.

$\therefore$ $a \geq a$, for all $a \in A$ (by definition of $\geq$)

$\therefore$ $\geq$ is reflexive.

(ii) Let $a, b \in A$, and $a \geq b$, $b \geq a$.

$\therefore$ by definition $b \leq a$, $a \leq b$.

$\because$ $(A, \leq)$ is a poset, $a = b$.

Thus, $a \geq b$, $b \geq a$ imply $a = b$.

$\therefore \geq$ is antisymmetric.

(iii) Let a, b, $c \in A$, and $a \geq b$, $b \geq c$.

$\therefore$ by definition $b \leq a$, $c \leq b$, i.e. $c \leq b$, $b \leq a$

$\because$ $(A, \geq)$ is a poset, we have $c \leq a$

$\therefore$ by definition $a \geq c$.

Thus, $a \geq b$, $b \geq c$ imply $a \geq c$.

$\therefore \geq$ is transitive.

$\therefore \geq$ is a partial order relation on A, and $(A, \geq)$ is a poset.

Note : $\geq$ is called the dual order, and $(A, \geq)$ is called the dual of the poset $(A, \leq)$.

Let $\underline{\underline{N}}$ be the set of natural numbers.

Let $a, b \in \underline{\underline{N}}$. Let $a \leq b$ mean 'a is a divisor of b'. Then $b \geq a$ mean 'b is a multiple of a'. The poset $(\underline{\underline{N}}, \geq)$ is the dual of $(\underline{\underline{N}}, \leq)$, and vice versa.

2.3.4 Covering Relation and Hasse Diagram

Let $(A, \leq)$ be a poset. We define a relation < on A by 'a < b if and only if $a \leq b$, but $a \neq b$', $a, b \in A$.

b is said to cover a if a < b and there is no element c in A such that a < c < b holds.

Let D_{20} be the set of all positive divisors of 20, i.e, D_{20} = {1, 2, 4, 5, 10, 20}.

Let $a \leq b$ mean 'a is a divisor of b', $a, b \in D_{20}$. $(D_{20}, \leq)$ is a poset. Here 10 covers 5, 20 covers 10, but 20 does not cover 5 although 5 < 20, because 5 < 10 < 20.

The covering relation can be used to give a diagramatic representation of a finite partially ordered set $(A, \leq)$. Each element of A is drawn as a vertex by a point or a small circle in the plane and a line segment or curve is drawn that goes upward from a to b whenever b covers a. These line segments or curves may cross each other but must not touch any vertices other than their endpoints. Such a diagram, with labeled vertices, uniquely determines its partial order. These diagrams are known as Hasse diagrams after the name

of the German mathematician Helmut Hasse (1898-1979).

Let us consider the finite poset $(D_{20}, \leq)$, where D_{20} is the set of positive divisors of 20, i.e., $D_{20} = \{1, 2, 4, 5, 10, 20\}$, and $a \leq b$ means 'a is a divisor of b'. The Hasse diagram for representing the above poset is given below.

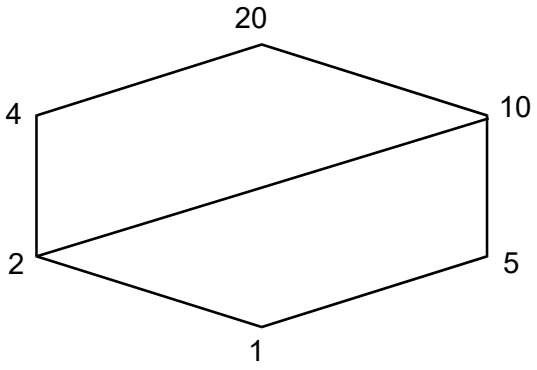


Fig 2.1



CHECK YOUR PROGRESS

Q 1: Let D_{30} be the set of positive divisors of 30. Let $a \leq b$ mean 'a is a divisor of b', $a, b \in D_{30}$. Show that $(D_{30}, \leq)$ is a poset. Draw the Hasse diagram of the poset.

Q 2: Let X = {1, 2, 3}. Let P(x) be the power set of X. Show that (P(x), $\leq$) is a poset where '$\leq$' means 'is a subset of', i.e. '$\subseteq$'. Draw the Hasse diagram of the poset.

Q 3: Draw the Hasse diagram of the poset (P(x), $\leq$), where X = {1, 2}, '$\leq$' means 'is a subset of'.

Q 4: Draw the Hasse diagram of the poset $(D_{36}, \leq)$, where D_{36} is the set of positive divisors of 36, and '$\leq$' means 'is a divisor of'.

2.3.5 Upper Bound and Lower Bound

Let $(A, \leq)$ be a poset and a, b be two elements of A.

An element $c \in A$ is said to be an upper bound of the pair a, b if $a \leq c$, and $b \leq c$.

An element $u \leq A$ is said to be a least upper bound (lub) or supremum (sup) of a, b if.

(i) u is an upper bound of a, b, i.e., if $a \leq u$, $b \leq u$; and

(ii) if $c \in A$ ia an upper bound of a, b; then $u \leq c$.

An element $d \in A$ is said to be a lower bound of a, b if $d \leq a$, and $d \leq b$.

An element $\upsilon \in A$ is said to be a greatest lower bound (glb) or infimum (inf) of a, b if -

(i) υ is a lower bound of a, b, i.e., $\upsilon \leq a$, $\upsilon \leq b$; and

(ii) if $d \in A$ is a lower bound of a, b; then $d \leq \upsilon$.

Theorem 2.1 : Let $(A, \leq)$ be a poset and $a, b \in A$

(i) If a, b have a least upper bound, then it is unique.

(ii) If a, b have a greatest lower bound, then it is unique.

Proof : (i) If possible, let u_1 and u_2 be two least upper bounds of a, b.

$\because$ u_1 is an upper bound of a, b; $a \leq u_1$, $b \leq u_1$

$\because$ u_2 is a least upper bound; $u_2 \leq u_1$

Interchanging the roles of u_1, u_2; we get

$u_1 \leq u_2$.

Now $(A, \leq)$ is a poset, and $u_2 \leq u_1$, $u_1 \leq u_2$.

$\therefore$ $u_1 = u_2$ (by antisymmetry).

i.e. lub is unique.

(ii) If possible, let υ_1 and υ_2 be two greatest lower bounds of a, b.

$\because$ υ_1 is an lower bound of a, b; $\upsilon_1 \leq a$, $\upsilon_1 \leq b$

$\because$ υ_2 is a greatest lower bound; $\upsilon_1 \leq \upsilon_2$

Interchanging the roles of υ_1, υ_2; we get

$\upsilon_1 \leq \upsilon_2$.

Now $(A, \leq)$ is a poset, and $\upsilon_1 \leq \upsilon_2$, $\upsilon_2 \leq \upsilon_1$.

$\therefore$ $\upsilon_1 = \upsilon_2$ (by antisymmetry).

i.e. glb is unique.

Note : Because of the uniqueness, we will use the article 'the',– the least upper bound, the greatest lower bound.

2.4 LATTICES AS POSETS

A partially ordered set $(L, \leq)$ in which every pair of elements a, b of L has a least upper bound and a greatest lower bound is called a lattice.

The unique least upper bound (lub) of a, b of L is, generally, denoted by $a \vee b$ (join or sum of a, b).

The unique greatest lower bound (glb) of a, b of L is, generally, denoted by $a \wedge b$ (meet or product of a, b).

Since the least upper bound and the greatest lower bound are unique, both $\vee$ and $\wedge$ are binary operations on L.

We note that every lattice $(L, \leq)$ is a poset, but every poset is not a lattice.

Let us consider the set A = {1, 2, 3, 4, 5}. Let $a \leq b$ mean 'a is a divisor of b', $a, b \in A$. Then $(A, \leq)$ is poset.

The lub of a, b = $a \vee b$

= the lcm of a, b

The glb of a, b = $a \wedge b$

= the gcb of a, b

Now lub of 2, 3 = $2 \vee 3$

= the lcm of 2, 3

= $6 \notin A$

$\therefore$ $(A, \leq)$ is not a lattice.

It is evident from the Hasse diagram.

The Hasse diagram is given below.

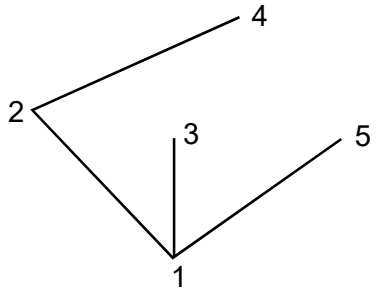


Fig 2.2

Some Examples of Lattices

1. Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a \leq b$ mean 'a is a divisor of b', $a, b \in \underline{\underline{N}}$.

   Then $(\underline{\underline{N}}, \leq)$ is a poset.

   The lub of a, b = $a \vee b$

   = lcm (a, b)

   The glb of a, b = $a \wedge b$

   = gcd (a, b).

   Clearly $a \vee b \in \underline{\underline{N}}$, $a \wedge b \in \underline{\underline{N}}$; a, b $a \in \underline{\underline{N}}$

   $\therefore$ $(\underline{\underline{N}}, \leq)$ is a lattice.

2. Let x be a nonempty set. Let P(x) denote the power set of X. Let $A \leq B$ mean 'A is a subset of B', $A, B \in P(x)$.

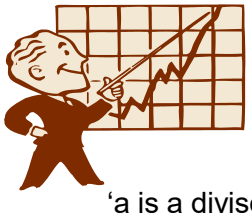
   Then $(P(x), \leq)$ is poset.

   The lub of A, B = $A \vee B = A \cup B$

   The glb of A, B = $A \wedge B = A \cap B$

   Clearly $A \vee B \in P(x)$; $A \wedge B \in P(x)$; $A, B \in P(x)$

   $\therefore$ $(P(x), \leq)$ is a lattice.



CHECK YOUR PROGRESS

Q 5: Let D_{32} be the set of positive divisors of 32, i.e. $D_{32} = \{1, 2, 4, 8, 16, 32\}$. Let $a \leq b$ mean 'a is a divisor of b', $a, b \in D_{32}$. Show that $(D_{32}, \leq)$ is a poset.

Draw a Hasse diagram of the poset.

Examine if $(D_{32}, \leq)$ is a lattice.

Q 6: Let X = {1, 2, 3}.

Let S = [{1, 2}, {2, 3}, {3, 1}, {1}, {2}, {3}]

Let $A \leq B$ mean 'A is a subset of B'; $A, B \in S$. Show that $(S, \leq)$ is a poset. Draw a Hasse diagram of the poset.

Examine if $(S, \leq)$ is a lattice.

Q 7: Let A be the set of real-valued functions defined on [0, 1].

Let $f \leq g$ mean 'f(x) $\leq$ g(x)'; x $\in$ [0, 1]; $f, g \in A$.

Show that $(A, \leq)$ is a poset.

Examine if $(A, \leq)$ is a lattice.

Q 8: Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a \leq b$ mean 'a is less than or equal to b'; $a, b \in \underline{\underline{N}}$.

Show that $(\underline{\underline{N}}, \leq)$ is a poset.

Examine if $(\underline{\underline{N}}, \leq)$ is a lattice.

Principle of Duality

Let $(A, \leq)$ be a poset.

We define a relation $\geq$ on A by '$a \geq b$ if and only if $b \geq a$'; for $a, b \in A$. Then $(A, \geq)$ is a poset, called the dual of the poset $(A, \leq)$. [2.3.3]

The Hasse diagram of the poset $(A, \geq)$ can be obtained from that of $(A, \leq)$ by simply turning it upside down.

Let D_{32} be the set of positive divisors of 32, i.e.,

$D_{32} = \{1, 2, 4, 8, 16, 32\}$

Let $a \leq b$ mean 'a is a divisor b', $a, b \in D_{32}$. Then $(D_{32}, \leq)$ is a poset.

Now, $(D_{32}, \geq)$ is also a poset where $b \geq a$ means 'b is a multiple of a'; $a, b \in D_{32}$.

The Hasse diagram for $(D_{32}, \leq)$ is show in Fig 2.3(a), whereas the Hasse diagram for $(D_{32}, \geq)$ is shown in Fig 2.3(b).

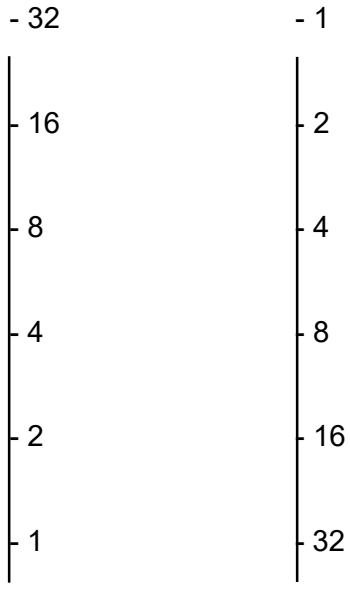


Fig 2.3 (a)

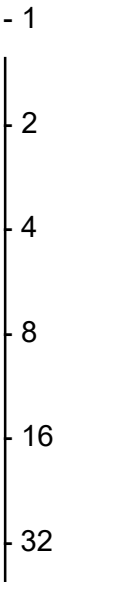


Fig 2.3 (b)

Now, if $(L, \leq)$ is a lattice, $(L, \geq)$ is also a lattice. The operations of join and meet on $(L, \leq)$ become the operations of meet and join respectively on $(L, \geq)$.

The principle of duality states that any statement in respect of lattices involving the operations $\vee$ and $\wedge$, and the relation $\leq$ and $\geq$ remains true, if $\vee$ is replaced by $\wedge$, and $\wedge$ is replaced by $\vee$; $\leq$ is replaced by $\geq$, and $\geq$ is replaced by $\leq$.

2.5 PROPERTICES OF LATTICES

Property I :

Let $(L, \leq)$ be a lattice; and $a, b, c \in L$.

Idempotent Laws :

1(a) $a \vee a = a$, **1(b)** $a \wedge a = a$

Commutative Laws :

2(a) $a \vee b = b \vee a$, **2(b)** $a \wedge b = b \wedge a$

Associative Laws :

3(a) $a \vee (b \vee c) = (a \vee b) \vee c$, **3(b)** $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

Absorption Laws :

4(a) $a \vee (a \wedge c) = a$, **4(b)** $a \wedge (a \vee b) = a$

Proof : 1(a) $a \vee a$ = lub of a, a = a

1(b) $a \wedge a$ = glb of a, a = a

Note : 1(b) is the dual of 1(a). 1(b) can be obtained from 1(a) by replacing $\vee$ by $\wedge$, lub by glb.

2 (a) $a \vee b$ = lub of a, b

= lub of b, a

$= b \wedge a$

2(b) Dual of 2(a). Replace $\vee$ by $\wedge$, lub by glb.

3(a) We know that $a \vee (b \vee c)$ is the least upper bound of a, $b \vee c$.

$\therefore a \leq a \vee (b \vee c)$ (1)

$b \vee c \leq a \vee (b \vee c)$ (2)

Again $b \vee c$ is the least upper bound of b, c.

$\therefore b \leq b \vee c$ (3)

$c \leq b \vee c$ (4)

Now $b \leq b \vee c$, and $b \vee c \leq a \vee (b \vee c)$

$\therefore b \leq a \vee (b \vee c)$ (5) (by transitivity)

Again $c \leq b \vee c$, and $b \vee c \leq a \vee (b \vee c)$

$\therefore c \leq a \vee (b \vee c)$ (6) (by transitivity)

Now, (1) and (5) imply that $a \vee (b \vee c)$ is an upper bound of a, and b, and hence by the definition of least upper bound, we have

$a \vee b \leq a \vee (b \vee c)$ (7)

Again, (6) and (7) imply that $a \vee (b \vee c)$ is an upper bound of c, and $a \vee b$, and hence by the definition of least upper bound, we have

$(a \vee b) \vee c \leq a \vee (b \vee c)$ (8)

Similarly $a \vee b \leq (a \vee b) \vee c$ (9)

$c \leq (a \vee b) \vee c$ (10)

$a \leq a \vee b$ (11)

$b \leq a \vee b$ (12)

Now $a \leq a \vee b$, and $a \vee b \leq (a \vee b) \vee c$

$\therefore a \leq (a \vee b) \vee c$ (13) (by transitivity)

Also, $b \leq a \vee b$, $a \vee b \leq (a \vee b) \vee c$

$\therefore b \leq (a \vee b) \vee c$ (14) (by transitivity)

From (10) and (14)

$b \vee c \leq (a \vee b) \vee c$ (15)

From (15) and (16), by antisymmetry of $\leq$, $a \vee (b \vee c) = (a \vee b) \vee c$.

3(b) Dual of 3(a)

Note : In view of 3(a), we can write $a \vee (b \vee c)$ and $(a \vee b) \vee c$ as $a \vee b \vee c$. Similarly, in view of 3(b) we can write $a \wedge (b \wedge c)$ and $(a \wedge b) \wedge c$ as $a \wedge b \wedge c$.

4(a) $a \wedge b$ is the greatest lower bound of a, b.

$\therefore a \wedge b \leq a$ (1)

$a \leq a$ (2)

It follows that a is an upper bound of a, and $a \wedge b$. Therefore, by the definition of least upper bound,

$a \vee (a \wedge b) \leq a$ (3)

On the other hand, by the definition of least upper bound.

$a \leq a \vee (a \wedge b)$ (4)

From (3) and (4), by antisymmetry of $\leq$, $a \vee (a \wedge b) = a$.

4(b) Dual of 4(a)



LET US KNOW

1. $a \le a \vee b$, and $b \le a \vee b$; $a \vee b$ is an upper bound of a and b.
2. If $a \le c$, and $b \le c$, then $a \vee b \le c$; $a \vee b$ is the least upper bound of a and b.
3. $a \wedge b \le a$ and $a \wedge b \le b$; $a \wedge b$ is a lower bound of a and b.
4. If $c \le a$ and $c \le b$, then $c \le a \wedge b$; $a \wedge b$ is the greatest lower bound of a and b.

Property II

Let $(L, \le)$ be a lattice, and $a, b \in L$. Then

1. $a \vee b = b$, if and only if $a \le b$
2. $a \wedge b = a$, if and only if $a \le b$
3. $a \wedge b = a$, if and only if $a \vee b = b$

[These three relations can also be written as

$a \le b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$]

Proof : 1. Let $a \vee b = b$ (1)

Now $a \le a \vee b$ (2)

$\therefore$ from (1) and (2) $a \le b$

Conversely, let $a \le b$

Also $b \le b$

$\therefore$ b is an upper bound of both a and b.

$\therefore$ by the definition of least upper bound, $a \vee b \le b$ (3)

Also, $a \vee b$ being an upper bound, $b \le a \vee b$ (4)

From (3) and (4), $a \vee b = b$ (by antisymmetry)

2. Let $a \wedge b = a$ (5)

Now $a \wedge b \le b$ (6)

$\therefore$ from (5) and (6) $a \le b$.

Conversely, Let $a \le b$

also $a \le a$

$\therefore$ a is a lower bound of both a and b.

$\therefore$ by the definition of greatest lower bound, $a \le a \wedge b$ (7)

Also, $a \wedge b$ being a lower bound $a \wedge b \le a$ (8)

From (7) and (8) $a \wedge b = a$ (by antisymmetry)

3. We have $a \wedge b = a \Leftrightarrow a \leq b$ (9)

Also we have $a \leq b \Leftrightarrow a \vee b = b$ (10)

Combining (9) and (10), we get $a \wedge b = a \Leftrightarrow a \vee b = b$.



LET US KNOW

Every chain is a lattice.

Let $(A, \leq)$ be a chain.

$\therefore$ we have either $a \leq b$ or $b \leq a$; $a, b \in A$.

Now $a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$

Accordingly, we get $a \vee b = b$ and $a \wedge b = a$

OR

$a \vee b = a$ and $a \wedge b = b$.

Hence every pair of elements a, b of A has a least upper bound and a greatest lower bound,

$\therefore$ $(A, \leq)$ is a lattice.

Property III

Let $(L, \leq)$ be a lattice, and $a, b, c, d \in L$.

1. If $a \leq b$,

   1(a) $a \vee c \leq b \vee c$ 1(b) $a \wedge c \leq b \wedge c$

   [This is known as the isotonic property.]

2. $a \leq c$ and $b \leq c$ if and only if $a \vee b \leq c$
3. $c \leq a$ and $c \leq b$ if and only if $c \leq a \wedge b$
4. If $a \leq b$ and $c \leq d$

   4(a) $a \vee c \leq b \vee d$ 4(b) $a \wedge c \leq b \wedge d$

Proof : 1(a) We know that $x \vee y = y$ if and only if $x \leq y$, $x, y \in L$.

Therefore, in order to prove that $a \vee c \leq b \vee c$,

we will prove that $(a \vee c) \vee (b \vee c) = b \vee c$.

Now $(a \vee c) \vee (b \vee c)$

$= ((a \vee c) \vee b) \vee c$, by associativity

$= (a \vee (c \vee b)) \vee c$, by associativity

$= (a \vee (b \vee c)) \vee c$, by commutativity

$= a \vee (b \vee c) \vee c$

$= (a \vee b) \vee (c \vee b)$ (i)

Since $a \leq b$ (given), $\therefore\ a \vee b = b$

Also $c \vee c = c$, by idempotency

$\therefore$ from (i), $(a \vee c) \vee (b \vee c) = b \vee c$

$\therefore\ a \vee c \leq b \vee c$.

1(b) We know that

$x \wedge y = x$, if and only if $x \leq y$, $x, y \in L$.

Therefore, in order to prove that $a \wedge c \leq b \wedge c$,

We will prove that $(a \wedge c) \wedge (b \wedge c) = a \wedge c$.

Now $(a \wedge c) \wedge (b \wedge c)$

$= ((a \wedge c) \wedge b) \wedge c$, by associativity

$= (a \wedge (c \wedge b)) \wedge c$, by associativity

$= (a \wedge (b \wedge c)) \wedge c$, by commutativity

$= a \wedge (b \wedge c) \wedge c$

$= (a \wedge b) \wedge (c \wedge c)$ (ii)

Since $a \leq b$ (given), $\therefore\ a \wedge b = a$

Also $c \wedge c = c$, by idempotency

$\therefore$ from (ii), $(a \wedge c) \wedge (b \wedge c) = a \wedge c$

$\therefore\ a \wedge c \leq b \wedge c$.

2. If $a \leq c$, we have $a \vee b \leq c \vee b$ (using 1(a) above)

Again $b \leq c \Leftrightarrow b \vee c = c$

$\Leftrightarrow c \vee b = c$, by commutativity

Hence $a \leq c$ and $b \leq c$ if and only if $a \vee b \leq c$.

3. If $c \leq a$, we have $c \wedge b \leq a \wedge b$ (using 1(b) above)

Again $c \leq b \Leftrightarrow c \wedge b = c$

Hence $c \leq a$ and $c \leq b$ if and only if $c \leq a \wedge b$.

4(a). If $a \leq b$, we have

$a \vee c \leq b \vee c$ {using 1(a)}

i.e. $a \vee c \leq c \vee b$ (iii), by commutativity

If $c \leq d$, we have

$c \vee b \leq d \vee b$ {using 1(a)}

i.e. $c \vee b \leq b \vee d$ (iv), by commutativity

$\therefore$ from (iii) and (iv), by transitivity, $a \vee c \leq b \vee d$.

4(b). If $a \leq b$, we have

$a \wedge c \leq b \wedge c$ {using 1(b)}

i.e. $a \wedge c \leq c \wedge b$ (v), by commutativity

If $c \leq d$, we have

$c \wedge b \leq d \wedge b$ {using 1(b)}

i.e. $c \wedge b \leq b \wedge d$ (vi), by commutativity

$\therefore$ from (v) and (vi), by transitivity, $a \wedge c \leq b \wedge d$.

Property IV

Let $(L, \leq)$ be a lattice, and $a, b, c \in L$. Then

1. $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$
2. $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

[The above two inequalities are known as Distributive Inequalities]

Proof 1. $\because$ $a \wedge b$ is the greatest lower bound of a, b,

$$\therefore \left.\begin{array}{l} a \wedge b \leq a \\ a \wedge b \leq b \end{array}\right\} \text{ (i)}$$

Again, since $b \vee c$ is the least upper bound of b, c,

$$\therefore \left.\begin{array}{l} b \leq b \vee c \\ c \leq b \vee c \end{array}\right\} \text{ (ii)}$$

From (i) and (ii), we have

$a \wedge b \leq b \vee c$, by transitivity

$$\therefore \left.\begin{array}{l} a \wedge b \leq a \\ a \wedge b \leq b \vee c \end{array}\right\}$$

$\therefore$ $a \wedge b$ is a lower bound of a, $b \vee c$.

$\therefore$ $a \wedge b \leq a \wedge (b \vee c)$ (iii)

Again, $a \wedge c$ is the greatest lower bound of a, c.

$$\therefore \left.\begin{array}{l} a \wedge c \leq a \\ a \wedge c \leq c \end{array}\right\} \text{ (iv)}$$

From (iv) and (ii)

$a \wedge c \leq b \vee c$, by transitivity

$$\therefore \left.\begin{array}{l} a \wedge c \leq a \\ a \wedge c \leq b \vee c \end{array}\right\}$$

$\therefore$ $a \wedge c$ is a lower bound of a, $b \vee c$.

$\therefore$ $a \wedge c \leq a \wedge (b \vee c)$ (v)

From (iii) and (v), $a \wedge (b \vee c)$ is an upper bound of $a \wedge b$, $a \wedge c$.

$\therefore$ $(a \wedge c) \vee (a \wedge c) \leq a \wedge (b \vee c)$

i.e. $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$.

2. Dual of the above result.

Property V

Let $(L, \leq)$ be a lattice; and $a, b, c \in L$. Then

$a \leq c$ if and only if $a \vee (b \wedge c) \leq (a \vee b) \wedge c$

[The above inequality is known as Modular Inequality.]

Proof : We have

$a \leq c \quad \Leftrightarrow \quad a \vee c = c \quad$ (i)

Again, by distributive inequality,

$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

i.e. $a \vee (b \wedge c) \leq (a \vee b) \wedge c$, using (i)

Conversely, Let $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

$\therefore \; a \leq a \vee (b \wedge c)$

$\leq (a \vee b) \wedge c$

$\leq c$, by definitions of lub and glb.

i.e. $a \leq c$.

Thus $a \leq c$ if and only if $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Property VI

Let $(L, \leq)$ be a lattice; and $a, b, c \in L$. Then

1. $a \leq b$, and $a \leq c$ imply $a \leq b \vee c$
2. $a \leq b$, and $a \leq c$ imply $a \leq b \wedge c$

Proof : 1. $b \vee c$ is the least upper bound of b, and c.

$\therefore \; b \leq b \vee c$.

Now $a \leq b$, $b \leq b \vee c$

$\therefore$ by transitivity, $a \leq b \vee c$.

2. $a \leq b$, $a \leq c$

$\therefore$ a is a lower bound of b, and c.

But $b \wedge c$ is the greatest lower bound of b, c.

$\therefore \; a \leq b \vee c$.



CHECK YOUR PROGRESS

Q 9: Let a, b be two positive integers.

Show that

max (a, min (a, b)) = a

min (a, max (a, b)) = a

Q 10: Let a, b be two positive integers.

Show that

lcm (a, gcd(a, b)) = a,

gcd (a, lcm(a, b)) = a.

Q 11: Let $(L, \leq)$ be a lattice; and $a, b, c, d \in L$.

If $a \leq b$, $b \leq c$, show that

(i) $a \vee b = b \wedge c$

(ii) $(a \wedge b) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Q 12: Let $(L, \leq)$ be a lattice; and $a, b, c, d \in L$.

Show that

(i) $(a \wedge b) \vee (c \wedge d) \leq (a \vee c) \wedge (b \vee d)$

(ii) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$

Q 13: Let $(L, \leq)$ be a lattice; and $a, b, c \in L$.

Show that the statement

$a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$ is self dual.

2.6 LATTICES AS ALGEBRAIC STRUCTURES

In mathematics, an algebraic structure is a nonempty set equipped with binary operation (s) satisfying certain axioms

Let L be a nonempty set equipped with two binary operations $\vee$ (join), and $\wedge$ (meet). Then $(L, \vee, \wedge)$ is a lattice if the following axioms are satisfied.

Commutative law

(1a) $a \vee b = b \vee a$ **1(b)** $a \wedge b = b \wedge a$

Associative law

(2a) $(a \vee b) \vee c = a \vee (b \vee c)$, **2(b)** $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

Absorption law

(3a) $a \vee (a \wedge b) = a$, **3(b)** $a \wedge (a \vee b) = a$, where $a, b, c \in L$.

Duality

Let $(L, \vee, \wedge)$ be a lattice. The dual of any statement in $(L, \vee, \wedge)$ is obtained by interchanging $\vee$ and $\wedge$. For example, the dual of $a \vee (a \wedge c) = a$ is $a \wedge (a \vee b) = a$. We note that the dual of each axiom of a lattice is also an

axiom. Accordingly, the dual of any theorem in a lattice is also a theorem.

Idempotent law

Let $(L, \vee, \wedge)$ be a lattice. Then (i) $a \vee a = a$, (ii) $a \wedge a = a$, for every $a \in L$.

Proof : (i) $a \vee a = a \vee (a \wedge (a \vee b))$, by absorption law

$= a$, by absorption law.

(ii) $a \wedge a = a \wedge (a \vee (a \wedge b))$, by absorption law.

$= a$, by absorption law.

Note : (ii) is the dual of (i), and vice versa. (ii) can also be obtained from (i) by replacing $\vee$ by $\wedge$, and $\wedge$ by $\vee$.

Example : Let X be a nonempty set. Let P(x) denote the power set of X, i.e., P(x) is the collection of all subsets of X.

We define $\vee$ and $\wedge$ on P(x) by

$A \vee B = A \cup B$,

$A \wedge B = A \cap B$, for all $A, B \in P(x)$

Clearly $A \vee B = A \cup B \in P(x)$, $A \wedge B = A \cap B \in P(x)$.

i.e., $\vee$ and $\wedge$ are binary operations on P(x).

Now 1(a) $A \vee B = A \cup B = B \cup A = B \vee A$, $A, B \in P(x)$

1(b) $A \wedge B = A \cap B = B \cap A = B \wedge A$.

2(a) $(A \vee B) \vee C = (A \cup B) \cup C = A \cup (B \cup C) = A \vee (B \vee C)$

2(b) $(A \wedge B) \wedge C = (A \cap B) \cap C = A \cap (B \cap C) = A \wedge (B \wedge C)$

$A, B, C \in P(x)$

3(a) $A \vee (A \wedge B) = A \cup (A \cap B) = A$

3(b) $A \wedge (A \vee B) = A \cap (A \cup B) = A$

$\therefore$ $(P(x), \vee, \wedge)$ is a lattice.

Theorem 2.2 : Two definitions given for a lattice are equivalent.

Proof : Firstly, we define a lattice as a poset. Then every pair of elements a, b of the poset $(L, \leq)$ has a least upper bound and a greatest lower bound.

We denote the unique least upper bound (lub) of a, b of L by $a \vee b$ (join of a, b).

We denote the unique greatest lower bound (glb) of a, b of L by $a \wedge b$ (meet of a, b).

Since the least upper bound and the greatest lower bound are unique,

both $\vee$ and $\wedge$ are binary operations on L.

We know that the following laws hold good in $(L, \leq)$.

Commutative law

1(a) $a \vee b = b \vee a$, 1(b) $a \wedge b = b \wedge a$

Associative law

2(a) $a \vee (b \vee c) = (a \vee b) \vee c$, 2(b) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

Absorption law

3(a) $a \vee (a \wedge b) = a$, 3(b) $a \wedge (a \vee b) = a$

$a, b, c \in L$.

Thus L is a nonempty set equipped with two binary operations $\vee$ and $\wedge$ such that the commutative law, associative law, absorption law hold good.

Thus we see that the definition of lattice as a poset leads to the definition of lattice as an algebraic structure.

Secondly, we define lattice as an algebraic structure. Then L is a nonempty set equipped with two binary operation $\vee$(join) and $\wedge$ (meet) such that the commutative law, associative law, absorption law hold good.

We define a relation $\leq$ on L such that for $a, b \in L$,

$a \leq b \Leftrightarrow a \wedge b = a$.

Now we show that $\leq$ is a partial order relation on L.

1. Let $a \in L$

Since $(L, \vee, \wedge)$ is a lattice, idempotent law holds good.

$\therefore a \wedge a = a$

Now, $a \leq b \Leftrightarrow a \wedge b = a$

$\therefore a \wedge a = a \Rightarrow a \Rightarrow a$

$\therefore \leq$ is reflexive.

2. Let $a, b \in L$.

Let $a \leq b$, and $b \leq a$.

Now $a \leq b \Rightarrow a \wedge b = a$

$b \leq a \Rightarrow b \wedge a = b$

$\because a \wedge b = b \wedge a$, (by commutativity)

$\therefore a = b$

Thus $a \leq b, b \leq a$ imply $a = b$

$\therefore \leq$ is antisymmetric.

3. Let $a, b, c \in L$

Let $a \leq b, b \leq c$

Now $a \leq b \Rightarrow a \wedge b = a$

$b \leq c \Rightarrow b \wedge c = b$

Now $a \wedge c = (a \wedge b) \wedge c, \quad \because a \wedge b = a$

$= a \wedge (b \wedge c),$ by associative law

$= a \wedge b, \quad \because b \wedge c = b$

$= a$

$\therefore a \leq c$

Thus $a \leq b, b \leq c$ imply $a \leq c$.

$\therefore \leq$ is transitive.

$\therefore \leq$ is a partial order relation on L, i.e. $(L, \leq)$ is a poset.

Now, we show that the greatest lower bound of a, b exists in L.

We have $(a \wedge b) \wedge a = a \wedge (b \wedge a)$, by associative law

$= a \wedge (a \wedge b)$, by commutative law

$= (a \wedge a) \wedge b$, by associative law

$= a \wedge b$, by idempotent law

$\therefore a \wedge b \leq a$

Similarly $a \wedge b \leq b$

$\therefore a \wedge b$ is a lower bound of a, b.

Let c be any lower bound of a, b. Then

$c \leq a$, and $c \leq b$

$\therefore c \wedge a = c$, and $c \wedge b = c$

Thus $c \wedge (a \wedge b) = (c \wedge a) \wedge b$

$= c \wedge b$

$= c$

$\therefore c \leq a \wedge b$, by definition of $\leq$.

$\therefore a \wedge b$ is the greatest lower bound of a, b.

Now we prove that $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$.

$a \wedge b = a \Rightarrow (a \wedge b) \vee b = a \vee b$

$\Rightarrow b \vee (a \wedge b) = a \vee b$, by commutative law

$\Rightarrow b \vee (b \wedge a) = a \vee b$, by commutative law

$\Rightarrow b = a \vee b$, by absorption law

Again $a \vee b = b \Rightarrow a \wedge (a \vee b) = a \wedge b$

$\Rightarrow a = a \wedge b$, by absorption law

Hence $a \wedge b = a \Leftrightarrow a \vee b = b$

Thus $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$.

Therefore, by duality we conclude that the least upper bound of a, b will be $a \vee b$.

Thus, we see that the definition of lattice as an algebraic structure leads to the definition of lattice as a poset.

2.7 SUBLATTICES

A nonempty subset M of a lattice $(L, \vee, \wedge)$ is called a sublattice of L if and only if M is closed under both the operations $\vee$ and $\wedge$, i.e., if $a, b \in M$; then $a \vee b \in M$, $a \wedge b \in M$.

Note : The sublattice itself is a lattice with respect to $\vee$ and $\wedge$.

Examples of sublattices

1. Let $D_{60} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$ be the set of positive divisors of 60.

Let $a, b \in D_{60}$

We define

$a \vee b$ = lcm of a, b

$a \wedge b$ = gcd of a, b.

Then $(D_{60}, \vee, \wedge)$ is a lattice.

Let $D_6 = \{1, 2, 3, 6\}$ be the set of positive divisors of 6.

Clearly, D_6 is a nonempty subset of D_{60}.

For every pair of $a, b \in D_6$,

$a \vee b \in D_6$, $a \wedge b \in D_6$

$\therefore$ D_6 is a sublattice of D_{60}.

2. Let X = {1, 2, 3}. Let P(x) be the power set of X, i.e.,

$P(x) = \{\{1, 2, 3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}, \{1\}, \{2\}, \{3\}, \phi\}$

Let $A, B \in P(x)$

We define

$A \vee B = A \cup B$

$A \wedge B = A \cap B$.

Then $\{P(x), \vee, \wedge\}$ is a lattice.

Let $M = \{\phi, \{1\}, \{2\}, \{1, 2\}\}$

Clearly, M is a nonempty subset of P(x). For every pair of $A, B \in M$.

$A \vee B \in M, A \wedge B \in M$.

$\therefore$ M is a sublattice of P(x).



CHECK YOUR PROGRESS

Q 14: Let x {1, 2, 3}. Let P(x) be the power set of X. $\{P(x), \vee, \wedge\}$, is a lattice where

$A \wedge B = A \cup B, A \vee B = A \cup B; A, B \in P(x)$.

Let $M = [\phi, \{1\}, \{2\}]$

Examine if M is a sublattice of P(x).

Q 15: Let $(L, \leq)$ be a lattice, and let a, b be elements of L such that $a \leq b$. The interval [a, b] is defined as the set of all $x \in L$ such that $a \leq x \leq b$.

Prove that [a, b] is a sublattice of L.

Q 16: Let D_{30} be the set of all positive divisors of 30. $(D_{30}, \leq)$ is a lattice where $a \leq b$ means 'a is a divisor of b'. Write down four sublattices of D_{30}.

2.8 DIRECT PRODUCT OF LATTICES

Let $(L_1, \vee, \wedge)$, and $(L_2, \vee, \wedge)$ be two lattices. Let $L = L_1 \times L_2$. Then L is a lattice under the binary operations $\vee$ and $\wedge$ defined on L as follows.

$(a_1, b_1) \vee (a_2, b_2) = (a_1 \vee a_2, b_1 \vee b_2)$,

$(a_1, b_1) \wedge (a_2, b_2) = (a_1 \wedge a_2, b_1 \wedge b_2)$,

for all $(a_1, b_1), (a_2, b_2) \in L$;

$a_1, a_2 \in L_1; b_1, b_2 \in L_2$.

Proof : Let $(a_1, b_1), (a_2, b_2) \in L = L_1 \times L_2$

$a_1, a_2 \in L_1; b_1, b_2 \in L_2$

$(L_1, \vee, \wedge)$ is a lattice.

$\therefore a_1 \vee a_2 \in L_1, a_1 \wedge a_2 \in L_1$

$(L_2, \vee, \wedge)$ is a lattice

$\therefore b_1 \vee b_2 \in L_2,\ b_1 \wedge b_2 \in L_2$

$\therefore (a_1 \vee a_2,\ b_1 \vee b_2) \in L_1 \times L_2 = L$

$(a_1 \wedge a_2,\ b_1 \wedge b_2) \in L_1 \times L_2 = L$

Thus, $\vee$ and $\wedge$ are binary operations defined on L.

Commutative law

1(a). $(a_1, b_2) \vee (a_2, b_2) = (a_1 \vee a_2,\ b_1 \vee b_2)$

$= (a_2 \vee a_1,\ b_2 \vee b_1)$

$= (a_2, b_2) \vee (a_1, b_1)$ ($\because$ L_1, L_2 are lattices)

1(b). Similarly, $(a_1, b_1) \wedge (a_2, b_2) = (a_2, b_2) \wedge (a_1, b_1)$

Associative law

2(a). Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in L = L_1 \times L_2$

$\therefore$ $a_1, a_2, a_3 \in L_1$; $b_1, b_2, b_3 \in L_2$

$((a_1, b_1) \vee (a_2, b_2)) \vee (a_3, b_3)$

$= (a_1 \vee a_2,\ b_1 \vee b_2) \vee (a_3, b_3)$

$= ((a_1 \vee a_2) \vee a_3,\ (b_1 \vee b_2) \vee b_3)$

$= (a_1 \vee (a_2 \vee a_3),\ b_1 \vee (b_2 \vee b_3))$ ($\because$ L_1, L_2 are lattices)

$= (a_1, b_1) \vee (a_2 \vee a_3,\ b_2 \vee b_3)$

$= (a_1, b_1) \vee (a_2 \vee b_2) \vee (a_3, b_3)$

2(b). Similarly

$((a_1, b_1) \wedge (a_2, b_2)) \wedge (a_3, b_3)$

$= (a_1, b_1) \wedge ((a_2, b_2) \wedge (a_3, b_3))$

Absorption law

3(a). $(a_1, b_1) \vee ((a_1, b_1) \wedge (a_2, b_2))$

$= (a_1, b_1) \vee (a_1 \wedge a_2,\ b_1 \wedge b_2)$

$= ((a_1 \vee (a_1 \wedge a_2),\ b_1 \vee (b_1 \wedge b_2))$

$= (a_1, b_1)$ ($\because$ L_1, L_2 are lattices)

3(b). Similarly

$(a_1, b_1) \wedge ((a_1, b_1) \vee (a_2, b_2))$

$= (a_1, b_1)$

Thus, $(L, \vee, \wedge)$ is a lattice, called the direct product of the lattices $(L_1, \vee, \wedge)$, $(L_2, \vee, \wedge)$.

Note : It must be borne in mind that the binary operations in L_1, L_2, L are different, although we have denoted the binary operations by the same symbols $\vee, \wedge$. Of course, the binary operations on L_1, L_2 may be identical.

Examples

1. Consider a lattice $(L, \leq)$ as shown in Fig 2.4(a), where L = {1, 2}. Draw the diagram of the lattice $(L^2, \leq)$, where L^2 = L x L.

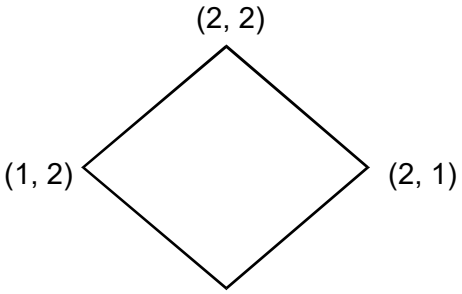


$(L, \leq)$

Fig 2.4(a)

Solution : L^2 = LxL = {(1, 1), (1, 2), (2, 1), (2, 2)}

The lattice $(L^2, \leq)$ is shown in Fig 2.4(b).



$(L^2, \leq)$

Fig 2.4(b)

2. Draw the Hasse diagram for representing the lattice $(D_{20}, \leq)$ of the positive divisors of 20, where $a \leq b$ means 'a is a divisor of b'. Show that it is same as that of the product of two chains with three and two elements.

Solution: D_{20} = {1, 2, 4, 5, 10, 20}.

The Hasse diagram is shown in Fig 2.5 (a)

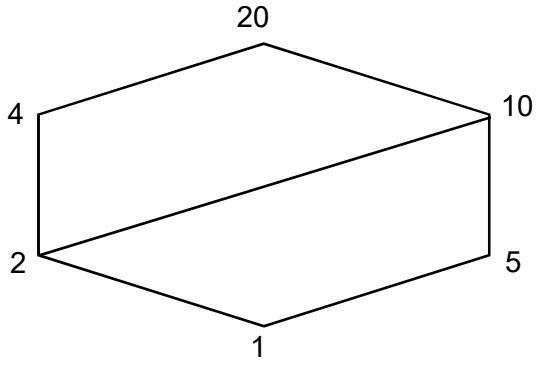


Fig 2.5 (a)

Let us consider the two chains $C_1 = \{0, 1, 2\}$, and $C_2 = \{0, 1\}$ containing three and two elements respectively.

Now, $C_1 \times C_2$

$= \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1)\}$

The diagram for $C_1 \times C_2$ is shown in Fig 2.5(b) which is the same as the diagram for the lattice of the positive divisors of 20.

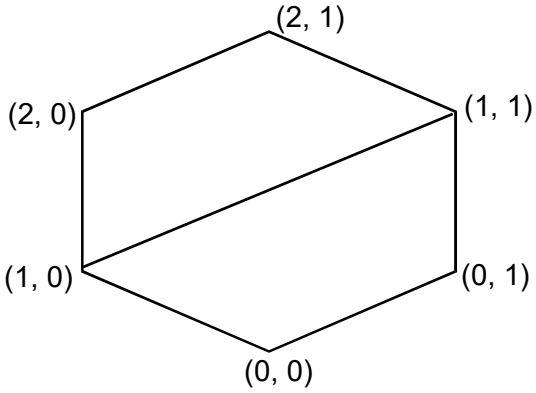


Fig 2.5 (b)

2.9 HOMOMORPHISM OF LATTICES

Let $(L_1, \vee_1, \wedge_1)$, and $(L_2, \vee_2, \wedge_2)$ be two lattices. A mapping.

$f : L_1 \to L_2$

is called a lattice homomorphism from the lattice $(L_1, \vee_1, \wedge_1)$ to the lattice $(L_2, \vee_2, \wedge_2)$ if for any $a, b \in L_1$,

$f(a \vee_1 b) = f(a) \vee_2 f(b)$,

$f(a \wedge_1 b) = f(a) \wedge_1 f(b)$.

Note : 1. Both the binary operations of join and meet are preserved under lattice homomorphism.



LET US KNOW

The word homomorphism has been derived from the Greek words homos (= of the same sort), and morphe (= form).

2. Order relations are also preserved under lattice homomorphism.

Let $\leq_1$, and $\leq_2$ be partial order relations on the lattices $(L_1, \vee_1, \wedge_1)$ and $(L_2, \vee_2, \wedge_2)$ respectively.

Let $f : L_1 \to L_2$ be a lattice homomorphism.

Let $a, b \in L_1$. Then

$a \leq_1 b$ if and only if $a \vee_1 b = b$.

Now $f(b) = f(a \vee_1 b)$

$= f(a) \vee_2 f(b)$ ($\because$ f is a homomorphism)

$\Leftrightarrow f(a) \leq_2 f(b)$.

Thus, $a \leq_1 b$ if and only if $f(a) \leq_2 f(b)$. i.e. orders are preserved.

3. If a lattice homomorphism $f : L_1 \to L_2$ is bijective (i.e., one-one and onto), then f is called a lattice isomorphism.

If there exists an isomorphism between two lattices, the lattices are said to be isomorphic.

Since lattice isomorphism preserves order relation,therefore isomorphic lattices can be represented by the same Hasse diagram.



LET US KNOW

The word isomorphism has been derived from the Greek words isos (= equal), and morphe (= form).

Examples :

1. Let A = {a, b, c}, where a, b, c are distinct, and B = {1, 2, 3}.

Let P(A) denote the power set of A, and P(B) denote the power set of B, i.e.,

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

$P(B) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{3, 1\}, \{1, 2, 3\}\}$

$(P(A), \cup, \cap)$ is a lattice,

$(P(B), \cup, \cap)$ is a lattice.

We define a mapping $f : P(A) \to P(B)$ by

$f(\phi) = \phi$, $f(\{a\}) = \{1\}$, $f(\{b\}) = \{2\}$, $f(\{c\}) = \{3\}$,

$f(\{a, b\}) = \{1, 2\}$, $f(\{b, c\}) = \{2, 3\}$, $f(\{c, a\}) = \{3, 1\}$,

$f(\{a, b, c\}) = \{1, 2, 3\}$.

Clearly f is bijective (i.e., one-one and onto).

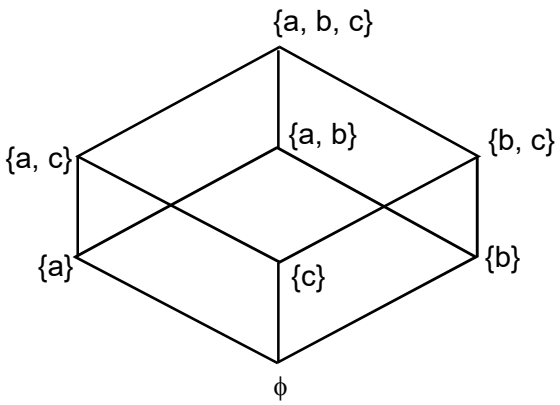
Moreover

$f(S \cup T) = f(S) \cup f(T)$

$f(S \cap T) = f(S) \cap f(T)$, for any $S, T \in P(A)$

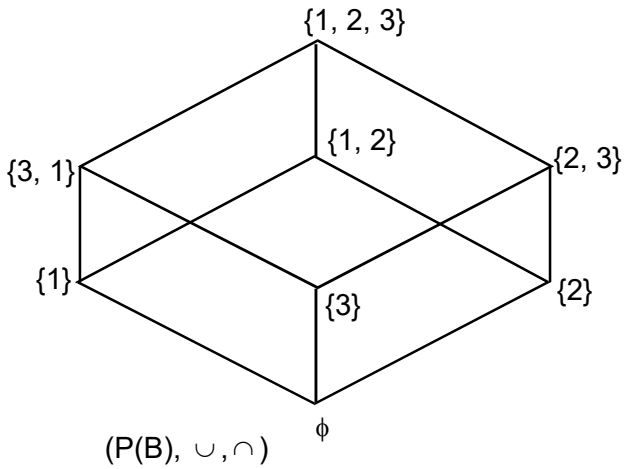
$\therefore$ f is an isomorphism.

We note that P(A) and P(B) have the same Hasse diagram as shown below.



$(P(A), \cup, \cap)$

Fig 2.6(a)



$(P(B), \cup, \cap)$

Fig 2.6(b)



CHECK YOUR PROGRESS

Q 17: Let A= {1, 2}, B = {a, b}; a, b are distinct. Let P(A), and P(B) denote the power set of A, and B respectively.

Show that there exists an isomorphism between the lattices $(P(A), \cup, \cap)$ and $(P(B), \cup, \cap)$.

Q 18: Let D_6 be the set of positive divisors of 6. Let $a, b \in D_6$.

We define $a \vee b$ = lcm of a, b; $a \wedge b$ = gcd of a, b.

Then $(D_6, \vee, \wedge)$ is a lattice.

Let L = {p, q}, where p, q are distinct

Let P(L) denote the power set of L.

$(P(L), \cup, \cap)$ is a lattice

Show that there exists an isomorphism between the lattices $(D_6, \vee, \wedge)$, and $(P(L), \cup, \cap)$,

Q 19: Let D_{30} be the set of positive divisors of 30. Let $a, b \in D_{30}$. We define $a \vee b$ = lcm of a, b; $a \wedge b$ = gcd of (a, b).

Then $(D_{30}, \vee, \wedge)$ is a lattice.

Let L = {p, q, r}, where p, q, r are distinct.

Let P(L) denote the power set of L.

$(P(L), \cup, \cap)$ is a lattice.

Show that there exists an isomorphism between the lattices $(D_{30}, \vee, \wedge)$ and $(P(L), \cup, \cap)$.

2.10 SOME SPECIAL LATTICES

2.10.1 Bounded Lattice

A lattice $(L, \leq)$ is said to have a least (or null) element 0 if for any element $x \in L$, we have $0 \leq x$.

L is said to have a greatest (or all) element 1 if for any element $x \in L$, we have $x \leq 1$.

L is bounded if L has both a least elemet 0 and greatest element 1.

Note 1 : A bounded lattice L is often denoted by $(L, \vee, \wedge, 0, 1)$.

2. If a least element and a greatest eletment exist in a lattice, then they are unique.
3. It must be borne in mind that 0 and 1 are symbolic names and, in general, have nothing to do with real numbers zero and one. O may be a null set, the real number one, ... Similarly 1 may be a set, a real number other than one., ...

Examples

1. Let $D_6 = \{1, 2, 3, 6\}$ be the set of positive divisors of 6. Let $a \leq b$ mean 'a is a divisor of b', where $a, b \in D_6$. Then $(D_6, \leq)$ is a lattice.

Now, $1 \leq x$ for every $x \in D_6$.

$x \leq 6$ for every $x \in D_6$.

$\therefore$ 1 is least element, and 6 is greatest element.

$\therefore$ $(D_6, \leq)$ is a bounded lattice.

2. Let $\underline{\underline{N}}$ be the set of natural numbers. Let $a \leq b$ mean 'a is less than or equal to b'; $a, b \in \underline{\underline{N}}$. Then $(\underline{\underline{N}}, \leq)$ is a lattice, where $\vee$ and $\wedge$ are given by $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$

Now $1 \leq x$ for every $x \in \underline{\underline{N}}$

$\therefore$ 1 is least element.

But the lattice has no greatest element.

$\therefore$ $(\underline{\underline{N}}, \leq)$ is not a bounded lattice.

3. Let $X = \{1, 2, 3\}$. Let P(x) be the power set of x. Then $(P(x), \leq)$ is a lattice where $A \leq B$ means 'A is a subset of B' i.e., $A \leq B$ means $A \subseteq B$; $A, B \in P(x)$ and $\vee$ and $\wedge$ are given by $A \vee B = A \cup B$, $A \wedge B = A \cap B$.

Now $\phi \subseteq A$ for every $A \in P(x)$

$A \subseteq X$ for every $A \in P(x)$

$\therefore$ ϕ is least element, and X is greatest element.

$\therefore$ $(P(x), \leq)$ is a bounded lattice.



CHECK YOUR PROGRESS

Q 20: Give an example of a lattice which has greatest element, but not least element.

Q 21: Give an example of a lattice which has neither greatest element nor least element.

Theorem 2.3 : Let $(L, \leq)$ be a lattice with least element 0 and greatest element 1

For any element $a \in L$,

(i) $a \vee 1 = 1$, and $a \wedge 1 = a$

(ii) $a \vee 0 = a$, and $a \wedge 0 = 0$

Proof : (i) Let $a \in L$

$\because$ 1 is greatest element, $\therefore a \vee 1 \leq 1$ (1)

Again $a \vee 1$ is the least upper bound of a and 1. $\therefore 1 \leq a \vee 1$ (2)

$\therefore$ from (1) and (2), $a \vee 1 = 1$

Again, $a \wedge 1$ is the greatest lower bound of a and 1.

$\therefore a \wedge 1 \leq a$ (3)

Also, $a \leq a$, and $a \leq 1$

$\therefore a \leq a \wedge 1$ (4) [Art 2.5 Property III (3)]

$\therefore$ from (3) and (4), $a \wedge 1 = a$

Thus, $a \vee 1 = 1$, and $a \wedge 1 = a$

(ii) Let $a \in L$.

$\because 0$ is least element $0 \leq a$. Also $a \leq a$

$\therefore a \vee 0 \leq a$ (5) [Art 2.5 Property III (2)]

Again $a \vee 0$ is the least upper bound of 0 and a. $\therefore a \leq a \vee 0$ (6)

$\therefore$ from (5) and (6), $a \vee 0 = a$

Again $a \wedge 0$ is the greatest lower bound of a and 0.

$\therefore a \wedge 0 \leq 0$ (7)

Also $0 \leq a$, and $0 \leq 0$

$\therefore 0 \leq a \wedge 0$ (8) [Art 2.5 Property III (3)]

$\therefore$ from (7) and (8), $a \wedge 0 = 0$

Thus, $a \vee 0 = a$, and $a \wedge 0 = 0$

Note : 1. Since $a \vee 0 = a$, and $a \wedge 1 = a$, 0 is the identity of the operation $\vee$, and 1 is the identity of the operation $\wedge$ of the bounded lattice $(L, \vee, \wedge)$.

2. By commutativity

$1 \vee a = a \vee 1 = 1$, $1 \wedge a = a \wedge 1 = a$

$0 \vee a = a \vee 0 = a$, $0 \wedge a = a \wedge 0 = 0$

Theorem 2.4 : Every finite lattice is a bounded lattice.

Proof : Let $(L, \leq)$ be a finite lattice, where $L = \{a_1, a_2, \ldots, a_n\}$, a_i's are distinct.

We put $b_1 = a_1$

$b_2 = a_2 \wedge b_1$

$b_3 = a_3 \wedge b_2$

In this way, $b_n = a_n \wedge b_{n-1}$

Then $b_1, b_2, \ldots., b_n$ all belong to L, and $b_n \leq a_i$, for all i = 1, 2, ..., n.

i.e. b_n is least element of L.

By associativity of the operation $\wedge$, we write

$b_n = a_1 \wedge a_2 \wedge a_3 \wedge \ldots. \wedge a_n$.

Thus, $a_1 \wedge a_2 \wedge a_3 \wedge \ldots. \wedge a_n$ is least element of L.

Similarly, we can show that

$a_1 \vee a_2 \vee a_3 \vee \ldots. \vee a_n$ is greatest element of L.

$\therefore$ L is bounded.

2.10.2 Distributive Lattice

A lattice (L, $\vee$, $\wedge$) is said to be distributive if for any elements a, b, c of L we have the following Distributive law.

(a) a $\vee$ (b c) = (a b) (a

(b) a (b c) = (a b) (a

Otherwise,L is said to be nondistributive.

Note : 1. In a distributive lattice, the operation distributes over and the operation distributes over

2. The two laws (a) and (b) are equivalent to one another. Let us suppose that the first one holds, i.e.,

a (b c) = (a b) (a

Now, (a b) (a c) = ((a b) a) (a b)

= (a (a b)) (c (a

(by commutative law)

= a (c (a

= a ((c a) (c

= (a (c a)) (b

(by associative law, and commutative law)

= (a (a c)) (b

= a (b .

Similarly, if we assume that the second one holds, we will get the first one. Therefore, it is sufficient to verify anyone of these two equalities.

Theorem 2.5 : Every chain is a distributive lattice.

Proof : Let (L,

(L,

Now, we prove anyone of the two distributive laws.

Let us consider all possible relations between three arbitrary elements a, b, c

For example, let a b, b

a

Now a b a

a a

b b

Now a (b c) = a

= a

= a

= (a b) (a

L is a distributive lattice.



CHECK YOUR PROGRESS

Q 22: Give an example of a distributive lattice.

Q 23: Give an example of a nondistributive lattice.

Theorem 2.6 : The direct product of two distributive lattices is a distributive lattice.

Proof : Let (L_1, , $_2$, ,

We know that $L = L_1 \times L_2$ is a lattice under the binary operations and

(a_1, b_1) $_2, b_2) = (a_1 a_2, b_1 b_2)$,

(a_1, b_1) $_2, b_2) = (a_1 a_2, b_1 b_2)$,

for all $(a_1, b_1), (a_2, b_2)$

$a_1, a_2 \in L_1$; $b_1, b_2 \in L_2$

Let $(a_3, b_3) \in$ $_1$; $a_3 \in L_1$, $b_3 \in L_2$

Now $(a_1, b_1) *$ $_2, b_2) *$ $_3, b_3))$

$= (a_1, b_1) *$ $_2 a_3), (b_2 * b_3))$

$= (a_1 * (a_2 * a_3), b_1 * (b_2 * b_3))$

$= (((a_1 * a_2) *$ $_1 * a_3)), ((b_1 * b_2) *$ $_1 * b_3)))$ (1)

Again $((a_1, b_1) *$ $_2, b_2)) *$ $_1, b_1) *$ $_3, b_3))$

$= (a_1 * a_2, b_1 * b_2) *$ $_1 * a_3, b_1 * b_3)$

$= (((a_1 * a_2) *$ $_1 * a_3)), ((b_1 * b_2) *$ $_1 * b_3)))$ (2)

From (1) and (2),

$(a_1, b_1) *$ $_2, b_2) *$ $_3, b_3))$

$= ((a_1, b_1) *$ $_2, b_2)) *$ $_1, b_1) *$ $_3, b_3))$

Thus, we have proved one of the two distributive laws.

$*$ L is a distributive lattice.

Theorem 2.7 : If (L, $*$,$*$) is a distributive lattice such that a$*$

a$*$c, and a$*$b = a$*$c, where a, b, c$*$

law holds good in a distributive lattice.

Proof : Let (L, $*$,$*$

Let a, b, c $*$L such that a$*$b = a$*$c, and a$*$b = a$*$

Now c$*$(a$*$

$=$ (c$*$a)$*$(c$*$

$=$ (a$*$c)$*$(c$*$

$=$ (a$*$b)$*$(c$*$

$=$ (b$*$a)$*$(c$*$

$=$ (b$*$a)$*$(b$*$

$=$ b$*$(a$*$

$=$ b$*$(a$*$

$=$ b$*$(b$*$

$=$ b, by absorption law. (1)

Again, c$*$(a$*$

$=$ c$*$(a$*$

$=$ c$*$(c$*$

$=$ c, by absorption law (2)

From (1) and (2), b = c.

2.10.3 Complemented Lattice

Let (L, ,

greatest element 1.

Let a

An element x

a x = 1, and a

Now a x = 1 x

a x = 0 x

if x is a complement of a, a is a complement of x.

Again 0 1 = 1 and 0

0 and 1 are complements of each other.

It must be borne in mind that 1 is the only complement of 0.

If possible, let x be another complement of 0, where x L, and x

0 x = 1, and 0

But 0

x = 1, which is a contradiction.

1 is the only complement of 0, and vice versa.

> An element in a bounded lattice may have no complement. An element, other than 0 and 1, may have more than one complement.

Let us consider the bounded lattice given in Fig 2.7

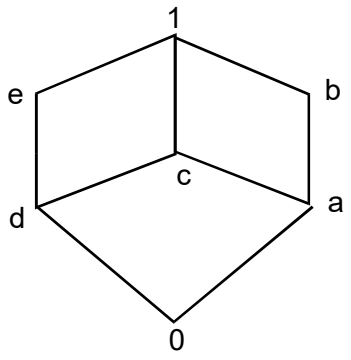


Fig 2.7

In the above lattice, 1 is the complement of 0, and vice versa.

Again, a and b have complements e, whereas the element c has no

complement.

If a bounded lattice is distributive, then complements, if exist, are unique.

Theorem 2.8 : Let (L, ,

Then complements, if exist, are unique.

Proof : Let a

complements of L; x, y

a x = 1, and a

a y = 1, and a

Now x = x

= x (a

= (x a) (x

= 1 (x y), x a = a

= x

Again, y = y

= y (a

= (y a) (y

= 1 (y x), y a = a

= y

= x

From (1) and (2), x = y.

Thus the complement of a is unique.

Definition : A lattice (L, , , 0, 1) is said to be complemented if L is bounded and every element in L has a complement.

Note : Every element a of a complemented and distributive lattice L has a unique complement, which is generally denoted by a'.



CHECK YOUR PROGRESS

Q 24: Prove that the lattice (D_{42},) of the set of positive divisors of 42 is a complemented lattice by finding the complements of all the elements. (a b in D_{42} means 'a is a divisor of b').

Q 25: Let X = {1, 2, 3}, and P(x) be the power set of X. Show that

(P(x),

(A

Theorem 2.9 : Let L(,

lattice. Then (a / = a/ b/

(a / = a/ b/,

a, b L, and a/ denotes the complement of a, i.e. De Morgan's laws hold good in a complemented distributive lattice.

Proof : Let L(,

a, b

Since L is complemented, the complements of a, b exist in L. Let the complements be a/, b/ respectively.

a / = 1, and a / = 0

b / = 1, and b / = 0

Now (a b) / b/)

= ((a b) /)) ((a b) /)), by distributive law

= (a (b /)) (a (b /)), by associative law

= (a / b)) (a

= ((a /) b)

= (1 b)

= 1

= 1 (1)

Again, (a b) / b/)

= (a / b/)) (b / b/)), by distributive law

= (a /) /)) (b / a/)), by distributive law and commutative law

= (0 /) ((b /)) /), by associative law

= 0 (0 /)

= 0

= 0 (2)

From (1) and (2), we conclude that a/ b/ is the complement of a

i.e. (a / = a/ b/. (3)

By the principle of duality, it follows from (3) that

(a) = a b .

Note : Augustus De Morgan (1806 – 1871) was a British mathematician. He was born in Madurai, India.



2.11 LET US SUM UP

- A relation R on a monempty set A is said to be a partial order relation if R is reflexive, antisymmetric, and transitive.
- A nonempty set A together with a partial order relation on A is called a partially ordered set (or a poset).
- A partially ordered set (L,
  has a least upper bound and a greatest lower bound is called a lattice.
- A lattice may be defined as an algebraic structure also. A nonempty set L equipped with two binary operations (join) and
  lattice if commutative law, associative law, and absorption law are satisfied.
- Two definitions given for a lattice are equivalent.
- A nonempty subset M of a lattice (L, ,
  and only if M is closed under both the operations and
- Let (L_1, $_1$, $_1$), and (L_2, $_2$, $_2$), be two lattices. A mapping
  f : L_1 $_2$
  is called a lattice homomorphism from the lattice (L_1, $_1$, $_1$) to the lattice (L_2, $_2$, $_2$) if for any a, b $_1$,
  f(a $_1$ b) = f(a) $_2$ f(b)
  f(a $_1$ b) = f(a) $_2$ f(b)

  If a lattice homomorphism f is bijective (i.e., one-one and onto), then f is called a lattice isomorphism.
- A lattice (L,) is said to have a least element 0 if for any element a L,
  0 x.

  A lattice (L,

x L, x

L is bounded if L has both a least element 0 and a greatest element 1.

- A lattice (L, ,

  L,

  (a) a (b c) = (a b) (a

  (b) a (b c) = (a b) (a

- Let (L, ,

  element 1. An element x L is called a complement of a

  a x = 1, and a

  A lattice L is said to be complemented if L is bounded and every element in L has a complement.

2.12 FURTHER READINGS

1) Lattice Theory : First Concepts and Distributive Lattices by George Gratzer (Dover Books on Mathematics).

2) Introduction to Lattice Theory with Computer Science Applications by Vijay K. Garg (Wiley).

2.13 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: D_{30} = {1, 2, 3, 5, 6, 10, 15, 30}

Let a b mean 'a is a divisor of b'; a, b $_{30}$.

(i) a is a divisor of a, for every a $_{30}$.

(ii) a is a divisor of b, b is a divisor of a imply a = b; a, b $_{30}$

(iii) a is a divisor of b, b is a divisor of c imply a is a divisor of c, a, b, c $_{30}$.

is a partial order relation on D_{30}. Thus (D_{30},) is a partially ordered set.

Hasse diagram

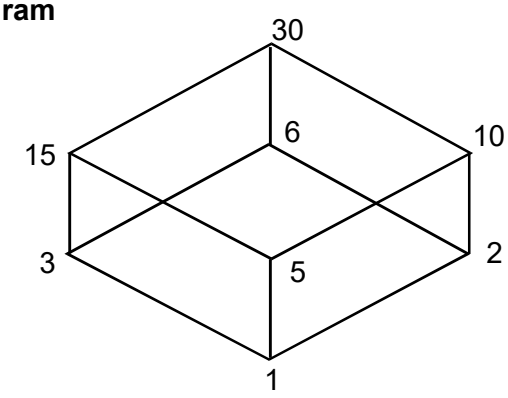


Fig 2.8

Ans to Q No 2: X = {1, 2, 3}

P(x) = [{1, 2, 3}, {1, 2}, {2, 3}, {3, 1}, {1}, {2}, {3},

Let A B mean 'A is a subset of B'; A, B

(i) A A, for every A

(ii) A B, B A imply A = B; A, B

(iii) A B, B C imply A C; A, B, C

is transitive.

is a partial order relation on P(x).

Thus, {P(x),

Hasse diagram

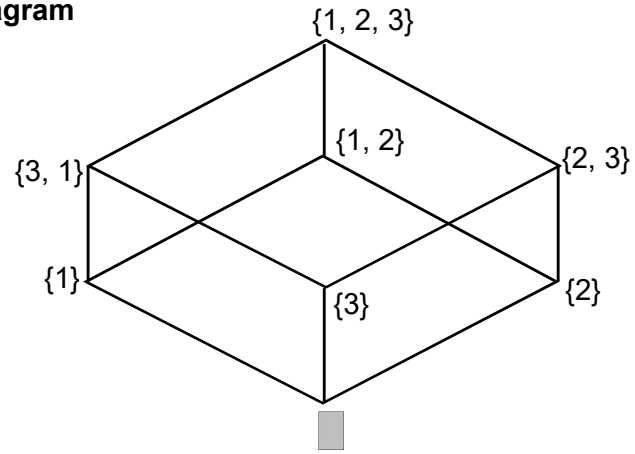


Fig 2.9

Ans to Q No 3: X = {1, 2}

P(x) = {{1, 2}, {1}, {2},

Hasse diagram of the poset (P(x),

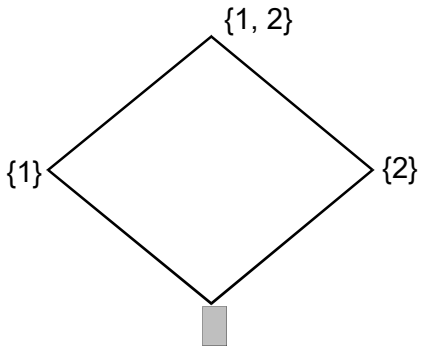


Fig 2.10

Ans to Q No 4: D_{36} = {1, 2, 3, 4, 6, 9, 12, 18, 36}

Hasse diagram of the poset (D_{36},

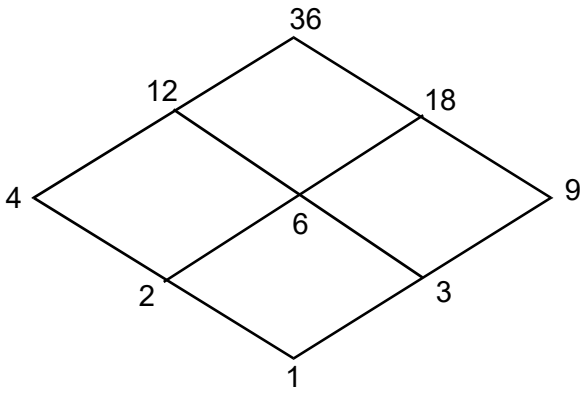


Fig 2.11

Ans to Q No 5: D_{32} = {1, 2, 4, 8, 16, 32}

Let a b mean 'a is a divisor of b'; a, b $_{32}$.

(i) a is a divisor of a, for every a $_{32}$.

(ii) a is a divisor of b, b is a divisor of a imply a = b; a, b $_{32}$

(iii) a is a divisor of b, b is a divisor of c imply a is a divisor of c; a, b, c $_{32}$.

$_{32}$. Thus (D_{32},

Hasse diagram

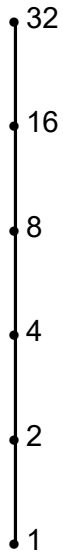


Fig 2.12

We have the lub of a, b = a

= the lcm of a, b

the glb of a, b = a

= the gcd of a, b

Clearly a b, a b 32, a, b 32

(D32,

Ans to Q No 6: X = {1, 2, 3}

S = {{1, 2}, {2, 3}, {3, 1}, {1}, {2}, {3}}

Let A B mean 'A is a subset of B; A, B

(i) A is a subset of A, for every A

(ii) A B, B A imply A = B; A, B

(iii) A B, B C imply A C; A, B, C

is a partial order relation on S. Thus (S,

Hasse diagram

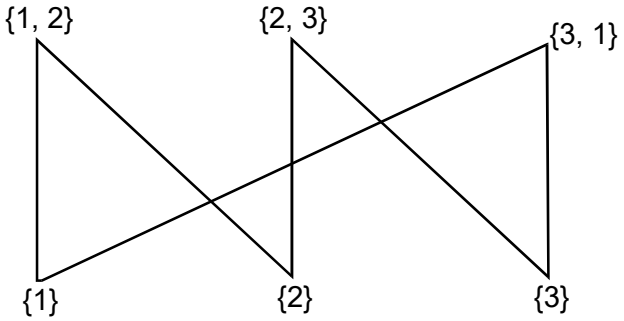


Fig 2.13

The lub of {1, 2}, {2, 3} = {1, 2} {2, 3} = {1, 2, 3}

(S,

Ans to Q No 7: Let A be the set of all real-valued functions defined on [0, 1]

Let f, g A; x

Let f g mean 'f(x)

(i) f(x)

A

(ii) f(x) g(x), g(x)

(iii) f(x) g(x), g(x) h(x) imply f(x) h(x), f, g, h A; x[0, 1]

is a partial order relation on A. Thus (A,

Let the real-valued function f g, f

f g(x) = max [f(x), g(x)], x

f g(x) = min [f(x), g(x)], x

f g and f g are the lub and the glb of f, g A respectively.

Ans to Q No 8: Let be the set of natural numbers. Let a

less than or equal to b'; a, b

(i) a a for every a

(ii) a b, b a imply a = b; a, b

(iii) a b, b c imply a c; a, b, c

is a partial order relation on . Thus (,

The lub of a, b = a

The glb of a, b = a

Clearly a b, a b

(,)

Ans to Q No 9: Let

Let a b mean 'a is less than or equal to b'; a, b

Then (,) is a lattice where and

a

a

Now min (a, max (a, b))

= a

= a (a

= a, by absorption law

max (a, min (a, b))

= a

= a (a

= a, by absorption law.

Ans to Q No 10: Let

Let a b mean 'a is a divisor of b'; a, b

Then (,) is a lattice where and

a

a

Now, lcm (a, gcd (a, b)) = a

= a (a

= a, by absorption law

gcd (a, lcm (a, b)) = a

= a (a

= a, by absorption law.

Ans to Q No 11: We have

a b, b

Where a, b, c are elements of a lattice (L,

(i) We know that

a b a

b c b

a b, b c imply a b = b

(ii) a b a

b c b

Again a b, b c imply a

Now a b a b = b, a c a

Now (a b) (b c) = a

(a b) (a c) = b

From (1) and (2), (a b) (b c) = (a b) (a

Ans to Q No 12: Let (L,) be a lattice, and a, b, c, d

(i) We know that

a b a, and c d

(a b) (c d) a

Again (a b) b, and (c d)

(a b) (c d) b

from (1) and (2)

(a b) (c d) (a c) (b

(ii) We know that

a b a

a b b, b b c and a b b

a b a, a c a and a b c

from (1), (2), and (3),

a b (a d) (b c) (c

Similarly

b c (a b) (b c) (c

c a (a b) (b c) (c

from (4), (5) and (6)

(a b) (b c) (c a) (a b) (b c) (c

Ans to Q No 13: The given statement is

a c a (b c) (a b)

The dual of (1) is obtained by replacing by , and vice versa, and by replacing by

the dual of (1) is

a c a (b c) (a b)

Which can be written as

c a (a b) c a (b

Replacing c by a and vice versa, we get

a c (c b) a c (b

i.e. a c a (b c) (a b)

Which is the same as (1)

the statement (1) is self dual.

Ans to Q No 14: X = {1, 2, 3}

P(x) = {{1, 2, 3}, {1, 2}, {2, 3}, {3, 1}, {1}, {2}, {3},

(P(x), ,

A B = A B, A B = A B; A, B

M = {

{1} {2} = {1} {2} = {1, 2}

M is not a sublattice of P(x).

Ans to Q No 15: Let (L,

a

Let us consider the interval [a, b] on L. It is defined as the set of all

x L such that a x

Let x, y

a x, x b

a y, y

Now, x b, y

b is an upper bound of x, y

x y b, x .

Again a x, x x y, x .

by transitivity a x .

Thus a x y

x y

Similarly, x y

[a, b] is a sublathice of L.

Ans to Q No 16: D_{30} = {1, 2, 3, 5, 6, 10, 15, 30}

Let a b mean 'a is a divisor of b'; a, b $_{30}$.

(D_{30},) is a lattice where and

a

a

Four sublattices of D_{30} are given below.

(i) L_1 = {1, 2, 6, 30}

(ii) L_2 = {1, 5, 15, 30}

(iii) L_3 = {1, 3, 6, 30}

(iv) L_4 = {1, 3, 15, 30}

Ans to Q No 17: A = {1, 2}

P(A) = {

B = {a, b}

P(B) = {

(P(A), ,)

(P(B), ,)

We define a mapping f : P(A) P(B) by f ( ) =

= {b}, f({1, 2}) = {a, b}.

Clearly f is one-one and onto, i.e., bijective.

Moreover

f(S T) = f(S)

f(S T) = f(S)

for any S, T

f is an isomorphism.

Ans to Q No 18: D_6 = {1, 2, 3, 6}

(D_6, ,) is a lattice where and

a b = lcm (a, b), a b = gcd (a, b); a, b $_6$.

L = {p, q}

P(L) = {

(P(L), ,)

We define a mapping f : D_6 P(L) by f(1) =

f(6) = {p, q}.

Clearly f is one-one and onto, i.e., bijective,

Now f(2

f(2) f(3) = {p}

f(2 3) = f(2)

f(2 3) = f(1) =

f(2) f(3) = {p} {q} =

f (2 3) = f(2)

In this way,

f(a b) = f(a)

f(a b) = f(a) f(b); a, b $_{6}$.

f is an isomorphism.

Ans to Q No 19: D_{30} = {1, 2, 3, 5, 6, 10, 15, 30}

(D_{30}, ,) is a lattice where and

a b = lcm (a, b), a b = gcd (a, b), a, b $_{30}$

L = {p, q, r}

P(L) = (

(P(L), ,

We define a mapping f : D_{30}

f(1) =

f(6) = {p, q}, f(10) = {q, r}, f(15) = {r, p}, f(30) = {p, q, r}

Clearly, f is one-one and onto, i.e, bijective f(5

f(5) f(15) = {r}

f(5 15) = f(5)

f(5

f(5) f(15) = {r}

f(5 15) = f(5)

In this way f(a b) = f(a)

f(a b) = f(a) f(b); a, b $_{30}$.

f is an isomorphism.

Ans to Q No 20: Let L be the set of negative integers.

Let a b mean ‘a is less than or equal to b’; a, b

Then (L,) is a lattice, where and

a b = max (a, b), a b = min (a, b); a, b

Now x –1, for every x

–1 is greatest element.

But the lattice has no least element.

Ans to Q No 21: Let be the set of integers. Let a

or equal to b'; a, b

Then (,) is a lattice, where and

a b = max (a, b), a

Clearly, the lattice has neither greatest element nor least element.

Ans to Q No 22: Let X = {1, 2, 3}

P(x) = {

i.e., P(x) is the power set of X.

P(x) is a lattice where and

A B = A B, A B = A B, A, B

Now for any A, B, C

A (B C) = (A B) (A

A (B C) = (A B) (A

P(x) is a distributive lattice.

Ans to Q No 23: Let us consider the diagram given below

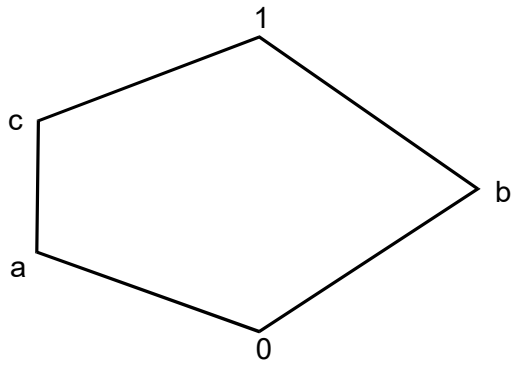


Fig 2.14

Now a (b c) = a

(a b) (a c) = 1

a (b c) (a b) (a

Thus, fig 2.14 is a nondistributive lattice.

Ans to Q No 24: D_{42} = {1, 2, 3, 6, 7, 14, 21, 42}

Let a b mean 'a is a divisor of b'; a, b $_{42}$.

(D_{42},) is a lattice where and

a b = lcm (a, b); a

Now 1 x, for every x $_{42}$

x 42, for every x $_{42}$

1 is least element, and 42 is greatest element.

1 42 = 42, 1

1 is the complement of 42, and vice versa.

Similarly

2 is the complement of 21, and vice versa [2

2

3 is the complement of 14, and vice versa,

6 is the complement of 7, and vice versa.

Thus, every element of D_{42} has a complement. So D_{42} is a complemented lattice.

Ans to Q No 25: X = {1, 2, 3}

P(x) = {

Let A B mean 'A is a subset of B'; A, B

(P(x),) is a lattice where and

A B = A B, A B = A

Now A, for every A

A X, for every A P(x).

is least element, and X is greatest element.

x = x, x =

is the complement of X, and vice versa.

{1} is the complement of {2, 3}, and vice versa.

[{1} {2, 3} = {1, 2, 3} = x, {1} {2, 3} =

{2} is the complement of {3, 1}, and vice versa.

{3} is the complement of {1, 2}, and vice versa.

Thus, every element of P(x) has a complemt. So, P(x) is a complemented lattice.

2.14 MODEL QUESTIONS

Q 1: Define a lattice and given an example.

Q 2: State and prove the isotonic property of a lattice.

Q 3: Define complement of an element of a lattice and a complemented lattice.

Q 4: Let D_{24} denote the set of all positive divisors of 24.

Let a b mean 'a is a divisor of b'; a, b $_{24}$.

(a) Show that (D_{24},

(b) Draw the Hasse diagram of the lattice.

(c) Write down a sublattice of D_{24} containing 5 elements, a sublattice containing 6 elements.

(d) Show that D_{24} is a complemented lattice by finding the complements of all the elements.

Q 5: Show that with an example that the union of two sublattices may not a sublattice.

*** ***** ***

The compound statement is false.

Ans to Q No 8: i) True, ii) False, iii) True, iv) False, v) True

Ans to Q No 9: i) True, ii) False, iii) True, iv) False, v) True, vi) True.

Ans to Q No 10: a) The variable that occur in the formula are P and Q, so we have to consider 4 possible combinations of truth values of two statements P and Q.

P	Q	~P	~Q	~P ∧ ~Q	~(~P ∧ ~Q)
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

b) The variable are P and Q, clearly there are 2^2 rows in the truth table of this formula.

P	Q	~P	~Q	~P ∨ Q	~Q ∨ P	(~P ∨ Q) ∧ (~Q ∨ P)
T	T	F	F	T	T	T
T	F	F	T	F	T	F
F	T	T	F	T	F	F
F	F	T	T	T	T	T

(c)

P	Q	P ∧ Q	P ∨ Q	(P ∧ Q) → (P ∨ Q)
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

(d)

P	Q	P → Q	Q ∧ (P → Q)	{Q ∧ (P → Q)} → P
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	T

Ans to Q No 11: (a)

P	Q	~P	~Q	$P \wedge \sim Q$	$Q \vee (P \wedge \sim Q)$	$\sim P \wedge \sim Q$	$Q \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$
T	T	F	F	F	T	F	T
T	F	F	T	T	T	F	T
F	T	T	F	F	T	F	T
F	F	T	T	F	F	T	T

All the entries in the last column are T, the given formula is a tautology.

(b)

P	Q	~P	$\sim P \vee Q$	$P \rightarrow Q$	$(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	F	F	T

All the entries in the last column are T, the given formula is a tautology.

Similarly, for (c) construct truth tables.

Ans to Q No 12:

Truth table for $\{(\sim P) \vee (\sim Q)\} \vee P$

P	Q	~P	~Q	$(\sim P) \vee (\sim Q)$	$\{(\sim P) \vee (\sim Q)\} \vee P$
T	T	F	F	F	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

The last column contains only T.

$\therefore$ $\{(\sim P) \vee (\sim Q)\} \vee P$ is a tautology.

Ans to Q No 13: Two statements are logically equivalent or simply equivalent if they have exactly the same truth values under all circumstances.

Ans to Q No 14: (a)

P	Q	~Q	$P \rightarrow Q$	$\sim (P \rightarrow Q)$	$P \wedge \sim Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

UNIT 4 : BOOLEAN ALGEBRA

UNIT STRUCTURE

4.1 Learning Objectives

4.2 Introduction

4.3 Definition of Boolean Algebra and Examples

4.4 Duality

4.5 Basic Theorems on Boolean Algebra

4.6 Boolean Algebra as Lattice

4.7 Boolean Algebra of Propositions

4.8 Two-Element Boolean Algebra

4.9 Let Us Sum Up

4.10 Further Readings

4.11 Answers To Check Your Progress

4.12 Model Questions

4.1 LEARNING OBJECTIVES

After going through this unit, you will able to learn

- definition of Boolean Algebra
- duality
- basic theorems on Boolean Algebra
- Boolean Algebra of propositions
- two-element Boolean Algebra.

4.2 INTRODUCTION

Boolean Algebra is an abstract mathematical structure after the name of ‘a largely self-taught English mathematician, philosopher and logician’ George Boole (1813-1864). Boole tried to formalise the process of logical reasoning using symbols instead of words. The celebrated American mathematician, electrical engineer, and cryptographer, ‘the father of information theory’ Claud Elwood Shannon (1916-2001) observed that electrical circuits could be analysed by using Boolean algebra. Today it is

the backbone of design and analysis of computer and other digital circuits. In this unit, we will state the definition of Boolean algebra put forward by the American mathematician Edward Vermilye Huntington (1874-1952) in 1904, basic theorems and other related topics.



LET US KNOW

'An axiom, postulate or assumption is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments.'

4.3 DEFINITION OF BOOLEAN ALGEBRA AND EXAMPLES

Let B be a nonempty set equipped with two binary operations + and . , a unary operation /, and two distinct elements 0, and 1. Then B is called a Boolean algebra if the follwing axioms are satisfied.

Commutative laws

1. (a) $a + b = b + a$, (b) $a . b = b . a$, for all $a, b \in B$

Distributive laws

2. (a) $a + (b . c) = (a + b) . (a + c)$

   (b) $a . (b + c) = (a . b) + (a . c)$, for all $a, b, c \in B$

Identity laws

3. (a) $a + 0 = a$, (b) $a . 1 = a$, for every $a \in B$

Complement laws

For every $a \in B$, there exists an element $a' \in B$ such that

4. (a) $a + a' = 1$, (b) $a . a' = 0$

Note :

1. A Boolean algebra has six parts, viz, a nonempty set B, two binary operations + and . , one unary operation $'$, two distinct elements 0 and 1. Thus, $(B, +, . , ', 0, 1)$ is a Boolean algebra.

   Later on we will simply write 'B is a Boolean algebra.'

2. 0 is the zero element, 1 is the unit element, and a' is the complement of a. It should be borne in mind that 0, and 1 are symbolic names.

They have, in general, nothing to do with the real numbers zero, and one.

3. The binary operations +, and . are called Boolean sum and Boolean product respectively. It should be borne in mind that + and . have nothing to do with ordinary addition and multiplication. We will drop the symbol ' . ' and use juxtaposition. For example, we will weite a . b as ab; a+(b.c) = (a+b) . (a+c) as a+bc = (a+b) (a+c).
4. The Boolean sum and the Boolean product may also be denoted by $\vee$ (join), and $\wedge$ meet respectively.

Example 1 : Let X = {1, 2, 3}. The power set of X is

P(x) = {ϕ, {1}, {2}, {3}, {1, 2}, {2, 3}, {3, 1}, {1, 2, 3} We define

$A+B = A \cup B$, $A.B = A \cap B$, for all $A, B \in P(x)$.

A' = complement of A

Now 1. (a) $A \cup B = B \cup A$

(b) $A \cap B = B \cap A$

2. (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

3. (a) We have $A \cup \phi = A$

(b) $A \cap \{1, 2, 3\} = A$

4. (a) $A \cup A' = \{1, 2, 3\} = X$

(b) $A \cap A' = \phi$

Thus, $(P(x), \cup, \cap, ', \phi, X)$ is a Boolean algebra.

We note that ϕ is the zero element, and X is the unit element.

Example 2 : Let X be a nonempty set, and P(x) be the power set of X.

Then P(x) is a Boolean algebra under the usual operations of union, intersection, and complementation in P(x), where ϕ is the zero element, and X is the unit element.

Example 3 : Let D_{35} be the set of positive divisors of 35, i.e., D_{35} = {1, 5, 7, 35}.

We define a+b = lcm of a, b

a . b = gcd of a, b, $a' = \frac{35}{a}$, for all $a, b \in D_{35}$.

1. (a) We have a+b = lcm of a, b

= lcm of b, a

= b+a.

(b) a . b = gcd of a, b

= gcd of b, a

= b. a, for all a, b $\in D_{35}$

2. (a) a+(b . c) = a+(gcd of b, c)

= lcm of (a, gcd (b, c))

= gcd of (lcm (a, b),lcm (a, c))

= (a+b) . (a+c), for all a, b, c $\in D_{35}$

(b) Similarly a. (b+c) = (a . b) + (a . c), for all a, b, c $\in D_{35}$

3. (a) a+1 = lcm (a, 1) = a

(b) a . 35 = gcd (a, 35) = a, for every a $\in D_{35}$

4. (a) $a + \frac{35}{a} = \text{lcm}\left(a, \frac{35}{a}\right) = 35$

(b) $a \,.\, \frac{35}{a} = \text{g.c.d}\left(a, \frac{35}{a}\right) = 1$

$\therefore$ (D_{35}, + , . , $^{/}$, 1, 35) is a Boolean algebra.

We note that 1 is the zero element, and 35 is the unit element.

Example 4 : Let D_{32} = {1, 2, 4, 8, 16, 32} be the set of positive divisors of 32.

We define a+b = lcm of a, b

a . b = gcd of a, b

$a^{/} = \frac{32}{a}$, for all a, b $\in D_{32}$.

In this case (D_{32}, + , . , $^{/}$, 1, 32) is not a Boolean algebra, for

$4 + \frac{32}{4}$ = 4+8 = lcm of 4, 8 = 8 $\neq$ 32.

Also $4 \,.\, \frac{32}{4}$ = 4. 8 = gcd of 4, 8 = 4 $\neq$ 1.



LET US KNOW

A square-free integer is an integer which is divisible by no perfect square other than 1.

For example, 35 is a square-free number since it is not divisible by a perfect square other than 1. On the other hand, 32 is not a square-free number, for 32 is divisible by 4, 16, which are perfect squares.

Example 5 : Let D_n be the set of positive divisors of n, where n>1, and n is a square-free positive integer.

We define a+b = lcm of a, b

a . b = gcd of a, b

$a' = \frac{n}{a}$, for all a, b $\in D_n$.

Using the properties of integers and of lcm and hcf, it can be easily shown that

1. (a) a+b = b+a, (b) a . b = b . a, for all a, b $\in D_n$
2. (a) a+(b . c) = (a+b) . (a+c)

   (b) a . (b+c) = (a . b) + (a . c), for all a, b, c $\in D_n$
3. (a) a+1 = lcm (a, 1) = a

   (b) a . n = gcd (a, n) = a, for every a $\in D_n$.
4. (a) $a+\frac{n}{a} = lcm\left(a, \frac{n}{a}\right) = n$

   (b) $a \,.\, \frac{n}{a} = gcd\left(a, \frac{n}{a}\right) = 1$

n is a square-free number. Therefore, a and $\frac{n}{a}$ have no common factor other than 1.

$\therefore$ $lcm\left(a, \frac{n}{a}\right) = n$, $gcd\left(a, \frac{n}{a}\right) = 1$

Thus, (D_n, + , . , $'$, 1, n) is a Boolean algebra. We note that 1 is the zero element and n is the unit element.



CHECK YOUR PROGRESS

Q 1: Let D_{70} be the set of positive divisors of 70.

Define a+b = lcm of a, b ; a . b = gcd (a, b), $a' = \frac{70}{a}$, for all a, b $\in D_{70}$.

Examine if D_{70} is a Boolean algebra.

Q 2: Let D_{27} be the set of positive divisors of 27. Define a+b = lcm (a, b); a . b = gcd (a, b), $a^{/} = \frac{27}{a}$, for all a, b $\in D_{27}$.

Examine if D_{27} is a Boolean algebra.

4.4 DUALITY

Let (B, +, . , $^{/}$, 0, 1) be a Boolean algebra. The dual of any statement in B is the statement obtained by interchanging the operations + and . , and interchanging 0 and 1. For example, the dual of a+(b . c) = (a+b) . (a+c) is a . (b+c) = (a . b) + (a . c). We note that the dual of each axiom of a Boolean algebra is also an axiom. Accordingly, the dual of any theorem in a Boolean algebra is also a theorem. This is known as the Principle of Duality.

In our subsequent discussions, we will drop the symbol . , and use juxtaposition. We will write a + bc = (a+b) (a+c).

Also we will write 'B is a Boolean algebra'.

4.5 BASIC THEOREMS ON BOOLEAN ALGEBRA

Theorem 4.1 : Let B be a Boolean algebra. Then

1. (a) The zero element 0 is unique.

   (b) The unit element 1 is unique.

2. (a) The complement of every element is unique.

3. (Involution law) for every a $\in$ B, $(a^{/})^{/}$ = a, i.e., the complement of the complement a is a itself.

4. (a) $0^{/}$ = 1, (b) $1^{/}$ = 0,

   i.e. the complement of the zero element is the unit element, and vice versa.

Proof : 1(a) If possible, let 0 and 0_1 be two zero elements of B.

$\therefore$ 0_1+0 = 0_1, ($\because$ 0 is zero element)

0 + 0_1 = 0, ($\because$ 0_1 is zero element)

But 0_1+0 = 0 + 0_1

$\therefore$ 0_1= 0.

Thus, the zero element is unique.

(b) If possible, let 1 and 1_1 be two unit elements of B.

$\therefore$ $1_1 . 1 = 1_1$, ($\because$ 1 is unit element)

$1. 1_1 = 1$, ($\because$ 1_1 is unit element)

But $1_1.1 = 1.1_1$

$\therefore$ $1_1 = 1$

Thus, the unit element is unique.

Note : 1(b) is the dual of 1(a), and vice versa. 1(b) can be obtained from 1(a) by replacing 0 by 1, and '+' by ' . '.

2. Let $a \in B$.

If possible, let e and f be two complements of a.

Let 0 be the zero element, and 1 be the unit element.

$\therefore$ $a+e=1$, $a . e = 0$

$a+f=1$, $a . f = 0$

Now $e = e . 1$

$= e . (a+f)$

$= (e . a) + (e . f)$, by distributive law

$= (a . e) + (e . f)$

$= 0 + (e . f)$

$= e . f$ (1)

Again $f = f . 1$

$= f. (a+e)$

$= (f . a) + (f . e)$, by distributive law

$= (a . f) + (f . e)$

$= 0 + (f . e)$

$= f . e$

$= e . f$ (2)

From (1) and (2), we see that e = f.

Thus, the complement of a is unique.

Note : We denote the complement of a by $a^/$.

3. Let $a \in B$

Let $a^/ \in B$ be the complement of a.

$\therefore$ by definition

$a+a' = 1$, $aa' = 0$

$\therefore$ by commutative law,

$a'+a = 1$, $a'a = 0$

This shows that a is the complement of a', i.e. $(a')' = a$.

4. (a) We know that $0+a = a$, and $a1 = a$, for every $a \in B$.

Replacing a by 1, and 0 respectively,

We get $0+1 = 1$, and $01 = 0$

This implies that the complement of 0 is 1, i.e. $0' = 1$.

(b) It is the dual of 4(a).

Theorem 4.2 : Let B be a Boolean algebra, and $a, b, c \in B$. Then the following laws hold good.

Idempotent laws

1. (a) $a+a = a$, (b) $a \cdot a = a$

Boundedness (or Dominance) laws

2. (a) $a+1 = 1$, (b) $a \cdot 0 = 0$

Absorption laws

3. (a) $a+(a \cdot b) = a$, (b) $a \cdot (a+b) = a$

Associative laws

4. (a) $(a+b)+c = a+(b+c)$, (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

De Morgan's laws

5. (a) $(a+b)' = a' \cdot b'$, (b) $(a \cdot b)' = a' + b'$

Proof : 1. (a) We have

$$\begin{aligned} a &= a+0 \\ &= a+(a \cdot a') \\ &= (a+a) \cdot (a+a') \\ &= (a+a) \cdot 1 \\ &= a+a \end{aligned}$$

Thus, $a+a = a$

(b) $$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot (a + a') \\ &= (a \cdot a) + (a \cdot a') \\ &= (a \cdot a) + 0 \\ &= a \cdot a \end{aligned}$$

Thus, a . a = a

Note : 1(b) is the dual of 1(a). 1(b) is obtained by interchanging + and . ,

and by interchanging 0 and 1 in 1(a).

2. (a) We have

$a+1 = (a+1) . 1$

$= (a+1) . (a+a')$

$= a+(1 . a')$

$= a+(a' . 1)$

$= a+a'$

$= 1$

(b) It is the dual of 2(a). We interchange + and . , and interchange 1 and 0 in 2(a)

Thus $a . 0 = (a . 0) + 0$

$= (a . 0) + (a . a')$

$= a . (0 + a')$

$= a . (a'+0)$

$= a . a'$

$= 0$

3. (a) We have

$a+(a . b) = (a . 1) + (a . b)$

$= a . (1+b)$

$= a . (b+1)$

$= a . 1$, by boundedness law

$= a$

(b) We have

$a . (a+b) = (a+0) . (a+b)$

$= a + (0 . b)$

$= a + (b . 0)$

$= a + 0$, by boundedness law

$= a$

Note : 3(b) is the dual of 3(a), and vice versa.

4(a) Let L = (a+b) + c,

R = a + (b+c)

Now a . L = a . ((a+b) + c)

= (a . (a+b)) + (a . c), by distributive law

= a + (a . c), by absorption law

= a, by absorption law.

Again a . R = a . (a+(b+c))

= a, by absorption law.

Thus, a . L = a . R

Again $a^{/}$. L = $a^{/}$. ((a+b) + c)

= ($a^{/}$. (a+b)) + ($a^{/}$. c), by distributive law

= (($a^{/}$. a) + ($a^{/}$. b)) + ($a^{/}$. c)

= ((a . $a^{/}$) + ($a^{/}$. b)) + ($a^{/}$. c)

= (0 + ($a^{/}$. b)) + ($a^{/}$. c)

= (($a^{/}$. b) +0) + ($a^{/}$. c)

= ($a^{/}$. b) + ($a^{/}$. c)

= $a^{/}$. (b+c)

Again, $a^{/}$. R = $a^{/}$. (a+(b+c))

= ($a^{/}$. a) + ($a^{/}$. (b+c))

= (a . $a^{/}$) + ($a^{/}$. (b+c))

= 0 + ($a^{/}$. (b+c))

= $a^{/}$. (b+c)

Thus, $a^{/}$. L = $a^{/}$. R

Now (a+b) + c = L

= L . 1

= 1 . L

= (a+$a^{/}$) . L

= L . (a+$a^{/}$)

= (L . a) + (L.$a^{/}$)

= (a . L) + ($a^{/}$. L)

= (a . R) + ($a^{/}$. R)

= (R . a) + (R . $a^{/}$)

= R . (a + $a^{/}$)

= R . 1

= R

= a + (b+c)

(b) It is the dual of 4(a). We replace + by . , and vice verse. Also we replace 0 by 1, and vice versa. Thus, we will get the result.

Note : In view of 4(a) and 4(b), we will write (a+b)+c and a+(b+c) as a+b+c; and (a . b) . c) and a . (b . c) as abc.

5. (a) We have

$(a+b) + (a' . b')$

$= (b+a)+(a' . b')$, by comutative law

$= b+(a+(a' . b'))$, by associative law

$= b+(a+a') . (a+b')$, by distributive law

$= b+1. (a+b')$

$= b+a+b'$

$= b+b'+a$

$= 1+a$

$= a+1$

$= 1$

Again, $(a+b) . (a' . b')$

$= ((a+b) . a') . b'$, by associative law

$= (a' . (a+b)) . b'$, by commutative law

$= ((a' . a) + (a' . b)) . b'$

$= (0+(a' . b)) . b'$

$= (a' . b) . b'$

$= a' . (b . b')$, by associative law

$= a' . 0$

$= 0$

Thus, $(a+b) + (a' . b') = 1$

$(a+b) + (a' . b') = 0$ (1)

From (1), we conclude that $(a' . b')$ is the complement of a+b, i.e.,

$(a+b)' = a' . b'$

(b) It is the dual of 5(a). Interchanging + and . , and 0 and 1, we get the result.

Note : Augustus De Morgan (1806-1871) was a British mathematician. He was born in Madurai, India.

Corollary to 5(a) and 5(b)

6(a) $(a'+b')' = a \cdot b$, 6(b) $(a' \cdot b')' = a+b$, where a, b are any two elements of the Banach algebra B.

Proof : 6(a) $\left(a' + b'\right)'$

$= \left(a'\right)' \cdot (b')'$, by De Morgan's law

$= a.b$

(b) $(a' \cdot b')' = (a')' + (b')'$, by De Morgan's law

$= a+b$

Theorem 4.3 : Let B a Boolean algebra.

For all a, b $\in$ B,

(1) $a+b = b$, (2) $a \cdot b = a$, (3) $a'+b = 1$,

(4) $a \cdot b' = 0$ are equivalent.

Proof : First we prove that (1) $\Rightarrow$ (2)

We have $a = a+(a \cdot b)$, by absorption law

$= (a+a) \cdot (a+b)$, by distributive law

$= a \cdot (a+b)$, $\because$ $a+a=1$

$= a \cdot b$, given $a+b = a$

i. e. $a \cdot b = a$

Thus, (1) $\Rightarrow$ (2)

Next we prove that (2) $\Rightarrow$ (1)

We have $a+b = (a \cdot b) + b$, given $a \cdot b = a$

$= b+ (a \cdot b)$, by commutative law

$= b+ (b \cdot a)$, by commutative law

$= b$, by absorption law.

Thus, (2) $\Rightarrow$ (1)

Thus, we see that (1) and (2) are equivalent. (A)

Now, we prove that (2) and (3) are equivalent.

First we prove that (2) $\Rightarrow$ (3)

$a'+b = (a \cdot b)' + b$, given $a \cdot b = a$

$= (a'+b') + b$, by De Morgan's law

$= a'+(b'+b)$, by associative law

$= a'+(b+b')$, by commutative law

$= a' + 1$, $\because\ b + b' = 1$

$= 1$, by boundedness law

Thus, (2) $\Rightarrow$ (3)

Next we prove that (3) $\Rightarrow$ (2)

$a = a \cdot 1$

$= a \cdot (a' + b)$, given $a' + b = 1$

$= a \cdot a' + a \cdot b$, by distributive law

$= 0 + a \cdot b$

$= a \cdot b$

i. e., $a \cdot b = a$

Thus, (3) $\Rightarrow$ (2)

Thus, we see that (2) and (3) are equivalent (B).

Now, we prove that (3) and (4) are equivalent.

First we prove that (3) $\Rightarrow$ (4)

We have $a \cdot b' = (a')' \cdot b'$, $\because\ (a')' = a$

$= (a' + b)'$, by DeMorgan's law

$= 1'$, given $a' + b = 1$

$= 0$, $\because\ 1' = 0$

Thus, (3) $\Rightarrow$ (4)

Next we prove that (4) $\Rightarrow$ (3)

We have $a' + b = a' + (b')'$, $\because\ (b')' = b$

$= (a \cdot b')'$, by De Morgan's law

$= 0'$, given $a \cdot b' = 0$

$= 1$,

Thus, (4) $\Rightarrow$ (3)

Thus, we prove that (3) and (4) are equivalent. (C).

From (A), (B) and (C), we conclude that (1), (2), (3) and (4) are equivalent.

Theorem 4.4 : Let B be a Boolean algebra, and a, b, $c \in B$. If $a+b = a+c$, and $a \cdot b = a \cdot c$, then $b = c$.

Proof : $b = b \cdot (b+a)$, by absorption law

$= b \cdot (a+b)$, by commutative law

$= b \cdot (a+c)$, given $a+b = a+c$

= b . a + b . c, by distributive law

= a . b + b . c, by commutative law

= a . c + b . c, given a . b = a . c

= (a+b) . c, by distributive law

= (a+c) . c, given a+b = a+c

= c . (a+c), by commutative law

= c . (c+a), by commutative law

= c , by absorption law.

Theorem 4.5 : Let B be a Boolean algebra, and a, b, c $\in$ B. If a+c = b+c, and $a+c^{/} = b+c^{/}$, then a = b.

Proof : We have a = a+0

= $a+c.c^{/}$

= $(a+c) . (a+c^{/})$, by distributive law

= $(b+c) . (b+c^{/})$, given

= $b+c.c^{/}$, by distributive law

= b+0

= b

Example 6 : Let B be a Boolean algebra, and a, b $\in$ B. Prove that

a+b = 0 if and only if a = 0, b = 0

Solution : Let a = 0, b = 0

Then a+b = 0+0 = 0

Conversely, Let a+b = 0

Now a = a+0

= $a + (b . b^{/})$

= $(a+b) . (a+b^{/})$

= $0 . (a+b^{/})$

= 0

Again b = b+0

= $b+(a . a^{/})$

= $(b+a) . (b+a^{/})$

= $(a+b) . (b+a^{/})$

= $0 . (b+a^{/})$

= 0

Example 7 : Let B be a Boolean algebra, and a, b, c ∈ B. Prove that the following four expressions are equal.

(i) (a+b) . ($a^{/}$+c) . (b+c)

(ii) a.c + $a^{/}$.b + b.c

(iii) (a+b) . ($a^{/}$+c)

(iv) a.c + $a^{/}$.b

Solution : We have

(a+b) . ($a^{/}$+c) . (b+c)

= (a+b) . (c+$a^{/}$) . (c+b), by commutative law

= (a+b) . (c+($a^{/}$.b)), by distributive law

= (a+b) . c + (a+b) . ($a^{/}$.b), by distributive law

= c .(a+b) + a . ($a^{/}$.b)+b . ($a^{/}$.b)

= c.a + c.b + (a. $a^{/}$) . b + (b.b) . $a^{/}$

= a.c + b.c + 0.b + b.$a^{/}$, b.b = b

= a.c + b.c + 0 + $a^{/}$.b

= a.c + $a^{/}$.b + b.c (A)

Again,

(a+b) . ($a^{/}$+c)

= (a+b) . $a^{/}$ + (a+b) . c, by distributive law

= a.$a^{/}$ + b.$a^{/}$ + a.c+b.c

= 0 + $a^{/}$.b + a.c + b.c

= a.c + $a^{/}$.b +b.c (B)

Again,

(a+b) . ($a^{/}$+c)

= a.c + $a^{/}$.b + b.c, from (B)

= a.c + $a^{/}$.b + b.c.1

= a.c + $a^{/}$.b + b.c.(a+$a^{/}$)

= a.c + $a^{/}$.b + (b.c).a + (b.c) .$a^{/}$

= a.c + b.(c.a) + $a^{/}$.b + $a^{/}$.(b.c)

= a.c + b.(a.c) + $a^{/}$.b + ($a^{/}$.b).c

= (a.c + (a.c).b) + ($a^{/}$.b + ($a^{/}$.b).c)

= a.c + $a^{/}$.b, (C), by absorption law.

From (A), (B) and (C), we conclude that the four expressions (i), (ii),

(iii), (iv) are equal.

Example 8 : Let B be a Boolean algebra and a, b ∈ B.

Show that $a.b + ((a+b')'.b)' = 1$

Solution : $a.b + ((a+b')'.b')'$

$= a.b + (a+b')'' + b'$, by De Morgan's law

$= a.b + (a'.b) + b'$, by De Morgan's law, $(b')' = b$

$= b.a + b.a' + b'$

$= b.(a+a') + b'$, by distributive law

$= b.1 + b'$

$= b + b'$

$= 1$

Example 9 : Show that no Boolean algebra can have three distinct elements.

Solution : If possible, let there be a Boolean algebra B with three distinct elements 0, 1 and a, i.e. B = {0, 1, a}.

Clearly $a \neq 0$, $a \neq 1$.

We know that $0' = 1$, and $1' = 0$. $\therefore$ $a = a'$

Now $a = a.a$, by idempotent law

$= a.a'$

$= 0$,

Which is a contradiction.

Therefore there cannot be a Boolean algebra with three distinct elements.



CHECK YOUR PROGRESS

Let B be a Boolean algebra, and a, b, c ∈ B.

Prove that (1 to 9).

Q 3: $a.(a.b)' = a.b'$

Q 4: $(a+b) \,.\, c = a+b$, if $a.c = a$, $b.c = b$

Q 5: $a.b' + a'.b = 0$ if and only if $a = b$

Q 6: $a'.b'.c + a.b'.c + a.b'.c' = a.b' + b'.c$

Q 7: $ab + abc + a'b + ab'c = b + ac$

Q 8: $(a+b)\,(b+c)\,(c+a) = ab + bc + ca$

Q 9: $(a+b')\,(b+c')\,(c+a') = (a'+b)\,(b'+c)\,(c'+a)$

Q 10: Show that the set B = {0, 1, a, b}, where all the elements are distinct, is a Boolean algebra under the operations +, . , and / defined by

+	0	1	a	b
0	0	1	a	b
1	1	1	1	1
a	a	1	a	1
b	b	1	1	b

.	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	a	0
b	0	b	0	b

/	
0	1
1	0
a	b
b	a



LET US KNOW

There cannot be a Boolean algebra containing three distinct elements, but there can be a Boolean algebra containing four distinct elements.

4.6 BOOLEAN ALGEBRA AS LATTICE

We know that every Boolean algebra B satisfies the associative, commutative, and the absorption laws. Therefore B is a lattice where + and . are the join ($\vee$) and meet ($\wedge$) operations respectively.

Again, for every element $a \in B$,

$a+1 = 1$, i.e, $a \vee 1 = 1$ implies $a \leq 1$,

and $a \cdot 0 = 0$, i.e., $a \wedge 0 = 0$ implies $0 \leq a$.

Furthermore, distributive laws and complement laws show that B is a distributive, complemented lattice.

Conversely, every bounded, distributive, and complemented lattice L satisfies the four axioms given in the definition of a Boolean algebra.

Thus, we have the following alternative definition.

A Boolean algebra B is a bounded, distributive, and complemented lattice.

Thus, a Boolean algebra B is a lattice. Therefore, it has a natural partial order relation $\leq$. We have proved that–

1. $a \vee b = b$, i.e., $a+b = b$ if and only if $a \leq b$.

2. $a \wedge b = a$, i.e., $a.b = a$ if and only if $a \leq b$

3. $a \wedge b = a$, i.e., $a.b = a$ if and only if $a \vee b = b$, i.e., $a+b = b$

(2.5 Property of Lattices, Property II)

Therefore, we define $a \leq b$ whenever the equivalent conditions $a+b = b$ and $a.b = a$ hold.

Moreover, in a Boolean algebra B

1. $a+b = b$, 2. $a.b = a$, 3. $a'+b = 1$, 4. $a.b' = 0$ are equivalent (Theorem 4.3).

Thus, in a Boolean algebra we define $a \leq b$ whenever anyone of the above four conditions holds.

4.7 BOOLEAN ALGEBRA OF PROPOSITIONS

Let S be the set of all propositions (or statements). Then S is a Boolean algebra under the binary operations $\vee$ (disjunction), $\wedge$ (conjunction), and the unary operation ~ (negation). The unit element is the tautology t, and the zero element is the contradiction f. We note that a tautology t is any proposition which is always true, whereas a contradiction f is any proposition which is always false.

Let $p, q \in S$, i.e., p, q are propositions

1 (a)

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

Thus, we have $p \vee q \equiv q \vee p$

1 (b) Similarly $p \wedge q \equiv q \wedge p$

Let $p, q, r \in S$, i.e., p, q, r are propositions

2 (a)

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

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

From the above table we see that $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

2 (b) Similarly, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

3 (a)

p	f	$p \vee f$
T	F	T
F	F	F

Thus, we have $p \vee f \equiv p$

3 (b)

p	t	$p \wedge t$
T	T	T
F	T	F

Thus, we have $p \wedge t \equiv p$

4(a)

p	~p	$p \vee$ ~p	t
T	F	T	T
F	T	T	T

Thus, we have $p \vee$ ~$p \equiv t$

4 (b)

p	~p	$p \wedge$ ~p	f
T	F	F	F
F	T	F	F

Thus, we have $p \wedge$ ~$p \equiv f$

Thus, we see that (S, $\vee$, $\wedge$, ~, f, t) is a Boolean algebra, where f is the zero element, and t is the unit element.

4.8 TWO-ELEMENT BOOLEAN ALGEBRA

Example 10 : Let A = {a} be a singleton set.

Let P(A) be the power set of A.

Clearly P(A) = {A, ϕ}.

Then P(A) is a Boolean algebra under the usual operations of union, intersection, and complementation of subsets. We exhibit the operations as follows.

$\cup$	A	ϕ
A	A	A
ϕ	A	ϕ

$\cap$	A	ϕ
A	A	ϕ
ϕ	ϕ	ϕ

/	A	ϕ
	ϕ	A

It can be easily verified the commutative laws, distributive laws, identity laws, and complement laws.

We note that ϕ is the zero element and A is the unit element.

Thus, (P(A), $\cup, \cap, ', \phi$, A) is a Boolean algebra.

Definition

Let B = {0, 1}, the set of bits (binary digits), with the binary operations of + and . , and the unary operation $'$ defined by the following tables.

+	1	0
1	1	1
0	1	0

.	1	0
1	1	0
0	0	0

/	1	0
	0	1

i.e.,

1+1 = 1, 1+0 = 1, 0+1 = 0, 0+0 = 0

1 . 1 = 1, 1 . 0 = 0, 0 . 1 = 0, 0 . 0 = 0

$1' = 0$, $0' = 1$.

It can be easily verified the commutative laws, distributive laws, identity laws, and complement laws.

We note that 0 is the zero element and 1 is the unit element.

Thus, (B, +, . , $'$, 0, 1) is a Boolean algebra, called a two-element Boolean algebra.



4.9 LET US SUM UP

- Boolean algebra is an abstract mathematical structure after the name of George Boole.
- Let B be a nonempty set equipped with two binary operations + and ., a unary operation $'$, and two distinct elements 0, and 1. Then B is called a Boolean algebra if the following axioms are satisfied.

Commutative law

1. (a) $a+b = b+a$, (b) $a.b = b.a$, for all $a, b \in B$

Distributive laws

2. (a) $a+(b.c) = (a+b) . (a+c)$

(b) $a . (b+c) = (a.b) + (a.c)$ for all $a, b, c \in B$

Identity laws

3. (a) $a+0 = a$, (b) $a.1 = a$, for every $a \in B$

Complement laws

For every $a \in B$, there exists an element $a' \in B$ such that

4. (a) $a+a' = 1$, (b) $a.a' = 0$

- A square-free integer is an integer which is divisible by no perfect square other than 1.
- Let D_n be the set of positive divisors of n, where n>1, and n is a square-free positive integer. D_n is a Boolean algebra if we define

  a+b = lcm of a, b

  a . b = gcd of a, b

  $a' = \frac{n}{a}$, for all $a, b \in D_n$.
- The dual of any statement in a Boolean algebra B is the statement obtained by interchanging the operations + and . , and interchanging 0 and 1.
- The dual of any theorem in a Boolean algebra is also a theorem.
- Let B be a Boolean algebra. Then

  1(a). The zero element 0 is unique.

  (b). The unit element 1 is unique.

  2. The complement of every element is unique.

  3. (Involution law) For every $a \in B$, $(a')' = a$.
- Let B be a Boolean algebra, and a, b, $c \in B$. Then the following laws hold good.

  Idempotent laws

  1(a). $a+a = a$, (b) $a.a = a$

  Boundedness (or Dominance) laws

  2(a). $a+1 = 1$, (b) $a.0 = 0$

Absorption laws

3(a). a+(a.b) = a, (b) a . (a+b) = a

Associative laws

4(a). (a+b) + c = a+(b+c) (b) (a.b) . c = a . (b.c)

De Morgan's laws

5(a). $(a+b)' = a'.b'$, (b) $(a.b)' = a'+b'$

- There cannot be a Boolean algebra containing three distinct elements, but there can be a Boolean algebra containing four distinct elements.
- A Boolean algebra B is a bounded, distributive and complemented lattice.
- Let S be the set of all propositions (or statements). Then S is a Boolean algebra under the binary operations $\vee$ (disjunction), $\wedge$ (conjunction) and unary operation ~ (negation). The unit element is the tautology t and the zero element is the contradiction f.
- Let B = {0, 1}, the set of bits (binary digits), with the binary operations + and . and the unary operation $'$ defined by the following tables.

+	1	0
1	1	1
0	1	0

.	1	0
1	1	0
0	0	0

/	1	0
	0	1

Then B is a Boolean algebra, called a two-element Boolean algebra.



4.10 FURTHER READINGS

1) *Elements of Discrete Mathematies* by C L Liu, D P Mohapatra (Mc Graw Hill Education (India) Private Limited).
2) *Theory and Problems of Discrete Mathematics* by seymour Lipschutz, Mare Lars Lipson (Tata Mc Graw-Hill Publishing Company Limited).
3) *Introduction to Discrete Mathematies* by M.K Sen, B.C Chakraborty (Books and Allied (P) Ltd.).
4) *Discrete Mathematies with Graph Theory and Combinatories* by T Veerarajan (Tata Mc Graw-Hill Publishing Company Limited).

5) *Graph Theory* by Frank Harary (Narosa Publishing House)

6) *Graphs and Their Uses* by Oystein Ore (Random House/The L. W. Singer Company)

7) *Discrete Mathematics* by M.K. Gupta (Krishna Prakashan Media (P) Ltd).

8) *A Textbook of Discrete Mathematics* by Swapan Kumar Sarkar (S. Chand & Company Ltd.)

9) Internet.



4.11 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: We have D_{70} = {1, 2, 5, 7, 10, 14, 35, 70}

We define a+b = lcm (a, b)

a . b = gcd (a, b)

$a' = \frac{70}{a}$, for all a, b $\in D_{70}$

1(a) We have a+b = lcm (a, b)

= lcm (b, a)

= b+a

(b) a . b = gcd (a, b)

= gcd (b, a)

= b . a, for all a, b $\in D_{70}$

2(a) a+(b.c) = a+gcd (b, c)

= lcm (a, gcd (b, c))

= gcd (lcm (a, b), lcm (a, c))

= (a+b) . (a+c), for all a, b, c $\in D_{70}$

(b) Similarly a . (b+c) = (a.b) + (a.c), for all a, b, c $\in D_{70}$

3(a) a+1 = lcm (a, 1) = a,

(b) a . 1 = gcd (a, 70) = a, for every a $\in D_{70}$

4(a) $a + \frac{70}{a} = \text{lcm}\left(a, \frac{70}{a}\right) = 70$

(b) $a \,.\, \frac{70}{a} = \text{gcd}\left(a, \frac{70}{a}\right) = 1$

$\therefore$ $(D_{70}, +, ., ', 1, 70)$ is a Boolean algebra.

We note that 1 is the zero element, and 70 is the unit element.

Ans to Q No 2: We have $D_{27} = \{1, 3, 9, 27\}$

$(D_{27}, +, ., ', 1, 27)$ is not a Boolean algebra, for

$3 + \frac{27}{3}$ = 3+9 = lcm (3, 9) = $9 \neq 27$

Also $3 \,.\, \frac{27}{3}$ = 3 . 9 = gcd (3, 9) = $3 \neq 1$.

Ans to Q No 3: We have $a \,.\, (a.b)'$

= $a.(a'+b')$, by De Morgan's law

= $(a.a') + (a.b')$, by distributive law

= $0 + (a.b')$

= $a \,.\, b'$

Ans to Q No 4: (a+b) . c = c.(a+b); by commutative law

= c . a + c.b; by distributive law

= a+b; c.a = a.c = a, c.b = b.c = b, (given)

Ans to Q No 5: Let a = b

$\therefore$ $a.b' + a'.b = b.b' + b'.$

= 0+0

= 0

Conversely, Let $a.b' + a'. b = 0$

$\therefore$ $a + a.b' + a'.b = a+0$

$\Rightarrow$ $(a + a.b') + a'.b = a$

$\Rightarrow$ $a + a'.b = a$; by absorption law

$\Rightarrow$ $(a + a') \,.\, (a+b) = a$, by distributive law

$\Rightarrow$ $1 \,.\, (a+b) = a$

$\Rightarrow$ $(a+b) = a$ (1)

Again $a.b' + a'.b = 0$

$\Rightarrow$ $a.b' + a'.b + b = 0+b$

$\Rightarrow$ $a.b' + (b + b.a') = b$

$\Rightarrow a.b' + b = b$, by absorption law

$\Rightarrow b + a.b' = b$

$\Rightarrow (b+a) . (b+b') = b$

$\Rightarrow (a+b) . 1 = b$

$\Rightarrow a + b = b$ (2)

From (1) and (2), we get a = b.

Ans to Q No 6: $a'.b'.c + a.b'.c + a.b'.c'$

$= a'.b'.c + a.b'.(c+c')$

$= a'.b'.c + a.b'.1$

$= a'.b'.c + a.b'$

$= b'.a'.c + b'.a$

$= b'.(a'.c + a)$

$= b'.(a+a'.c)$

$= b'.((a+a') . (a+c))$

$= b' . 1 . (a+c)$

$= b'. (a+c)$

$= b'.a + b'.c$

$= a . b' + b'.c$

Ans to Q No 7: $ab + abc + a'b + ab'c$

$= (ab + a'b) + (abc + ab'c)$

$= (ba + ba') + (acb + acb')$

$= b(a+a') + ac(b+b')$

$= b1 + ac1$

$= b + ac$

Ans to Q No 8: $(a+b) (b+c) (c+a)$

$= (a+b) ((b+c (c+a))$

$= (a+b) ((b+c)c + (b+c)a)$

$= (a+b) (c(b+c) + a(b+c))$

$=(a+b) (cb+cc+ab+ac)$

$= (a+b) (cb+c+ab+ac)$, $cc = c.c = c$

$= a (cb+c+ab+ac) + b(cb+c+ab+ac)$

$= a(cb)+ac+a(ab)+a(ac)+b(cb)+bc+b(ab)+b(ac)$

$= a(bc)+ac+(aa)b+(aa)c+b(bc)+bc+b(ba)+(ba)c$

= abc+ac+ab+ac+(bb)c+bc+(bb)a+(ab)c,

$\because$ aa = a.a = a

= abc+ac+ab+ac+bc+bc+ba+abc,

$\because$ bb = b.b = a

=(abc+abc)+(ac+ac)+(ab+ab)+(bc+bc)

= abc+ac+ab+bc,

$\because$ abc + abc = abc, etc.,

= ac(b+1)+ab+bc

= ac.1 + ab+bc

= ab + bc + ca

Ans to Q No 9: We have

$(a+b')\ (b+c')\ (c+a')$

$= ((a+b')\ (b+c')\ (c+a')$

$= ((a+b')\ b + (a+b')c')\ (c+a')$

$= (ab+b'b+ac'+b'c')\ (c+a')$

$= (ab+ac'+b'c')\ (c+a'),\ b'b = bb' = b.b' = 0$

$= (ab+ac'+b'c')c + (ab+ac'+b'c')a'$

$= abc + ac'c + b'c'c+aba'+ac'a'+b'c'a'$

$= abc + a0 + b0 + aa'b + aa'c' + a'b'c',\ c'c = 0$

$= abc + 0 + 0 + 0b + oc' + a'b'c',\ aa' = 0$

$= abc + a'b'c'$

Similarly, we can prove that

$(a'+b)\ (b'+c)\ (c'+a) = abc + a'b'c'$

$\therefore\ (a+b')\ (b+c')\ (c+a') = (a'+b)\ (b'+c)\ (c'+a).$

Ans to Q No 10: From the given tables, we see that

1(a). x+y = y+x, (b) x.y = y.x, for all x, y $\in$ B

2(a). x+(y.z) = (x+y) . (x+z), for all x, y, z $\in$ B.

(b) x.(y+z) = (x.y) +(x.z), for all x, y, z $\in$ B.

3(a) x+0 = x, (b) x . 1 = x, for every x $\in$ B

From the table we see that $0' = 1$, $1' = 0$, $a' = b$, $b' = a$, and

4(a) $x+x' = 1$, (b) $x.x' = 0$, for every x $\in$ B.

Thus, (B, +, . , $'$, 0, 1) is a Boolean algebra.



4.12 MODEL QUESTIONS

Q 1: Define a Boolean algebra and give an example.

Q 2: Define Boolean algebra as a lattice.

Q 3: Let B be a Boolean algebra prove that.

(i) the zero element 0 is unique,

(ii) the unit element 1 is unique.

Q 4: Prove the

(i) idempotent laws,

(ii) boundedness laws,

(iii) absorption laws,

(iv) associative laws,

(v) De Morgan's laws.

of Boolean algebra.

Q 5: Let S be the set of all propositions. Prove that S is a Boolean algebra under the binary operations disjunction, conjuction and the unary operation negation.

Q 6: Let D_{18} be the set of positive divisors of 18.

Define a+b = lcm of a, b

a . b = gcd of a, b

$a' = \frac{18}{a}$, for all a, b $\in D_{18}$

Examine if (D_{18}, +, . , $'$, 1, 18) is a Boolean algebra.

Q 7: Let D_{66} be the set of positive divisors of 66.

Define a+b = lcm of a, b

a . b = gcd of a, b

$a' = \frac{66}{a}$, for all a, b $\in D_{66}$.

Examine if (D_{66} , +, . , $'$, 1, 66) is a Boolean algebra.

*** ***** ***

UNIT 5 : COMBINATORICS

UNIT STRUCTURE

5.1 Learning Objectives

5.2 Introduction

5.3 The Pigeonhole Principle

5.4 Counting principle

5.4.1 The Rule of Sum

5.4.2 The Rule of product

5.5 Permutation

5.6 Combination

5.7 Principle of Inclusion-Exclusion

5.8 Let Us Sum Up

5.9 Answers to Check Your Progress

5.10 Further Readings

5.11 Model Questions

5.1 LEARNING OBJECTIVES

After going through this unit, you will able to know-

- the Pigeonhole Principle
- the rule of sum
- the rule of product
- permutation
- combination
- principle of Inclusion-Exclusion

5.2 INTRODUCTION

Combinatorics is an important branch of mathematics that deals with the counting problems. In this unit, we will discuss some of counting tools of combinatorics like pigeonhole principle, rule of sum and product, permutations, combination and principle of inclusion-exclusion. Combinatorics is applied in various branches of computer science.

5.3 THE PIGEONHOLE PRINCIPLE

Statement: The pigeonhole principle states that if (n+1) pigeon occupies' 'n' holes, then at least one hole has more than one pigeon.

Proof: We assume that (n+1) pigeon occupies' 'holes.

We have to prove that at least one hole has more than one pigeon.

Suppose we consider that at least one hole has not more than one pigeon.

Therefore, each and every hole has exactly one pigeon.

Since, there are 'n' holes, which implies, we have totally 'n' pigeon which is a contradiction that there are (n+1) pigeon.

Hence, at least one hole has more than one pigeon.

The pigeonhole principle is very useful in counting methods. To apply the pigeonhole principle, we have to decide objects (pigeons) and categories of the desired characteristic (pigeonholes) and be able to count the number of objects and the number of pigeonholes. We can also apply this principle to other objects besides pigeons and pigeonholes.

Now, we discuss the generalized form of the pigeon principle.

Generalized Pigeonhole principle:

Statement: If 'm' pigeon occupies 'n' holes (m > n), then at least one hole has more than $\left[\frac{m-1}{n}\right]+1$ pigeon

Proof: We assume that 'm'pigeon occupies 'n' holes (m>n).

We have to prove that at least one hole has more than $\left[\frac{m-1}{n}\right]+1$ pigeon.

Suppose we consider that at least one hole has not more than $\left[\frac{m-1}{n}\right]+1$ pigeon.

Each and every hole has exactly $\left[\frac{m-1}{n}\right]+1$ pigeon.

Since we have n holes, so there are $\left[\frac{m-1}{n}\right]+1$ pigeon.

$\Rightarrow$ m–1+n pigeon.

$\Rightarrow$ m+1–n pigeon.

Which is a contradiction to the assumption, that there are *m* pigeon.

Therefore,at least one hole has more than $\left[\frac{m-1}{n}\right]+1$ pigeon.

Note: For is a real number, [x] represents the greatest integer less than or equal to *x*.

Let us discuss some examples related to Generalized Pigeonhole principle

Example 1: Show that among 200 people, at least17 of them were born in the same month.

Solution: Here, No. of Pigeon = m = No. of People = 200

No. of Holes = n = No. of Month = 12

Then by generalized pigeon hole principle

$\left[\frac{200-1}{12}\right]+1=17$, were born in the same month.

Example 2: Show that if 25 dictionaries in a library contain a total of 40,325 pages, then one of the dictionaries must have at least 1614 pages.

Solution: Here, No. of Pigeon = m = No. of People = 40,325

No. of Holes = n = No. of Month = 25

Then by generalized pigeon hole principle

$\left[\frac{40325-1}{25}\right]+1=1614$ pages.

5.4 COUNTING PRINCIPLE

The two basic counting principles are:

1. The rule of sum
2. The rule of product

5.4.1 The rule of sum

If one job can be performed in ways and another job can be performed in ways, then the total number of ways in which either of the two jobs can be performed in (m+n) ways.

The rule can be extended to any finite number of jobs. Thus,

if *r* works can be done in $n_1, n_2, \ldots, n_r$ ways and if they cannot be done simultaneously, then any one of the works can be performed in $(n_1 + n_2 + \ldots + n_r)$ ways.

Example 3: In a class there are 12 boys and 8 girls. The teacher wants to select either a boy or a girl to represent the class in a function. In how many ways can the teacher make this selection?

Solution: The teacher is to perform either of the following two jobs:

(a) Selecting a boy among 12 boys (or)

(b) Selecting a girl among 8 girls

The first job can be performed in 20 ways and the second in 10 ways.

Therefore, by the rule of sum either of the two jobs can be performed in (12+8) = 20 ways.

Example 4: There are 30 mathematics books and 25 Computer science books in a library. In how many ways a mathematics book or a science book can be selected?

Solution: We are to select one book, a mathematics book or a computer science book.

One mathematics book can be selected in 30 ways. One computer science book can be selected in 25 ways.

By the rule of sum, a mathematics book or a computer science book can be selected in (30+25) i.e., 55 ways.

5.4.2 The rule of product

If one job can be performed in *m* ways and another job can be performed in ways, then the total number of ways in which both the jobs can be performed in *(mn)* ways.

The rule can be extended to any finite number of jobs. Thus, if a work can be done in *r* successive steps, and the first step can be done in n_1 ways, the second step can be done in n_2 ways, and in this way, the *r* th step can be done in n_r ways, then the work can be done in $(n_1 x\ n_2 x \ldots x\ n_r)$ ways.

Example 5: How many different bit strings of length eight are there?

Solution: Each of the eight bits can be selected in two ways because each bit is either 0 and 1.

By the product rule, there are a total of 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 = 256 of different bit strings of length eight.

Example 6: There are 25 boys and 20 girls in a class. A teacher wants to select one boy and one girl. In how many ways can this be done?

Solution: One boy can be selected in 25 ways. One girl can be selected in 20 ways. Thus, the first step (i.e., to select one boy) can be done in 25 ways, the second step (i.e., to select one girl) can be done in 20 ways.

Therefore, by the rule of product,one boy and one girl can be selected in 25 x 20 i.e., 500 ways.

Example 7: How many three digits odd numbers can be formed by using the digits 2, 3, 4, 5, 6, 7 if

(a) the repetition of digits is not allowed?

(b) the repetition of digits is allowed?

Solution: For odd numbers, we must have 3, 5 or 7 at the unit's place.

So, there are 3 ways of filling the unit's place.

(a) Since the repetition of digits is not allowed, the ten's place can be filled with any of the remaining 5 digits in 5 ways. Now, remaining 4 digits can be filled in 4 ways.

So, by the rule of product, the required numbers =3x5x 4 = 60.

(b) Since repetition of digits is allowed, so each of the ten's and hundred's place can be filled in 6 ways = 3 x 6 x 6 = 108.



CHECK YOUR PROGRESS 1

Q 1: Show that if eight colors are used to paint 60 cars, at least eight cars will have the same colour.

Q 2: How many different license plates is available if each plate contains a sequence of three letters followed by three digits?

Q 3: In a class there are 20 boys and 10 girls. The teacher wants to select either a boy or a girl to represent the class in a function. In how many ways can the teacher make this selection?

Q 4: In how many ways a candidate can answer all the questions of a true-false test consisting of 10 questions?

Q 5: There are 6 multiple choice questions in an examination. How many sequences of answers are possible if the first three questions have 4 choices each and the next three have 5 each?

5.5 PERMUTATION

Suppose we have 40 mathematics books of different topics and we have to arrange it in a book shelf which can hold only 20 books. We have to choose 20 books out of 40 books and then arrange them on the shelf. We can choose any 20 books as we like and then arrange them on the shelf in whatever manner we like. Thus, the process of arranging 20 books out of 40 books has the following two steps:

Step 1: First we select 20 books out of 40 books according to our choice. It may be of different topics like number theory, algebra, calculus, topology etc.

Step 2: After selecting 20 books out of 40 books we proceed to arrange them on the shelf. We can arrange them on the shelf in any manner we like, for example, it is up to us whether we put a book on number theory or topology in the first place and so on.

From the above example, we come with two types of problem.

(a) Selection

(b) Arrangement

The process of selecting objects is called Combination and the process of arranging objects is called permutation.

Examples relating to combination are

(a) Formation of a 4-member committee from 12 members.

(b) Formation of a team from a number of players.

Examples relating to permutation are

(a) Arrangement of books on a shelf.

(b) Formation of numbers with the given digits.

(c) Formation of words with the given letters.

Now we define the term 'Permutation'

Definition: Each of the distinct arrangement which can be made by taking some or all of a number of things at a time is called a permutation. By permutation we mean the arrangement of objects in a particular order.

The number of permutations of distinct things taken at a time is denoted *P (n, r).*

The letter *'P'* is an abbreviation of the word permutation. So, *P (7, 3)* means the number of permutations of 7 objects taken 3 at a time.

The value of *P (n, r)* :

To find the number of permutations of *n* distinct things taken *r* at a time.

The first object can be chosen in *n* different ways. So, we are left with *(n –1)* objects. Therefore, the second object can be chosen in *(n –1)* ways. Similarly, the third object can be chosen in *(n–2)* ways. In this way, the last object, i.e., the *r* th object can be chosen in *(n–r+1)* ways. Consequently, by the product rule, there are *n(n–1) (n–2), . . ., (n–r+1)* way of ordered arrangment Thus,

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

$$= \frac{n(n-1)(n-2),\ldots,(n-r+1)(n-r)(n-r-1)\ldots 3.2.1}{(n-r)(n-r-1)\ldots 3.2.1}$$

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

Note: (a) Factorial Notation: The product of natural numbers from 1 to *n* is denoted by n! and read as factorial *n*.

Thus, n! = n(n–1) (n–2) 3.2.1

5! = 5 x 4 x 3 x 2 x 1 = 120

(a) We know that $P(n, r) = \frac{n!}{(n-r)!}$

Putting $r = 0, P(n, 0) = \frac{n!}{n!} = 1,$

Putting $r = n, P(n, n) = \frac{n!}{0!} = n!$ $[\because 0! = 1]$

Example 8: Find the value of *r* if P(5, r) = 60.

Solution: Given P(5, r) = 60

$\Rightarrow$ P(5, r) = 5 x 4 x 3

$\Rightarrow$ P(5, r) = P(5, 3)

$\Rightarrow$ r = 3

Example 9: In how many ways can 6 persons occupy 3 vacant seats ?

Solution: Total number ways =P (6, 3)

$$= \frac{6!}{3!}$$

= 6 x 5 x 4

= 120 Ways

Example 10: Find the number of ways that a party of six persons can arrange themselves in a row of six chairs.

Solution: The six persons can arrange themselves in a row of six chairs in P(6, 6) ways.

The number of ways that a party of six persons can arrange themselves in a row of six chairs = P(6, 6).

$$= \frac{6!}{(6-6)!}$$

= 6 !

= 720

Example 11: How many four-digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8, if repetitions of digits are not allowed?

Solution: The number of 4-digit numbers.

= the number of 4-permutations of 6 objects (digits)

= P (6,4)

= 6 x 5 x 4 x 3 = 360

Example 12: How many four-digits even numbers can be formed from the digits 1, 2, 3, 5, 7, 8 if repetition of digits is not allowed?

Solution: One's place can be filled up in 2 ways (one of the digits 2, 8). The other three places can be filled up in ${}^5P_3$.

the required number of numbers $= 2 \times {}^5P_3$

$$= 2 \times \frac{5!}{(5-3)!}$$

$$= 2 \times \frac{5 \times 4 \times 3 \times 2!}{2!}$$

$= 120$

Important results of Permutation:

1. If there are elements of which n_1 are alike of one kind, n_2 are alike of second kind; n_3 are alike of third kind and so on and n_r are r^{th} of kind, where $(n_1 + n_2 + \ldots + n_r) = n$.

   Then, number of permutations of n objects $= \frac{n!}{(n_1!)(n_2!)(n_3!)\ldots(n_1!)}$

2. Number of permutations of n distinct objects taking n objects at a time $= P(n, n) = n!$

Example 13: How many different words can be formed with the letters of the word 'MISSISSIPPI'?

Solution: There are 11 letters in the word 'MISSISSIPPI' in which there are four I's, fourS's, two P's and one M's.

$\therefore$ The required number words $= \frac{11!}{4!4!2!}$

$= 34650$

5.6 COMBINATION

The word Combination means selection. Suppose we are required to make a selection of any three objects from four objects *a, b, c* and *d.* The different selections are *abc, bdc, cda* and *abd*. Here *abc* and *bca* denote the same selection. These four selections *abc, bdc, cda* and *abd* are called combinations.

The number of combinations of n distinct objects taken r at a time is denoted by $C(n,r)$.The letter "C" is an abbreviation of the word Combination. So, $C(5,2)$ means the number of combinations of 5 objects taken 2 at a time.

The value of C(n, r) :

To find the number of combinations of *n* distinct things taken *r* at a time.

Each of these combinations contains *r* things and all these things are permuted among themselves.

$\therefore$ The number of permutations obtained is *r!*

Hence from all the *C(n, r)* combinations, we get *C(n, r)x r!* permutations.

C(n, r) x r! gives all the permutations of *n* distinct things taken *r* at a time i.e., P(n, r).

Hence, C(n, r) x r! = P(n, r)

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

$$= \frac{n!}{r!(n-r)!} \left[\because P(n, r) = \frac{n!}{(n-r)!} \right]$$

Example 14: From a group of 16 players, a team of 11 players is to be chosen. In how many ways this can be done?

Solution: There are 16 players in a group. We have to select 11 players from the group.

The number of ways = C(16, 11)

$$= \frac{16!}{11!(16-11)!}$$

$$= \frac{16 \times 15 \times 14 \times 13 \times 12 \times 11!}{11!5!}$$

$$= \frac{16 \times 15 \times 14 \times 13 \times 12}{5 \times 4 \times 3 \times 2 \times 1}$$

= 4368

Example 15: How many triangles can be formed by joining the vertices of a hexagon?

Solution: There are 6 vertices of a hexagon. One triangle is formed by selecting a group of 3 vertices from given 6 vertices. This can be done in *C(6, 3)* ways.

Number of triangles = *C(6, 3)*

$$= \frac{6!}{3!3!}$$

$$= 20$$

Example 16: In how many ways can a committee of 6 gentlemen and 3 ladies be formed out of 9 gentlemen and 6 ladies?

Solution: 6 gentlemen can be selected from 9 gentlemen in ${}^9C_6$ ways. 3 ladies can be selected from 6 ladies can be selected in ${}^6C_3$ ways.

by the product rule, the number of committees = ${}^9C_6 \times {}^6C_3$

$$= \frac{9!}{6!3!} \times \frac{6!}{3!3!}$$

$$= \frac{9 \times 8 \times 7}{3 \times 2 \times 1} \times \frac{6 \times 5 \times 4}{3 \times 2 \times 1}$$

$$= 3 \times 4 \times 7 \times 5 \times 4$$

$$= 1680$$

Some important results of combination:

(a) C(n, 0) = 1

(b) C(n, n) = 1

(c) C(n, r) = C(n, n–r)

(d) C(n, r) + C(n, r+1) = C(n+1, r+1)

5.7 PRINCIPLE OF INCLUSION-EXCLUSION

The Principle of Inclusion and Exclusion allows us to find the cardinality of a union of sets by knowing the cardinalities of the individual sets and all possible intersections of them.

The Principle of Inclusion and Exclusion is that for two finite sets A and B, is $|A \cup B| = |A| + |B| - |A \cap B|$

The result can be generalized to three and four finite sets:

(i) $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

(ii) $|A \cup B \cup C \cup D| =$

$$|A| + |B| + |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D|$$
$$+ |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$$

Example 17: How many positive integers not exceeding 1000 are divisible by 7 or 11?

Solution: Let *A* denote the set of positive integers not exceeding 1000 that are divisible by 7.

Let *B* denote the set of positive integers not exceeding 1000 that are divisible by 11.

Then, $|A| = \left[\frac{1000}{7}\right] = [142.8] = 142$

$|B| = \left[\frac{1000}{11}\right] = [90.9] = 90$

$|A \cap B| = \left[\frac{1000}{7 \times 11}\right] = [12.9] = 12$

The number of positive integers not exceeding 1000 that are divisible either 7 or 11 is $|A \cup B|$.

By Principle of Inclusion -Exclusion

$|A \cup B| = |A| + |B| - |A \cap B|$

= 142 + 90 – 12

= 220

There are 220 positive integers not exceeding 1000 divisible by either 7 or 11.

Example 18: Find the number of integers between 1 to 250 that are not divisible by any of the integers 2, 3, 5 and 7.

Solution: Let A denote the integer from 1 to 250 that are divisible by 2.

Let *B* denote the integer from 1 to 250 that are divisible by 3.

Let *C* denote the integer from 1 to 250 that are divisible by 5.

Let *D* denote the integer from 1 to 250 that are divisible by 7.

Then, $|A| = \left[\frac{250}{2}\right] = [125] = 125$

$|A| = \left[\frac{250}{3}\right] = [83.33] = 83$

$|C| = \left[\frac{250}{5}\right] = [50] = 50$

$|D| = \left[\frac{250}{7}\right] = [35.71] = 35$

Now,

The number of integer between 1 to 250 that are divisible by 2 & 3

$= |A \cap B| = \left[\frac{250}{2 \times 3}\right] = [41.66] = 41$

The number of integer between 1 to 250 that are divisible by 2 & 5

$= |A \cap C| = \left[\frac{250}{2 \times 5}\right] = [25] = 25$

The number of integer between 1 to 250 that are divisible by 2 & 7

$= |A \cap D| = \left[\frac{250}{2 \times 7}\right] = [17.86] = 17$

The number of integer between 1 to 250 that are divisible by 3 & 5

$= |B \cap C| = \left[\frac{250}{3 \times 5}\right] = [16.66] = 16$

The number of integer between 1 to 250 that are divisible by 3 & 7

$= |B \cap D| = \left[\frac{250}{3 \times 7}\right] = [11.90] = 11$

The number of integer between 1 to 250 that are divisible by 3 & 7

$= |C \cap D| = \left[\frac{250}{5 \times 7}\right] = [7.14] = 7$

The number of integer between 1 to 250 that are divisible by 2, 3 & 5 $= |A \cap B \cap C| = \left[\frac{250}{2 \times 3 \times 5}\right] = [8.33] = 8$

The number of integer between 1 to 250 that are divisible by 2, 3 & 7 $= |A \cap B \cap D| = \left[\frac{250}{2 \times 3 \times 7}\right] = [5.95] = 5$

The number of integer between 1 to 250 that are divisible by 2, 5 & 7 $= |A \cap C \cap D| = \left[\frac{250}{2 \times 5 \times 7}\right] = [3.57] = 3$

The number of integer between 1 to 250 that are divisible by 3, 5 & 7 $= |B \cap C \cap D| = \left[\frac{250}{3 \times 5 \times 7}\right] = [2.38] = 2$

The number of integer between 1 to 250 that are divisible by 2, 3, 5 & 7 $= |A \cap B \cap C \cap D| = \left[\frac{250}{2 \times 3 \times 5 \times 7}\right] = [1.19] = 1$

By principle of Inclusion –Exclusion

$|A \cup B \cup C \cup D|$

$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D|$
$+ |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$

$= (125+83+50+35) - (41+25+17+16+11+7) + (8+5+3+2) - 1$

$= 293 - 117 + 18 - 1 = 193$

Now,

The number of integers not divisible by any of 2, 3, 5 and 7 = Total $- |A \cup B \cup C \cup D|$

$= 250 - 193$

$= 57$



CHECK YOUR PROGRESS 2

Q 6: Find the number of different 4 letter words with or without meanings that can be formed from the letters of the word 'NUMBER'?

Q 7: How many different words can be formed from the letters of the word 'ASSAM'?

Q 8: In how many ways 5 persons be selected from amongst 10 persons?

Q 9: How many diagonals are there in a polygon of 8 sides?

Q 10: How many integers between 1 to 100 that (a) not divisible by 7, 11 or 13 (b) divisible by 3 but not by 7?



5.8 LET US SUM UP

- Combinatorics deals with counting the number of ways of arranging or selecting objects from a finite collection under specified rules.
- The pigeonhole principle states that if (n+1) pigeon occupies"holes, then at least one hole has more than one pigeon.
- If 'm' pigeon occupies 'n' holes (m > n), then at least one hole has

more than $\left[\frac{m-1}{n}\right]+1$ pigeon

- If one job can be performed in *m* ways and another job can be performed in ways, then the total number of ways in which either of the two jobs can be performed in (m+n) ways.
- If one job can be performed in ways and another job can be performed in ways, then the total number of ways in which both the jobs can be performed in *(mn)* ways.
- Each of the distinct arrangement which can be made by taking some or all of a number of things at a time is called a permutation. The number of permutations of distinct things taken *r* at a time is denoted P(n, r) and $P(n, r) == \frac{n!}{!(n-r)!}$

  Thus P(n,r) =Total number of permutations of *n* distinct things taken *r* at a time.
- The number of combinations of *n* distinct objects taken *r* at a time is denoted by C (n, r) and. $C(n, r) = \frac{n!}{r!(n-r)!}$.

  Thus C(n, r) = Total number of combinations of *n* distinct things taken *r* at a time.
- The Principle of Inclusion and Exclusion allows us to find the cardinality of a union of sets by knowing the cardinalities of the individual sets and all possible intersections of them.



5.9 FURTHER READINGS

1) Rao, G. S. S. Bhishma. *Discrete Structures and Graph Theory*. SciTech Publications (India) PVT Ltd, 2003

2) Sharma, J.K. *Discrete Mathematics*. Macmillan Publishers India Ltd, 2011.

3) Balaji, G. *Discrete Mathematics*. Balaji Publishers, 2015.

4) Singaravelu, A. & Jeyaraman, M.P. *Discrete Mathematics*. Meenakshi Agency,2016.

5) Satyanarayana, B. & Prasad, K.S. *Discrete Mathematics and Graph Theory*. PHI Learning Private Limited, 2009.

6) Rao, G.S. *Discrete Mathematical Structure*. New Age international (P) Limited, 2009.

7) Singh, Y.N. *Mathematical Foundation of Computer Science*, New Age international Publishers, 2005.

8) Lipschutz, S & Lipson, M.L. Schaum's outline of *Theory and Problems of Discrete Mathematics*, McGraw-Hill, 2007.

9) Chandrasekaran, N &Umaparvathi, M. *Discrete Mathematics*, PHI Learning Private Limited, 2010.

10) Tremblay, J.P. & Manohar, *Discrete Mathematical Structures with Applications to Computer Science,* Tata McGraw Hill Education Private Limited, 1997.

5.10 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: We assume that 60 cars(pigeons) are assign 8 colors(pigeonholes). Hence, by the generalized pigeonhole principle, at least $\left[\frac{60-1}{8}+1\right]$ cars will have the same colour.

Ans to Q No 2: There are 26 choices for each of the three letters and 10 choices for each of the three digits. Hence, by the product, there are a total of 26 x 26 x 26 x 10 x 10 x 10 = 17,576,000 license plate.

Ans to Q No 3: First question can be answered in 2 ways (either true of false).

Similarly, each of the questions can be answered in 2 ways.

= 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2

$= 2^{10} = 1024$

Ans to Q No 4: Do yourself.

Ans to Q No 5: Here we have to perform 6 jobs of answering 6 multiple choice questions.Each of the first three questions can be answered in 4 ways and each of the next three can be answered in 5 different ways.

So by the rule of product, the total number of different sequence = 4 x 4 x 4 x 5 x 5 = 8000.

Ans to Q No 6: There are 6 letters in the word'NUMBER'.

So, the number of 4 letter words = P(6, 4)

$$= \frac{6!}{(6-4)!}$$

$$= 360$$

Ans to Q No 7: There are 5 letters in the word 'ASSAM' in which there are two A's, two S's and one M's.

The required number words $= \frac{5!}{2!2!} = 30$

Ans to Q No 8: The selection can be done in C(10, 5) ways

$$C(10, 5) = = \frac{10!}{5!(10-5)!} = 252 \text{ ways}$$

Ans to Q No 9: Number of diagonals = C(8, 2) – 8 = 20

Ans to Q No 10: (1) Let A, B and C denote respectively the number of integers between 1 to 100 that are divisible by 7, 11 and 13.

Now, $$|A| = \left[\frac{100}{7}\right] = [14.28] = 14$$

$$|B| = \left[\frac{100}{11}\right] = [9.09] = 9$$

$$|C| = \left[\frac{100}{13}\right] = [7.69] = 7$$

Now,

The number of integers between 1 to 100 that are divisible by 7 & 11

$$= |A \cap B| = \left[\frac{100}{7 \times 11}\right] = [1.29] = 1$$

The number of integers between 1 to 100 that are divisible by 7 & 13

$= |A \cap C| = \left[\frac{100}{7 \times 13}\right] = [1.09] = 1$

The number of integers between 1 to 100 that are divisible by 11 & 13

$= |B \cap C| = \left[\frac{100}{11 \times 13}\right] = [0.69] = 0$

The number of integers between 1 to 100 that are divisible by 7, 11 &

13 = $|A \cap B \cap C| = \left[\frac{100}{7 \times 11 \times 13}\right] = [0.99] = 0$

The number of integers between 1-100 that are divisible by 7, 11 or 13 is $|A \cup B \cup C|$

By principle of Inclusion – Exclusion

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

= 14 + 9 + 7 – (1 + 1 + 0) + 0

= 30 – 2

= 28

$\therefore$ The number of integers not divisible by 7, 11 and 13 =

Total – $|A \cup B \cup C|$

= 100 – 28

= 72

(2) Let and denote the number of integer between 1 to 100 that are divisible by 3 and 7 respectively.

$|A| = \left[\frac{100}{3}\right] = [33.33] = 33$,

$|B| = \left[\frac{100}{7}\right] = [14.28] = 14$

The number of integers between 1 to 100 that are divisible by 7 & 3 =

$|A \cap B| = \left[\frac{100}{7 \times 3}\right] = [4.76] = 4$

$\therefore$ The number of integers not divisible by 3 but not by 7 = $|A| - |A \cap B|$

= 33 – 4

= 29



5.11 MODEL QUESTIONS

Q 1: Show that atleast two people must have their birthday in the same month if 13 people are assembled in a room.

Q 2: Show that if 9 colors are used to paint 100 houses atleast 12 houses will be of the same color.

Q 3: How many different three letter initials are there that begin with the letter *A* ?

Q 4: A license plate contains two English letters, followed by two digits, followed by two English letters, followed by four digits. How many license plates can be made if repetition of letters and digits are allowed?

Q 5: How many 4-digit numbers are there?

Q 6: How many four-letter words can be formed using *a, b, c, d, e, f* if (a) repetition is allowed (b) repetition is not allowed.

Q 7: How many members of {1, 2, 3, ..., 105} have nontrivial factors in common with 105?

Q 8: How many arrangements can be made with the letters of the word 'MATHEMATICS'?

Q 9: Find the number of the integers between 1 to 100 that are divisible by
(i) 2, 3, 5 or 7
(ii) 2, 3, 5 but not by 7.

Q 10: Find n if $P(n, 4) : P(n-1, 3) = 9 : 1$.

*** ***** ***

UNIT 6 : BASIC ALGEBRAIC STRUCTURE

UNIT STRUCTURE

6.1 Learning Objectives

6.2 Introduction

6.3 Binary Operation

- 6.3.1 Commutative Binary Operation
- 6.3.2 Associative Binary Operation
- 6.3.3 Identity Element
- 6.3.4 Inverse of an Element

6.4 Group

- 6.4.1 Subgroup
- 6.4.2 Coset
- 6.4.3 Cyclic Group
- 6.4.4 Normal Subgroup
- 6.4.5 Quotient Group

6.5 Ring

6.6 Integral Domain and Field

6.7 Let Us Sum Up

6.8 Further Readings

6.9 Answers To Check Your Progress

6.10 Model Questions

6.1 LEARNING OBJECTIVES

After going through this unit, you will able to learn

- binary operations on a set
- groups, subgroups, cosets, cyclic groups, normal subgroups, quotient groups
- rings, commutative rings
- integral domains and fields.

6.2 INTRODUCTION

In mathematics, an algebraic structure is a nonempty set equipped with a binary operation or a collection of operations (binary many operations) satisfying certain postulates. Group and Ring are two such algebraic structures. In this unit we will study groups – subgroups, cosets, cyclic groups, normal subgroups, quotient groups. Also we will study rings, integral domains and fields.

6.3 BINARY OPERATION

Let us consider the set $\underline{\underline{N}}$ of natural numbers.

For every ordered pair $(a, b) \in \underline{\underline{N}} \times \underline{\underline{N}}$, we get a unique $a+b \in \underline{\underline{N}}$. So we can define a function.

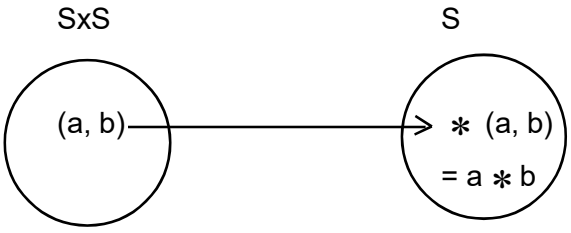
$f : \underline{\underline{N}} \times \underline{\underline{N}} \rightarrow \underline{\underline{N}}$, $f(a, b) = a+b$



This function is known as a binary operation of $\underline{\underline{N}}$. Thus, addition is a binary operation on $\underline{\underline{N}}$.

Similarly, multiplication is a binary operation on $\underline{\underline{N}}$; for every ordered pair $(a, b) \in \underline{\underline{N}} \times \underline{\underline{N}}$, we get a unique $ab \in \underline{\underline{N}}$. But subtraction is not a binary operation on $\underline{\underline{N}}$; for every ordered pair $(a, b) \in \underline{\underline{N}} \times \underline{\underline{N}}$, we do not get $a–b \in \underline{\underline{N}}$. We have $(2, 3) \in \underline{\underline{N}} \times \underline{\underline{N}}$, but $2–3 = –1 \notin \underline{\underline{N}}$.

Definition : A binary operation $*$ on a nonempty set S is a function from S x S to S, i.e., $* : S \times S \rightarrow S$, $*(a, b) = a * b$; $a, b \in S$.



Here the image of (a, b) under the function $*$ i.e., $*(a, b)$ is denoted by $a * b$.

Thus, $*$ is a binary operation of S if $a * b \in S$, for all $a, b \in S$. In this case S is said to be closed under $*$.

Number of binary operations on a finite set

Let A, B be two finite sets, and n(A) = m, and n(B) = n; where n(A) denotes the number of elements of A.

Then the number of functions from A to B is n^m.

[The first element of A can be associated in n ways, the second element can be associated in n ways, and lastly, the m^{th} element can be associated in n ways.

$\therefore$ the number of functions

= n. n. . . . n (m factors) = n^m]

We know that n(A xA) = mm = m^2

$\therefore$ number of binary operations on **A**

= number of functions from A x A to A

= m^{m^2}.

Examples

1. Addition is a binary operation on $\underline{\underline{N}}$.
2. Subtraction is not a binary operation on $\underline{\underline{N}}$.
3. Multiplication is a binary operation on $\underline{\underline{N}}$.
4. Addition is a binary operation on $\underline{\underline{Z}}$,the set of integers.
5. Addition is not a binary operation on the set S = $\underline{\underline{Z}}$ – {0} of nonzero integers, for $3 \in S$, $-3 \in S$, but $3+(-3) = 0 \notin S$.
6. Subtraction is a binary operation on $\underline{\underline{Z}}$.
7. Let S be the collection of all real matrices. Matrix addition is not a binary operation on S. We cannot find the sum of a 2 x 3 matrix and a 3 x 4 matrix.
8. Let M_{nxn} be the collection of all mxn real matrices. Matrix addition is a binary operation on M_{mxn}.
9. Let M_{nxn} be the collection of all nxn real matrices. Matrix multiplication is a binary operation of M_{nxn}.
10. Addition (also multiplication) is a binary operation on the set $\underline{\underline{C}}$ of complex numbers.

Example 1: Is $*$ defined by axb = a–b+10 a binary operation on $\underline{\underline{Z}}$, the set of integers?

Solution : Let a, b $\in \underline{\underline{Z}}$

Clearly, a–b+10 $\in \underline{\underline{Z}}$, $\forall$ a, b $\in \underline{\underline{Z}}$

i.e., a $*$ b $\in \underline{\underline{Z}}$, $\forall$ a, b $\in \underline{\underline{Z}}$

$\therefore$ $*$ is a binary operation on $\underline{\underline{Z}}$.

Example 2: Is $*$ defined by a $*$ b = $\frac{ab}{5}$ a binary operation on $\underline{\underline{Q}}$, the set of rational numbers ?

Solution : Let a, b $\in \underline{\underline{Q}}$

$\therefore$ ab $\in \underline{\underline{Q}}$ (the product of two rational numbers is a rational number)

$\therefore$ $\frac{ab}{5} \in \underline{Q}$

i.e. a $*$ b $\in \underline{\underline{Q}}$, $\forall$ a, b $\in \underline{\underline{Q}}$

$\therefore$ $*$ is a binary operation on $\underline{\underline{Q}}$.

Example 3: Let P be the set of all subsets of a nonempty set S. Show that union and intersection are two binary operations on P.

Solution : Let A, B $\in$ P, i.e., A $\subseteq$ S, B $\subseteq$ S

$\therefore$ A $\cup$ B $\subseteq$ S, i.e. A $\cup$ B $\in$ P

$\therefore$ $\cup$ is a binary operation on P.

Similarly, A $\cap$ B $\in$ P, $\forall$ A, B $\in$ P

$\therefore$ $\cap$ is a binary operation on P.

Operation (or composition) Table

Let S be a finite set and the number of elements of S be small. We can construct a table, known as the operation (or composition) table, due to Arthur Cayley (1821-1895), as follows.

Let S = $\{a_1, a_2, a_3\}$

We write the elements a_1, a_2, a_3 in a horizontal row as well as in a vertical column and write the binary operation $*$ in the top left corner. Now we enter each of the $9(=3^2)$ entries $a_i * a_j$ (i = 1, 2, 3; j = 1, 2, 3) in the $(i, j)^{th}$ cell as shown in Table 6.1. Each of the 9 entries belongs to S, since $*$ is a binary operation on S.

$*$	a_1	a_2	a_3
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$

Table 6.1

Example 4: Is multiplication a binary operation on S = {–1, 0, 1} ?

Solution : Each of the 9 entries belongs to S.

$\therefore$ multiplication is a binary operation on S.

x	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Table 6.2

Example 5: Is addition a binary operation on S = {–1, 0, 1}?

Solution : $-2 \notin S$

$2 \notin S$

$\therefore$ addition is not a binary operation on S.

+	–1	0	1
–1	–2	–1	0
0	–1	0	1
1	0	1	2

Table 6.3

Example 6: Is $*$ defined by $a * b = |a - b|$ a binary operation on S = {0, 1, 2}?

Solution : $0 * 0 = |0 - 0| = 0$,

$0 * 1 = |0 - 1| = 1$,

$0 * 2 = |0 - 2| = 2$,

$1 * 0 = |1 - 0| = 1$,

$1 * 1 = |1 - 1| = 0$,

$1 * 2 = |1 - 2| = 1$,

$2 * 0 = |2 - 0| = 2$,

$2 * 1 = |2 - 1| = 1$,

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Table 6.4

$2 * 2 = |2 - 2| = 0$,

From the table we see that $*$ is a binary operation on S = {0, 1, 2}.

6.3.1 Commutative Binary Operation

A binary operation $*$ on a nonempty set S is commutatiive if $a * b = b * a$, for $a, b \in S$.

Note : For a finite set, a binary operation is commutative if and only if the entries in the operation table are symmetric with respect to the principal diagonal.

For example, the entries in Table 6.4 are symmetric with respect to the principal diagonal 0, 0, 0. Therefore, $*$, defined in Example 5, is commutative on S = {0, 1, 2}.

Example 7: Is the binary operation $*$ defined by $a * b = a - b + 5$ commutative on $\underline{\underline{Z}}$, the set of integers?

Solution : We have $a * b = a - b + 5$, $a, b \in \underline{\underline{Z}}$.

$3 * 5 = 3 - 5 + 5 = 3$

$5 * 3 = 5 - 3 + 5 = 7$

Clearly $3 * 5 \neq 5 * 3$

$\therefore$ $*$ is not commutative on $\underline{\underline{Z}}$.

Example 8: Let $\underline{\underline{Q}}$ be the set of rational numbers. Let $*$ be a binary operation on $\underline{\underline{Q}}$ defined by $a * b = ab^2$, for all $a, b \in \underline{\underline{Q}}$. Is $*$ commutative?

Solution : We have $a * b = ab^2$, for all $a, b \in \underline{\underline{Q}}$.

$3 * 5 = 3 \times 5^2 = 75$

$5 * 3 = 5 \times 3^2 = 45$

Clearly $3 * 5 \neq 5 * 3$

$\therefore$ $*$ is not commutative on $\underline{\underline{Q}}$.

Note : An example that disproves a statement is a counterexample. We have cited counterexamples in Example 7, and in Example 8.

6.3.2 Associative Binary Operation

A binary operation $*$ on a nonempty set S is associative if $(a * b) * c = a * (b * c)$, for all $a, b, c \in S$

Example 9: Is the binary operation $*$ defined by $a * b = a–b+5$ associative on $\underline{\underline{Z}}$?

Solution : Let $a, b, c \in \underline{\underline{Z}}$

$(a * b) * c = (a–b+5) * c$

$= (a–b+5) – c+5$

$= a – b – c + 10$

$a * (b * c) = a * (b–c+5)$

$= a – (b–c+5) + 5$

$= a – b + c – 5 + 5$

$= a – b + c$

$\therefore (a * b) * c \neq a * (b * c)$

$\therefore *$ is not associative on $\underline{\underline{Z}}$.

Example 10: Let X be the set of rational numbers excluding 1. We define $*$ on X as follows.

$a * b = a+b–ab$, for all $a, b \in X$.

Show that $*$ is a binary operation on X. Examine if $*$ is (i) commutative, (ii) associative.

Solution : Let $a, b \in X$.

$\therefore$ a, b are two rational numbers, and $a \neq 1$, $b \neq 1$.

Now $a+b–ab$ is a rational number and $a+b–ab \neq 1$, for if $a+b–ab = 1$,

then $a+b–ab–1 = 0$

i.e. $(a–1)–b(a–1) = 0$

i.e. $(a–1)(1–b) = 0$

i.e. $a–1 = 0$, or $1–b = 0$

i.e. $a = 1$, or $b = 1$, which is a contradiction.

$\therefore a+b–ab \in X$

i.e. $a * b \in X$, for all $a, b \in X$,

$\therefore *$ is a binary operation on X.

Second Part

$a * b = a+b–ab$

$= b+a–ba$

$= b * a$, for all $a, b \in X$,

$\therefore *$ is commutative on X.

Again $(a * b) * c$

$= (a+b-ab) * c$

$= (a+b-ab)+c - (a+b-ab)c$

$= a+b-ab+c-ac-bc+abc$

$= a+b+c-ab-bc-ca+abd$

$a * (b * c) = a * (b+c-bc)$

$= a+(b+c-bc)-a(b+c-bc)$

$= a+b+c-bc-ab-ac+abc$

$= a+b+c-ab-bc-ca+abc$

$\therefore (a * b) * c = a * (b * c)$, for all $a, b, c \in X$.

$\therefore *$ is associative on X.

6.3.3 Identity Element

Let S be a nonempty set equipped with a binary operation $*$. An element $e \in S$ is called an identity element for $*$ if $a * e = a = e * a$, for all $a \in S$.

Note: Identity element for a binary, if it exists, is unique.

Examples

1. Multiplication is a binary operation on $\underline{\underline{N}}$. There exists $1 \in N$ such that $a1 = a = 1a$, for all $a \in \underline{\underline{N}}$.
   $\therefore$ 1 is the identity for multiplication in $\underline{\underline{N}}$.
2. Addition is a binary operation on $\underline{\underline{Z}}$. There exists $0 \in \underline{\underline{Z}}$ such that $a+0 = a = 0+a$, for all $a \in \underline{\underline{Z}}$.
   $\therefore$ 0 is the identity for addition in $\underline{\underline{Z}}$.
3. Addition is a binary operation on $\underline{\underline{N}}$. But there does not exist identity element for addition in $\underline{\underline{N}}$.
4. Matrix addition is a binary operation on M_{mxn}, the set of all mxn real matrices. Then mxn null matrix 0 is the identity for matrix addition in M_{mxn}.

6.3.4 Inverse of an Element

Let S be a nonempty set equipped with a binary operation $*$, and with identity element e. An element $b \in S$ is called inverse of

a under $*$ if $a * b = e = b * a$

Note : 1. Inverse of an element under a binary operation, if it exists, is unique.

2. Generally inverse of a is denoted by a^{-1}.
3. In case of real numbers, inverse of a under addition (i.e.,additive inverse) is denoted by –a, whereas inverse of a ($a \neq 0$) under multiplication (i. e.), multiplicative inverse is denoted by $\frac{1}{a}$.

Examples

1. Multiplication is a binary operation on $\underline{\underline{N}}$, and $1 \in \underline{\underline{N}}$ is the identity for multiplication. But no element of $\underline{\underline{N}}$, except 1, possesses inverse under multiplication in $\underline{\underline{N}}$.
2. Addition is a binary operation on $\underline{\underline{Z}}$, and $0 \in \underline{\underline{Z}}$ is the identity for addition. For every $a \in \underline{\underline{Z}}$, there exists $-a \in \underline{\underline{Z}}$ such that

   $a+(-a) = 0 = (-a) + a$

$\therefore$ – a is the inverse of a under addition.

6.4 GROUP

A nonempty set G, equipped with a binary operation $*$, is called a group if the following postulates are satisfied.

(i) Associativity

$(a * b) * c = a * (b * c)$, for all $a, b, c \in G$

(ii) Existence of identity

There exists $e \in G$ such that

$a * e = a = e * a$, for all $a \in G$

(iii) Existence of inverse for every $a \in G$, there exists $b \in G$ such that

$a * b = e = b * a$

b is called inverse of a.

We write : $(G, *)$ is a group.

Furthermore, if $*$ is commutative, G is called an Abelian group, after the name of the celebrated Norwegian mathematician Niels Henrik Abel (1802-1829).



LET US KNOW

A nonempty set G equipped with a binary operation is called a semigroup if the binary operation is associative.

Note : 1. In order to be a group, there must be a nonempty set equipped with a binary operation satisfying the postulates mentioned above. Later on, we will simply write 'Let G be a group". It should be borne in mind that there is a binary operation on G.

2. We will drop the binary operation symbol and simply write 'ab'. It should be borne in mind that this is not our usual multiplication.

Finite and Infinite Groups

A group G is finite if the set G is finite; otherwise it is infinite group.

Order of a group

The number of elements of a finite group G is called the order of G. Symbolically, it is denoted by 0(G) or |G|.

Example 11: Let G = {1}

Clearly multiplication is a binary operation on G.

Moreover, all the postulates for a group are satisfied.

$\therefore$ G is a group under multiplication. Furthermore, G is an Abelian group.

Example 12: Let G = {–1, 1}, the set consisting of the square roots of unity.

(i) From the table we see that multiplication is a binary operation on G.

x	–1	1
–1	1	–1
1	–1	1

Table 6.5

(ii) We know that multiplication of real numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element of G possesses inverse in G.

1 is the inverse of 1.

–1 is the inverse of –1.

$\therefore$ G is a group under multiplication.

(v) Moreover, multiplication of real numbers is commutative.

$\therefore$ G is an Abelian group.

Note : We have seen that, for every positive integer n, there exists an Abelian group of order n.

Example 13: Let $G = \{z : z \text{ is complex and } z^n = 1\}$, i.e., G is the consisting of the nth roots of unity, n is a natural number.

(i) Let $z_1, z_2 \in G$

$\therefore\ z_1^n = 1, z_2^n = 1$

Now $(z_1 z_2)^n = 1, \therefore z_1 z_2 \in G$

$\therefore$ multiplication is a binary operation on G.

(ii) We know that multiplication of complex number is associative.

(iii) There exists $1 \in G$ such that 1z = z1, for all $z \in G$.

$\therefore$ 1 is the identity element.

(iv) Let $z \in G \qquad \therefore z_1^n = 1$

Now $\frac{1}{z}$ is a complex number and $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$

$\therefore \frac{1}{z} \in G$

Thus, for every $z \in G$, there exists $\frac{1}{z} \in G$ such that

$$z\frac{1}{z} = 1 = \frac{1}{z}z$$

$\therefore \frac{1}{z}$ is inverse of z.

$\therefore$ G is a group under multiplication of complex numbers.

(v) Moreover multiplication of complex numbers is commutative

$\therefore$ G is an Abelian group.

Example 14: Let $\underline{\underline{Z}}$ be the set of integers.

(i) Let $a, b \in \underline{\underline{Z}}$

$\therefore$ $a+b \in \underline{\underline{Z}}$, for all $a, b \in \underline{\underline{Z}}$

i.e., addition is a binary operation on $\underline{\underline{Z}}$.

(ii) We know that multiplication of integers is associative.

(iii) We have $0 \in \underline{\underline{Z}}$, and a+0 = a = 0+a, for all $\in \underline{\underline{Z}}$

$\therefore$ 0 is the identity.

(iv) for every $a \in \underline{\underline{Z}}$, there exists $-a \in \underline{\underline{Z}}$ such that $a+(-a) = 0 = (-a)+a$.

$\therefore$ $\underline{\underline{Z}}$ is a group under addition.

(v) Moreover, addition of real numbers is commutative.

$\therefore$ $\underline{\underline{Z}}$ is an Abelian group under addition.

Note : $\underline{\underline{Z}}$ is an infinite group under addition.

Some other examples are the following :

- $\underline{\underline{Q}}$ is an Abelian group under addition.
- $\underline{\underline{R}}$ is an Abelian group under addition.
- $\underline{\underline{Q}}_0$ The set of nonzero rational numbers is an Abelian group under multiplication.
- $\underline{\underline{R}}_0$, the set of nonzero real numbers is an Abelian group under multiplication.
- $\underline{\underline{C}}$ is an Abelian group under addition.
- $\underline{\underline{C}}_0$ the set of nonzero complex numbers is an Abelian group under multiplication.

Example 15: Let $G = \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} : \alpha \text{ is a real number} \right\}$

(i) Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in G$,

$$A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G$$

α, β are real numbers.

Now $A_\alpha A_\beta = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$= \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \cos\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}$$

$$= A_{\alpha+\beta} \in G$$

i.e., matrix multiplication is a binary operation on G.

(ii) We know that matrix multiplication is associative.

(iii) We have $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$= \begin{pmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{pmatrix} \in G$$

and $A_\alpha I = A_\alpha = IA_\alpha$, for all $A_\alpha \in G$

$\therefore$ I is the identity element.

(iv) We have $\left|A_\alpha\right| = \begin{vmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{vmatrix}$

$$= \cos^2\alpha + \sin^2\alpha = 1 \neq 0$$

$\therefore$ A_α^{-1} exists

Now $\text{adj}\, A_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$

$$\therefore A_\alpha^{-1} = \frac{1}{\left|A_\alpha\right|} \text{adj}\, A_\alpha$$

$$= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \in G$$

$\therefore$ G is a group under matrix multiplication,

(v) Moreover $A_\alpha A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta A_\alpha$

$\therefore$ G is an Abelian group.

Example 16: Let $G = \left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \text{ is real, } x \neq 0 \right\}$

(i) Let $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$, $\begin{pmatrix} y & y \\ y & y \end{pmatrix} \in G$

x, y are real numbers; $x \neq 0$, $y \neq 0$

Now $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} xy+xy & xy+xy \\ xy+xy & xy+xy \end{pmatrix}$

$$= \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G$$

xy is real, and $xy \neq 0$.

(ii) We know that matrix multiplication is associative.

(iii) We have $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \in G$,

and $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \\ \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$

Similarly $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity element.

(iv) For every $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G$, we have $\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} \in G$

such that $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$\therefore \begin{pmatrix} \frac{1}{4x} & \frac{1}{4x} \\ \frac{1}{4x} & \frac{1}{4x} \end{pmatrix}$ is the inverse of $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$.

$\therefore$ G is a group under matrix multiplication.

(v) Moreover $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix}$

$$= \begin{pmatrix} 2yx & 2yx \\ 2yx & 2yx \end{pmatrix}$$

$$= \begin{pmatrix} y & y \\ y & y \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\therefore$ G is an Abelian group under matrix multiplication.

Remark : We note that the identity element is $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$

Example 17: Let G be the set of rational numbers excluding 1. We define $*$ on G as follows.

$a * b = a+b-ab$, for all $a, b \in G$.

(i) $*$ is a binary operation on G. (Example 10)

(ii) $*$ is associative on G (Example 10)

(iii) We have $0 \in G$ and

$a * 0 = a+0-a0 = a$

$0 * a = 0+a-0a = a$

$\therefore$ 0 is the identity under $*$

(iv) For every $a \in G$, There exists $\frac{a}{a-1} \in G$ such that

$$a * \frac{a}{a-1} = a + \frac{a}{a-1} - a \cdot \frac{a}{a-1}$$

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

$$= \frac{a^2 - a + a - a^2}{a-1}$$

$$= \frac{0}{a-1} = 0$$

Note : That $\frac{a}{a-1} \neq 1$, for if $\frac{a}{a-1} = 1$

then a = a–1

i.e. –1 = 0, absurd

Similarly $\frac{a}{a-1} * a = 0$

$\therefore$ $\frac{a}{a-1}$ is the inverse of a under $*$

$\therefore$ G is a group under $*$

(v) Moreover $*$ is commutative on G. (Example 10)

$\therefore$ G is an Abelian group under $*$

Theorem 6.1 : Let G be a group. Then

(i) identity element is unique,

(ii) inverse of each element in G is unique,

(iii) $(a^{-1})^{-1} = a$, for all $a \in G$, where a^{-1} denotes the inverse of a,

(iv) $(ab)^{-1} = b^{-1}a^{-1}$, for all a, $b \in G$

(v) $ab = ac \Rightarrow b = c$ (left cancellation law)

$ba = ca \Rightarrow b = c$ (right cancellation law), for all a, b, $c \in G$

Proof. (i) If possible let e & f be two identities of G

$\therefore$ ef = e = fe [$\because$ f is identity]

ef = f = fe [$\because$ e is identity]

$\therefore$ e = f

Thus, identity element is unique.

Note : In view of the above theorem, we write 'the identity', not 'an identity'.

(ii) Let $a \in G$ and e be the identity of G.

If possible, let b and c be two inverses of a.

$\therefore$ ab = e = ba [$\because$ b is inverse of a]

ac = e = ca [$\because$ c is inverse of a]

Now b = be [$\because$ e is identity]

= b(ac) [$\because$ e = ac]

$= (ba)c$ [$\because$ by associativity]

$= ec$ [$\because$ $ba = e$]

$= c$ [$\because$ e identity]

Thus, inverse of a is unique.

Note : In view of the above theorem, we write 'the inverse of a', not 'an inverse of a'.

(iii) We have $aa^{-1} = e = a^{-1}a$

$\therefore$ a^{-1} is the inverse of a, and vice versa, a is the inverse of a^{-1}, i.e., $(a^{-1})^{-1} = a$.

(iv) Let e be the identity of G, and $a, b \in G$.

Now $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= aea^{-1}$

$= aa^{-1}$

$= e$

$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$

$= b^{-1}eb$

$= b^{-1}b$

$= e$

$\therefore$ $b^{-1}a^{-1}$ is the inverse of ab, i.e., $(ab)^{-1} = b^{-1}a^{-1}$

(v) We have $ab = ac$

Now $a \in G \Rightarrow a^{-1} \in G$

$\therefore$ $a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [by associativity]

$\Rightarrow eb = ec$ [$aa^{-1} = e = a^{-1}a$]

$\Rightarrow b = c$ [$\because$ e is the identity]

Again $ba = ca$

$\because$ $(ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [by associativity]

$\Rightarrow be = ce$

$\Rightarrow b = c$ [$\because$ e is the identity]

Example 18: If, in a group G, every element is its own inverse, prove that G is Abelian.

Solution : Let G be a group. Let a, b ∈ G.

∴ $a^{-1} = a$, $b^{-1} = b$ (given)

Now a, ∈ G, b ∈ G ⇒ ab ∈ G

$ab = (ab)^{-1}$ (given)

$= b^{-1}a^{-1}$ [Theorem 1 (iv)]

= ba, for all a, b ∈ G.

∴ G is Abelian.

Example 19: Prove that a group G is Abelian if and only if $(ab)^2 = a^2b^2$, for all a, b ∈ G.

Solution : Let a, b ∈ G

∴ ab ∈ G, ba ∈ G.

$(ab)^2 = a^2b^2$

⇔ (ab) (ab) = (aa) (bb)

⇔ a(ba)b = a(ab)b

⇔ (ba)b = (ab)b, [by left cancellation law]

⇔ ba = ab, [by right cancellation law]

⇔ G is Abelian.



CHECK YOUR PROGRESS

Q 1: Let S be a finite set having 4 elements. What is the number of binary operations on S?

Q 2: Is ∗, defined by $a * b = \frac{a}{b}$, a binary operation on $\underline{\underline{R}}$, the set of real numbers?

Q 3: Let S = {–1, 1, –i, i}, i = $i = \sqrt{-1}$. Is multiplication a binary operation on S?

Q 4: Let $\underline{\underline{Q}}$ be the set of rational numbers. Show that ∗ defined by a ∗ b = a+ab is a binary operation on $\underline{\underline{Q}}$.

Examine if ∗ is (i) commutative, (ii) associative.

Q 5: Show that the set G consisting of the cube roots of unity is an Abelian group under usual multiplication.

Q 6: Show that the set G consisting of the fourth roots of unity is an Abelian group under usual multiplication.

Q 7: Show that the set G consisting of all 2x2 nonsingular matrices over reals is a group under matrix multiplication.

Q 8: Let $G = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \text{ is real, } x \neq 0 \right\}$. Show that G is an Abelian group under matrix multiplication.

Q 9: Let $G = \left\{ \begin{pmatrix} x & x & x \\ x & x & x \\ x & x & x \end{pmatrix} : x \text{ is real, } x \neq 0 \right\}$ Show that G is an Abelian group under matrix multiplication.

Q 10: Let G be a group and e be the identity of G. If $a^2 = e$, for all $a \in G$, prove that G is Abelian.

Q 11: Show that a group of order four is always Abelian.

6.4.1 Subgroup

Let us consider the set $\underline{\underline{Z}}$ of integers. We know that $\underline{\underline{Z}}$ is a group under addition.

Let $2\underline{\underline{Z}} = \{0, \pm 2, \pm 4, \ldots.\}$ be the set of even integers.

Clearly $2\underline{\underline{Z}}$ is a nonempty subset of $\underline{\underline{Z}}$.

Moreover, $2\underline{\underline{Z}}$ is also a group under addition.

In this case $2\underline{\underline{Z}}$ is said to be a subgroup of $\underline{\underline{Z}}$.

Definition : A nonempty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G. Symbolically, we write $H \leq G$.

Note : (1) If e is the identity of G, {e} is also a subgroup of G, called the trivial subgroup of G. All other subgroups of G are nontrivial. {e} is also called the identity subgroup of G.

(2) G itself is a subgroup of G, called the improper subgroup of G. All other subgroups are proper. [John B. Fraleigh, A First Course in Abstract Algebra (First Indian Reprint, 2003)]

Every group has at least two subgroups, viz., the trivial subgroup, i.e., the identity subgroup, and the group itself.

Example 20: Let us consider

$G = \{-1, 1, -i, i\}$, $i = \sqrt{-1}$

We know that G is a group under multiplication.

Let H = {–1, 1}.

We have $H \subseteq G$.

Also H is a group under multiplication.

$\therefore H \leq G$

The set of real numbers $\underline{\underline{R}}$ is a group under addition. The set $\underline{\underline{R}}+$ of positive real numbers is a group under multiplication. $\underline{\underline{R}}+$ is a subset of $\underline{\underline{R}}$, but not a subgroup of $\underline{\underline{R}}$. Binary operations are different.

Theorem 6.2: Let H be a subgroup of a group G. Then

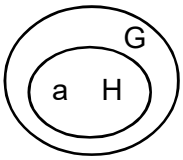
(i) the identity element of H is the identity element of G,

(ii) the inverse of any element of H is the same as the inverse of the element of G.

Proof : Let G be a group, and $H \leq G$

(i) If possible, let e be the identity of G, and f be the identity of H.

Let $a \in H$



$\therefore$ af = a = fa [$\because$ f is the identity of H]

Again $a \in H \Rightarrow a \in G$.

$\therefore$ ae = a = ea [$\because$ e is the identity of G]

$\therefore$ af = ae

$\Rightarrow$ f = e [by left cancellation law]

(ii) Let e be the identity of G.

$\therefore$ e is also the identity of H.

Let $a \in H$.

If possible, let b the inverse of a in H, and c be the inverse of a in G.

$\therefore$ ab = e = ba

ac = e = ca

$\therefore$ ab = ac

$\Rightarrow$ b = c [by left cancellation law]

Note : If H, K are two subgroups of a group G, and e is the identity of G, then e is also the identity of H as well as of K. So H and K have at least one common element, viz, the identity element. Thus, we conclue that there cannot be two disjoint subgroups of a group.

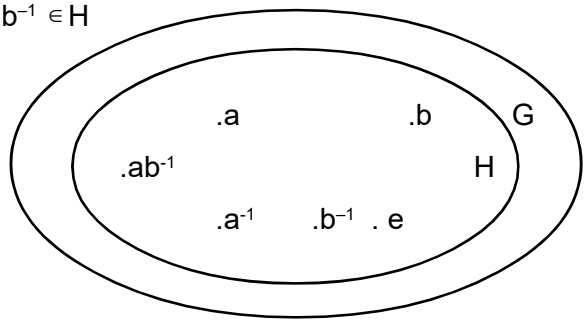
Theorem 6.3: A nonempty subset H of a group G is a subgroup of G if and only if $a, b \in H \Rightarrow ab^{-1} \in H$.

Proof : Let $H \leq G$, and $a, b \in H$

$b \in H \Rightarrow b^{-1} \in H$ [$\because$ H is a group]

Now $a \in H, b^{-1} \in H$

$\therefore ab^{-1} \in H$



Conversely, Let $H \subseteq G$ such that $a, b \in H \Rightarrow ab^{-1} \in H$.

(i) Now $a, a \in H \Rightarrow aa^{-1} \in H$ [by the given condition]

$\Rightarrow e \in H$,

Where e is the identity of G

(ii) $e \in H, a \in H \Rightarrow ea^{-1} \in H$ [by the given condition]

$\Rightarrow a^{-1} \in H$

$\therefore$ every element of H has inverse in H.

(iii) $b \in H \Rightarrow b^{-1} \in H$, by (ii)

Now $a \in H, b^{-1} \in H \Rightarrow a\left(b^{-1}\right)^{-1} \in H \Rightarrow ab \in H$

(iv) The binary operation is associative on H as it is associative on G.

$\therefore$ H is a group under the same binary operation in G. Also $H \subseteq G$.

$\therefore H \leq G$

Note : (1) If G is an additive group, i.e., if G is a group under addition, then a nonempty subset H of G is a subgroup of G if and only if a, b $\in H \Rightarrow a–b \in H$.



LET US KNOW

An Abelian group cannot have a nonabelian subgroup.

Let G be an Abelian group. Then the binary operation is commutative on G.

Let $H \leq G$.

The binary operation is commutative on H as it is commutative in G.

$\therefore$ H is also Abelian.

Thus, every subgroup of an Abelian group is Abelian.

Theorem 6.4 : The intersection of two subgroups of a group is again a subgroup of the group.

Proof : Let G be a group, and e be the identity of G.

Let $H \leq G$, $K \leq G$

We note that $H \cap K$ is nonempty, i.e., $H \cap K \neq \phi$, for at least the identity element.

$e \in H \cap K$

Let $a, b \in H \cap K$.

$a \in H \cap K \Rightarrow a \in H$ and $a \in K$

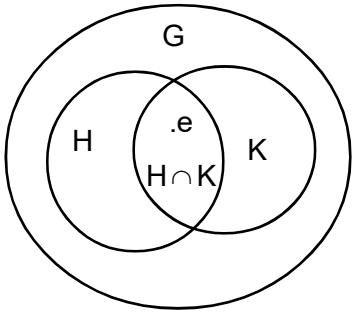
$b \in H \cap K \Rightarrow b \in H$ and $b \in K$

Now $a, b \in H$ and $H \leq G$ $\quad \therefore ab^{-1} \in H$

$a, b \in K$ and $K \leq G$ $\quad \therefore ab^{-1} \in K$

$ab^{-1} \in H$ and $ab^{-1} \in K \Rightarrow ab^{-1} \in H \cap K$.

$\therefore H \cap K \leq G$



Note : The union of two subgroups is not necessarily a subgroup.

Let $\underline{\underline{Z}} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ be the additive group of integers.

Let $2\underline{\underline{Z}} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

$3\underline{\underline{Z}} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Clearly $2\underline{\underline{Z}} \leq \underline{\underline{Z}}$, $\quad 3\underline{\underline{Z}} \leq \underline{\underline{Z}}$

Now $2 \in 2\underline{\underline{Z}} \cup 3\underline{\underline{Z}}$, $\quad 3 \in 2\underline{\underline{Z}} \cup 3\underline{\underline{Z}}$

But $2+3 = 5 \notin \underline{\underline{Z}} \cup 3\underline{\underline{Z}}$

$\therefore$ addition is not a binary operation on $2\underline{\underline{Z}} \cup 3\underline{\underline{Z}}$.

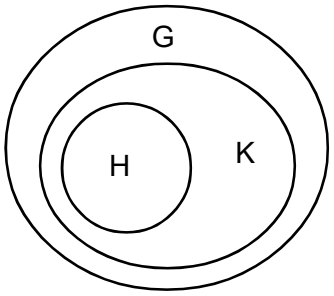
$\therefore$ $2\underline{\underline{Z}} \cup 3\underline{\underline{Z}}$ cannot be a group.

Theorem 6.5 : The union of two subgroups is a subgroup if and only if one of them is contained in the other.

Proof : Let G be a group, and $H \leq G$, $K \leq G$.

Let $H \subseteq K$. Then $H \cup K = K$

$\because K \leq G$, $\therefore H \cup K \leq G$



Conversely, Let $H \leq G$, $K \leq G$ such that $H \cup K \leq G$. Let e be the identity of G.

We are to prove that either $H \subseteq K$ or $K \subseteq H$.

If possible, let it not be true.

$\therefore H \not\subseteq K$ and $K \not\subseteq H$

$\therefore$ there exists $a \in H$ such that $a \notin K$. Also, there exists $b \in K$ such that $b \notin H$.

Now $a \in H \Rightarrow a \in H \cup K$

$b \in K \Rightarrow b \in H \cup K$

$\because H \cup K \leq G$, $\therefore ab \in H \cup K$.

This $\Rightarrow ab \in H$ or $ab \in K$.

If $ab \in H$, then $a \in H$, $ab \in H \Rightarrow a^{-1}(ab) \in H$

$\Rightarrow (a^{-1}a)b \in H$

$\Rightarrow eb \in H$

$\Rightarrow b \in H$

Which is a contradiction.

Similarly, if $ab \in K$, then $ab \in K$, $b \in K$

Then $(ab)b^{-1} \in K$

$\Rightarrow a(bb^{-1} \in K$

$\Rightarrow ae \in K$

$\Rightarrow a \in K$,

Which is a contradiction

So, our assumption is wrong

$\therefore$ either $H \subseteq K$ or $K \subseteq H$.

6.4.2 Coset

Let G be a group and $H \leq G$.

Let $a \in G$

The set $Ha = \{Ha : h \in H\}$ is called a right coset of H in G.

Similarly, the set $aH = \{ah : h \in H\}$ as called a left coset of H in G.

Note: (1) Right (or left) coset cannot be empty.

We have $e \in H$.

$\therefore$ $ea = a \in Ha$ $\therefore$ $Ha \neq \phi$

Similarly, $ae = a \in aH$. $\therefore$ $aH \neq \phi$

(2) $H \leq G$, but Ha or aH is not necessarily a subgroup of G.

(3) If H is a subgroup of the additive group G, and $a \in G$, the right coset of H in G is given by

$H + a = \{h + a : h \in H\}$

Similarly, the left coset of H in G is given by

$a + H = \{a + h : h \in H\}$



LET US KNOW

H is a right coset as well as a left coset of H in G, for

$He = \{he : h \in H\} = \{h : h \in H\} = H$

$eH = \{eh : h \in H\} = \{h : h \in H\} = H$, e is the identity of G.

Example 21: Let us consider the additive group of integers $\underline{\underline{Z}}$.

We know that $2\underline{\underline{Z}} = \{0, \pm 2, \pm 4, \pm 6, \ldots .\} \leq \underline{\underline{Z}}$

We have

$0 + 2\underline{\underline{Z}} = \{0, \pm 2, \pm 4, \pm 6, \ldots\} = 2\underline{\underline{Z}}$

$1 + 2\underline{\underline{Z}} = \{\pm 1, \pm 3, \pm 5, \ldots\}$

$2 + 2\underline{\underline{Z}} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$

$3 + 2\underline{\underline{Z}} = \{\pm 1, \pm 3, \pm 5, \ldots\}$, and so on.

Thus, we see that

$2\underline{\underline{Z}} = 2 + 2\underline{\underline{Z}} = 4 + 2\underline{\underline{Z}} = \ldots .$

$1 + 2\underline{\underline{Z}} = 3 + 2\underline{\underline{Z}} = 5 + 2\underline{\underline{Z}} = \ldots .$

$\therefore$ $2\underline{\underline{Z}}$ has two distinct left cosets,

viz., $2\underline{\underline{Z}}$ and $1 + 2\underline{\underline{Z}}$ such that

$2\underline{\underline{Z}} \cup (1+2\underline{\underline{Z}}) = \underline{\underline{Z}}$

$2\underline{\underline{Z}} \cap (1+2\underline{\underline{Z}}) = \phi$

Similarly, $2\underline{\underline{Z}}$ has two distinct right cosets $2\underline{\underline{Z}}$ and $2\underline{\underline{Z}} + 1$ such that

$2\underline{\underline{Z}} \cup (2\underline{\underline{Z}}+1) = \underline{\underline{Z}}$

$2\underline{\underline{Z}} \cap (2\underline{\underline{Z}}+1) = \phi$

Theorem 6.6: Let G be a group and $H \leq G$.

Then (i) $aH = H \Leftrightarrow a \in H$; $Ha = H \Leftrightarrow a \in H$

(ii) $aH = bH \Leftrightarrow a^{-1}b \in H$; $Ha = Hb \Leftrightarrow ab^{-1} \in H$; $a, b \in G$

Proof : (i) Let $aH = H$

We have $ae \in aH$, e is the identity of G

$\Rightarrow ae \in H \quad [\because aH = H]$

$\Rightarrow a \in H$

Conversely, let $a \in H$

Let $x \in aH$

This $\Rightarrow x = ah$, for some $h \in H$

Now $a \in H, h \in H \quad \therefore ah \in H \Rightarrow x \in H$

Thus, $x \in aH \Rightarrow x \in H$

$\therefore aH \subseteq H \quad (1)$

Again, let $y \in H$

$\because a \in H, \quad \therefore a^{-1} \in H$

$\therefore a^{-1}y \in H$

$\Rightarrow a^{-1}y = h_1$ for some $h_1 \in H$

$\Rightarrow a(a^{-1}y) = ah_1$

$\Rightarrow (a\, a^{-1})y = ah_1$

$\Rightarrow ey = ah_1$

$\Rightarrow y = ah_1 \in aH.$

Thus, $y \in H \Rightarrow y \in aH$

$\therefore H \subseteq aH \quad (2)$

From (1) and (2), $aH = H$

Similarly $Ha = H \Leftrightarrow a \in H$

(ii) $aH = bH$, where $a, b \in G$

$\Leftrightarrow a^{-1}(aH) = a^{-1}(bH)$

$\Leftrightarrow (a^{-1}a)\, H = (a^{-1}b)H$

$\Leftrightarrow eH = (a^{-1}b)H$

$\Leftrightarrow H = (a^{-1}b)H$

$\Leftrightarrow a^{-1}b \in H$, [using (i)]

Similarly, $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Theorem 6.7: Any two left (or right) cosets of a subgroup are either disjoint or identical.

Proof : Let G be a group and $H \leq G$.

Let $a, b \in G$.

Then aH, bH are two left cosets of H in G. Clearly aH, bH are either disjoint or not disjoint.

Let aH, bH be not disjoint, i.e., $aH \cap bH \neq \phi$.

Let $x \in aH \cap bH$

$\Rightarrow x \in ah$ and $x \in bH$

Now $x \in aH \Rightarrow x = ah_1$ for some $h_1 \in H$

$x \in bH \Rightarrow x = bh_2$ for some $h_2 \in H$

$\therefore ah_1 = bh_2$

$\Rightarrow (ah_1)h_1^{-1} = (bh_2)h_1^{-1}$

$\Rightarrow ah_1h_1^{-1} = bh_2h_1^{-1}$

$\Rightarrow ae = bh_2h_1^{-1}$, where e is the identity of G.

$\Rightarrow a = bh_2h_1^{-1}$

Similarly $b = a_1 h_2^{-1}$

Let $p \in aH \Rightarrow p = ah_3$ for some $h_3 \in H$

$= bh_2h_1^{-1}h_3$

$\in bH, \quad \because h_2h_1^{-1}h_3 \in H$

Thus $p \in aH \Rightarrow p \in bH \qquad \therefore aH \subseteq bH \qquad (1)$

Again let $q \in bH \Rightarrow q = bh_4$ for some $h_4 \in H$.

$= ah_1h_2^{-1}h_4$

$\in aH, \quad \because h_1h_2^{-1}h_4 \in H$

Thus, $q \in bH \Rightarrow q \in aH. \qquad \therefore bH \subseteq aH \qquad (2)$

From (1) and (2), aH = bH.

Thus, aH, bH are either disjoint or identical.

Theorem 6.8: (Lagrange's Subgroup Order Theorem)

The order of a subgroup of a finite group divides the order of the group.

Proof : Let G be a finite group, and let 0(G) = n, and $H \leq G$.

Let e be the identity of G.

Case 1. Let H = {e}.

There is nothing to prove. 0(H) = 1, and 1 divides n.

Case 2. Let H = G. Hence 0(H) = 0(G).

There is nothing to prove.

Case 3. Let $H \neq \{e\}$, $H \neq G$.

Let 0(H) = m, m<n

Let $H = \{H_1, h_2, h_3, \ldots, h_m\}$, where h_i's are distinct.

Let $a \in G$, $a \notin H$.

Let us consider the left coset

$aH = \{ah_1, ah_2, ah_3, \ldots, ah_m\}$

We claim that all the elements in aH are distinct, for if $ah_i = ah_j$, $1 \leq i \leq m$, $1 \leq j \leq m$, $i \neq j$; then $h_1 = h_j$ (by left cancellation law), which is a contradiction.

Again, no element of H is equal to any element of aH, for if $h_i = ah_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, $i \neq j$; then $h_i h_j^{-1} = ah_j h_j^{-1}$, i.e., $h_i h_j^{-1} = ae$, i.e., $a = h_i h_j^{-1} \in H$, i.e., $a \in H$, which is a contradiction.

Thus, we have listed m+m = 2m elements of G. If this exhausts all the elements of G, then 2m = n.

$\therefore$ m divides n.

If not, let $b \in G$, $b \notin H$, $b \notin aH$.

Let us consider

$bH = \{bh_1, bh_2, \ldots, bh_m\}$

Clearly, all the elements in bH are distinct. No element of H is equal to any element of bH.

Again, no element of aH is equal to any element of bH, for if $ah_i = bh_j$, $1 \leq i \leq m$, $1 \leq j \leq n$, $i \neq j$, then $ah_i h_j^{-1} = bh_j h_j^{-1}$, i.e. $ah_i h_j^{-1} = be$, i.e., $b = ah_i h_j^{-1} \in aH$, ($\because h_i h_j^{-1} \in H$), i.e., $b \in aH$, which is a contradiction.

Thus, we have listed m+m+m = 3m elements of G. If this

exhausts all the elements of G, then 3m = n.

$\therefore$ m divides n.

If not, we proceed as above. Since G is finite, we must stop somewhere, say, after k times.

$\therefore$ mk = n $\Rightarrow$ m divides n.

Note : Joseph Louis Lagrange (1736 - 1813) was a famous mathematician 'born at Turin of once prosperous parents with French and Italian backgrounds.'

Remark : The converse of Lagrange's theorem is not true.



CHECK YOUR PROGRESS

Q 12: Let $\underline{\underline{Z}}$ be the additive group of integers. Let m be a fixed integer. Show that the set. $m\underline{\underline{Z}}$ = {0, $\pm$m, $\pm$2m, $\pm$3m, ...}, where m is a fixed integer, as a subgroup of $\underline{\underline{Z}}$.

Q 13: Let G be the group consisting of all 2 x 2 nonsingular real matrices under matrix multiplication. Let

$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \text{ are reals, } ad-bc = 1 \right\}$. Show that H is a subgroup of G.

Q 14: Give an example to show that a group cannot be expressed as the union of two of its proper subgroups.

6.4.3 Cyclic Group

Definition : A group G is said to be cyclic if there exists an element a in G such that every element of G can be expressed in the form a^n, $n \in \underline{\underline{Z}}$. a is said to be a generator of G. Symbolically, we write G = <a>, i.e., G is a cyclic group generated by a.

Note : If the group G is additive, every element of G is expressed in the form na.

Example 22: We know that G = {–1, 1} is a group under multiplication.

We have $(-1)^1 = 1$, $(-1)^2 = 1$

$\therefore$ G is a cyclic group generated by –1, i.e., G = <–1>.

Example 23: We know that G = {1, ω, ω^2} is a group under multiplication, ω is a complex cube root of unity.

We have $\omega^1 = \omega$, $\omega^2 = \omega^2$, $\omega^3 = 1$

$\therefore$ G is a cyclic group generated by ω, i.e., G = $<\omega>$

Again $(\omega^2)^1 = \omega^2$, $(\omega^2)^2 = \omega^4 = \omega^3\omega = 1\omega = \omega$,

$(\omega^2)^3 = \omega^6 = (\omega^3)^2 = 1^2 = 1$

$\therefore$ G is also generated by ω^2 i.e., G = $<\omega^2>$



LET US KNOW

Generator is not unique. If a is a generator, then its inverse a^{-1} is also a generator. Thus, there may be more than one generator.

Example 24: We know that G = {–1, 1, –i, i} is a group under multiplication, $i = \sqrt{-1}$.

We have $i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

$\therefore$ G is a cyclic group generated by i, i.e., G = <–i>

Similarly, G = <–i>

Example 25: Let $\underline{\underline{Z}}$ be the additive group of integers.

Let $x \in \underline{\underline{Z}}$ Then x = 1x

$\therefore$ $\underline{\underline{Z}}$ is a cyclic group generated by 1, i.e., $\underline{\underline{Z}}$ = <1>.

Similarly, $\underline{\underline{Z}}$ = <–1>

Theorem 6.9: Every cyclic group is Abelian.

Proof : Let G = <a> be a cyclic group.

Let $x, y \in G$.

Then there exist integers m, n such that $x = a^m$, $y = a^n$

Now $xy = a^m a^n$

$= a^{m+n}$

$= a^{n+m}$

$= a^n a^m$

$= yx$

$\therefore$ G is Abelian

Theorem 6.10: If a is a generator of a cyclic group G, Then its inverse a^{-1} is also a generator of G.

Proof : Let G = <a> be a cyclic group.

Let $x \in G$

Then there exists integer m such that $x = a^m = (a^{-1})^{-m}$

$\therefore$ $G = \langle a^{-1} \rangle$



LET US KNOW

An algorithm is 'a mathematical procedure or method to obtain a result.'

Division Algorithm for $\underline{\underline{Z}}$

If b is a positive integer and a is any integer, then there exist unique integers q and r such that

$a = bq + r, 0 \leq r < b$

Theorem 6.11: A subgroup of a cyclic group is cyclic.

Proof : Let G = <a>be a cyclic group.

Let $H \leq G$.

Let e be the identity of G.

Case 1: If H = {e}, there is nothing to prove.

Case 2: If H = G, then also the result is obvious.

Case 3: Let $H \neq G$, $H \neq \{e\}$.

Each element of H is a power of a.

Let m be the least positive integer such that $a^m \in H$.

Let $x \in H$

Then $x = a^p$ for some p.

Now, by Division Algenthm, there exist unique integers q and r such that

$p = mq + r$, where $0 \leq r < m$

$\therefore$ $r = p - mq$

$\therefore$ $a^r = a^{p-mq} = a^p(a^m)^{-q} = x\,(a^m)^{-q}$

Now $x(a^m)^{-q} \in H$ $\therefore$ $a^r \in H$.

But m is the least positive integer such that $a^m \in H$. $\therefore$ r must be 0.

$\therefore$ q = mq

This $\Rightarrow$ $x = a^p = a^{mq} = (a^m)^q$

$\therefore$ H = $<a^m>$ is a cyclic group.

Theorem 6.12: A group of prime order is cyclic.

Proof : Let G be a finite group, and 0(G) = p, where p is a prime number.

Let e be the identity of G.

Let $a \in G$ such that $a \neq e$.

Let $H = \{a^n : n \text{ is an integer}\}$

Clearly H is a cyclic subgroup of G.

By Lagrange's subgroup order theorem, 0(H) divides 0(G), i.e., 0(H) divides p.

This $\Rightarrow$ 0(H) = 1 or p.

But $0(H) \neq 1$, $\because a \neq e$

$\therefore$ 0(H) = p = 0(G)

$\therefore$ H = G

$\therefore$ G is a cyclic group generated by a.

Note :

1. A group of order one is always Abelian.
2. A group of order two (i.e., if a group has two elements) is always Abelian, since 2 is a prime number.
3. A group of order three is always Abelian, since 3 is a prime number.
4. A group of order five is always Abelian, since 5 is a prime number.



LET US KNOW

A group of prime order is cyclic, and a cyclic group is Abelian. Therefore, a group of prime order is Abelian.

6.4.4 Normal Subgroup

Definition : A subgroup H of a group G is said to be a normal subgroup of G if aH = Ha, for all $a \in G$, i.e., if its left and right cosets

coincide. symbolically we write $H \lhd G$.

Note : A group G has at least two normal subgroups, viz., G and {e}. A group, having no normal subgroups other than G and {e}, is called a simple group.

Example 26: Let $G = \{-1, 1, -i, i\}$

We know that G is a group under multiplication.

Let $H = \{-1, 1\}$, and $H \leq G$.

Now $1H = \{-1, 1\} = H1$

$(-1)H = \{1, -1\} = H(-1)$

$iH = \{-i, i\} = Hi$

$(-i)H = \{i, -i) = H(-i)$

Thus, $aH = Ha$, for all $a \in G$.

$\therefore H \lhd G$

Note : In the above example, H has two distinct left (or right) cosets, viz, H, iH. We note that iH is not a subgroup of G.



LET US KNOW

Let G be a group, and H be a subgroup of G. If $a \in G$, then the coset aH (or Ha) may not be a subgroup of G.

Theorem 6.13: Every subgroup of an Abelian group is normal.

Proof : Let G be an Abelian group.

Let $H \leq G$

Let $a \in G$

Now $aH = \{ah : h \in H\}$

$= \{ha : h \in H\}$, [$\because$ G is a Abelian]

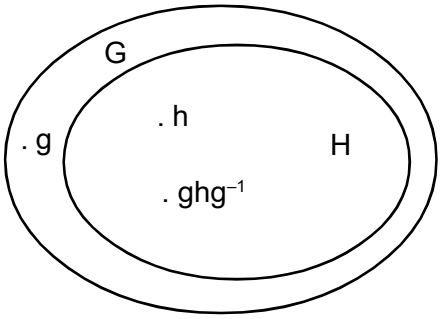
$= Ha$

$\therefore H \lhd G$.

Theorem 6.14 : A subgroup H of a group G is a normal subgroup of G if and only if $ghg^{-1} \in H$, for all $g \in G$, $h \in H$.

Proof : Let G be a group.

Let e be the identity of G.



Let $H \lhd G$.

$\therefore$ $aH = Ha$, for all $a \in G$

Let $g \in G$, $h \in H$

$\therefore$ $gh \in gH$

$\Rightarrow gh \in Hg$, [$\because gH = Hg$, H being normal in G]

$\Rightarrow gh = h_1 g$, for some $h_1 \in H$.

$\Rightarrow ghg^{-1} = h_1 gg^{-1}$

$\Rightarrow ghg^{-1} = h_1 e$

$\Rightarrow ghg^{-1} = h_1 \in H$

i.e., $ghg^{-1} \in H$.

Conversely, let $H \leq G$ such that $gh\, g^{-1} \in H$, for all $g \in G$, $h \in H$.

Let $a \in G$, $\therefore$ $ah \in aH$

Now $aha^{-1} \in H$, by the given condition

$\Rightarrow (aha^{-1})a \in Ha$

$\Rightarrow ah(a^{-1}a) \in Ha$

$\Rightarrow ahe \in Ha$

$\Rightarrow ah \in Ha$

Thus $ah \in aH \Rightarrow ah \in Ha$

$\therefore$ $aH \subseteq Ha$ (1)

Now $ha \in Ha$

We take $a^{-1} = b$

$\therefore$ $bh\, b^{-1} \in H$, by the given condition.

$\Rightarrow a^{-1} h (a^{-1})^{-1} \in H$

$\Rightarrow a^{-1} ha \in H$

$\Rightarrow a(a^{-1}ha) \in aH$

$\Rightarrow (aa^{-1})ha \in aH$

$\Rightarrow eha \in aH$

$\Rightarrow$ $ha \in aH$

Thus, $ha \in Ha \Rightarrow ha \in aH$

$\therefore$ $Ha \subseteq aH$ (2)

From (1) and (2), $aH = Ha$

$\therefore$ $H \lhd G$

Theorem 6.15 : The inter section of any two normal subgroups of a group is again a normal subgroup of the group.

Proof : Let G be a group, and let $H \lhd G$, $K \lhd G$.

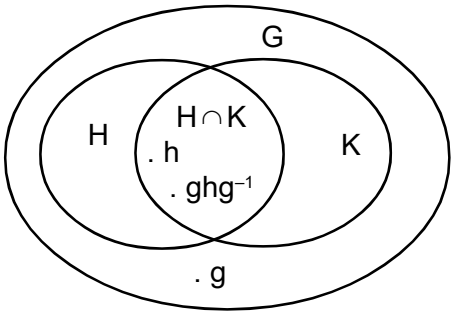
$\therefore$ $H \leq G$, $K \leq G$, and so $H \cap K \leq G$.

Let $g \in G$, $h \in H \cap K$

$h \in H \cap K \Rightarrow h \in H$ and $h \in K$

Now $g \in G$, $h \in H$ and $H \lhd G$

$\therefore$ $gh\,g^{-1} \in H$



Again, $g \in G$, $h \in K$, and $K \lhd G$.

$\therefore$ $ghg^{-1} \in K$

Thus, $ghg^{-1} \in H$ and $ghg^{-1} \in K$

$\therefore$ $ghg^{-1} \in H \cap K$

$\therefore H \cap K \lhd G$.

Note : The union of two normal subgroups is not necessarily a normal subgroup.



LET US KNOW

There is no difference in the argument if the condition in theorem 14 is replaced by $g^{-1} hg \in H$, for all $g \in G$, $h \in H$.

6.4.5 Quotient Group

Let G be a group, and H be a normal subgroup of G.

$\because$ H is normal in G, therefore, there is no distinction between a left coset and its corresponding right coset. So, by a coset we mean left coset (or right coset).

Let G/H denote the collectin of all cosets of H in G.

Let $a, b \in G \quad \therefore aH, bH \in G/H$.

We define a binary operation in G/H by the rule.

$(aH)(bH) = abH; \quad ab \in G$

We show that the binary operation is well defined.

Let $aH = cH$,

$bH = dH, a, b, c, d \in G$

Now $aH = cH \Rightarrow a^{-1}(aH) = a^{-1}(cH)$

$\Rightarrow (a^{-1}a)H = a^{-1}cH$

$\Rightarrow eH = a^{-1}cH$, e is the identity of G

$\Rightarrow H = a^{-1}cH$

$\Rightarrow a^{-1}c \in H$ [Theorem 6.6 (i)]

$\Rightarrow a^{-1}c = h_1$, for some $h_1 \in H$.

Similarly $bH = dH \Rightarrow b^{-1}d \in H$

$\Rightarrow b^{-1}d = h_2$, for some $h_2 \in H$

Now $(ab)^{-1}(cd) = (b^{-1}a^{-1})(cd)$

$= b^{-1}(a^{-1}c)d$

$= b^{-1}h_1 d$

$= b^{-1}dh_1$ [$\because dH = Hd$]

$= h_2h_1 \in H$

$\Rightarrow (ab)^{-1}(cd)H = H$

$\Rightarrow abH = cdH$

Thus $\left.\begin{matrix} aH = cH \\ bH = dH \end{matrix}\right\} \Rightarrow abH = cdH$

$\therefore$ the binary operation defined above is well defined.

Theorem 6.16 : Let G be a group, and H be a normal subgroup of G. The set G/H consisting of all the cosets of H in G is a group under the binary operation defined by

$(aH)(bH) = abH;\ a, b \in G$

Proof : (i) It is given that the binary operation is $(aH)(bH) = abH \in G/H$; $a, b \in G$.

The binary operation as well defined.

(ii) Let $a, b, c \in G$

$\therefore\ aH, bH, cH \in G/H$

Now $((aH)(bH))(cH) = (abH)(cH)$

$= (ab)cH$

$= a(bc)H$, $[\because G$ is a group, $(ab)c = a(bc)]$

$= (aH)(bcH)$

$= (aH)((bH)(cH))$

$\therefore$ the binary operation is associative.

(iii) Let e be the identity of G.

$\therefore\ eH = H \in G/H$

Now $(aH)H = (aH)(eH) = aeH = aH$

$H(aH) = (eH)(aH) = eaH = aH$

$\therefore H$ is the identity

(iv) $a \in G \Rightarrow a^{-1} \in G$

$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

$(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$

$\therefore\ a^{-1}H$ is the inverse of aH.

$\therefore\ G/H$ is a group under the binary operation defined above.

Note : The group G/H is known as the quotient group (or factor group) of G by H.

Theorem 6.17: Every quotient group of an Abelian group is Abelian.

Proof : Let G be a group, and $H \leq G$.

$\because G$ is Abelian, $\therefore$ H is normal in G.

So, we can construct the quotient group G/H.

Let $a,b \in G \ \ \therefore aH, bH \in G/H$

Now $(aH)(bH)=(ab)H=(ba)H$ $[\because G$ is abelian,$ab=ba]$

$\therefore\ G/H$ is Abelian.

Theorem 6.18: Every quotient group of a cyclic group is cyclic.

Proof:Let G = <a> be a cyclic group.

Let $H \leq G$. $\because$ G is cyclic. $\because$ G is abelian and therfore,H is normal in G.So we can construct the quotient group G/H.

Let $x \in G$ $\quad \therefore xH \in G/H$

Now $x = a^m$ for some integer m

Let m>0

Now $xH = a^m H$

$= (a.a.a. \ldots .a)H$

$= (aH)\,(aH)\,(aH) \ldots . (aH)$

$= (aH)^m$

$\therefore$ G/H is a cyclic group generated by aH. We can prove the result easily for m = 0, m<0 .



CHECK YOUR PROGRESS

Q 15: Let G be the multiplicative group consisting of the cube roots of unity. Is the group simple ? Justify your answer.

Q 16: Let $\underline{\underline{Z}}$ be the additive group of integers. Show that the set $3\underline{\underline{Z}} = \{0, \pm 3, \pm 6, \ldots .\}$ is a normal subgroup of $\underline{\underline{Z}}$. Write down the elements of the quotient group $\underline{\underline{Z}}/3\underline{\underline{Z}}$.

6.5 RING

A nonempty set R, equipped with two binary operations, called addition (+) and multiplication (.), is called a ring if the following postulates are satisfied.

(i) R is an additive Abelian group.

(ii) R is a multiplicative semigroup.

(iii) The two distributive laws hold good, viz.,

a.(b+c) = a.b+a.c, (left distributive law)

(a+b).c = a.c +b.c, (right distributive law), for all a, b, c $\in$ R.

Group is an algebraic structure equipped with one binary operation. Ring is an algebraic structure equipped with two binary operations.

Note : 1. In order to be a ring, there must be a nonempty set equipped with two binary operations, viz., + and . , satisfying the postuates mentioned above. Later on we will simply write 'Let R be a ring'. It should be borne in mind that there are two binary operations, viz.+and., on R.

2. It should also be borne in mind that the binary operations + and . are not necessarily our usual addition and multiplication.

3. Since R is an additive Abelian group, the additive identity, denoted by 0, belongs to R. It is called the zero element of R. Here 0 is a symbol. It should not be confused with the real number zero. We note that 0 is unique.

4. If $a, b \in R$, then $-b \in R$ ($\because$ R is an additive group) $\therefore$ $a+(-b) \in R$. $a+(-b)$ is generally denoted by $a-b$.

5. a.b is generally written as ab.

Commutative Ring

A ring R is said to be commutative if $ab = ba$, for all $a, b \in R$.

Ring with unity

A ring R is said to be a ring with unity if there exists an element $e \in R$ such that $ae = a = ea$, for all $a \in R$.

Note : 1. Unity (or multiplicative identity or unit element) is generally denoted by 1. It should not be confused with real number one.

2. A ring may or may not have a unity.

3. If R is a ring with unity, unity may be same as the zero element. For example, {0} is a commutative ring with unity, known as the zero ring. Here 0 is the additive as well as the multiplicative identity.

Theorem 6.19: If R is a ring with unity, then unity is unique.

Proof : Let R be a ring with unity. If possible, let e and f be two multiplicative identities of R.

$\therefore$ $ef = f = fe$, [$\because$ e is identity]

$ef = e = fe$, [$\because$ f is identity]

$\therefore$ $e = f$

Note : In view of the above theorem, we write 'the unity'.

Example 26: Let $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \text{ are integers} \right\}$

I. (i) Let $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$, $\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$, a, b, c, d are integers.

Now $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ matrix addition is a binary operation on R.

(ii) We know that matrix addition is associative.

(iii) We have $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$

and $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore$ $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element.

(iv) For every $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$, there exists $\begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} \in R$ such that

$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$

$\therefore$ $\begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix}$ is the additive inverse of $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

(v) We know that matrix addition is commutative.

$\therefore$ R is an Abelian group under matrix addition.

II. (i) We have $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} \in R$

$\therefore$ matrix multiplication is a binary operation on R.

(ii) We know that matrix multiplication is associative.

$\therefore$ R is a semigroup under matrix multiplication.

III. We know that matrix multiplication is distributive over matrix addition.

Thus, R is a ring under matrix addition and matrix multiplication.

We have $\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \in R$, $\begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} \in R$

$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix}$

$\begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 0 & 0 \end{pmatrix}$

$\therefore \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 3 & 4 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$

$\therefore$ R is a noncommutative ring

Again there does not exist any element $X \in G$ such that

$$X\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} X,$$

for all $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$.

$\therefore$ R is a ring without unity.

Example 27: Let R be the set of all 2 x 2 matrices over integers.

I. Clearly R is an Abelian group under matrix addition.

II. R is a semigroup under matrix multiplication.

III. The two distributive laws are satisfied.

$\therefore$ R is a ring under matrix addition and matrix multiplication.

We know that matrix multiplication is not, in general, commutative.

$\therefore$ R is a noncommutative ring. We have $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$, and

AI = A = IA, for every $A \in R$.

$\therefore$ R is a ring with unity.

Example 28: Let $2\underline{\underline{Z}}$ be the set of even integers.

I. $2\underline{\underline{Z}}$ is an Abelian group under usual addition.

II. $2\underline{\underline{Z}}$ is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ $2\underline{\underline{Z}}$ is a ring under usual addition and multiplication.

Moreover, $2\underline{\underline{Z}}$ is a commutative ring. $2\underline{\underline{Z}}$ is a ring without unity, for $1 \notin 2\underline{\underline{Z}}$.

Example 29: Let $\underline{\underline{Z}}$ be the set of integers.

I. $\underline{\underline{Z}}$ is an Abelian group under addition.

II. $\underline{\underline{Z}}$ is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ $\underline{\underline{Z}}$ is a ring under usual addition and multiplication.

Moreover, $\underline{\underline{Z}}$ is a commutative ring.

It is also a ring with unity, $1 \in \underline{\underline{Z}}$

- The set $\underline{\underline{Q}}$ of rational numbers is a commutative ring with unity.
- The set $\underline{\underline{R}}$ of real numbers is a commutative ring with unity.
- The set $\underline{\underline{C}}$ of complex numbers is a commutative ring with unity.

Example 30: Let C[a, b] denote the set of all real-valued continuous functions defined on [a, b]; a, b are real numbers.

Let $f, g \in C[a, b]$.

We define

$(f+g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\, g(x), \quad x \in [a, b]$

I. (i) We have $(f+g)(x) = f(x) + g(x)$

Also, the sum of two continuous functions is continuous.

$\therefore$ $f + g$ is continuous, and, so, $f+g \in C[a, b]$

(ii) Let $f, g, h \in C[a, b]$, $x \in [a, b]$

$((f+g) + h)(x) = (f+g)(x) + h(x)$

$= (f(x) + g(x)) + h(x)$

$= f(x) + (g(x) + h(x))$

{f(x), g(x), h(x) are real numbers}

$= f(x) + (g+h)(x)$

$= (f + (g+h))(x)$, for all $x \in [a, b]$

$\therefore$ $(f + g) + h = f+(g+h)$

i.e., addition of functions is associative.

(iii) We have

$0 : [a, b] \to \underline{\underline{R}}$, $0(x) = 0$, $\forall\, x \in [a, b]$

Clearly $0 \in C[a, b]$, and

$0+f = f = f+0$

(iv) For every $f \in C[a, b]$, we define

$-f : [a, b] \to \underline{\underline{R}}$, $(-f)(x) = -f(x)$

Clearly $-f \in C[a, b]$, and

{$f+(-f)(x) = f(x) + (-f)(x)$

$= f(x) - f(x)$

$= 0$

$= 0(x)$

$\therefore$ $f + (-f) = 0$

Similarly, $(-f) + f = 0$

(v) $(f+g)(x) = f(x) + g(x)$

$= g(x) + f(x)$, (f(x), g(x) are real numbers)

$= (g+f)(x)$, $() \; x \in [a, b]$

$\therefore \; f+g = g+f.$

$\therefore$ C[a, b] is an Abelian group under addition of functions.

II. (i) $(fg)(x) = f(x)\, g(x) \in R$

Also, the product of two continuous functions is continuous.

$\therefore$ fg is continuous, and, so, $fg \in C[a, b]$.

$\therefore$ multiplication of functions is a binary operation on C [a, b].

(ii) $((fg)\, h)(x) = (fg)(x)\, h(x)$

$= (f(x)\, g(x)\}\, h(x)$

$= f(x)\, \{g(x)\, h(x))$

($\because$ f(x), g(x), h(x) are real numbers)

$= f(x)\, (gh)(x)$

$= (f(gh))(x)$, for all $x \in [a, b]$

$\therefore \; (fg)\, h = f(gh)$

i.e., multiplication of functions is a associative on C[a, b].

$\therefore$ C[a, b] is a semigroup under multiplication of functions.

III. $((f+g)\, h)(x) = (f+g)(x)\, h(x)$

$= (f(x) + g(x))\, h(x)$

$= f(x)\, h(x) + g(x)\, h(x)$

$= (fh)(x) + (gh)(x)$

$= (fh + gh)(x), \; \forall \; x \in [a, b]$

$\therefore \; (f+g)h = fh + gh$

Similarly $f(g+h) = fg + fh$.

$\therefore$ C [a, b] is a ring under addition and multiplication of functions.

Furthermore, $(fg)(x) = f(x)\, g(x)$

$= g(x)\, f(x)$

$= (gf)(x), \; \forall \; x \in [a, b]$

$\therefore \; fg = gf$

$\therefore$ C[a, b] is a commutative ring.

We have $i : [a, b] \to \underline{\underline{R}}$, $i(x) = 1, \; \forall \; x \in [a, b]$

Clearly $i \in C[a, b]$

Now $(fi)(x) = f(x)\, i(x) = f(x)\, 1 = f(x)$

$\therefore \; fi = f$

Similarly if = f.

$\therefore$ C[a, b] is a ring with unity.

Theorem 6.20: Let R be a ring. Then

(i) $a0 = 0a = 0$, for all $a \in R$

(ii) $a(-b) = (-a)b = -(ab)$, for all $a, b \in R$

(iii) $(-a)(-b) = ab$, for all $a, b \in R$

(iv) $a(b-c) = ab - ac$, for all $a, b, c \in R$.

Proof : (i) We have

$a0 = a(0+0)$

$= a0 + a0$, by left distributive law.

$\therefore a0+0 = a0 + a0$

$\Rightarrow 0 = a0$, by left cancellation law in the additive group R.

i.e. $a0 = 0$

(ii) We have $a0 = 0$

This $\Rightarrow a\{(-b) + b\} = 0$, $[\because (-b)+b = 0]$

$\Rightarrow a(-b) + ab = 0$, by left distributive law

$\Rightarrow a(-b)$ is the additive inverse of ab.

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

Similarly $(-a)b = -(ab)$

(iii) We have $(-a)(-b)$

$= m(-b)$, taking $m = -a$

$= -(mb)$, using (ii)

$= -((-a)b)$

$= -(-(ab))$, using (ii)

$= ab$

(iv) $a(b-c) = a(b+(-c))$

$= ab + a(-c)$, by left distributive law

$= ab - ac$, by (ii)



CHECK YOUR PROGRESS

Q 17: Give an example of a commutative ring with unity having one element.

Q 18: Give an example of a noncommutative ring without unity.

Q 19: Give an example of a noncommutative ring with unity.

Q 20: Give an example of a commutative ring without unity.

Q 21: Give an example of an infinite commutative ring with unity.

Q 22: Let $\underline{\underline{R}}^2 = \{(a, b) : a, b \text{ are reals}\}$

We define (a, b) + (c, d) = (a+c, b+d)

(a, b) (c, d) = (ac, bd),

a, b, c, d are real numbers.

Show that $\underline{\underline{R}}^2$ is commutative ring with unity.

6.6 INTEGRAL DOMAIN AND FIELD

Let us consider the ring R of all 2 x 2 matrices over integers.

Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \in R$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix} \in R$.

Here A is not a null matrix, B is not a null matrix, i.e., $A \neq 0$, $B \neq 0$.

But $AB = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$

$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$

i.e., AB is a null matrix.

Thus, we see that $A \neq 0$, $B \neq 0$; but AB = 0

Again, let us consider the ring $\underline{\underline{Z}}$ integers. If $a, b \in \underline{\underline{Z}}$ and $a \neq 0$, $b \neq 0$; then $ab \neq 0$.

Definition: An element $a(\neq 0)$ in a ring R is called a zero divisor if there exists an element $b(\neq 0)$ in R such that ab = 0 or ba = 0.

We see that the ring R of all 2 x 2 matrices over integers has zero divisor, whereas the ring $\underline{\underline{Z}}$ of integers has no zero divisors, for if $a \in \underline{\underline{Z}}$, $b \in \underline{\underline{Z}}$, $a \neq 0$, $b \neq 0$, then $ab \neq 0$, $ba \neq 0$.

Cancellation laws

Let R be a ring. The additive cancellation laws hold good in R, since R is an additive Abelian group.

So, by cancellation laws in a ring, we mean multiplicative cancellation laws (cancellation of nonzero elements).

The cancellation laws hold good in R if $ab = ac \Rightarrow b = c$, $ba = ca \Rightarrow b = c$, where $a, b\, c \in R$, $a \neq 0$.

Theorem 6.21: The cancellation laws hold good in a ring R if and only if R has no zero divisors.

Proof : Let the cancellation laws hold good Let $a, b \in R$ such that $ab = 0$.

If $a \neq 0$, then $ab = 0$

$\Rightarrow ab = a0$

$\Rightarrow b = 0$, by cancellation law

Similarly, if $b \neq 0$, then

$ab = 0$

$\Rightarrow ab = 0b$

$\Rightarrow a = 0$, by cancellation law.

So, there can be no zero divisors. Conversely, let there be no zero divisors in R.

Let $a, b, c \in R$, and $ab = ac$, $a \neq 0$

Now $ab = ac$

$\Rightarrow ab + (-(ac)) = ac + (-(ac))$

$\Rightarrow ab - ac = 0$

$\Rightarrow a(b-c) = 0$

$\because a \neq 0$, and R is without zero divisors,

$\therefore b-c = 0 \Rightarrow b = c$.

Thus, if $a \neq 0$, $ab = ac \Rightarrow b = c$

Similarly, if $a \neq 0$, $ba = ca \Rightarrow b = c$.

Thus, the cancellation laws hold good in R.

Definition : A commutative ring with unity $e \neq 0$, and containing no zero divisors is called an Integral Domain.

> The simplest example of an integral domain is the ring $\underline{\underline{Z}}$ of integers. It is a commutative ring, has unity, and is without zero divisors.

Note : An integral domain may be considered as a generalization of $\underline{\underline{Z}}$.

Definitions: Let R be a ring with unity $e \neq 0$. If every nonzero element of R has multiplicative inverse in R, then R is called a Division Ring (or a Skew Field).

A commutative division ring is called a Field.

The simplest example of a field is the ring $\underline{\underline{R}}$ of real numbers. It is commutative, has unity, and every nonzero element has multiplicative inverse in $\underline{\underline{R}}$.

Similarly, the ring $\underline{\underline{C}}$ of complex numbers is also a field.

Note : The ring $\underline{\underline{Z}}$ of integers is not a field. (Why?)

THeorem 6.22: Every field is an integral domain.

Proof : Let F be a field.

Let a, b $\in$ F such that $a \neq 0$, and ab = 0

$\because$ $a \neq 0$, $a^{-1} \in F$ ($\because$ F is a field)

Now ab = 0

$\Rightarrow$ $a^{-1}(ab) = a^{-1}0$

$\Rightarrow$ $(a^{-1}a)b = 0$

$\Rightarrow$ eb = 0, e is the identity of F

$\Rightarrow$ b = 0

Similarly, if $b \neq 0$, and ab = 0, then a = 0

$\therefore$ F has no zero divisors.

Thus, F is a commutative ring with unity containing no zero divisors.

$\therefore$ F is an integral domain.

Note : The converse of the above theorem is not true, i.e., every integral domain is not a field.

Let us consider the ring $\underline{\underline{Z}}$ of integers. We know that $\underline{\underline{Z}}$ is an integral domain. But only two elements, viz., –1 and 1 have multiplicative inverses in $\underline{\underline{Z}}$.

$\therefore$ $\underline{\underline{Z}}$ is not a field.

However we have the following.

Theorem 6.23: A nonzero finite integral domain is a field.

Proof : Let $R = \{a_1, a_2, a_3, \ldots, a_n\}$ be a finite nonzero integral domain, where all the a_i's are distinct.

Let a_1 be the zero element of R.

Let us consider the nonzero elements $a_2, a_3, \ldots, a_n$.

Let a_p be not the unity of R ($p \neq 1$).

Let us consider the products

$a_p a_2, a_p a_3, \ldots, a_p a_n$.

All these elements belong to R. Also all the elements are distinct, for if $a_p a_i = a_p a_j$, $2 \le i \le a$, $2 \le j \le n$, $i \ne j$ then $a_p a_i - a_p a_j = 0$

$\Rightarrow a_p (a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$, [$\because a_p \ne 0$, and R is without zero divisors].

$\Rightarrow a_i = a_j$, which is a contradiction.

Now, one of $a_p a_2, a_p a_3, \ldots, a_p a_n$ must be unity. Let $a_p a_q = e$, where e is the unity of R.

Then $a_p a_q = e = a_q a_p$

$\therefore$ a_p has multiplicative inverse in R.

If a_p is the unity of R, then a_p has multiplicative inverse in R.

Thus, every nonzero element of R has multiplicative inverse in R.

$\therefore$ R is a field.



CHECK YOUR PROGRESS

Q 23: Does the ring $\underline{\underline{Q}}$ of rational numbers contain zero divisors? Justify.

Q 24: Let R be the ring of all 2 x 2 matrices over integers. Do the cancellation laws hold good in R ? Justify.

Q 25: Is the ring $2\underline{\underline{Z}}$ of even integers an integral domain ? Justify.



6.7 LET US SUM UP

- A binary operation $*$ on a nonempty set S is a function from S x S to S.
- If S is a finite set having m elements, the number of binary operations on S is m^{m^2}.
- A binary operation $*$ on a nonempty set S is commutative if $a * b = b * a$, for all $a, b \in S$.
- A binary operation $*$ on a nonempty set S is associative if $(a * b) * c = a * (b * c)$, for all $a, b, c \in S$.
- An element e on a nonempty set S equipped with a binary operation $*$ is called an identity element if $a * e = a = e * a$, for all $a \in S$.

- An element b in a nonempty set S equipped with a binary operation $*$ is called an inverse element of $a \in S$ if $a * b = e = b * a$.
- A group is an algebraic structure, i.e., a nonempty set equipped with a binary operation satisfying three postulates, viz., associativity, existence of identity, existence of inverse.
- A nonempty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G.
- A nonempty set R, equipped with two binary operations, called addition (+) and multiplication (.), is called a ring if the following postulates are satisfied.
  (i) R is an additive Abelian group.
  (ii) R is a multiplicative semigroup.
  (iii) The two distributive laws hold good.
- A ring R is said to be commutative if ab = ba, for all $a, b \in R$.
- A ring R is said to be a ring with unity if there exists an element $e \in R$ such that ae = a = ea, for all $a \in R$.
- An element $a \neq 0$ in a ring R is called a zero divisor if there exists an elements $b(\neq 0)$ in R such that ab = 0 or ba = 0.
- A commutative ring with unity $e \neq 0$ and containing no zero divisors is called an integral domain.
- Let R be a ring with unity $e \neq 0$. If every nonzero element of R has multiplicative inverse in R. Then R is called a division ring (or a skew field).
  A commutative division ring is a field.



6.8 FURTHER READINGS

1) *A Course in Abstract Algebra* by Vijay K Khanna and S K Bhambri (Vikas Publishing House Private Limited)
2) *Higher Algebra* (Abstract and Linear) by Sadhan Kumar Mapa.

6.9 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Number of elements of S = 4, i.e. n(S) = 4

$\therefore$ number of binary operations on S = $4^{4^2} = 4^{16}$

Ans to Q No 2: No, since $0 \in R$

Ans to Q No 3: From the table, we see that multiplication is a binary operation on S:

x	–1	1	–i	i
–1	1	–1	i	–i
1	–1	1	–i	i
–i	i	–i	–1	1
i	–i	i	1	–1

Table 6.6

Ans to Q No 4: Let $a, b \in \underline{\underline{Q}}$, where $\underline{\underline{Q}}$ is the set of rational numbers.

$\because$ $a, b \in \underline{\underline{Q}}$, $\therefore$ $ab \in \underline{\underline{Q}}$, and

$\therefore$ $a+ab \in \underline{\underline{Q}}$

i.e. $a * b \in \underline{\underline{Q}}$

$\therefore$ $*$ is a binary operation on $\underline{\underline{Q}}$.

We have $3 * 5 = 3+3x5 = 3+15 = 18$

$5 * 3 = 5+5x3 = 5+15 = 20$

$\therefore$ $3 * 5 \neq 5 * 3$

$\therefore$ $*$ is not commutative.

$(a * b) * c = (a+ab) * c$; $a, b, c \in \underline{\underline{Q}}$

$= (a+ab) + (a+ab)c$

$= a+ab+ac+abc$

$a * (b * c) = a * (b+bc)$

$= a+a(b+bc)$

$= a+ab+abc$

$\therefore$ $*$ is not associative.

Ans to Q No 5: Let $G = \{1, \omega, \omega^2\}$ be the set consisting of the cube roots of

unity. Here ω is a complex cube root of unity. We know that $\omega^3 = 1$,

$\omega^4 = \omega^3\omega = 1\omega = \omega$.

x	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Table 6.6

(i) From the table we see that multiplication is a binary operation on G.

(ii) We know that multiplication of complex numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element of G possesses inverse in G.

1 is the inverse of 1

ω is the inverse of ω^2

ω^2 is the inverse of ω

$\therefore$ G is a group under multiplication.

(v) Moreover multiplication of complex numbers is commutative.

$\therefore$ G is an Abelian group.

Ans to Q No 6: Let G = {–1, 1, –i, i} be the set consisting of the fourth roots of unity, $i = \sqrt{-1}$

(i) From table 6.6, we see that multiplication is a binary operation on G.

(ii) We know that multiplication of complex numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element of G possesses inverse in G.

1 is the inverse of 1.

–1 is the inverse of –1.

–i is the inverse of i.

i is the inverse of –i.

$\therefore$ G is a group under multiplication.

(v) Moreover multiplication of complex numbers is commutative.

$\therefore$ G is an Abelian group.

Ans to Q No 7: Let $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \text{ are reals}, ad - bc \neq 0 \right\}$

(i) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in G$

Where a, b, c, d, e, f, g, h are real numbers.

Now $AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix}$

$$= \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

Now $|A| = ad - bc \neq 0$

$|B| = eh - gf \neq 0$

$|AB| = |A|\,|B| \neq 0$

$\therefore AB \in G$

(ii) We know that matrix multiplication is associative.

(iii) We have $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$|I| = 1 \neq 0$

$\therefore I \in G$, and I is the identity.

(iv) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \neq 0$$

$\therefore A^{-1}$ exists.

Now $\text{adj}A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$$\therefore A^{-1} = \frac{1}{|A|}\,\text{adj}A = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$= \frac{1}{ad - bc}\,(ad - bc)$$

$$= \frac{1}{ad - bc} \neq 0$$

$\therefore A^{-1} \in G$

$\therefore$ G is a group under matrix multiplication.

Ans to Q No 8: Let $G = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \text{ is real}, x \neq 0 \right\}$

(i) Let $A = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in G, \quad B = \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} \in G$ where x, y are real numbers,

$x \neq 0, y \neq 0$

$$AB = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix} \in R \text{, xy is real, } xy \neq 0 \in G$$

(ii) We know that matrix multiplication is associative.

(iii) We have $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity.

(iv) For every $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in G$, there exists $\begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{pmatrix}$ such that

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 0 \end{pmatrix}$ is the inverse of $\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$, $x \neq 0$

$\therefore$ G is a group under matrix multiplication.

(v) Furthermore

$$AB = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} yx & 0 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} y & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = BA$$

$\therefore$ AB = BA

$\therefore$ G is an Abelian group under matrix multiplication.

Ans to Q No 9: Do yourself.

Here the identity element is $\begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}$

The inverse of $\begin{pmatrix} x & x & x \\ x & x & x \\ x & x & x \end{pmatrix}$ is $\begin{pmatrix} \frac{1}{9x} & \frac{1}{9x} & \frac{1}{9x} \\ \frac{1}{9x} & \frac{1}{9x} & \frac{1}{9x} \\ \frac{1}{9x} & \frac{1}{9x} & \frac{1}{9x} \end{pmatrix}$

Ans to Q No 10: Let G be a group, and e be the identity of G.

It is given that $a^2 = e$, for all $a \in G$

Now $a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$

Let $a, b \in G \quad \therefore a = a^{-1}, b = b^{-1}$

Now $ab = a^{-1} b^{-1} = (ba)^{-1}$, $[ba \in G, \therefore (ba)^{-1} = ba]$

$= ba$

$\therefore$ G is Abelian.

Ans to Q No 11: Let G be a group having 4 elements.

Let G = {e, a, b, c}, where all the elements are distinct, and e is the identity of G.

Clearly, e is its own inverse.

If each of the remaining three elements is its own inverse, then G is Abelian. (Ref. Example 18]

If not, let $b^{-1} = c$, $c^{-1} = b$. Then $a^{-1} = a$.

Now let us complete the operation table.

$\because a^{-1} = a, \therefore aa = e$

Again, each element of G must appear exactly once in every row or column of the operation table.

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table 6.8

$\therefore$ ab = b or ab = c

Now $ab = b \Rightarrow ab = eb \Rightarrow a = e$ (by right cancellation law), which is a contradiction.

$\therefore$ ab = c, and $\therefore$ ac = b.

$\because b = c^{-1}, \therefore bc = e$

$\therefore$ ba = a or ba = c

ba = a $\Rightarrow$ b = e, which is a contradiction.

$\therefore$ ba = c and bb = a

Again, $\because$ $c = b^{-1}$, $\therefore$ cb = e

$\therefore$ ca = a or ca = b

ca = a $\Rightarrow$ c = e, which is a contradiction.

$\therefore$ ca = b and $\therefore$ cc = a

We see that the operation table is symmetrical about the principal diagonal.

$\therefore$ G is Abelian.

Ans to Q No 12: $\underline{\underline{Z}}$, the additive group of integers.

$\underline{\underline{Z}}$ = {0, m, $\pm$2m, $\pm$3m, . . . },

Where m is a fixed integer.

Now $m\underline{\underline{Z}} \neq \phi$

Let a, b $\in m\underline{\underline{Z}}$

Then there exist some integers p, q such that a = pm, b = qm

Now a – b = pm – qm

= (p – q)m $\in m\underline{\underline{Z}}$

$\therefore$ $m\underline{\underline{Z}} \leq \underline{\underline{Z}}$

Ans to Q No 13: G, the group consisting of all 2 x 2 nonsingular real matrices under matrix multiplication.

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \text{ a, b, c, d are reals } ad - bc = 1 \right\}$$

Clearly $H \neq \phi$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, a, b, c, d are reals, ad – bc = 1}

Now $|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = 1$

Let B $\in$ H $\therefore$ |B| = 1

Now B is nonsingular, $\therefore$ B^{-1} exists.

Now $BB^{-1} = I \Rightarrow |BB^{-1}| = |I| \Rightarrow |B|\,|B^{-1}| = 1$

$$\Rightarrow |B^{-1}| = \frac{1}{|B|} = 1$$

$\therefore$ $B^{-1} \in H$

Now $|AB^{-1}| = |A|\,|B^{-1}| = 1$

$\therefore\ AB^{-1} \in H$

$\therefore\ H \leq G$.

Ans to Q No 14: $\underline{\underline{Z}} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$, the additive group of integers.

$2\underline{\underline{Z}} = (0, \pm 2, \pm 4, \pm 6, \ldots\}$

and $3\underline{\underline{Z}} = (0, \pm 3, \pm 6, \pm 9, \ldots\}$

are two proper subgroups of $\underline{\underline{Z}}$.

Clearly $\underline{\underline{Z}} \neq 2\underline{\underline{Z}} \cup 3\underline{\underline{Z}}$

Ans to Q No 15: $G = \{1, \omega, \omega^2\}$ be the multiplicative group consisting of the cube roots of unity.

[Check your progress 1 (5)]

G has no other normal subgroups other that G and {1}.

$\therefore$ G is a simple group.

Ans to Q No 16: $\underline{\underline{Z}} = (0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$ is the additive group of integers.

$3\underline{\underline{Z}} = (0, \pm 3, \pm 6, \ldots\}$ is a subgroup of

is an Abelian group.

We know that every subgroup of an Abelian group is normal.

3 is a normal subgroup of

$\therefore$ We can construct the quotient group $\underline{\underline{Z}}/3\underline{\underline{Z}}$. The elements of the quotient group , 1=3 , 2+3

Ans to Q No 17: {0} is a commutative ring with unity.

Ans to Q No 18: Example 26

Ans to Q No 19: Example 27

Ans to Q No 20: Example 28

Ans to Q No 21: Example 29

Ans to Q No 22: Try yourself

(0, 0) is the zero element.

(1, 1) is the unity.

Ans to Q No 23: Let a, b

Let a 0, b

Then ab 0, ba

does not contain zero divisors.

Ans to Q No 24: We have

A 0, B

Thus, R contains zero divisors.

We know that the cancellation laws hold good in a ring if and only if the ring has no zero divisors.

cancellation laws do not hold good in R.

Ans to Q No 25: We know that a commutative ring with unity e containing no zero divisors is an integral domain.

2 does not contain unity. 2



6.10 MODEL QUESTIONS

Q 1: Let S be a finite set having 3 elements. How many binary operations can be defined on S ?

Q 2: Let G be the set of odd integers. A binary operation $*$ on G is defined as follows.

$a * b = a+b-1$; $a, b \in G$.

Show that G is an Abelian groip under $*$.

Q 3: Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1} b^{-1}$, for all a, b $\in$ G.

Q 4: Let G be an Abelian group. Prove that the set $H = \{x \in G : x = x^{-1}\}$ is Abelian.

Q 5: Prove that every group of order

Q 6: Let be the set of integers. We define and ( ) on

a

a( )b = a+b–ab, for all a, b

Examine if is a commutative ring with unity under , (

Q 7: Give an example of an integral domain which is not a field.

*** ***** ***

UNIT 7 : GRAPH THEORY

UNIT STRUCTURE

7.1 Learning Objectives

7.2 Introduction

7.3 Basic Concepts

- 7.3.1 Definition of a Graph
- 7.3.2 Loop and Parallel Edges; Simple Graph
- 7.3.3 Incidence and Degree

7.4 Different Types of Graphs

- 7.4.1 Finite Graph, Infinite Graph, Null Graph
- 7.4.2 Complete Graph
- 7.4.3 Regular Graph
- 7.4.4 Bipartite Graph
- 7.4.5 Complete Bipartite Graph
- 7.4.6 Directed Graph

7.5 Walk, Path and Cycles

7.6 Subgraph of a Graph

7.7 Connected and Disconnected Graphs

7.8 Graph isomorphis

7.9 Eulerian Graph and Hamiltonian Graph

- 7.9.1 Eulerian Graph
- 7.9.2 Hamiltonian Graph

7.10 Let Us Sum Up

7.11 Further Readings

7.12 Answers To Check Your Progress

7.13 Model Questions

7.1 LEARNING OBJECTIVES

After going through this unit, you will be able to learn-

- basic concepts of a graph
- different types of graph

- isomorphism of graphs
- subgraphs
- Euler graphs, bipartite graphs, Hamiltouian paths and circuits.

7.2 INTRODUCTION

The term ‘graph’ is familiar to us. Generally, by a graph, we mean ‘the set of all points in the plane whose coordinates (x, y), in some coordinate system, satisfy an equation in x and y.’ For example, we know how to draw the graph of the equation 2x + 3y = 6. It is a straight line. But in graph theory, the term ‘graph’ bears a different meaning. In graph theory, graphs, according to Oystein Ore, ‘are simple geometrical figures consisting of points and lines connecting some of these points.’

Let us suppose that five teams have joined a football tournament. Let the teams be A, B, C, D, E. Suppose A has played three matches each with C, D, E; B two matches with C, D; C three matches with A, B, D; D three matches with A, B, C; E one match with A.

The above situation can be represented by a diagram. Each team can be represented by a point or a small circle. Two teams (points) can be connected by a line segment or an arc. Such a representation is called a graph. Figure 7.1 (a) represents the graph of the above tournament.

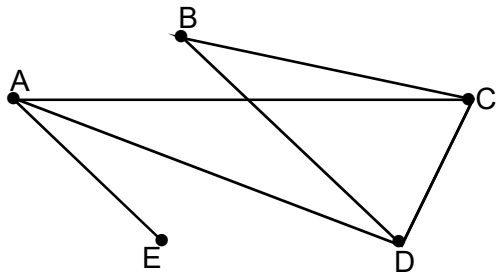


Fig 7.1 (a)

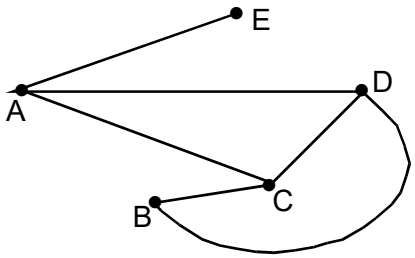


Fig 7.1 (b)

It can be represented in different way also {Fig 7.1(b)}.

The celebrated swiss mathematician Leonhard Euler (1707-1782) is regarded as the father of graph theory. He settled a famous unsolved problem of that time known as the konigsberg Bridge problem. Two islands in the river pregel in the historic prussian city of konigsberg (now kaliningrad

in Russia) were connected to each other and the river banks by seven bridges as shown in Fig 7.2.

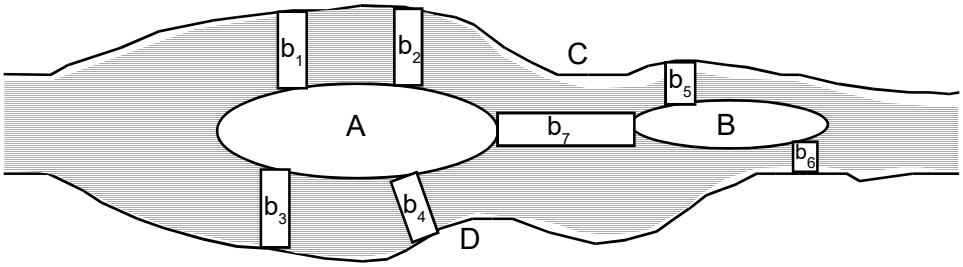


Fig 7.2

Let the islands be denoted by A, B; and the river banks be denoted by C, D; and the seven bridges be denoted by b_1, b_2, b_3, b_4, b_5, b_6, b_7. The problem was to start at any of the four land areas A, B, C, D; walk across each bridge exactly once, and return to the starting point. Euler converted the problem as a problem of graph theory and proved it to be impossible.

Nowadays graph theory is immensely used in different branches of industry and technology.

In this unit we introduce the concept of graph, and study different types of graphs.

7.3 BASIC CONCEPTS

7.3.1 Definition of a Graph

A graph G = (V, E) consists of two things, viz.,

(i) a nonempty set V, called the set of vertices or nodes or points;

(ii) a set E (may be empty), called the set of edges such that there is a mapping from the set E to a set of pairs of elements of V.

If an edge $e \in E$ is associated with a pair (u, v), where $u, v \in V$, then u and v are said to be adjacent. u and v are called the endpoints of e, and e is said to join or connect u and v.

It is customary to represent a graph with the help of a diagram and refer to it as the graph. A vertex is represented by a point or a little circle. An edge is represented by a line segment or an arc joining the two vertices. Vertices can be placed in arbitrary positions

in the plane.

A graph having p vertices and q edges is called a (p, q) graph, The graph having one vertex and no edge, i.e., (1, 0) graph is trivial.

Example 1 : Let $V = \{v_1, v_2, v_3, v_4, v_5\}$

$E = \{e_1, e_2, e_3, e_4, e_5\}$

such that e_1 is associated with (v_1, v_2), e_2 is associated with (v_2, v_3), e_3 is associated with (v_3, v_4), e_4 is associated with (v_4, v_5), e_5 is associated with (v_5, v_1).

Then, G = (V, E) is a graph [Fig7.3]

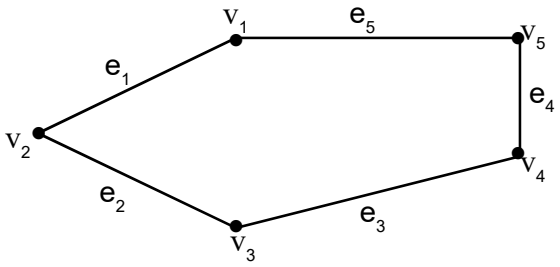


Fig 7.3

Example 2 : Let $V = \{v_1, v_2, v_3\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$

such that e_1 is associated with (v_1, v_1), e_2 is associated with (v_1, v_2), e_3 is associated with (v_1, v_2), e_4 is associated with (v_2, v_3), e_5 is associated with (v_1, v_3), e_6 is associated with (v_1, v_3).

Then, G = (V, E) is a graph [Fig7.4]

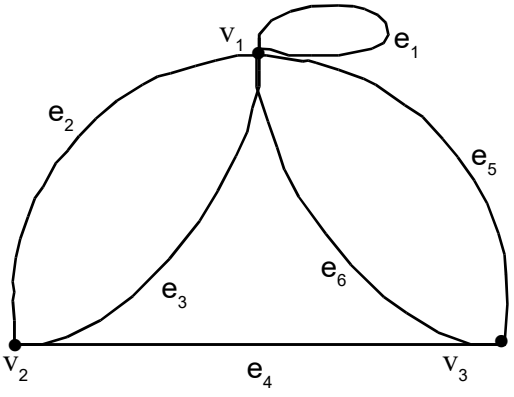


Fig 7.4



CHECK YOUR PROGRESS

Q 1: Let $V = \{v_1, v_2, v_3, v_4, v_5\}$

$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$

such that e_1 is associated with (v_1, v_2), e_2 with (v_1, v_3), e_3 with (v_3, v_2), e_4 with (v_3, v_5), e_5 with (v_2, v_5), e_6 with (v_2, v_4), e_7 with (v_4, v_5).

Give the pictorial representation of the above graph.

Q 2: Describe formally the graphs shown below :

(i)

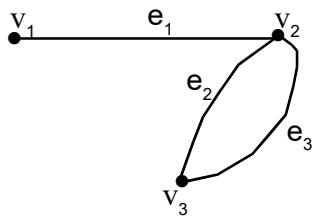


Fig 7.5

(ii)

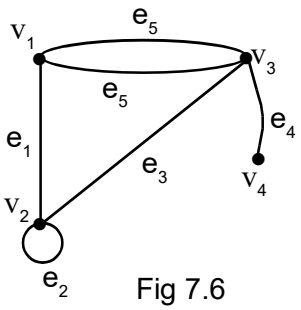


Fig 7.6

7.3.2 Loop and Parallel Edges; Simple Graph

Let us consider Fig 7.4. The edge e_1 is from the vertex v_1 to itself. Such an edge is called a loop. Thus, an edge of a graph that joins a vertex to itself is called a loop. Here the endpoints are one and the same.

Again, let us consider Fig 7.4. Here the edge e_2 connects the vertices v_1 and v_2. Also the edge e_3 connects the vertices v_1 and v_2. Thus, two distinct edges are associated with the same pair of vertices. Such edges are called parallel edges. If in a graph, certain pairs of vertices are joined by more than one edge, then such edges are called parallel edges. In Fig 7.4, e_2 and e_3 are parallel edges. Also, the edges e_5 and e_6 are parallel edges.

Let us consider the graph given in Example 1 (Fig 7.3). This graph does not contain any loop. Also, it does not contain parallel edges. Such a graph is called a simple graph.

A graph that

(i) does not contain any loop, and (ii) does not contain any parallel edges is called a simple graph.

A graph that contains some parallel edges is called a multigraph.

A graph that contains loops and parallel edges is called a pseudograph. The graph in FIg 7.4 is a pseudograph.



CHECK YOUR PROGRESS

Q 3: Give an example of a simple graph.

Q 4: Give an example of a graph containing a loop, but not containing parallel edges.

Q 5: Give an example of a graph containing parallel edges, but not containing a loop.

Q 6: Give an example of a graph containing a loop and parallel edges.

2.3.3 Incidence and Degree

Let G be a graph, and v be a vertex of G. If v is an endpoint of some edge e, e is said to be incident with the verex v, and v is incident with the edge e.

The degree of the vertex v, is the number of edges incident with v. Generally it is denoted by d(v). If G is a graph with n vertices, the maximum degree of a vertex is (n–1)

Note : A loop at a vertex contributes 2 to the degree of that vertex.

Example 3: Let G = (V, E) be a graph given by

$V = \{v_1, v_2, v_3\}$

$E = \{e_1, e_2, e_3, e_4\}$

such that e_1 is associated with (v_1, v_2), e_2 with (v_2, v_3), e_3 with (v_3, v_3), e_4 with $(v_1\ v_3)$.

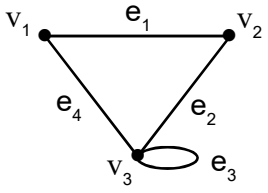


Fig 7.7

e_1 contributes 1 to the degree of v_1. Also e_4 contributes 1 to the degree of v_1. Thus $d(v_1) = 1+1 = 2$, Similarly $d(v_2) = 2$. Again, the loop e_3 contributes 2 to the degree of v_3. e_2 contributes 1, e_4 contributes 1.

Thus $d(v_3) = 2+1+1 = 4$

Now, sum of the degrees

$= d(v_1) + d(v_2) + d(v_3)$

$= 2+2+4 = 8 = 2x4$

= twice the number of edges, an even number.

Example 4: Let us consider Fig 7.1 (Example 1)

$d(v_1) = 2+1+1+1+1 = 6$ (2 from loop e_1, 1 from each of e_2, e_3, e_5, e_6)

$d(v_2) = 1+1+1 = 3$ (1 from each of e_2, e_3, e_4)

$d(v_3) = 1+1+1 = 3$ (1 from each of e_4, e_5, e_6)

Sum of the degrees

$= d(v_1) + d(v_2) + d(v_3)$

$= 6+3+3 = 12 = 2x6$

= twice the number of edges, an even number.

Now, we prove the following theorem,

Theorem 7.1 : (The Handshaking Theorem)

Statement : The sum of the degrees of all the vertices of a graph is twice the number of edges.

Proof : Let G be a graph.

Let the number of edges be n.

Let e be an edge. Then e is either a loop or incident with two distinct vertices.

Let e be a loop on a vertex v. Then e contributes 2 to the sum of the degrees of v.

Again, let e be incident with two distinct vertices u, and v. Then e contributes 1 to the degrees of each vertex. Thus, if the sum of the degrees of the vertices is taken, each edge contributes 2 to this sum.

Thus, the sum of the degrees of all vertices of a graph is twice the number of edges, i.e., 2n.

Corollary

1. The sum of the degrees of all vertices of a graph is an even number.

Proof : Let G be a graph having n edges. Then, the sum of the degrees of all vertices is 2n, which is an even number.



LET US KNOW

1. A vertex is called an even degree vertex if the degree of the vertex is even.
2. A vertex is called an odd degree vertex if the degree of the vertex is odd.
3. A vertex is called an isolated vertex if the degree of the vertex is zero.
4. A vertex is called a pendant vertex if the degree of the vertex is one.
5. If G is a graph with n vertices, the maximum degree of a vertex is (n–1).

Theorem 7.2: In a graph, the number of vertices of odd degree is even.

Proof : Let G be a graph. Let there be n odd degree vertices $v_1, v_2, v_3, \ldots, v_n$; and m even degree vertices $u_1, u_2, u_3, \ldots . u_m$.

We know that the sum of the degrees of all the vertices of a graph is twice the number of edges, and so is an even number.

$\therefore$ $[d(v_1) + d(v_2) + \ldots .+ d(v_n)] + [d(u_1) + d(u_2) + \ldots .+ d(u_m)]$

= an even number

i.e. $\sum_{i=1}^{n} d(v_i) + \sum_{j=1}^{n} d(u_j)$ = an even number (1)

RHS of (1) is even.

$\therefore$ LHS of (1) is also even.

Now, each $d(u_j)$ is even.

$\therefore$ $\sum_{j=1}^{m} d(u_j)$ is even

$\therefore$ $\sum_{i=1}^{n} d(v_i)$ is even.

Since each d(v_i) is add, and $\sum_{i=1}^{n} d(v_i)$ is even. Therefore the number of terms contained in $\sum_{i=1}^{n} d(v_i)$ must be even.

Thus, the number of vertices of odd degree is even.

Hence the proof is complete.

Let us consider the following graph.

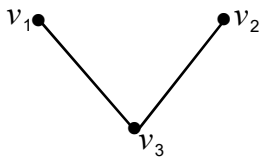


Fig 7.8

Clearly the graph is simple. It has no loops and parallel edges.

The graph has 3 vertices, viz, v_1, v_2, v_3.

d(v_1) = 1, d(v_2) = 2, d(v_3) = 1

Two vertices are of the same degree 1.

Now we prove the following theorem.

Theorem 7.3 : If G is a simple graph with at least two vertices, then G has at least two vertices of the same degree.

Proof : Let G be a simple graph. Let the number of vertices of G be n where $n \geq 2$.

Since the graph is simple, it has no loops and parallel edges. Therefore the degree of each vertex is $\leq$ (n–1).

If possible, let all the vertices of G be of different degrees. Therefore, the possible degrees for n vertices of G are as follows.

0, 1, 2, 3, ..., n–1.

Let u be a vertex with degree zero. Then u is an isolated vertex.

Let v be a vertex with degree n–1. Then v has (n–1) vertices adjacent to it. Now v is not adjacent to itself. Therefore, every vertex of G, other than v, is adjacent to v. Therefore, u is also adjacent to v, which is a contradiction to the fact that u is an isolated vertex. So, our assumption is wrong. Therefore, all the vertices of G cannot be of different degrees. Thus, G has at least two vertices of the same degree.

Note : The converse of the above theorem is not true.

Let us consider Example 2 (Fig 7.4)

d(v_1) = 6, d(v_2) = 3, d(v_3) = 3

The vertices, v_2 and v_3 are of the same degree. But the graph is not simple. It has loop as well as parallel edges.

Thus, a graph with two vertices of the same degree may not be simple.



CHECK YOUR PROGRESS

Q 3: Write down the number of vertices, the number of edges, and the degree of each vertex of the following graphs. Identify the pendant vertex if any. Also verify that the sum of the degrees of the vertices is twice the number of edges.

(i)

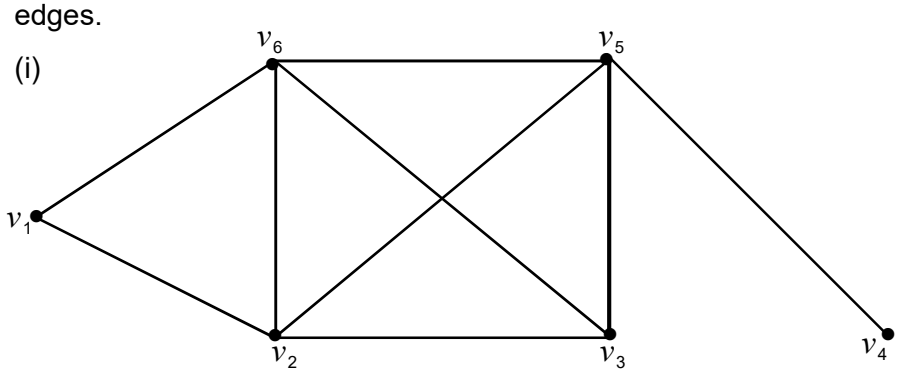


Fig 7.8

(ii)

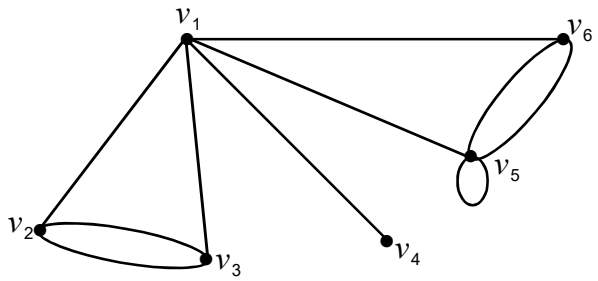


Fig 7.9

Q 8: Can there be a graph with 5 vertices such that the degrees of the vertices are 5, 5, 5, 4, 2 ?

Q 9: A graph G has 16 edges, and each vertex is of degree 4. Find the number of vertices.

Q 10: A graph contains 21 edges, 3 vertices are of degree 4 each, and the remaining vertices are of degree 2 each. Find the total number of vertices.

Q 11: A graph contains 35 edges, 4 vertices are of degree 5 each, 5 vertices are of degree 4 each, 4 vertices are of degree 3 each, and the remaining vertices are of degree 2 each. Find the total number of vertices. Also find the number of vertices with degree 2.

Q 12: Draw a simple graph with 5 vertices each of degree 2.

Q 13: Draw a simple graph with 5 vertices having degrees (i) 3, 3, 3, 3, 2; (ii) 3, 3, 3, 3, 4.

Q 14: Draw a graph with 6 vertices having each vertex of degree 3.

Q 15: Let G be a graph with 7 vertices having degrees 4, 1, 2, 2, 3, 5, 5. Find the number of edges of G.

Q 16: Write down the number of vertices, the number of edges, and the degree of each vertex of the following graph. Verify that the number of edges is a multiple of the degree of each vertex.

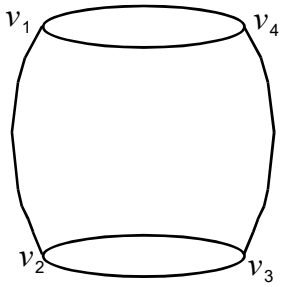


Fig 7.10

Q 17: If all the vertices of a graph are each of odd degree k, show that the number of edges of the graph is a multiple of k.

Q 18: Prove, in a graph, that the sum of degrees of all the vertices with odd degree is always even.

Q 19: Let G be a simple graph with n vertices. Show that the degree of a vertex of G cannot exceed (n–1).

Q 20: Can there be a simple graph with seven vertices having degrees 1, 3, 3, 4, 5, 6, 6 ? Justify your answer.

Q 21: Can there be a simple graph with six vertices having degrees 1, 2, 3, 4, 5, 5 ? Justify your answer.

Q 22: Can there be a simple graph with five vertices having degrees 2, 2, 4, 4, 4? Justify your answer.

Q 23: Let G be a (p, q) graph all of whose vertices have degree k or (k+1). If G has n(>0) vertices each of degree k, and m vertices each of degree (k+1), show that n = (k+1)p – 2q.

7.4 DIFFERENT TYPES OF GRAPHS

7.4.1 Finity Graph, Infinite Graph, Null Graph

A graph is said to be finite if it has a finite number of vertices and a finite number of edges. Otherwise, it is called an infinite graph.

Note : The finite graph with one vertex and no edges, i.e., a single point, is called the trivial graph.

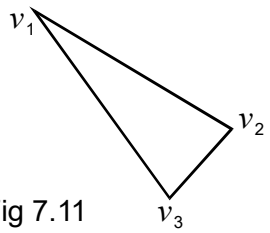


Fig 7.11
Finite graph

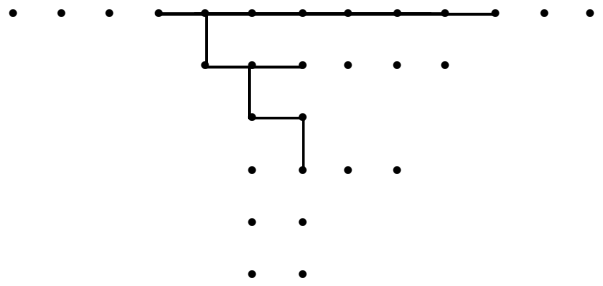


Fig 7.12
Infinite graph



Fig 7.13 Trivial graph.

Null Graph

A graph whose edge set is empty is called a null graph. Thus, a null graph does not contain any edges in it.

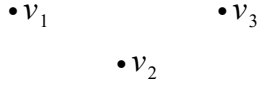


Fig 7.14 Null Graph

7.4.2 Complete Graph

A simple graph G is said to be complete (or universal) if there is exactly one edge between each pair of distinct vertices. Generally the complete graph with n vertices is denoted by K_n.

The complete graphs K_1, K_2, K_3, K_4, K_5, K_6 are shown in Fig 7.

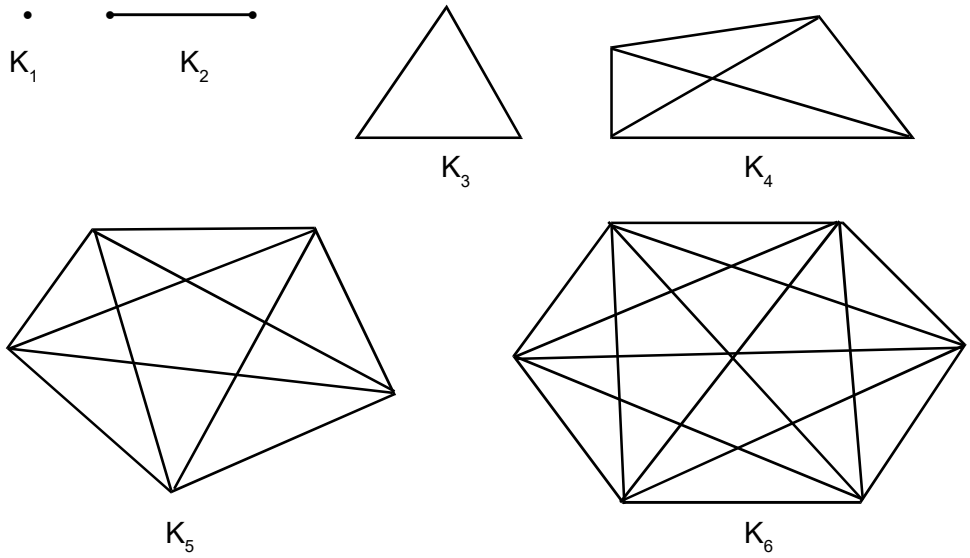


Fig 7.15

K_1 has no edge (number of edges in 0).

K_2 has one edge (${}^2C_2 = 1$).

K_3 has three edges $\left({}^3C_2 = \frac{3\times(3-1)}{2} = 3 \right)$.

K_4 has six edges $\left({}^4C_2 = \frac{4\times(4-1)}{2} = 6 \right)$.

K_5 has ten edges $\left({}^5C_2 = \frac{5\times(5-1)}{2} = 10 \right)$.

K_6 has fifteen edges $\left({}^6C_2 = \frac{6\times(6-1)}{2} = 15 \right)$.

Theorem 7.4 : A complete graph with n vertices consits of ${}^nC_2$ i.e $\frac{n(n-1)}{2}$ edges. $(n \geq 2)$

Proof : Let G be a complete graph.

Let the number of vertices of G be n.

Since G is a simple graph, it has no loops and parallel edges.

Since G is a complete graph, each vertex of G is connected to each of the remaining (n–1) vertices. Therefore, degree of each vertex is (n–1).

$\therefore$ the sum of the degrees of all the vertices = n(n–1).

Let the total number of edges be e.

We know that the sum of the degree of all the vertices of a graph is twice the number of edges. (Theorem 7.1)

$\therefore$ n(n–1) = 2e

$\therefore \quad e = \frac{n(n-1)}{2} = {}^{n}C_{2}$

Note : The maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.

7.4.3 Regular Graph

If every vertex of a simple graph G has the same degree, then the graph is called a regular graph. If the degree of each vertex of a regular graph is k, then it is called k-regular.

Let us consider the graphs K_1, K_2, K_3, K_4, K_5, K_6 given in Fig 7.5

K_1 is 0 regular.

The degree of each vertex of K_2 is 1. Therefore, K_2 is 1-regular.

The degree of each vertex of K_3 is 2. Therefore, K_3 is 2-regular.

The degree of each vertex of K_4 is 3. Therefore, K_4 is 3-regular.

K_5 is 4-regular.

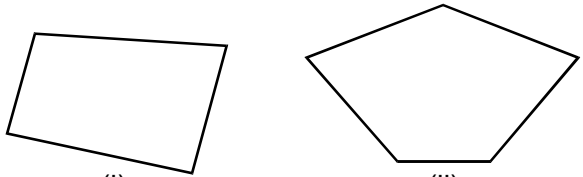
K_6 is 5-regular.

Note : K_n is (n–1) - regular graph.

Example 5 : (a) Give 2 examples of 2-regular graphs.

(b) Give 2 examples 3-regular graphs.

Solution : (a) The following two graphs are 2-regular.



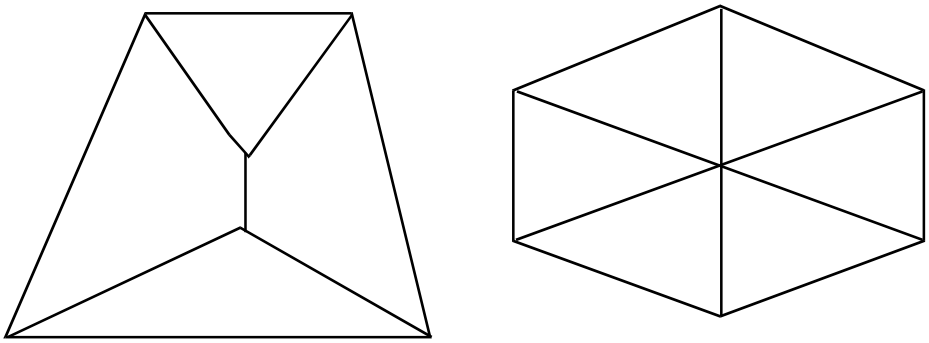
(i) (ii)

Fig 7.16

Both the graphs are simple.

The degree of each vertex of both the graphs is 2.

(b) The following two graphs are 3-regular.



(i) (ii)

Fig 7.17

Both the graphs are simple.

The degree of each vertex of both the graphs is 3.

Example 6: Let G be a k-regular graph, and let the number of vertices be p. What is the number of edges ?

Solution: Let u be a vertex of G. Since G is k-regular, therefore d(u) = k, for all vertices u of G.

Let the number of edges be q.

We know that the sum of the degrees of all the vertices of a graph is twice the number of edges. (Theorem 7.1)

$\therefore \quad \Sigma d(u) = 2q$

or, k + k + k + ...+ k = 2q ($\because$ there are p vertices)

(p terms)

or, kp = 2q

$\therefore \quad q = \frac{kp}{2}$

Thus the number of edges is $\frac{kp}{2}$.

7.4.4 Bipartite Graph

A simple graph G = (V, E) is said to be bipartite if the vertex set V can be partitioned into two subsets V_1 and V_2 such that each edge of G connects a vertex of V_1 to a vertex of V_2. It must be borne in mind that no edge in G connects either two vertices in V_1 or two

vertices in V_2 .

Note : A bipartite graph can have no loop.

Example 7: Let V = $\{v_1, v_2, v_3, v_4, v_5\}$

$V_1 = \{v_1, v_2\}$

$V_2 = \{v_3, v_4, v_5\}$

$V_1 \subseteq V$, $V_2 \subseteq V$, $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \phi$

Let E = $\{e_1, e_2, e_3, e_4, e_5\}$ such that e_1 is associated with (v_1, v_4), e_2 is associated with (v_2, v_5) e_3 is associated with (v_1, v_3), e_4 is associated with (v_1, v_5), e_5 is associated with (v_2, v_3).

Then G = (V, E) is a bipartite graph

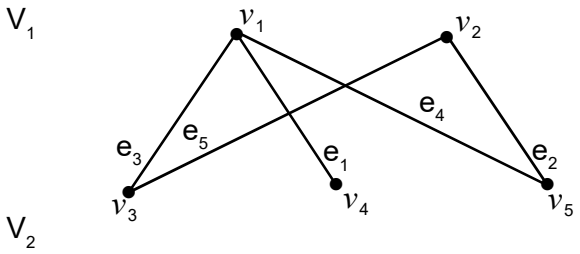


Fig 7.18

Example 8: Let V = $\{v_1, v_2, v_3, v_4, v_5, v_6\}$

$V_1 = \{v_1, v_2, v_3\}$

$V_2 = \{v_4, v_5, v_6\}$

$V_1 \subseteq V$, $V_2 \subseteq V$, $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \phi$

Let E = $\{e_1, e_2, e_3, e_4, e_5, e_6\}$ such that e_1 is associated with (v_1, v_4), e_2 with (v_1, v_6), e_3 with (v_2, v_4), e_4 with (v_3, v_5), e_5 with (v_2, v_6), e_6 with (v_3, v_6).

Then G = (V, E) is a bipartite graph.

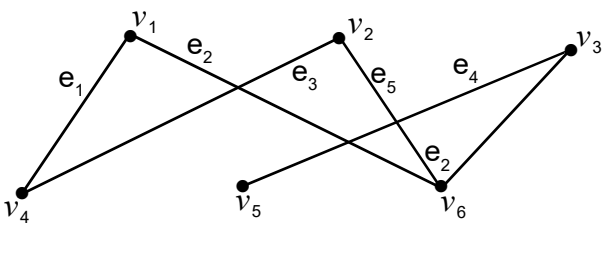


Fig 7.19

Theorem 7.5: The number of edges in a bipartite graph with n vertices is at most $\frac{n^2}{4}$.

Proof: Let G = (V, E) be a bipartite graph having n vertices.

Let the vertx set V be partitioned into two subsets V_1 and V_2 such that each edge of G connects a vertex of V_1 to a vertex of V_2.

Let the number of vertices in V_1 be x.

$\therefore$ the number of vertices in V_2 is (n–x),

If each of the x vertices in V_1 is connected to each of the (n–x) vertices in V_2, then the maximum number of edges is obtained.

$\therefore$ the maximum number of edges is x(n–x).

Let $f(x) = x(n–x) = xn–x^2$

$\therefore$ $f'(x) = n–2x$

$f'(x) = 0$ gives $n–2x = 0 \Rightarrow x = \frac{n}{4}$

Now $f''(x) = 0–2x1 = –2$

$\therefore$ $f''\left(\frac{n}{4}\right) = -2 < 0$

$\therefore$ f(x) is maximum when $x = \frac{n}{2}$.

$\therefore$ the number of edges is maximum when $x = \frac{n}{2}$

$\therefore$ the maximum number of edges

$= f\left(\frac{n}{2}\right)$

$= \frac{n}{2}\left(n - \frac{n}{2}\right)$

$= \frac{n}{2} \cdot \frac{n}{2}$

$= \frac{n^2}{4}$.

7.4.5 Complete Bipartite Graph

A Simple graph G = (V, E) is said to be complete bipartite if the vertex set V can be partitioned into two subsets V_1 and V_2 such that each vertex of V_1 is connected to each vertex of V_2. Generally the complete bipartite graph is denoted by $K_{m, n}$ where m is the number of vertices in V_1 and n is the number of vertices in V_2.

Note : $K_{m, n}$ has m+n vertices, and mn edges.

Example 9: Let V = $\{v_1, v_2, v_3, v_4, v_5\}$

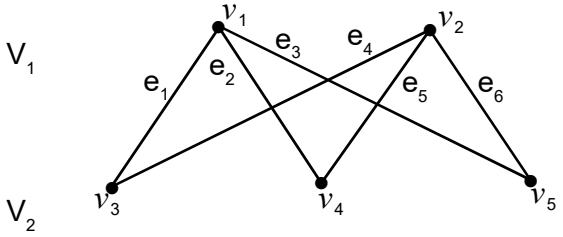
$V_1 = \{v_1, v_2\}$

$V_2 = \{v_3, v_4, v_5\}$

$V_1 \subseteq V$, $V_2 \subseteq V$, $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \phi$

Let E = {e_1, e_2, e_3, e_4, e_5, e_6} such that e_1 is associated with (v_1, v_3), e_2 is associated with (v_1, v_4), e_3 is associated with (v_1, v_5), e_4 is associated with (v_2, v_3), e_5 is associated with (v_2, v_4), e_6 is associated with (v_2, v_5).

Then $K_{2, 3}$ is a complete bipartite graph.



$K_{2, 3}$ graph; vertices 5, edges 6.

Fig 7.20

Example 10: Let V = $\{v_1, v_2, v_3, v_4, v_5, v_6\}$

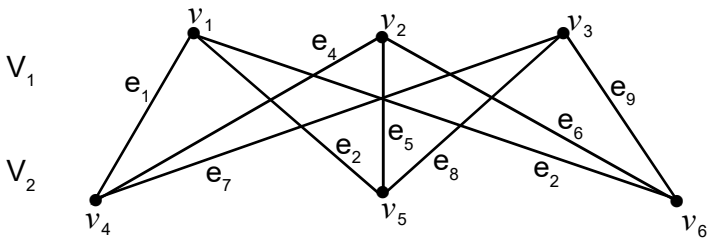
$V_1 = \{v_1, v_2, v_3\}$

$V_2 = \{v_4, v_5, v_6\}$

$V_1 \subseteq V$, $V_2 \subseteq V$, $V_1 \cup V_2 = V$, $V_1 \cap V_2 = \phi$

Let E = {e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9} such that e_1 is associated with (v_1, v_4), e_2 with (v_1, v_5), e_3 with (v_1, v_6), e_4 with (v_2, v_4), e_5 with (v_2, v_5), e_6 with (v_2, v_6), e_7 with (v_3, v_4), e_8 with (v_3, v_5), e_9 with (v_3, v_6).

Then $K_{3, 3}$ is a complete bipartite graph.



$K_{3, 3}$ graph; vertices 6, edges 9

Fig 7.21

7.4.6 Directed Graph

Let G = (V, E) be a graph. If each edge e ∈ E is associated with an ordered pair of vertices, then G is called a directed graph (or a digraph). In the diagram of a directed graph, each edge e beginning at the vertex u and ending at the vertex v is represented by means of an arrow. u is called the initial vertex and v is called the terminal vertex.

Let us consider Fig 7.22. It is a directed graph. The edge e_1 begins at v_1, and ends at v_2. For e_1, v_1 is the initial vertex, and v_2 is the terminal vertex. For e_2, v_2 is the initial vertex and v_2 is the terminal vertex. For e_3, v_3 is the initial vertex and v_1 is the terminal vertex.

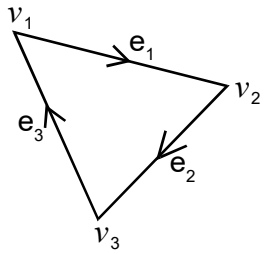


Fig 7.22

Let us consider the graph given in Fig 7.23. It is a directed graph. There are four vertices, viz, v_1, v_2, v_3, v_4, and seven edges, viz, e_1 e_2, e_3, e_4, e_5, e_6, e_7. We note that for the loop e_1, v_1 is the initial as well as the terminal vertex.

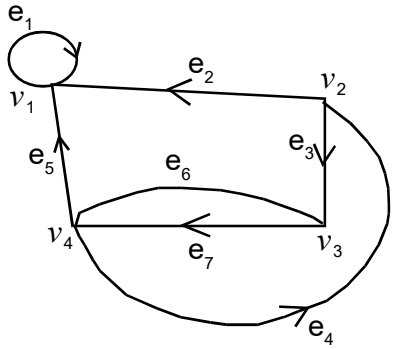


Fig 7.23

Indegree : The number of edges directed into a vertex v in a directed graph is called the indegree of the vertex v. We denote the indegree of v by id (v).

Outdegree : The number of edges directed out of a vertex v in a directed graph is called the outdegree of the vertex v. We denote the outdegree of v by od (v).

In the directed graph given in Fig 7.23

id (v_1) = 3, id (v_2) = 1, id (v_3) = 2, id (v_4) = 1

od (v_1) = 1, od (v_2) = 2, od (v_3) = 1, od (v_4) = 3.

Sum of the indegrees

= id (v_1) + id (v_2) + id (v_3) + id (v_4)

= 3 + 1 + 2 + 1 = 7

Sum of the outdegrees

= od (v_1) + od (v_2) + od (v_3) + od (v_4)

= 1 + 2 + 1 + 3 = 7

We note that sum of the indegrees

= Sum of the outdegrees

= number of edges.

Theorem 7.6 : In a directed graph,

the sum of indegrees of the vertices

= the sum of outdegrees of the vertices

= the number of edges.

Proof : Each edge of a directed graph begins at one vertex and ends at one vertex. Therefore, each edge contibutes 1 each to the sum of the indegrees and to the sum of the outdegrees.

$\therefore$ the sum of indegrees of the vertices

= the sum of outdegrees of the vertices

= the number of edges.

Note : 1. A vertex v with zero indegree is called a source.

2. A vertex v with zero outdegree is called a sink.



CHECK YOUR PROGRESS

Q 24: For the following directed graphs, verify that the sum of indegrees of the vertices.

= the sum of outdegrees of the vertices

= the number of edges.

(a)

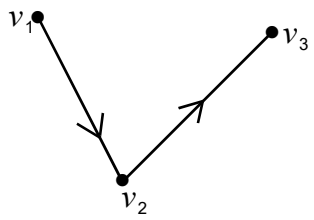


Fig 7.24

(b)

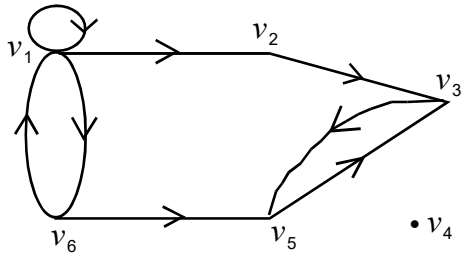


Fig 7.25

(c)

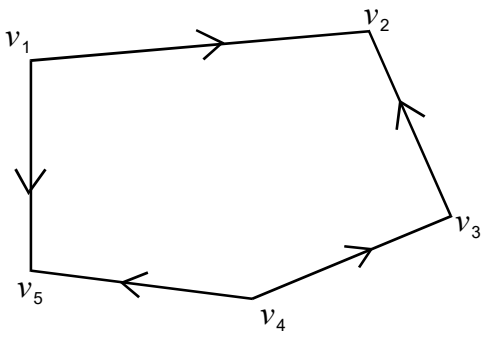


Fig 7.26

Q 25: (a) Exhibit the complete bipartite graph on 2 and 4 vertices.

(b) Exhibit the complete bipartite graph on 4 and 4 vertices.

7.5 WALK, PATH AND CYCLES

Let G = (V, E) be a graph. Let u, and v be two vertices in G.

A walk from u to v in G is a finite alternating sequence of vertices and edges.

u = v_1, e_1, v_2, e_2, v_3, e_3, . . ., v_{n-1}, e_{n-1}, v_n, e_n, $v_{n+1} = v$ beginning with u and ending with v such that v_1 and v_{i+1} are end points of the edge e_i for i = 1, 2, ..., n. u is called the initial vertex and v is called the terminal vertex.

The length of a walk is the number of edges it contains; the repeated edges, if any, are also counted. Clearly, the length of the walk given above is n. A walk of length zero is just a single vertex.

A walk is closed if the initial vertex = the terminal vertex.

A walk is open if the initial vertex $\neq$ the terminal vertex.

A walk in which no edge is repeated is called a trail.

A closed trial of non zero length is called a circuit.

A trail with no repeated vertices is called a path. A path on n vertices is generally denoted by P_n.

No edge (and no vertex) is repeated in a path.

A trail of nonzero length from a vertex u to itself is called a cycle if except for the initial and the terminal vertices that are both equal to u, there are no repeated vertices in the walk.

A cycle with three edges is called a **triangle**.

A cycle is called even if it contains **even** number of edges.

A cycle is called odd if it contains **odd** number of edges.

Walk

(edges and vertices may be repeated)

Open Walk	**Closed Walk**
(initial and terminal vertices are different	(initial and terminal vertices are same
↓	↓
Trail	**Circuit**
(edges are not repeated)	(edges are not repeated)
↓	↓
Path	**Cycle**
(vertices also are not repeated)	(vertices also are not repeated except the initial and terminal vertices that are both equal)

Example 11 : Let us consider the following graph.

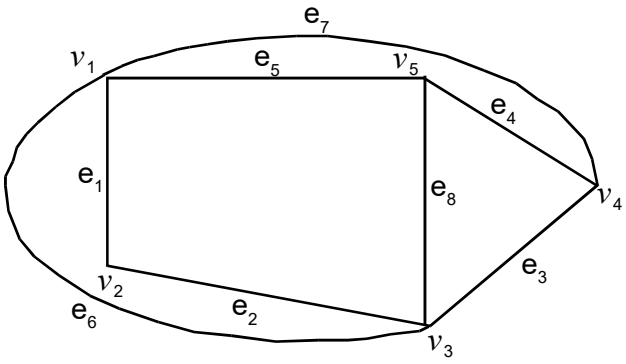


Fig 7.27

Let us consider the following finite alternating sequences of vertices and edges.

(i) $\alpha = (v_1, e_1, v_2)$.

α is a walk of length 1 as it contains 1 edge.

α is an open walk since $v_1 \neq v_2$.

No edge is repeated. So α is a trail of length 1.

No vertex is repeated. So α is a path.

α is not a cycle as the initial vertex $\neq$ the terminal vertex.

Every walk of length 1 is a path.

(ii) $\beta = (v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_8, v_3)$

β is a walk of length 5 as it contains 5 edges.

β is an open walk since $v_1 \neq v_3$.

All the edges are distinct. No edge is repeated. So β is a trail of length 5.

The vertex v_3 is used twice. So β is not a path.

Every trail is not a path.

(iii) $\gamma = (v_1, e_6, v_3, e_3, v_4, e_4, v_5)$

γ is a walk of length 3 as it contains 3 edges.

γ is an open walk since $v_1 \neq v_5$.

All the vertices are distinct. No vertex is repeated.

All the edges are distinct. No edge is repeated.

Therefore γ is a path of length 3.

(iv) $\delta = (v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_7, v_1)$

δ is a walk of length 4 as it contains 4 edges.

δ is a closed walk as the initial vertex = the terminal vertex.

No edge is repeated. So δ is a trail of length 4.

There are no repeated vertices except the initial vertex and the terminal vertex that are both equal.

Therefore δ is a cycle.

We note that δ is not a path as the vertex v_1 is used twice.

A cycle is not a path as the first and the last vertices are the same.

(v) $\rho = (v_5, e_8, v_3, e_3, v_4, e_4, v_5)$

ρ is a walk of length 3 as it contains 3 edges.

ρ is a closed walk as the initial vertex = the terminal vertex.

No edge is repeated. So ρ is a trail of lenght 3.

There are no repeated vertices except the initial vertex and the terminal vertex that are both equal.

Therefore ρ is a cycle.

Since ρ is a cycle with 3 edges, therefore ρ is a triangle.

Example 12: Let us consider the complete graph K_5 given below.

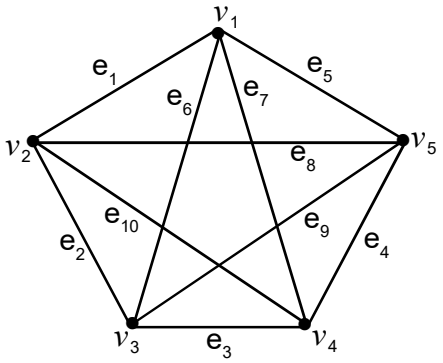


Fig 7.28

Let us consider the following finite alternating sequences of vertices and edges.

(i) $\alpha = (v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_7, v_1, e_6, v_3, e_3, v_4, e_4, v_5)$

α is a walk of length 7 as it contains 7 edges.

α is an open walk since $v_1 \neq v_5$.

Edge e_3 is used twice.

Vertex v_1 is used twice.

Vertex v_3 is used twice.

Vertex v_4 is used twice.

α is not a path.

(ii) $\beta = (v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5)$

β is a walk of length 4 as it contains 4 edges.

β is an open walk since $v_1 \neq v_5$.

No edge is repeated. So α is a trail.

No vertex is repeated. So α is a path.

Note : We see that α is a walk joining two distinct vertices v_1 and v_5, and

β is a path joining the vertices v_1 and v_5. The path β is contained in the walk α.

Now we prove the following theorem.

Theorem 7.7 : If there is a walk joining two distinct vertices in a graph, there is a path joining them contained in the walk.

Proof : Let G be a graph and u, v be two distinct vertices of G.

Let W = (u = v_1, e_1, v_2, e_2, . . ., v_n= v) be a walk joining the vertices u, v.

If this is not a path, then v_i = v_j for some i < j < n. This shows that there is a closed walk from to v_i to v_j. We remove this closed walk from W, and form a new walk W_1 from u to v. If this walk is a path, we stop. If not, we proceed as above.

Again we note that an edge is traced only after tracing an end vertex. So if all the vertices in a walk are distinct, edges cannot repeat, i.e., all the edges are also distinct.

Thus, we obtain a path from u to v.



LET US KNOW

If all the vertices in a walk are distinct, all the edges are also distinct. Hence, a path is always a trail.

7.6 SUBGRAPH OF A GRAPH

Let G = (V, E) be a graph.

A graph H = (V′, E′) is called a subgraph of G if the vertices and edges of H are contained in the vertices and edges of G respectively, i.e., H is a subgraph of G if V′ ⊆ V, E′ ⊆ E.

Note : V′ is a nonempty subset of V.

Example 13 : G = (V, E) be a graph where

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} are given by the figure

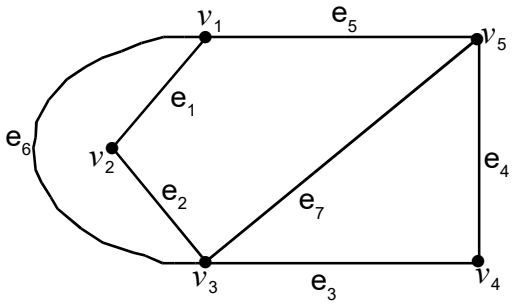


Fig 7.29

(i) Then H = (V_1, E_1) is a subgraph of G where

$V_1 = \{v_1, v_2, v_5\}$

$E_1 = \{e_1, e_5\}$

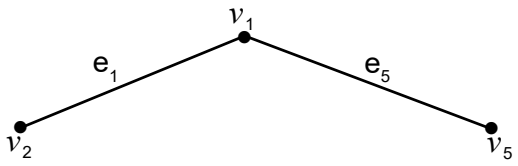


Fig 7.30

Note : The above subgraph H of the graph G is a **vertex deleted subgraph** of G. The vertices v_3, v_4 have been deleted. Deletion of the vertices will go with the deletion of the edges incident with these vertices. The edges incident with the vertex v_3 are e_2, e_3, e_6, e_7. So, these four vertices have been deleted. Again, the edges incident with the vertex v_4 are e_3, e_4. The edge e_3 has already been deleted. So, we delete e_4. Thus, we are left with e_1, e_5.

It should be borne in mind that deletion of a vertex goes with the deletion of any edge incident with it.

(ii) K = (V_2, E_2) is a subgraph of G where

$V_2 = \{v_1, v_2, v_3, v_4, v_5\}$

$E_2 = \{e_1, e_2, e_7, e_5\}$

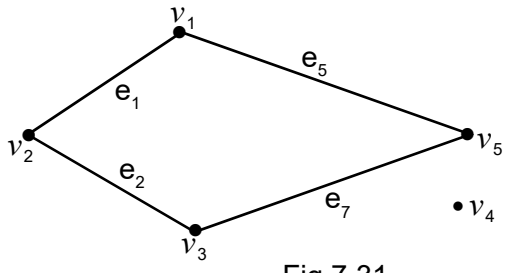


Fig 7.31

Note : The above subgraph K of the graph G is an edge **deleted subgraph** of G. The edges e_3, e_4, e_6 have been deleted. It should be borne in mind that

deletion of an edge does not go with the deletion of its adjacent vertices.

Definition : A subgraph H = (V/, E/) of a graph G = (V, E), where V/ is a nonempty subset of V, and E/ consists of only those edges that are incident on the elements of V/, is called an induced subgraph of G.

Example 14 : L = (V_3, E_3) is an induced subgraph G = (V, E) of Example 13, where

$V_3 = \{v_1, v_2, v_3\}$

$E_3 = \{e_1, e_2, e_6\}$

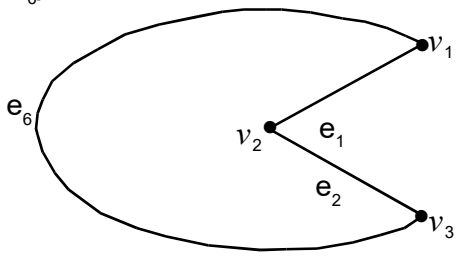


Fig 7.32 (a)



CHECK YOUR PROGRESS

Q 26: Examine if the graph given by Fig 7.33 (a) is (a) a subgraph of the graph given by Fig 7.33 (b), (b) a subgraph of the graph given by Fig 7.33 (c)

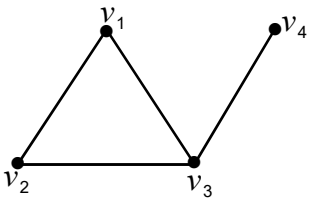


Fig 7.33 (a)

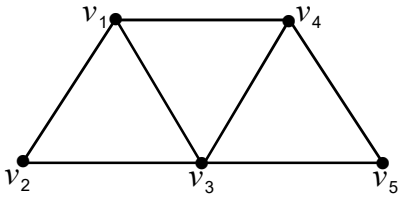


Fig 7.33 (b)

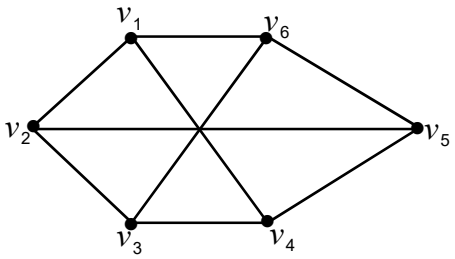


Fig 7.33 (c)

Q 27: Draw all the subgraphs of the complete graph K_2.

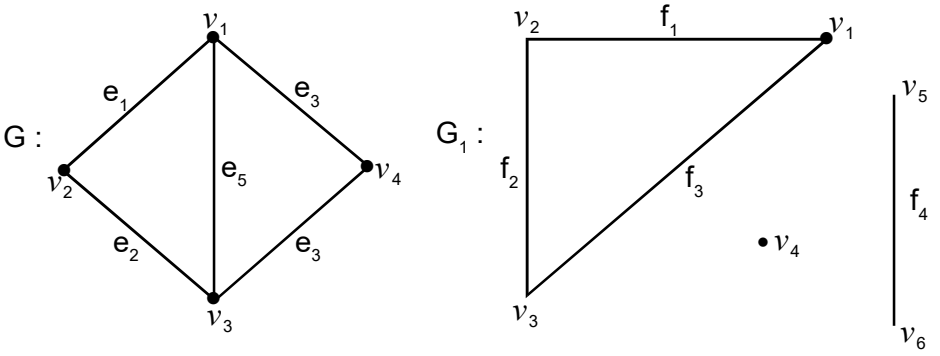
Q 28: Draw all the subgraphs of the complete graph K_3.

7.7 CONNECTED AND DISCONNECTED GRAPHS

Two vertices u and v of a graph G are connected if there exists a path that starts at u and ends at v.

A graph G is connected if there is a path between any two of its vertices; otherwise the graph is called a disconnected graph.

Let us consider the graphs given below.



(a) (b)

Fig 7.34

The graph in Fig 7.34 (a) is connected.

The graph in Fig 7.34 (b) is disconnected. Since, for example, the vertices v_3 and v_4 are not connected.

A connected subgraph H of a graph G is called a **connected component** of G if H is not contained in any larger connected subgraph of G.

The graph G_1 in Fig 7.34 (b) has three connected components, viz., the subgraphs induced by the vertex sets $\{v_1, v_2, v_3\}$, $\{v_4\}$, $\{v_5, v_6\}$. We note that the isolated vertex v_4 itself forms a connected component of the graph.

Note : A graph with one vertex is connected. If it is disconnected, there exists two distinct vertices which are not joined by a path, which is not possible as the graph does not have two distinct vertices.

Property : 'u is connected to v' is an equivalence relation on the vertex set V of a graph G. (We note that any vertex u is connected to itself)

Proof : Let us consider the relation R on the vertex set V of a graph G defined as follows.

For all u, $v \in V$, the pair (u, v) $\in R$, i.e., u R v if and only 'u is connected to v'.

Reflexive : Every vertex u is connected to itself, i.e., (u, u) $\in R$, i.e., uRu, for every u $\in V$.

$\therefore$ R is reflexive.

Symmetric : Let (u, v) $\in R$, i.e., uR v i.e. there is a path from u to v. Then that same sequence of vertices and edges in reverse order gives a path from v to u.

Thus, if (u, v) $\in R$, then (v, u) $\in R$ i.e., if uR v, then vRu.

$\therefore$ R is symmetric.

Transitive : Let (u, v) $\in R$, i.e., uR v, and (v, w) $\in R$, i.e., vRw there is a path, say P_1, from u to v, and a path, say P_2, from v to w. We can join these two paths at v to create a walk from u to w. This walk can be used to obtain a path from u to w.

Thus, if (u, v) $\in R$, (v, w) $\in R$; then (u, w) $\in R$, i.e., if uR v, vRw, then uRw.

$\therefore$ R is transitive.

Thus, R is an equivalence relation.

Note : Every equivalence class of the above equivalence relation R is a connected component of G. Hence every graph can be partitioned into a finite number of components. Thus, we see that a graph G is a connected graph if and only if G has one component.

Theorem 7.8 : A graph G is disconnected if and only if the vertex set V of G can be partitioned into two nonempty, disjoint subsets V_1 and V_2 such that there exists no edge in G whose one end vertex is in V_1 and the other in V_2.

Proof: Let G = (V, E) be a disconnected graph.

Let u $\in V$.

Let V_1 be the set of all those vertices which are joined by paths to u. Clearly $V_1 \neq \phi$, since at least u $\in V_1$.

Since G is disconnected, V_1 does not contain all vertices of G. Let V_2 be the set of vertices of G which are not in V_2. Then V_2 is nonempty and no vertex in V_1 is joined to any vertex in V_2.

Thus, the set V can be partitioned into two nonempty subsets V_1, V_2 such that $V_1 \cap V_2 = \phi$, $V_1 \cup V_2 = V$.

Conversely, let the vertex set V of G be partitioned into two nonempty, disjoint subsets V_1 and V_2 such that there exists no edge in G whose one end vertex is in V_1 and the other in V_2. Let u, v be any two arbitrary vertices such that $u \in V_1$, $v \in V_2$. Now u, and v are not connected as there exists no edge whose one end vertex is in V_1 and the other in V_2. Thus, G is disconnected.

Theorem 7.9 : If a graph G (connected or disconnected) has exactly two vertices of odd degree, there is a path joining these two vertices.

Proof : Case 1 : Let G be connected.

Let u and v be the only vertices of G which are of odd degree.

We know that the number of odd degree vertices in a graph is even.

Clearly, there is a path joining u and v, since G is connected.

Case 2 : Let G be disconnected.

Let u, and v be the only vertices of G which are of odd degree.

Let us consider the connected component C such that u belongs to C.

Clearly C is a connected subgraph of G.

We know that the number of odd degree vertices in a graph is even.

Since u, and v are the only odd degree vertices in G, it follows that $v \in C$.

Thus, there is a path joining these two vertices.

Theorem 7.10 : Let G be a simple graph on n vertices. If G has k connected components, then the number m of edges of G satisfies.

$$n - k \le m \le \frac{(n-k)(n-k+1)}{2}$$

Proof : Case 1 : First we prove that $m \ge n - k$

We prove $m \ge n - k$ by induction on the number of edges of G.

There is nothing to prove if G is a null graph. (m = 0, n = k).

Let G contain as few edges as possible, say m_0.

Then the removal of any edge of G must increase the number of connected components by 1, and the graph that remains has n vertices,

k+1 connected components, and m_0–1 edges. It follows from the induction hypothesis that $m_0 - 1 \geq n-(k+1)$ which gives $m_0 \geq n-k$, as required.

Case 2 : Next we prove that

$$m \leq \frac{(n-k)\,(n-k+1)}{2}$$

Let the k connected components be $C_1, C_2, C_3, \ldots, C_k$. Let n_i be the number of vertices in the component C_i for i = 1, 2, . . . , k. Then

$n_1 + n_2 + n_3 + \ldots + n_k = n$

i.e. $\sum_{i=1}^{k} n_i = n$

Here G is a simple graph. Therefore,each C_i is a simple graph.So, the maximum possible number of edges in C_i is $\frac{n_i(n_i-1)}{2}$. Therefore,

$$m \leq \sum_{i=1}^{k} \frac{1}{2} n_i\,(n_i-1) = \frac{1}{2}\sum_{i-1}^{k} n_i^{\,2} - \frac{1}{2}\sum_{i-1}^{k} n_i$$

$$= = \frac{1}{2}\sum_{i-1}^{k} n_i^{\,2} - \frac{1}{2}n \qquad (1)$$

Now for any k positive integers $n_1, n_2, \ldots, n_k$, we have

$(n_1 - 1) + (n_2 - 1) + \ldots + (n_k - 1)$

$= (n_1 + n_2 + \ldots + n_k) - k = n-k.$

$\therefore\ [(n_1-1) + (n_2-1) + \ldots + (n_k-1)]^2 = (n-k)^2$

or, $(n_1-1)^2 + (n_2-1)^2 + \ldots + (n_k-1)^2 + 2(n_1-1)(n_2-1) + 2(n_1-1)(n_3-1) + \ldots$

$= (n-k)^2$

or, $(n_1-1)^2 + (n_2-1)^2 + \ldots + (n_k-1)^2 \leq (n-k)^2.$

or, $n^2_1 + n^2_2 + \ldots + n^2_k - 2(n_1+n_2+\ldots+n_k) + (1+1+\ldots+1) \leq (n-k)^2$

or, $\sum_{i-1}^{k} n_i^{\,2} \leq -2n + k \leq (n-k)^2$

or, $\sum_{i-1}^{k} n_i^{\,2} \quad (n-k)^2 + 2n-k \qquad (2)$

$\therefore$ from (1) and (2),

$$m \leq \frac{1}{2}\sum_{i-1}^{k} n^2_i - \frac{1}{2}n$$

$$\leq \frac{1}{2}\left\{(n-k)^2 + 2n - k\right\} - \frac{1}{2}n$$

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

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

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

Thus, the proof is complete.

Corollary 1 : If a simple graph G with n vertices has more than $\frac{(n-1)(n-2)}{2}$ edges, then G is connected.

Proof : Let G be a simple graph with n vertices. Let the number of edges be more than $\frac{(n-1)(n-2)}{2}$.

Let the number of connected components of G be k. Then G can have at most $\frac{1}{2}(n-k)(n-k+k+1)$ edges. So we must have.

$$\frac{1}{2}(n-k)(n-k+1) > \frac{1}{2}(n-1(n-2)$$

This is possible only when k = 1. Thus G has only one connected component, i.e., G itself.

$\therefore$ G is connected.

Corollary 2: If G is connected, then k = 1.

$\therefore$ from theorem 7.10

$$n-1 \le m \le \frac{1}{2}n(n-1).$$



CHECK YOUR PROGRESS

Q 29: Which of the graphs given below are connected?

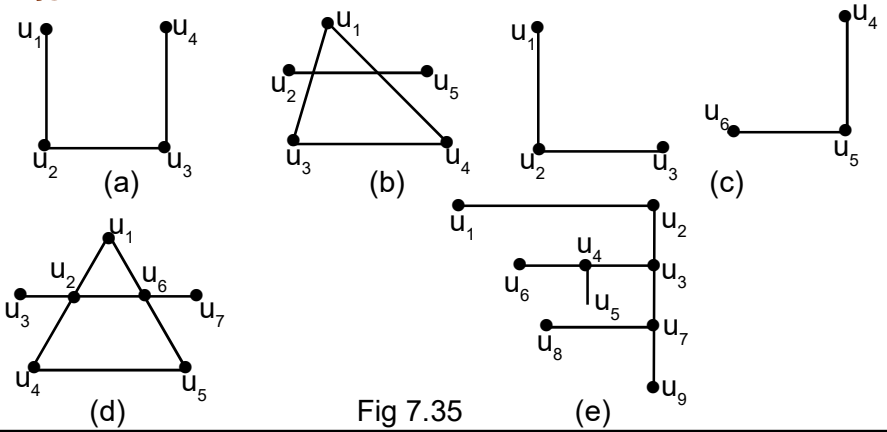


Fig 7.35

Q 30: Find the connected components of the graph given below.

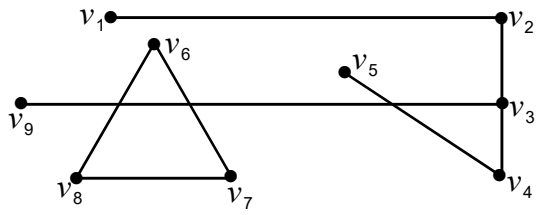


Fig 7.36

Q 31: Let G be a simple graph with 6 vertices and 11 edges. Examine if the graph G is connected.

Q 32: Give an example to show that a subgraph of a connected graph is not necessarily connected.

Q 33: Let G be a connected graph with at least two vertices. If the number of edges in G is less than the number of vertices, show that G has at least one vertex of degree one.

Q 34: Let G be a simple graph with at most 2n vertices. If the degree of each vertex is at least n, show that G is connected.

7.8 GRAPH ISOMORPHISM

Let G = (V_1, E_1), and H = (V_2, E_2) be two simple graphs.

An isomorphism of simple graphs G and H is a bijective (one-one and onto) mapping between the vertex sets V_1 and V_2

$f = V_1 \rightarrow V_2$

such that any two vertices u and v of G are adjacent in G if and only if f(u) and f(v) are adjecent in H. This type of bijective mapping is known as edge-preserving bijective mapping.

If an isomorphiem exists between two simple graphs G an H, the graphs are called isomorphic. We write $G \cong H$ or G = H. We do not distinguish between isomorphic graphs even though they may be drawn in different manners. It may be mentioned that the word 'isomorphic' has been derived from two greek words, viz., 'iso' - the same, and 'morphe'– shape or form.

Example 15 : Let us consider the graphs G = (V_1, E_1), and H = (V_2, E_2) given below–

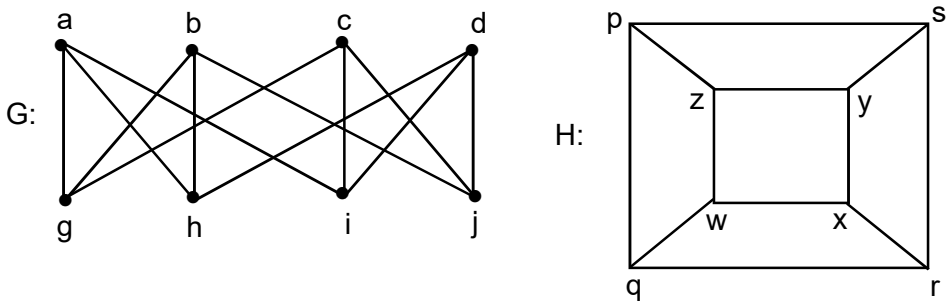


Fig 7.37

Here V_1 = {a, b, c, d, g, h, i, j}

V_2 = {p, q, r, s, w, x, y, z}

Let f : $V_1 \rightarrow V_2$ be a mapping defined by f(a) = p, f(b) = y, f(c) = w, f(d) = r, f(g) = z, f(h) = s, f(i) = q, f(j) = x.

Clearly, f is one-one and onto, i.e., f is a bijective mapping.

We note that

1. a and g are adjacent in G; and p = f(a) and z = f(g) are adjacent in H.
2. a and i are adjacent in G; and p = f(a) and q = f(i) are adjacent in H.
3. a and h are adjacent in G; and p = f(a), and s = f(h) are adjacent in H.
4. b and g are adjacent in G; and y = f(b) and z = f(g) are adjacent in H.
5. b and h are adjacent in G; and y = f(b) and s = f(h) are adjacent in H.
6. b and j are adjacent in G; and y = f(b) and x = f(j) are adjacent in H.
7. c and g are adjacent in G; and w = f(c) and z = f(g) are adjacent in H.
8. c and i are adjacent in G; and w = f(c) and q = f(i) are adjacent in H.
9. c and i are adjacent in G; and w = f(c) and x = f(j) are adjacent in H.
10. d and h are adjacent in G; and r = f(d) and s = f(h) are adjacent in H.
11. d and j are adjacent in G; and r = f(d) and s = f(i) are adjacent in H.
12. d and j are adjacent in G; and r = f(d) and x = f(j) are adjacent in H.

Thus, we see that f preserves adjacency of the vertices.

$\therefore$ f is a graph isomorphism.

i.e. G $\cong$ H.

We see that

(i) number of vertices in G

= number of vertices in H = 8

(ii) number of edges in G

= number of edges in H = 12

(iii) degree of each of the vertices in G is 3, degree of each of the vertices in H is 3, i.e. the corresponding vertices have the same degree.

Note : We note that isomorphic graphs have

(i) the same number of vertices,

(ii) the same number of edges, and

(iii) the corresponding vertices with the same degree.

If any of these conditions is not satisfied, the graphs cannot be isomorphic.

However, these conditions are not sufficient for graph isomorphism, i.e., if these conditions are satisfied, then the graphs may not be isomorphic as seen from the following example.

Example 16 : Let us consider the graphs $G = (V_1, E_1)$ and $H = (V_2, E_2)$ given below :

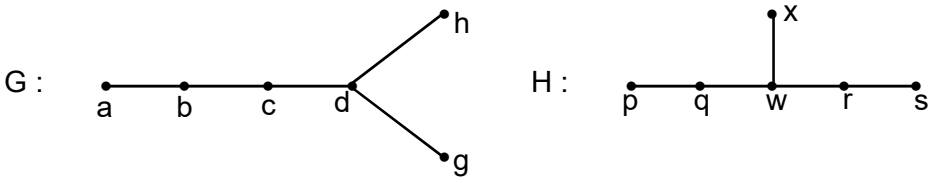


Fig 7.38

Here $V_1 = \{a, b, c, d, g, h\}$

$V_2 = \{p, q, r, s, w, x\}$

Let $f : V_1 \rightarrow V_2$ be a mapping defined by f(a) = p, f(b) = q, f(c) = r, f(d) = w, f(g) = s, f(h) = x

Clearly f is a one-one and onto mapping, i.e., a bijective mapping.

Here, number of vertices in G

= number of vertices in H = 6

number of edges in G

= number of edges in H = 5

Degree of a = 1, Degree of f(a) = p = 1

Degree of b = 2, Degree of f(b) = q = 2

Degree of c = 2, Degree of f(c) = r = 2

Degree of d = 3, Degree of f(d) = w = 3

Degree of g = 1, Degree of f(g) = s = 1

Degree of h= 1, Degree of f(h) = x = 1

Thus, we see that all the three conditions are satisfied. But the graphs are not isomorphic. Why?

b and c are adjacent in G, whereas f(b) = q and f(c) = r are not adjacent in H.

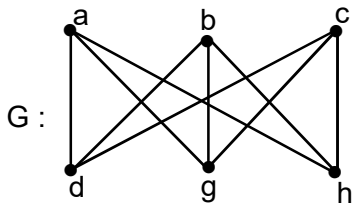
∴ f is not a graph isomorphism



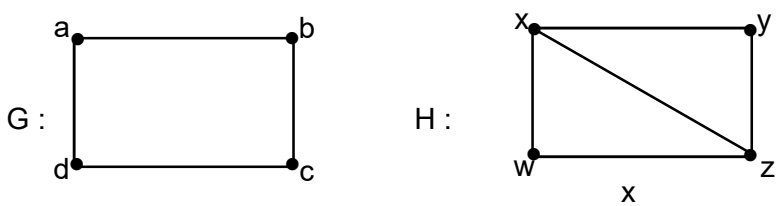
CHECK YOUR PROGRESS

Q 35: Examine if each of the following pairs of graphs is isomorphic or not.

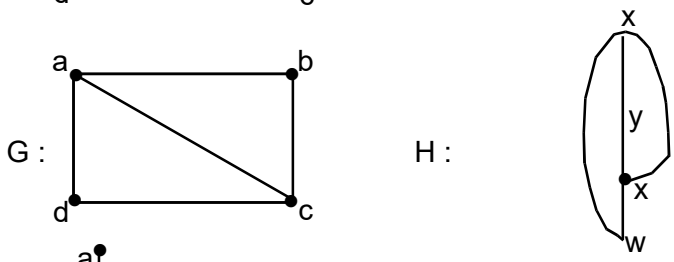
(i)



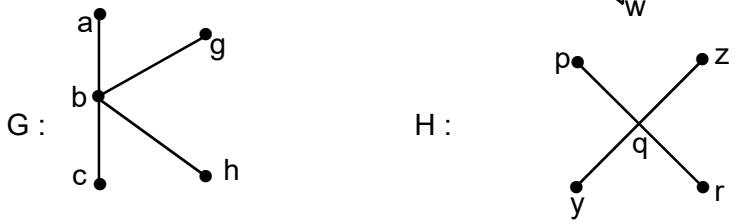
(ii)



(iii)



(iv)



(v)

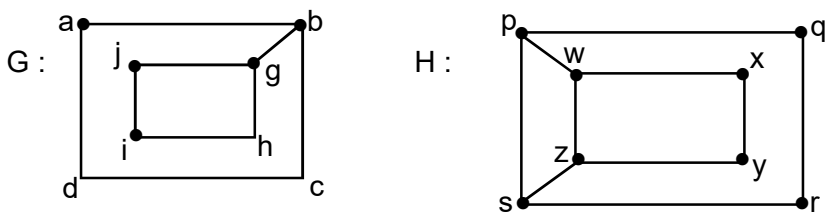


Fig 7.39

7.9 EULERIAN GRAPH AND HAMILTONIAN GRAPH

7.9.1 Eulerian Graph

We know that a trail is a walk in which no edge is repeated. A closed trail is a trail whose initial vertex and terminal vertex are the same. A closed trail is called a circuit.

A circuit in a graph that includes all the edges of the graph is called an Eulerian circuit.

A graph G is said to be Eulerian if G contains only one vertex and no edges or G has an Eulerian circuit.

Example 17 : Let us consider the graph given by Fig : 7.40

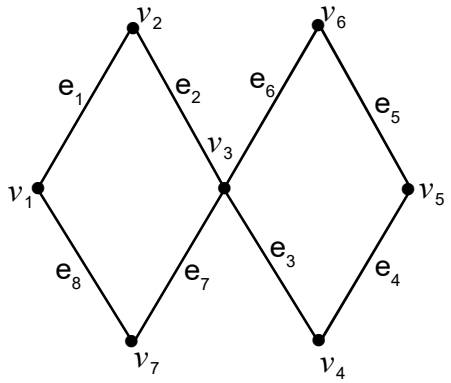


Fig 7.40

Clealy, the circuit

v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_3, e_7, v_7, e_8, v_1

is an Eulerian circuit

It begins at v_1, and ends at v_1.

It includes all the edges of the graph, and no edge is repeated. (Vertex is repeated.)

Therefore, the graph given by Fig 7.40 is an Eulerian graph.

Example 18 : Let us cousider the graph given by Fig 7.41.

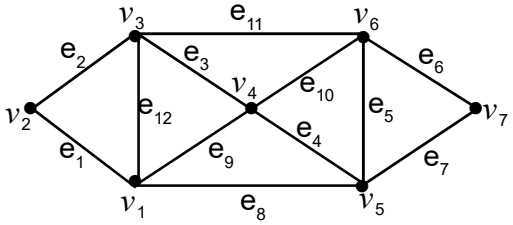


Fig 7.41

Clearly the circuit

$v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_5, e_8, v_1, e_9, v_4, e_{10}, v_6, e_{11}, v_3, e_{12}, v_1$ is an Eulerian circuit.

It begins at v_1, and ends at v_1.

It includes all the edges of the graph and no edge is repeated. (Vertex is repeated)

Therefore, the graph given by Fig 7.41 is an Eulerian graph.

Example 19 : Let us consider the graph given by Fig 7.42.

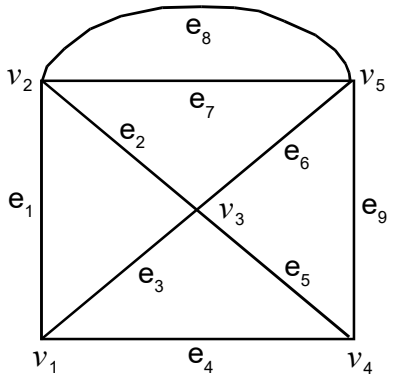


Fig 7.42

We consider the trail

$v_1, e_1, v_2, e_2, v_3, e_3, v_1, e_4, v_4, e_5, v_3, e_6, v_5, e_7, v_2, e_8, v_5, e_9, v_4$.

It begines at v_1, and ends at v_4.

It. includes all the edges of the graph and no edge is repeates. (Vertex is repeated.)

A trial containing all the edges of a graph is called an Eulerian trail. The trail given in Fig 7.42 is an Eulerian trail. Such a trail is also called traversable trail.

A traversable trial is finite and connected.

Theorem 7.11 : A finite connected graph is Eulerian if and only if each vertex has even degree.

Proof : Let G be a finite connected graph.

Let G be an Eulerian graph.

If G has only one vertex v, and no edges, then degree of v is zero, which is an even number.

Let G contain more than one vertex. Then G contains an Eulerian circuit $v_1, e_1, v_2, e_2, v_3, e_3 \ldots, e_{n-1}, v_n, e_n, v_{n+1}$, where $v_{n+1} = v_1$.

In this Eulerian circuit, the vertices $v_1, v_2, v_3, \ldots v_n$ may not be distinct. Some of the vertices may be repeated, but all the edges are distinct.

Clearly, the pair of sucessive edges e_1 and e_{i+1}, $1 \leq i \leq n-1$, contribute 2 to the degree of the vertex v_{i+1}. Thus, the degree of each of the vertices $v_2, v_3, \ldots, v_n$ is 2, which is an even number. Moreover, the vertex v_1, gets a contribution of 2 to its degree from the initial and terminal edges e_1 and e_n.

Thus, all the verticees are of even degree.

Conversely, let all the vertices of the graph G be of even degree.

Let G contain only one vertex. Let it be v. There may exist no loop or one loop or more than one loop, but finite number of loops at v. If there is no loop at v, then (v) is an Eulerian circuit of G. Suppose G has finite number of loops $e_1, e_2, \ldots, e_n$ $(n \geq 1)$ at v. Then $(v, e_1, v, e_2, \ldots, e_n, v)$ is an Eulerian circuit of G. Thus, G is an Eulerian graph.

Let G contain more than one vertex.

Let v be any vertex in G. We construct a walk H starting at v and going through the edges of G such that no edge is traversed more than once. Since every vertex of G is of even degree, we can exit from every vertex that we enter. Since v is of even degree, we will arrive at v when the traversing comes to an end. If this closed walk contains all the edges of G, then G is a Eulerian graph. If not, we remove from G all the edges in H, and obtain a graph K formed by the remaining edges. Clearly, every vertex of K is of even degree. Since G is connected, K must touch H at least at one vertex u. Starting from u, we construct a new walk in graph K. Since all the vertices of K are of even degree, the walk must terminate at vertex u. Now the walk K can be combined with H to form a new walk,

which starts and ends at vertex v. This argument can be repeated until we obtain an Eulerian circuit which traverses all the edges of G. Thus, G is an Eulerian graph.

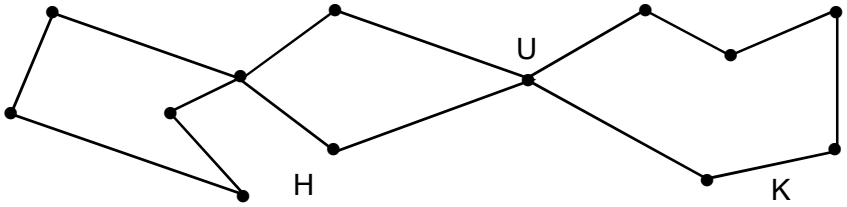


Fig 7.43

Example 17 : Examine if the complete graph K_5 is Eulerian.

Solutuon : We know that K_5 is a connected graph.

Again, the degree of each vertex of K_5 is (5–1) i.e. 4, which is an even number.

$\therefore$ K_5 is an Eulerian graph.

Example 18 : The graph given in Fig 7.44 is known as **Petersen graph,** after the name of Julius Peter Christian Petersen (1839-1910) who constructed this graph in 1898. The graph is drawn as a pentagon with a pentagram inside, with five spokes. The graph has 10 vertices, and 15 edges.

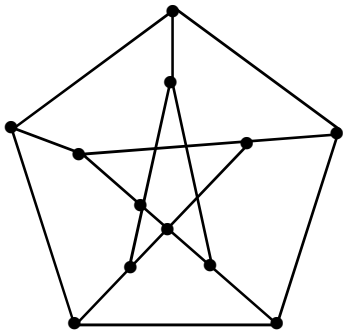


Fig 7.44

Each vertex of Petersen graph is of degree 3, which is an odd number. Therefore Petersen graph is not Eulerian.

Example 19: Konigsberg Bridge Problem

We have already stated the Konigsberg Bridge Problem in 7.2.

Two islands in the river pregel in the historic prussian city of Konigsberg (now Kaliningrad in Russia) were connected to each

other and the river banks by seven bridges as shown in Fig 7.2.

Let the islands be denoted by A, B; and the river banks be denoted by C, D; and the seven bridges be denoted by b_1, b_2, b_3, b_4, b_5, b_6, b_7. The problem was to start at any of the four land areas A, B, C, D; walk across each bridge exactly once; and return to the starting point. The swiss mathematician Leonhard Euler of the eighteen century converted the problem as a problem of graph theory and proved it to be impossible.

The graph of the above problem is shown in Fig 7.45.

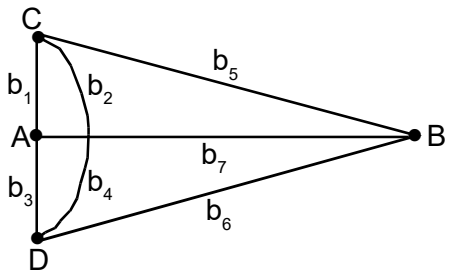


Fig 7.45

We may think of the two islands A, B and the river banks C, D as the vertices of the graph and edges as the bridges.

Now d(A) = 5, d(B) = 3, d(C) = 3, d(D) = 3

Thus, degree of each of the vertices is an odd number. Therefore, the graph is not Eulerian, i.e., the graph cannot be traversed completely in a single circular path.



LET US KNOW

A pentagram is a five-pointed star that is formed by drawing a continuous line in five straight segments.



CHECK YOUR PROGRESS

Q 36: Examine if the following graphs are Eularian

(i) the complete graph K_4

(ii) the complete bipartite graph $K_{2,3}$

(iii) the complete bipartite graph $K_{3,3}$

(iv) the graph of the tetrahedron

(v) the graph of the octahedron.

Q 37: Examine if the graph given in Fig 7.46 is Eulerian. If it is Eulerian, write down an Eulerian circuit.

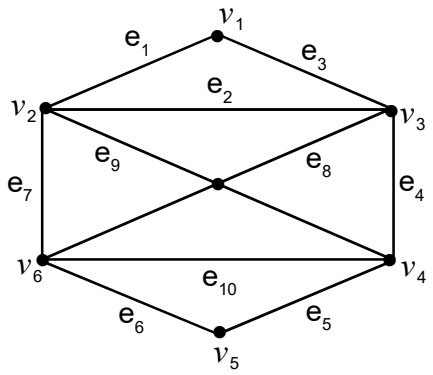


Fig 7.46

Q 38: For what value of n is the complete graph K_n on n vertices Eulerian?

Q 39: For what values of n, m is $K_{n, m}$ Eulerian?

7.9.2 Hamiltonian Graph

A Hamiltonian circuit in a graph G is a closed walk that visits every vertex in G exactly once, except the initial and the terminal vertices (which are one and the same) which appear twice. A graph containing a Hamiltonian circuit is called a Hamiltorian graph, after the name of the famous Irish mathematician Sir William Rowan Hamilton (1805-1865).

Note : 1. A complete graph K_n with more than two (n>2) vertices is Hamiltonian for an edge exists between any two vertices and a circuit can be formed by beginning at any vertex and by visiting the remaining vertices in any order.

2. A given graph may contain more than one Hamiltonian circuit.

3. An Eulerian circuit traverses every edge in a graph exactly once, whereas a Hamiltonian circuit visits each vertex in a graph exactly once.

Example 20: Let us consider the graph given in Fig 7.47

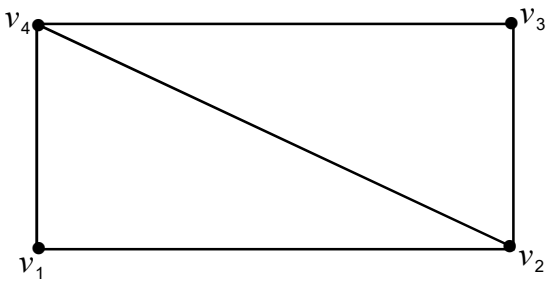


Fig 7.47

The graph contains a Hamiltonian circuit, viz.,

$$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$$

We note that all the vertices appear exactly once, except the initial and terminal vertices; but not all edges.



CHECK YOUR PROGRESS

Q 40: Show, by an example, that a graph may contain more than one Hamiltonian circuit.

Q 41: Give an example of a graph which is Hamiltonian as well as Eulerian.

Q 42: Give an example of a graph which is Eulerian, but not Hamiltonian.

Q 43: Give an example of a graph which is Hamiltonian, but not Eulerian.

Q 44: Give an example of a graph which contains an Eulerian circuit and a Hamiltonian circuit that are distinct.

Q 45: Give an example of a graph which is neither Eulerian nor Hamiltonian.

Q 46: Find the condition such that the complete bipartite graph $K_{m,n}$ has a Hamiltonian circuit.

Q 47: Examine if the graph of octahedron is a Hamiltonian graph.

Q 48: Examine if the graph of dodecahedron is a Hamiltonian graph.



7.10 LET US SUM UP

- A graph G = (V, E) consists of two things, viz.
  (i) a nonempty set V, called the set of vertices or nodes or points.
  (ii) a set E (may be empty), called the set of edges such that there is a mapping from the set E to a set of pairs of elements of V.
  If an edge $e \in E$ is associated with a pair (u, v), where u, $v \in V$, then u and v are said to be adjacent. u and v are called the endpoints of e, and e is said to join or connect u and v.
- An edge of a graph that joins a vertex to itself is called a loop.
- If in a graph certain pairs of vertices are joined by more than one edge, then such edges are called parallel edges.
- A graph that does not cordain any loop, and does not contain any parallel edges is called a simple graph.
- A simple graph G is said to be complete (or universal) if there is exactly one edge between each pair of distinct vertices.
- If every vertex of a simple graph G has the same degree, then the graph is called a regular graph.
- A graph H = (V', E') is called a subgraph of a graph G = (V, E) if $V' \subseteq V$, $E' \subseteq E$. (V' is a nonempty subset of V).
- A graph G is connected if there is a path between any two of its vertices; otherwise the graph is called a disconnected graph.
- A circuit in a graph that includes all the edges of the graph is called an Eulerian circuit. A graph containing only one vertex and no edges or an Eulerian circuit is called an Eulerian graph.
- An Eulerian circuit traverses every edge in a graph exactly once, whereas a Hamiltonian circuit visits each vertex exactly once.
- A graph containing a Hamiltonian circuit is called a Hamiltonian graph.



7.11 FURTHER READINGS

1) **Graph Theory** by Frank Harary (BNarosa Publishing House).

2) **Introduction to Graph Theory** by Robin J. Wilson (Addison Wesley Longman Limited).

3) **Discrete Mathematics with Graph Theory and Combinatonics** by T Veerarajan (Tata McGraw - Hill Publishing Company Limited).



7.12 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1:

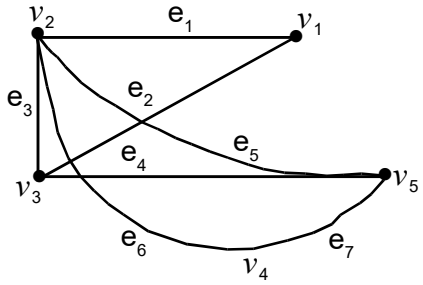


Fig 7.48

Ans to Q No 2: (i) Let V = $\{v_1, v_2, v_3\}$

E = $\{e_1, e_2, e_3\}$

such that e_1 is associated with (e_1, e_2), e_2 is associated with (v_2, v_3), e_3 is associated with (v_2, v_3).

(ii) Let V = $\{v_1, v_2, v_3, v_4\}$

E = $\{e_1, e_2, e_3, e_4, e_5, e_6\}$

Such that e_1 is associated with (v_1, v_2), e_2 with (v_2, v_2), e_3 with (v_2, v_3), e_4 with (e_3, e_4), e_5 with (v_1, v_3), e_6 with (v_1, v_3).

Ans to Q No 3: Let V = $\{v_1, v_2, v_3\}$

E = $\{e_1, e_2, e_3\}$

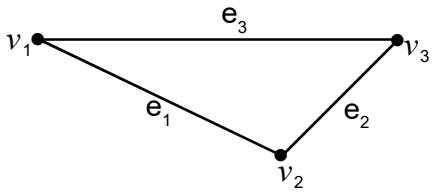


Fig 7.49

Such that e_1 is associated with (v_1, v_2), e_2 with (v_1, v_3), e_3 with (v_1, v_3).

The graph has neither loop nor parallel edges.

$\therefore$ G = (V, E) is a simple graph.

Ans to Q No 4: Let V = {v_1, v_2, v_3}

E = {e_1, e_2, e_3, e_4}

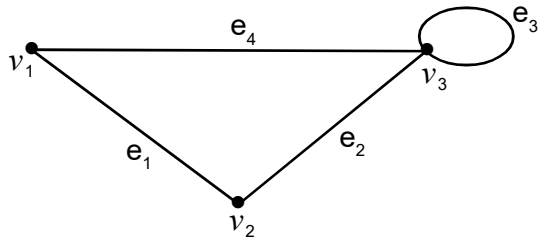


Fig 7.50

Such that e_1 is associated with (v_1, v_2), e_2 is associated with (v_2, v_3), e_3 is associated with (v_3, v_3), e_4 is associated with (v_3, v_1).

The graph has a loop e_3 from v_2 to v_3. It has no parallel edges.

Thus G = (V, E) is a graph containing a loop, but not containing parallel edges.

Ans to Q No 5: Let V = {v_1, v_2, v_3}

E = {e_1, e_2, e_3, e_4}

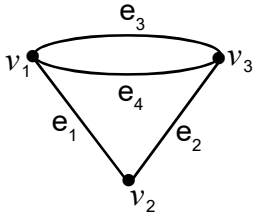


Fig 7.51

such that e_1 is associated with (v_1, v_2), e_2 is associated with (v_2, v_3), e_3 with (v_3, v_1), e_4 with (v_3, v_1).

The graph has no loop, but parallel edges e_3 and e_4.

Thus G = (V, E) is a graph containing parallel edges, but not a loop.

Ans to Q No 6: Let $V = \{v_1, v_2, v_3\}$

$E = \{e_1, e_2, e_3, e_4, e_5\}$

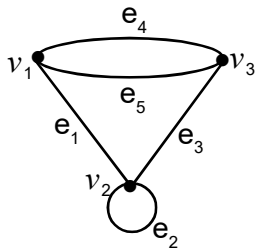


Fig 7.52

such that e_1 is associated with (v_1, v_2), e_2 with (v_2, v_2), e_3 with (v_2, v_3), e_4 with (v_3, v_1), e_5 with (v_3, v_1).

The graph has a loop e_2 from v_2 to v_2. Moreover it has parallel edges e_4, and e_5.

Thus, G = (V, E) is a graph containing a loop and parallel edges.

Ans to Q No 7: Number of vertices = 6

Number of edges = 9

$d(v_1) = 2$, $d(v_2) = 4$, $d(v_3) = 3$, $d(v_4) = 1$, $d(v_5) = 4$, $d(v_6) = 4$

We have $d(v_4) = 1$. $\therefore v_4$ is a pendant vertex.

Sum of degrees of the vertices

$= d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) + d(v_6)$

$= 2 + 4 + 3 + 1 + 4 + 4 = 18$

= 2 x 9 = twice the number of edges.

(ii) Number of vertices = 6

Number of edges = 10

$d(v_1) = 5$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 1$

$d(v_5) = 2 + 1 + 1 + 1 = 5$, $d(v_6) = 3$

[Loop contributes 2]

We have $d(v_4) = 1$ $\therefore v_4$ is a pendant vertex.

sum of degrees of the vertices

$= d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) + d(v_6)$

$= 5 + 3 + 3 + 1 + 5 + 3 = 20$

= 2 x 10 = twice the number of edges.

Ans to Q No 8: Sum of degrees of the vertices

= 5 + 5 + 5 + 4 + 2 = 21, an odd number.

We know that the sum of the degrees of all vertices of a graph is an even number.

∴ there cannot be a graph with 5 vertices having 5, 5, 5, 4, 2 as degrees of vertices.

Ans to Q No 9: Number of edges = 16

Degre of each vertex = 4

Let the number of vertices be n.

∴ sum of degrees of vertices = 4n

We know that

sum of degrees of vertices = twice the number of edges.

∴ 4n = 2 x 16

∴ n = 8

∴ the required number of vertices is 8.

Ans to Q No 10: Number of edges = 21

Number of vertices of degree 4 each = 3

Degrees of the remaining vertices = 2

Let the number of vertices be n.

∴ sum of degrees of vertices

= 3 x 4 +2 (n–3)= 12 + 2n – 6 = 2n + 6

We know that

sum of degrees of vertices = twice the number of edges.

∴ 2n + 6 = 2 x 21

or 2n = 42 – 6 = 36

∴ n = 18

∴ total number of vertices = 18

Ans to Q No 11: Number of edges = 35

Number of vertices of degree 5 each = 4

Number of vertices of degree 4 each = 5

Number of vertices of degree 3 each = 4

Degrees of remaining vertices = 2

Let the number of vertices be n.

∴ Number of vertices of degree 2 each

= n – (4+5+4) = n – 13

∴ sum of degrees of vertices

= 4x5 + 5x4 + 4x3 + 2(n–13)

= 20 + 20 + 12 + 2n – 26 = 2n + 26

We know that sum of degrees of vertices = twice the number of edges.

∴ 2n + 26 = 2 x 35

or 2n = 70 – 26 = 44

∴ n = 22

∴ total number of vertices = 22

Number of vertices with degree 2 = 22 – 13 = 9

Ans to Q No 12:

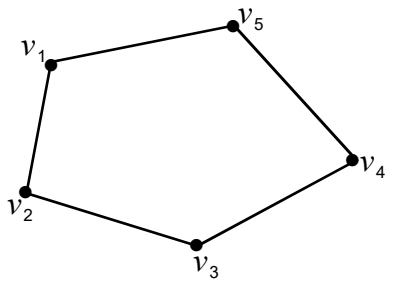


Fig 7.53

Clearly the graph is simple. It has naither loops nor parallel edges. It has 5 vertices.

d(v_1) = d(v_2) = d(v_3) = d(v_4) = d(v_5) = 2.

Ans to Q No 13: (i)

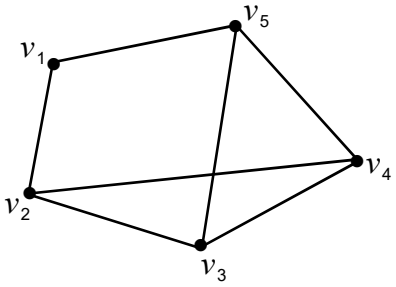


Fig 7.54

Clearly the above graph is a simple graph. It has neither loops nor parallel edges. It has 5 vertices.

d(v_1) = 2, d(v_2) = d(v_3) = d(v_4) = d(v_5) = 3.

(ii)

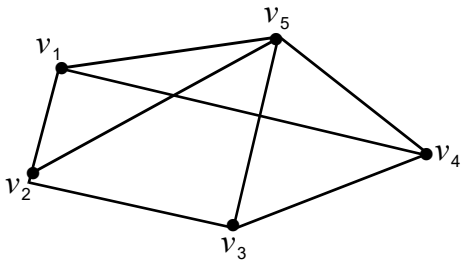


Fig 7.55

Clearly the above graph is a simple graph. It has neither loops nor parallel edges. It has 5 vertices.

$d(v_1) = d(v_2) = d(v_3) = d(v_4) = 3$, $d(v_5) = 4$

Ans to Q No 14:

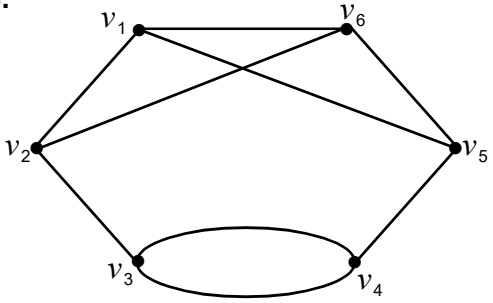


Fig 7.56

The graph has 6 vertices. It has parallel edges. So it is not simple.

$d(v_1) = d(v_2) = d(v_3) = d(v_4) = d(v_5) = d(v_6) = 3$

Ans to Q No 15: Let the number of edges be n.

We know that

sum of degrees of vertices = twice the number of edges.

$\therefore$ 4 + 1 + 2 + 2 + 3 + 5 + 5 = 2n

or 2n = 22

$\therefore$ n = 11

$\therefore$ total number of edges = 11

Ans to Q No 16: Number of vertices = 4

Number of edges = 6

$d(v_1) = d(v_2) = d(v_3) = d(v_4) = 3$

Number of edges = 6 = 3 x 2

= a multiple of degree of each vertex.

Ans to Q No 17: We know that the number of odd degree vertices is even.

Let the vertices be $v_1, v_2, v_3, \ldots, v_{2n}$

We have

$d(v_1) = d(v_2) = d(v_3) = \ldots\ldots\ldots d(v_{2n}) = k$, an odd number.

Let the number of edges be x.

$\therefore d(v_1) + d(v_2) + d(v_3) + \ldots\ldots\ldots + d(v_{2n}) = 2x$

or $k + k + k + \ldots + k = 2x$

or $2nk = 2x$

$\therefore x = nk$

$\therefore$ number of edges is a multiple of k, which is an odd number.

Ans to Q No 18: Please see Theorem 2.

Ans to Q No 19: Let G be a simple graph with n vertices. Since G is a simple graph, it has no loops and parallel edges.

Let u be a vertex of G. Then u can be adjacent to the remaining (n–1) vertices. Thus, the degree of u cannot exceed (n–1).

Ans to Q No 20: If possible, let there be a simple graph with 7 vertices having degrees 1, 3, 3, 4, 5, 6, 6.

There are two vertices each of degree 6. Therefore, each of these two vertices is adjacent to every other vertex. Therefore, the degree of each vertex is at least 2. But there is a vertex with degree 1, which is a contradiction.

Thus, there cannot be a simple graph with 7 vertices having degrees 1, 3, 3, 4, 5, 6, 6.

Ans to Q No 21: Do yourself.

Ans to Q No 22: If possible, let there be a simple graph with 5 vertices having degrees 2, 2, 4, 4, 4.

There are three vertices each of degree 4. Therefore, each of these three vertices is adjacent to every other vertex. Therefore, the degree of each vertex is at least 3. But there is a vertex with degree 2, which is a contradiction.

Thus, there cannot be a simple graph with 5 vertices having degrees 2, 2, 4, 4, 4.

Ans to Q No 23: Let G be a (p, q) graph.

$\therefore$ G has p vertices, and q edges.

Now n+ m = p (1)

Again, sum of the degrees of vertices = twice the number of edges.

$\therefore$ kn + (k+1)m = 2q

or, kn + (k+1) (p–n) = 2q, from (1)

or, kn + kp – kn + p – n = 2q

or, kp + p – 2q = n

i.e. n = (k+1)p – 2q

Ans to Q No 24: (a) From Fig 7.24

id (v_1) = 0, id (v_2) = 1, id (v_3) = 1

od (v_1) = 0, od (v_2) = 1, od (v_3) = 1

sum of the indegrees = 0 + 1 + 1 = 2

sum of the outdegrees = 1 + 1 + 0 = 2

number of edges = 2

Thus, sum of the indegrees

= sum of the outdegrees

= number of edges.

(b) From Fig 7.25

id (v_1) = 2, id (v_2) = 1, id (v_3) = 2, id (v_4) = 0, id (v_5) = 2, id (v_6) = 1

od (v_1) = 3, od (v_2) = 1, od (v_3)=3, od (v_4)=0, od (v_5) = 1, od (v_6) = 1

sum of the indegrees = 2 + 1 + 2 + 0 + 2 + 1 = 8

sum of the outdegrees = 3 + 1 + 1 + 0 + 1 + 2 = 8

number of edges = 8

Thus, sum of the indegrees

= sum of the outdegrees

= number of edges.

(c) From Fig 7.26

id (v_1) = 0, id (v_2) = 2, id (v_3) = 1, id (v_4) = 0, id (v_5) = 2

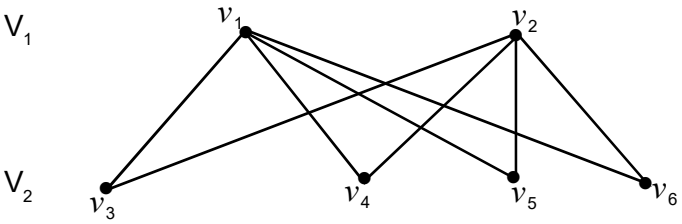
od (v_1) = 2, od (v_2) = 0, od (v_3) = 1, od(v_4) = 2, od (v_5) = 0

sum of the indegrees

= sum of the outdegrees

= number of edges = 5

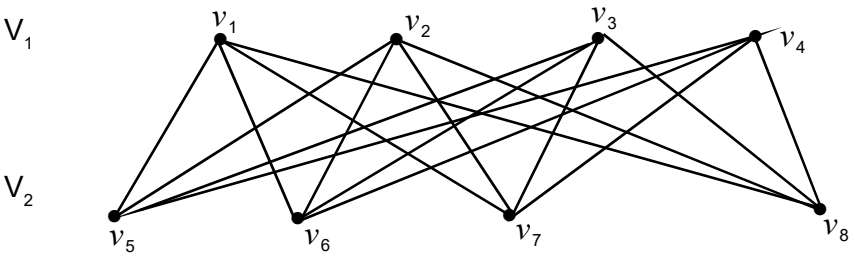
Ans to Q No 25: (a)



$K_{2,4}$ graph; vertices 6, edges 8

Fig 7.57

(b)



$K_{4,4}$ graph; vertices 8, edges 16.

Fig 7.58

Ans to Q No 26: (a) Clearly the graph given in Fig 7.33(a) is a subgraph of the graph given in Fig 7.33(b).

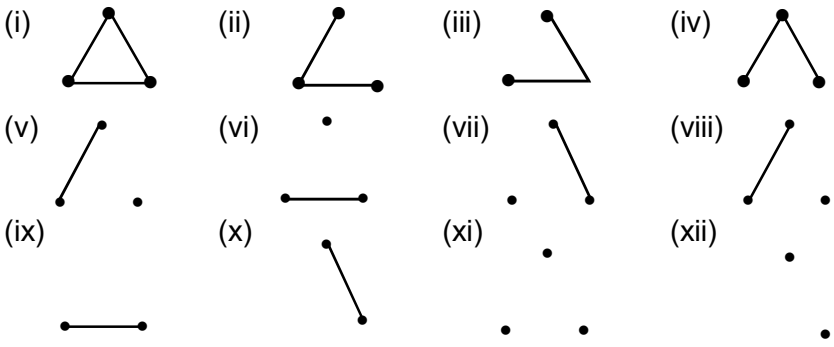
(b) The graph given in Fig 7.33 (a) is not a subgraph of the graph given in Fig 7.33(c). The graph given in Fig 7.33(c) does not contain any 'triangle'.

Ans to Q No 27: K_2 has 4 subgraphs as shown below

(i) , (ii) , (iii) , (iv) ,

Fig 7.59

Ans to Q No 28: K_3 has 17 subgraphs as shown below



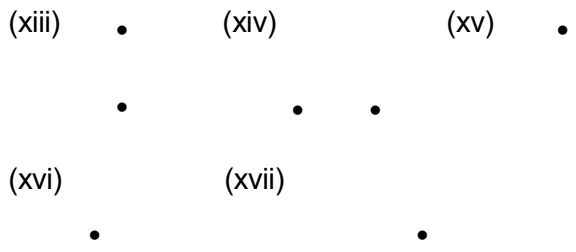


Fig 7.60

Ans to Q No 29: (a) We take u_1. We see that u_1 is connected to each of the vertices u_2, u_3, u_4.

$\therefore$ the graph is connected.

(b) u_1 is not connected to u_2. $\therefore$ the graph is not connected.

(c) u_3 is not connected to u_4. $\therefore$ the graph is not connected.

(d) We see that u_1 is connected to each of the vertices u_2, u_3, u_4, u_5, u_6, u_7. $\therefore$ the graph is connected.

(e) We see that u_1 is connected to each of the vertices u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9. $\therefore$ the graph is connected.

Ans to Q No 30: We take the vertex v_1. We see that v_1 is connected to each of the vertices v_2, v_3, v_4, v_5, v_9.

$\therefore$ one of the connected components is $\{v_1, v_2, v_3, v_4, v_5, v_9\}$

Now we take the vertex v_6 that is not included in the above component.

We see that v_6 is connected to each of the vertices v_7, v_8.

$\therefore$ the other component is $\{v_6, v_7, v_8\}$.

Ans to Q No 31: We know that if a simple graph G with n vertices has more than $\frac{(n-1)(n-2)}{2}$, then G is connected.

Here n = 6

$\therefore$ G must have more than

$\frac{(6-1)\times(6-2)}{2}$ i.e., 10 edges.

Here G has 11 (>10) edges.

$\therefore$ G is connected.

Ans to Q No 32: Let us consider the complete graph K_3 (Fig 7.61 (a)). Clearly K_3 is connected.

We delete the edges e_1, and e_2. We see that the subgraph obtained

by deleting the edges e_1, and e_2 is not connected (Fig 7.61 (b))

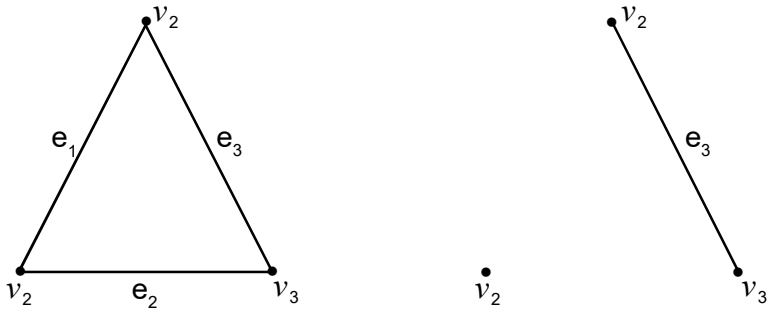


Fig 7.61

Ans to Q No 33: Let G be a connected graph with at least 2 vertices.

Let the number of vertices be n. Clearly $n \geq 2$.

Since G is connected, G has no isolated vertices. Therefore, there is no vertex of degree zero.

If possible, let G have no vertex of degree 1.

$\therefore$ the degree of each vertex is at least 2.

$\therefore$ the sum of the degrees of the vertices is at least 2n.

We know that the sum of the degrees of vertices is twice the number of edges.

$\therefore$ the number of edges is at least n, which is a contradiction.

$\therefore$ our assumption is wrong.

So, G has at least one vertex of degree 1.

Ans to Q No 34: If possible, let G be not connected.

Then G can be partitioned into connected components $C_1, C_2, \ldots, C_k$, where $n \geq 2$.

It is given that degree of each vertex is at least n. Moreover the graph is simple. Therefore, each vertex has at least n adjacent vertices.

Therefore, each component contains at least (n+1) vertices.

Therefore, the number of vertices is at least $k(n+1) \geq 2(n+1) > 2n$, which is a contradication since G has at most 2n vertices.

$\therefore$ our assumption is wrong.

Thus, G is connected.

Ans to Q No 35: (i) Let $V_1 = \{a, b, c, d, g, h\}$

$V_2 = \{p, q, r, x, y, z\}$

Let $f : V_1 \rightarrow V_2$ be a mapping defined by

f(a) = p, f(b) = q, f(c) = r,

f(d) = x, f(g) = y, f(h) = z.

Clearly, f is one-one and onto, i.e., f is a bijective mapping.

We note that

1. a and d are adjacent in G; and f(a) = p and f(d) = x are adjacent in H.
2. a and g are adjacent in G; and f(a) = p and f(g) = y are adjacent in H.
3. a and h are adjacent in G; and f(a) = p and f(h) = z are adjacent in H.
4. b and d are adjacent in G; and f(b) = q and f(d) = x are adjacent in H.
5. b and g are adjacent in G; and f(b) = q, and f(g) = y are adjacent in H.
6. b an h are adjacent in G; and f(b) = q and f(h) = z are adjacent in H.
7. c and d are adjacent in G; and f(c) = r and f(d) = x are adjacent in H.
8. c and g are adjacent in G; and f(c) = r and f(g) = y are adjacent in H.
9. c and h are adjacent in G; and f(c) = r and f(h) = z are adjacent in H.

Thus, we see that f preserves adjacency of the vertices.

$\therefore$ f is a graph isomorphism.

i.e., $G \cong H$.

(ii) The number of edges in G is 4, whereas the number of edges in H is 5.

$\therefore$ G and H are not isomorphic.

(iii) Isomorphic

Try yourself.

(iv) Isomorphic

Try yourself.

(v) Isomorphic

Try yourself.

Ans to Q No 36: (i) K_4 is a connected graph.

Degree of each vertex of K_4 is (4–1) i.e. 3, which is an odd number.

$\therefore$ K_4 is not an Eulerian graph.

(ii) Let us consider the complete bipartite graph $K_{2,3}$ (Fig 7.20).

$d(v_1) = 3$, which is an odd number.

$\therefore$ the graph is not Eulerian.

(iii) Let us consider the complete bipartite graph $K_{3,3}$ (Fig 7.21)

Each vertex is of degree 3, which is an odd number.

$\therefore$ the graph is not Eulerian.

(iv) the graph of the tetrahedron is shown in Fig 7.62.

It has 4 vertices, and 6 edges. Each of the vertices is of degree 3, which is an odd number.

$\therefore$ the graph is not Eulerian.

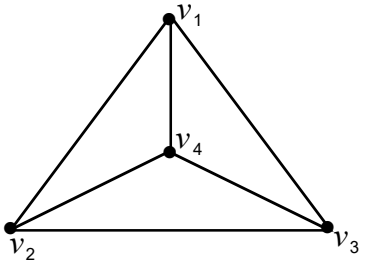


Fig 7.62

(v) The graph of the octahedron is shown in Fig 7.63. It has 6 vertices and 12 edges.

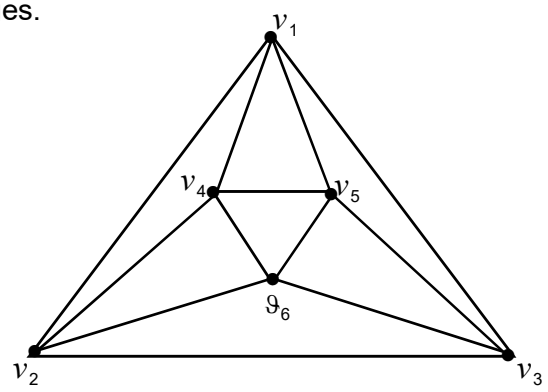


Fig 7.63

Each of the vertices is of degree 4, which is an even number. Therefore, the graph is Eulerian.

An Eulerian circuit is

$v_1 \to v_2 \to v_3 \to v_6 \to v_2 \to v_4 \to v_1 \to v_5 \to v_4 \to v_6 \to v_5 \to v_3 \to v_1$

It begins at v_1, and ends at v_1.

It includes all the edges of the graph and no edge is repeated. (vertex is repeated)

Ans to Q No 37: d(v_1)=2, d(v_2)=4, d(v_3)=4, d(v_4)=4, d(v_5)=2, d(v_6)=4

Each of the vertices is of even degree, Therefore, the graph is Eulerian.

An Eulerian circuit is

$v_1 \to v_3 \to v_4 \to v_5 \to v_6 \to v_4 \to v_2 \to v_3 \to v_6 \to v_2 \to v_1$

It begins at v_1, and ends at v_1.

It includes all the edges of the graph and no edge is repeated. (vertex is repeated)

Ans to Q No 38: We know that K_n is an (n–1) regular graph. Therefore, it is Eulerian if (n–1) is even, i.e., if n is odd.

Ans to Q No 39: We know that $K_{n, m}$ has n vertices of degree m, and m vertices of degree n.

$\therefore$ the graph of $K_{n, m}$ is Eulerian if both n and m are even.

Ans to Q No 40: Let us consider the graph of the octahedron (Fig 7.63)

A Hamiltonian circuit is as follows

$v_1 \to v_4 \to v_2 \to v_6 \to v_5 \to v_3 \to v_1$

Another Hamiltonian circuit is as follows.

$v_1 \to v_2 \to v_4 \to v_5 \to v_6 \to v_3 \to v_1$

$\therefore$ the graph is Hamiltonian.

Another example

Let us consider the complete bipartite graph $K_{3, 3}$ (Fig 7.21)

A Hamiltonian circuit is as follows.

$v_1 \to v_4 \to v_2 \to v_5 \to v_3 \to v_6 \to v_1$

Another Hamiltonian circuit is as follows.

$v_1 \to v_5 \to v_3 \to v_6 \to v_2 \to v_4 \to v_1$

$\therefore$ the graph is Hamiltonian.

Ans to Q No 41: Let us consider the complete bipartite graph $K_{2,2}$

(Fig 7.64)

Let us consider the circuit $v_1, e_1, v_3, e_2, v_2, e_4, v_4, e_3, v_1$

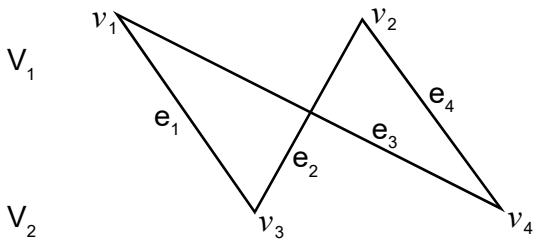


Fig 7.64

Clearly the above circuit is Hamiltonian as well as Eulerian.

$\therefore$ the graph is Hamiltonian as well as Eulerian.

Ans to Q No 42: Let us consider he graph given in Fig 7.65

We have

$d(v_1) = 2$, $d(v_2) = 2$, $d(v_3) = 4$, $d(v_4) = 2$, $d(v_5) = 2$

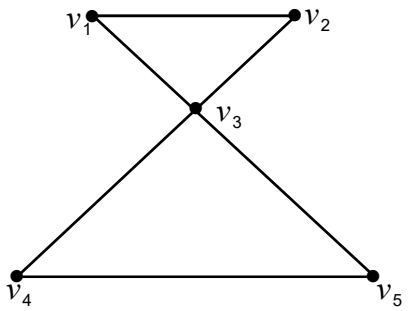


Fig 7.65

Thus, each vertex is of even degree.

$\therefore$ the graph is Eulerian

Clearly, we see that there is no Hamiltonian circuit. Vertex v_3 will be repeated.

Ans to Q No 43: Let us consider the graph given in Fig 7.66.

The graph is Hamiltonian. A Hamiltonian circuit is as follows.

$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_6 \rightarrow v_1$

$\therefore$ the graph is not Eulerian,

as $d(v_2) = 3$, $d(v_5) = 3$.

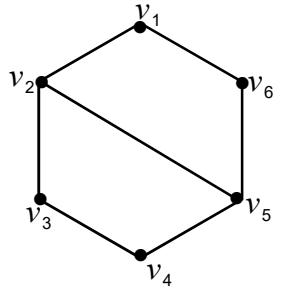


Fig 7.66

Ans to Q No 44: Let us consider the graph given in Fig 7.67.

An Eulerian circuit is as follows.

v_1, e_1, v_2, e_2, v_3, e_6, v_1, e_5, v_3, e_3, v_4, e_4, v_1.

A Hamiltonian circuit is as follows. $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_1$.

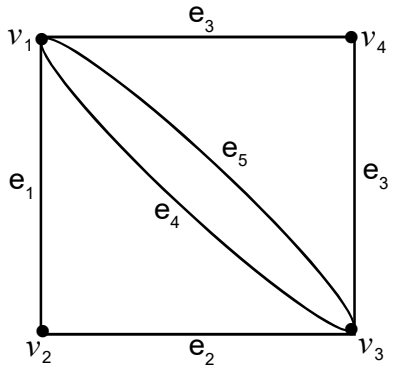


Fig 7.67

Ans to Q No 45: Let us consider the graph given in Fig 7.68.

The graph is not Eulerian as d(v_2) = 3, d(v_4) = 3.

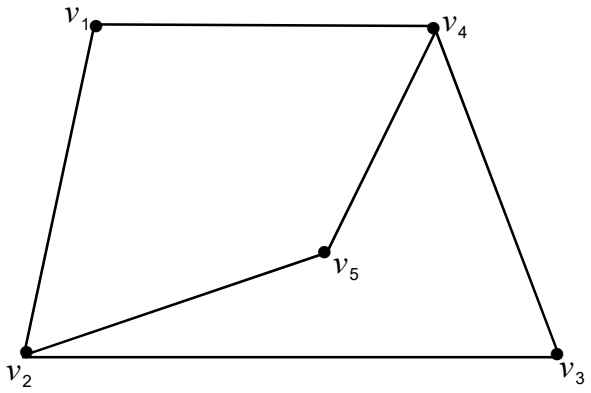


Fig 7.68

Again no circuit passes through each of the vertices exactly once.

$\therefore$ the graph is not Hamiltonian.

Ans to Q No 46: The vertex set of $K_{m, n}$ can be partitioned into two subsets V_1 and V_2. V_1 contains m vertices, V_2 contains n vertices. Each edge in $K_{m, n}$ joins a vertex in V_1 to a vertex in V_2. Since Hamiltonian circuit is a closed walk that traverses each vertex of the graph exactly once, therefore Hamiltonian circuit in $K_{m, n}$ exists only when m = n and m = $n \geq 2$.

Ans to Q No 47: See Ex 40

Ans to Q No 48: Let us consider the graph given in Fig 7.69.

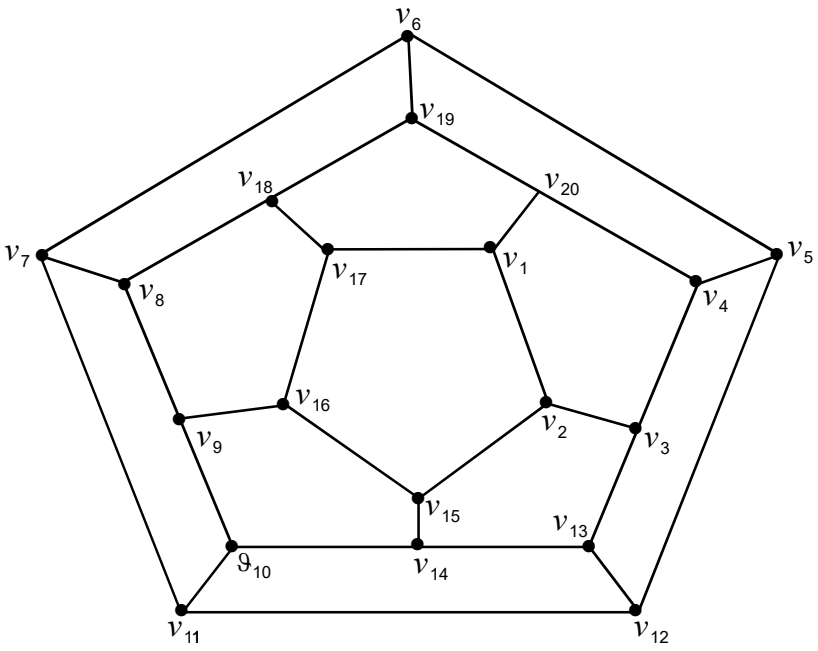


Fig 7.69

It is a dodecahedron. It has 20 vertices and 30 edges.

A Hamiltonian circuit is as follows.

$v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_6 \rightarrow v_7 \rightarrow v_8 \rightarrow v_9 \rightarrow v_{10} \rightarrow v_{11} \rightarrow$
$v_{12} \rightarrow v_{13} \rightarrow v_{14} \rightarrow v_{15} \rightarrow v_{16} \rightarrow v_{17} \rightarrow v_{18} \rightarrow v_{19} \rightarrow v_{20} \rightarrow v_{11}$.

$\therefore$ the graph is a Hamiltonian graph.



7.13 MODEL QUESTIONS

Q 1: Define (a) simple graph, (b) multigraph, (c) pseudograph, and give an example of each.

Q 2: Define a complete graph and give an example. Can a complete graph be a regular graph? Justify your answer.

Q 3: Define (a) a bipartite graph, (b) a complete bipartite graph, and give an example of each.

Q 4: Prove that the sum of the degrees of all the vertices of a graph is twice the number of edges.

Q 5: Prove that the number of edges in a bipartite graph with n vertices is at most $\frac{n^2}{4}$.

Q 6: State Konigsberg Bridge Problem. Represent the problem with the help of a graph. Examine if the problem has a solution.

Q 7: Prove that a finite connected graph is Eulerian if and only if each vertex has even degree.

*** ***** ***

UNIT 8 : TREES

UNIT STRUCTURE

8.1 Learning Objectives

8.2 Introduction

8.3 Trees

- 8.3.1 Properties of a Tree
- 8.3.2 Distance and Centres in a Tree
- 8.3.3 Rooted and Binary Trees

8.4 Counting Trees

8.5 Spanning Trees

8.6 Fundamental Circuits

8.7 Spanning Trees in a Weighted Graph

8.8 Connectivity and Separability

- 8.8.1 Cutset
- 8.8.2 Edge-Connectivity
- 8.8.3 Cut Vertex-Set
- 8.8.4 Vertex-Connectivity
- 8.8.5 Separable Graph
- 8.8.6 Cut-Vertex

8.9 Flow Network

8.10 Matrix Representation of Graphs

- 8.10.1 Adjacency Matrix
- 8.10.2 Incidence Matrix
- 8.10.3 Path Matrix
- 8.10.4 Cutset Matrix
- 8.10.5 Circuit Matrix

8.11 Let Us Sum Up

8.12 Further Readings

8.13 Answers To Check Your Progress

8.14 Model Questions

8.1 LEARNING OBJECTIVES

After going through this unit, you will able to know

- trees, properties of trees
- rooted ,and binary trees
- connectivity and separability
- matrix representation of graphs.

8.2 INTRODUCTION

The concept of tree in graph theory was developed by the German physicist and mathematician Gustav Robert Kirchhoff (1824-1887) in connection with his work on electric networks, and by the British mathematician Arthur cayley (1821-1895) in connection with his work on the enumeration of chemical molecules. Nowadays trees are used in many areas of knowledge including linguistics. Again matrix representation of a graph has several advantages. In this unit we will study trees, properties of trees, and related topics. Also we will study matrix representation of graphs,– incidence matrix, adjacency matrix etc.

8.3 TREES

The term ‘tree’ was coined by Arthur Cayley in 1857.

A graph having no cycles is called acyclic.

A tree is a connected acyclic graph.

A graph which does not contain any cycle is called a forest. Thus the components of a forest are trees.

> **Note :** Loops and parallel edges form cycles. Therefore, a tree must be a simple graph.

Example 1: Let us consider the graphs given in Fig 8.1

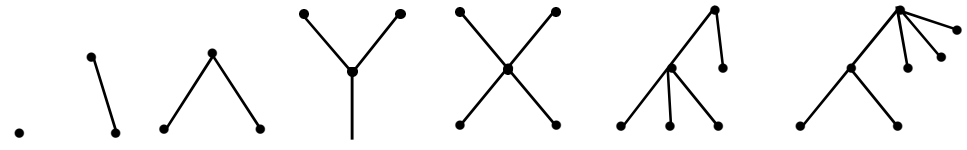


Fig 8.1

Each of the graphs is a connected acyclic graph. Therefore, each of the graphs is a tree.

The graph 8.1 (a) has 1 vertex and no (zero = 1 – 1) edge.

The graph 8.1 (b) has 2 vertices and 1 (= 2–1) edge.

The graph 8.1 (c) has 3 vertices and 2 (=3–1) edges.

The graph 8.1 (d) has 4 vertices and 3 (=4–1) edges.

The graph 8.1 (e) has 5 vertices and 4 (=5–1) edges.

The graph 8.1 (f) has 6 vertices and 5 (=6–1) edges.

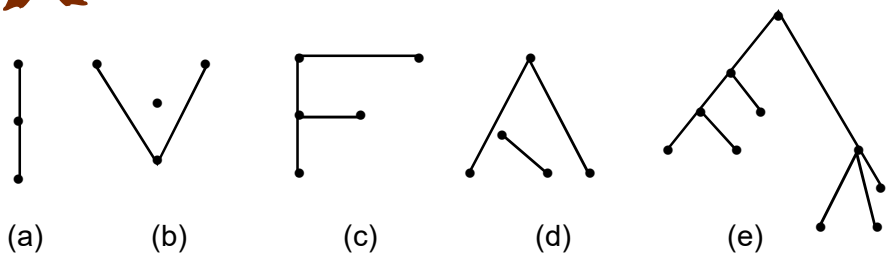
The graph 8.1 (g) has 7 vertices and 6 (=7–1) edges.

A tree with n vertices has (n–1) edges.



CHECK YOUR PROGRESS

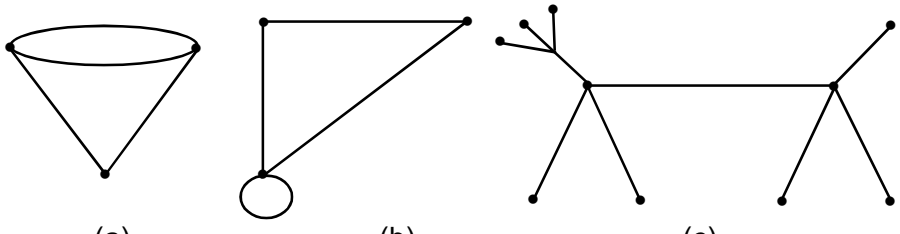
Q 1: Which of the following graphs are trees and which are not? Justify your answer.



(a) (b) (c) (d) (e)

Fig 8.2

Q 2: Which of the following graphs are trees and which are not ? Justify your answer.



(a) (b) (c)

Fig 8.3

8.3.1 Properties of a Tree

A tree has several interesting properties. The following theorem lists some simple properties of trees.

Theorem 8.1 : Let T be a graph with n vertices. Then the following statements are equivalent.

(i) T is a tree.

(ii) T is acyclic and has (n–1) edges.

(iii) T is connected and has (n–1) edges.

(iv) T is connected and every edge is a bridge.

(v) Any two vertices of T are connected by exactly one path.

Proof : If n = 1, there is nothing to prove. We assume that $n \geq 2$.

We prove that

(i) $\Rightarrow$ (ii) , (ii) $\Rightarrow$ (iii) , (iii) $\Rightarrow$ (iv) , (iv) $\Rightarrow$ (v) , (v) $\Rightarrow$ (i) . Then all the statements will be equivalent.

(i) $\Rightarrow$ (ii) :

T is a tree. (given)

$\therefore$ T does not have cycles, i.e., T is acyclic. Now we prove that the number of edges of T is (n–1).

If n = 1, the number of edges is 0 (=1–1).

$\therefore$ the result is true for n = 1.

We assume that the result is true for n = k, where k is a positive integer and 1 < k < n.

$\therefore$ every tree with k vertices has (k–1) edges.

Now we remove any edge of T. Since T is acyclic, removal of an edge disconnects T into two graphs, say T_1 and T_2, where T_1 and T_2 are connected and acyclic.

$\therefore$ T_1 and T_2 are trees.

Let the vertices in T_1 and T_2 be n_1 and n_2 respectively.

$\therefore$ $n_1 + n_2 = n$

Also $n_1 < n$, $n_2 < n$.

$\therefore$ by our assumption, the number of edges in T_1 and T_2 are $(n_1–1)$, and $(n_2–1)$ respectively.

$\therefore$ the total number of edges in T_1 and T_2 is $(n_1–1) + (n_2 –1)$, i. e., $n_1+n_2–2$.

This number alongwith the edge which has been removed gives the total number of edges in the whole graph. Thus, the total

number of edges is $n_1+n_2 - 2+1$, i.e., n–1.

Thus the result is true for all n.

(ii) $\Rightarrow$ (iii) :

We are given that T is acyclic and has (n–1) edges.

It is required to prove that T is connected.

If possible, let T be disconnected.

Let $T_1, T_2, \ldots, T_t$ be connected components of T, where t >1.

Let the number of vertices in each T_i be P_i, i = 1, 2, . . ., t. Let the number of edges in each T_i be q_i, i = 1, 2, . . ., t.

Now, $p = p_1 + p_2 + \ldots + p_t$

$q = q_1 + q_2 + \ldots + q_t$

Now, every T_i is connected and acyclic.

$\therefore$ every T_i is a tree, i = 1, 2, . . ., t

$\therefore$ $q_i = p_i - 1$, (from (i) $\Rightarrow$ (ii)

$\therefore$ $p - 1 = q$

$= q_1 + q_2 + \ldots + q_t$

$= (p_1-1)+(p_2-1) + \ldots + (p_t-1)$

$= (p_1+p_2 + \ldots + p_t) - t$

$= p - t.$

This is possible only when t = 1, which is a contradiction to the fact that t > 1.

So, our assumption is wrong.

$\therefore$ T must be connected.



LET US KNOW

An edge e in a graph G is called a bridge in G if the removal of e disconnects G.

The edge e in the graph given in Fig 8.4 is a bridge.

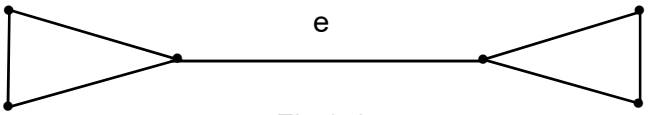


Fig 8.4

(iii) $\Rightarrow$ (iv) :

We are given that T is connected, and has n vertices, and (n–1) edges.

It is required to prove that every edge in T is a bridge.

If possible, let there be one edge which is not a bridge.

If this edge is removed, the number of vertices will be (n–2), This is not possible when T is connected.

So, our assumption is wrong.

$\therefore$ every edge is a bridge.



LET US RECALL

If G is simple connected graph with n vertices and m edges, then $n-1 \leq m \leq \frac{1}{2}n(n-1)$ (Theorem 7.9 cor 2)

(iv) $\Rightarrow$ (v) :

We are given that T is connected, and every edge is a bridge.

It is required to prove that any two vertices of T are connected by exactly one path.

If possible, let a given pair of vertices be connected by two paths. Then they will form a cycle, which is a contradiction to the fact that every edge is a bridge. So, our assumption is wrong.

Thus, any two vertices of T are connected by exactly one path.



LET US KNOW

An edge e of a graph G is a bridge if and only if e does not belong to any cycle of G.

(v) $\Rightarrow$ (i) :

We are given that any two vertices of T are connected exactly by one path.

It is required to prove that T is a tree.

Since any two vertices of T are connected exactly by one

path, therefore T is connected.

Also T is acyclic for if there is cycle ($v_0, v_1, \ldots, v_{n-1}, v_n = v_0$), Then we can find two distinct paths (v_0, v_1), and ($v_0 = v_n, v_{n-1}, \ldots, v_2, v_1$) connecting the vertices v_0, and v_1, which is a contradiction to the fact that any two vertices of T are connected exactly by one path.

Thus, T is connected and acyclic.

$\therefore$ T is a tree.

Theorem 8.2 : A connected graph T with $n \geq 2$ vertices is a tree if and only if the sum of the degrees of the vertices is 2(n–1).

Proof : Let T be a tree with n vertices.

$\therefore$ the number of edges is (n–1).

$\therefore$ the sum of the degrees of the vertices

= 2(n–1). [Theorem 7.1]

Conversely, let T be a connected graph with n vertices, and the sum of the degrees of the vertices is 2(n–1).

$\therefore$ the number of edges $= \frac{2(n-1)}{2} = n-1$

Thus, T is a connected graph with n vertices, and (n–1) edges.

$\therefore$ T is a tree

Example 2: Can there be a tree with 10 vertices such that the sum of the degrees of the vertices is 22 ? Justify your answer.

Solution : Number of vertices = 10

$\therefore$ number of edges = 10 – 1 = 9.

$\therefore$ the sum of the degrees of the vertices

= 2 x 9 = 18.

$\therefore$ there cannot be a tree with 10 vertices such that the sum of the degrees of the vertices is 22.

Minimum Number of Pendant Vertices in a Tree



LET US RECALL

A vertex is called a pendant vertex if the degree of the vertex is one.

Let us consider the graph

v_1 ——————— v_2

d(v_1) = 1, d(v_2) = 1. $\therefore$ v_1 and v_2 are pendant vertices.

Let T be a tree with n vertices. Then T has (n–1) edges.

Each edge contributes 2 to the degrees of vertices. Therefore, the sum of the degrees of all the vertices in T is 2(n–1).

Let the number of pendant vertices be x. Therefore the sum of the degrees of the pendant vertices is x.

Now 2(n–1) is to be divided among n vertices. Moreover there cannot be a vertex with zero degree in a true.

$\therefore \quad \frac{2(n-1)-x}{n-x} \geq 2$

or $2n - 2 - x \geq 2n - 2x$

$\therefore \quad x \geq 2$

Thus, there must be at least 2 vertices with degree 1 in a tree.



CHECK YOUR PROGRESS

Q 3: A tree has p vertices of degree 1, 2 vertices of degree 2, 4 vertices of degree 3, and 3 vertices of degree 4. Find the value of p.

Q 4: Can a connected acyclic graph contain eleven vertices and nine edges ? Justify your answer.

Q 5: Can a connected acyclic graph contain six vertices having degrees 1, 3, 4, 4, 6 ? Justify your answer.

Q 6: A tree has two vertices of degree 2, one vertex of degree 3, and three vertices of degree 4. How many vertices of degree 1 does it have ?

Q 7: A tree has 2n vertices of degree 1, 3n vertices of degree 2, and n vertices of degree 3. Find the number of vertices and edges in the tree ?

8.3.2 Distance and Centres in a Tree

Distance between two vertices

Let us consider a connected graph G. The distance between vertices u and v in G, denoted by d(u, v), is the length of the shortest path between u and v.

Let us consider the connected graph given in Fig. 8.6

We are to find the distance between v_1 and v_4.

Source of the paths between v_1 and v_4 are (e_1, e_2, e_3), (e_{10}, e_3), (e_8, e_7, e_3), ...

Clearly the shortest path is (e_{10}, e_3). Its length is 2.

$\therefore$ d(v_1, v_4) = 2.

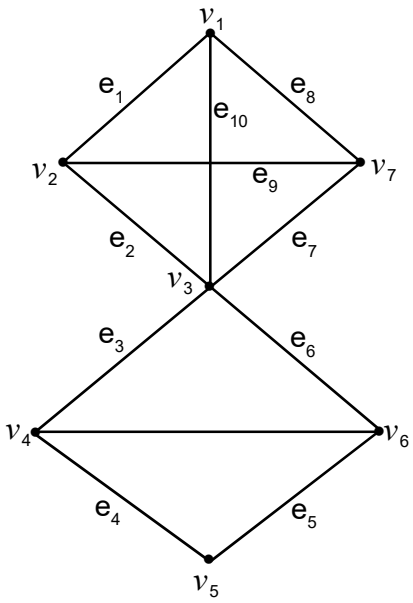


Fig 8.6

Let us consider the tree given in Fig 8.7. Clearly

d(v_1, v_2) = 2, d(v_1, v_3) = 1, d(v_1, v_4) = 2, d(v_1, v_5) = 3, d(v_1, v_6) = 3.

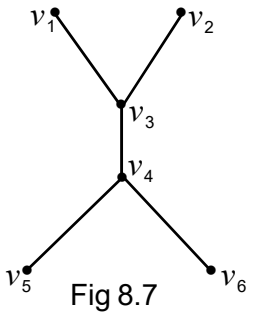


Fig 8.7

Eccentricity of a vertex

The eccentricity of a vertex v in a graph G, denoted by E(v), is the distance between v and the vertex v_i farthest from v in G. Symbolically.

E(v) = max d(v, v_i)

$i \in G$.

Centre of a graph

A vertex of a graph G whose eccentricity is minimum is called a centre of the graph G.

Example 3 : Find the eccentricity of each of the vertices of the tree given in Fig 8.7. Also find the centre (s) of the tree.

Solution : E(v_1)

= max {d(v_1, v_2), d(v_1, v_3), d(v_1, v_4), d(v_1, v_5), d(v_1, v_6)}

= max (2, 1, 2, 3, 3)

= 3

Similarly, E(v_2) = 3, E(v_3) = 2, E(v_4) = 2, E(v_5) = 3, E(v_6) = 3.

Thus, there are 2 vertices v_3 and v_4 having the same minimum eccentricity, viz., 2. Therefore, the tree has two centrces, viz., v_3 and v_4.

Note : Every tree has a centre consisting of one vertex or two adjacent vertices. The centre is the middle vertex or middle two vertices in every longest path.

We note that if there is one vertex, then it is centre of the tree. If there are two vertices joined by can edge, then these two vertices are centres of the tree.



CHECK YOUR PROGRESS

Q 8: Find the eccentricity of each of the vertices of the graph given in Fig. 8.8. Also find the centre (s) of the tree.

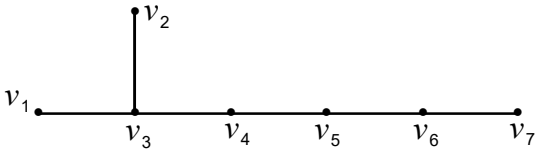


Fig 8.8

8.3.3 Rooted and Binary Trees

Rooted tree

A tree is a connected acyclic graph. A tree in which one vertex, called the root, is distinguished from all others, is called a rooted tree.

Let the root of a tree T be r. We know that tere is a unique simple path from the root r to any other vertex v in T. This determines a direction to the edges of T. Thus T may be regarded as a directed graph.

Note : 1. Any tree may be made a rooted tree by selecting one of the vertices as the root.

2. Usually the root is kept at the top of the diagram. Of course, some authors keep it at the bottom. [Harary]

3. The root serves as a point of reference for other vertices in the tree.

Rooted trees with 4 vertices are shown in Fig 8.9.

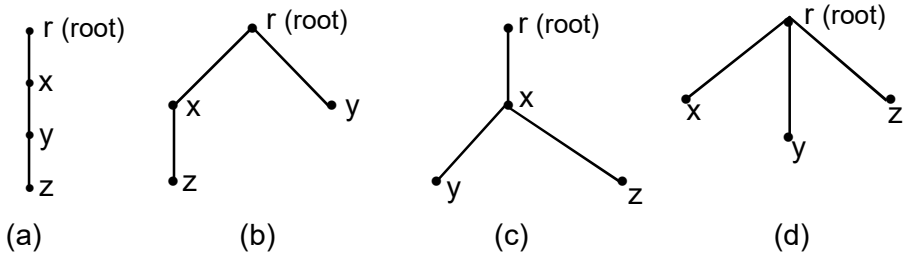


Fig 8.9

The length of the path from the root of a rooted tree to any vertex v is called the level (or depth or height) of v.

The root is said to be at level zero. The maximum level of any vertex is called the depth (or height) of the tree.

Every vertex that is reachable from a given vertex v is called a descendent of v.

The vertices that are reachable from v through a single edge are called the children of v. In this case v is called the parent. The parent of a vertex is unique.

Root is the only vertex without any parent.

If a vertex v has no children, then v is called a leaf (or a terminal vertex or a pendant vertex). The degree of a leaf is one. A non-pendant vertex is called an internal vertex. Root is also considered as an internal vertex.

Let us consider the tree given in Fig 8.10.

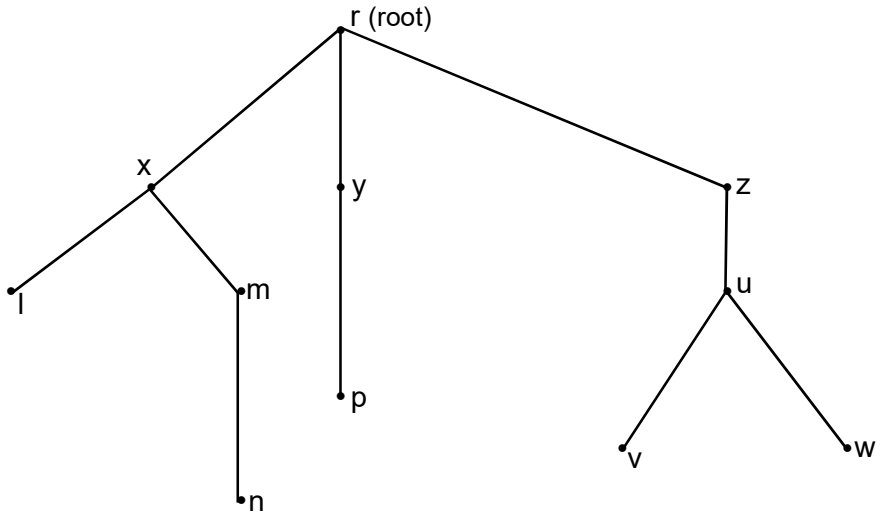


Fig 8.10

We note that level (r) = 0,

level (x) = level (y) = level (z) = 1,

level (l) = level (m) = level (p) = level (u) = 2,

level (n) = level (v) = level (w) = 3.

The height of the tree is 3.

The vertices l, m, n are descendents of x.

The vertices u, v, w are desendents of z.

l, m are children of x. x is parent of l, m. Similarly v, w are children of u. u is the parent of v, w.

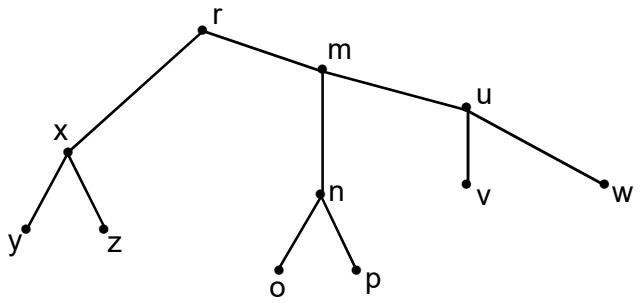
The vertices l, n, p, v, w have no children. Therefore, they are leaves of the tree.

The vertices r, x, m, y, z, u are internal vertices of the tree.

Binary tree

A full binary tree is a tree in which there is exactly one vertex of degree two and each of the remaining vertices is of degree one or three. Clearly, a full binary tree has three or more vertices. Since the vertex of degree two is distinct from all other vertices, it serves as a root. Therefore, every full binary tree is a rooted tree.

A full binary tree is shown in Fig 8.11.



A full binary tree.

Fig 8.11

Theorem 8.3 : Every full binary tree has an odd number of vertices.

Proof : Let the number of vertices of a full binary tree be n.

We know that every vertex of a full binary tree, apart from the root, is of odd degree. The root is of even degree, viz., 2. Each of the remaining (n–1) vertices is of odd degree.

We know that the number of vertices of odd degree in a graph is even.

Therefore (n–1) is even. This implies that n is odd.

Theorem 8.4 : There are $\frac{1}{2}(n+1)$ pendant vertices in a full binary tree with n vertices.

Proof : Let the number of vertices of a full binary tree be n.

There is exactly one vertex (root) of degree two.

Let the number of pendant vertices i.e., vertices of degree one be p.

$\therefore$ the number of vertices of degree 3 is (n–1–p).

$\therefore$ the sum of the degrees of all the vertices

= 1 x 2 + p x 1 + (n–1–p) x 3

= 2 + p + 3n – 3 – 3p = 3n – 2p – 1

We know that each edge contributes two degrees.

$\therefore$ the number of edges of the tree

$= \frac{1}{2}(3n - 2p - 1)$

Again we know that the number of edges of a tree with n vertices is (n–1).

$\therefore\ n - 1 = \frac{1}{2}(3n - 2p - 1)$

or, 2n–2 = 3n–2p–1

or, 2p = 3n–1 – 2n+2

or, 2p = n+1

i.e., $p = \frac{1}{2}(n + 1)$

Thus, the number of pendant vertices is $\frac{1}{2}(n + 1)$.

Corollary : If the number of internal vertices of a full binary tree is i. Then the number of pendant vertices is (i+1), and the total number of vertices is (2i+1).

Proof : Let the total number of vertices be n, and the number of pendant vertices (i.e. vertices of degree 1) be p.

Number of vertex of degree two = 1

Number of vertices of degree 3 = n–p–1.

Then $p = \frac{(n + 1)}{2}$

Now, total number of internal vertices, i.e., total number non-pendant vertices = 1+n–p–1 = n–p.

$\therefore$ i = n–p = $n - \frac{n + 1}{2} = \frac{2n - n - 1}{2} = \frac{n - 1}{2}$

$\therefore$ 2i = n–1

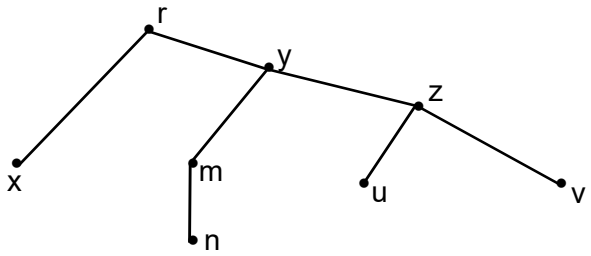
i.e. n = 2i + 1

Again $p = \frac{n+1}{2} = \frac{2i+1+1}{2} = i+1$

Thus, the number of pendant vertices is (i+1), and the total number of vertices is (2i+1).

A binary tree is a rooted tree in which every internal vertex has at most two children.

A binary tree is shown in Fig 8.12



A binary tree

Fig 8.12

Theorem 8.5 : The minimum height of a binary tree with n vertices is equal to $[\log_2 (n+1)–1]$, where [m] denotes the smallest integer greater than or equal to m.

Proof : Let the height of the binary tree be h.

Let n_i be the number of vertices at level i. Then

$n_0 = 1$,

$n_1 \leq 2^1$,

$n_2 \leq 2^2$, ... ,

$n_h \leq 2^h$,

Now $n = n_0 + n_1 + n_2 + \ldots + n_h$

$\leq 1 + 2^1 + 2^2 + \ldots + 2^h$

$= \frac{1.2^{h+1}-1}{2-1}$

$= 2^{h+1} – 1$

or $n + 1 \leq 2^{h+1}$

or $2^{h+1} \geq n + 1$

or $h + 1 \geq \log_2(n+1)$

or $h \geq \log_2(n+1) - 1$

$\therefore$ Minimum value of $h = [\log_2 (n+1) - 1]$.

8.4 COUNTING TREES

How many trees are there on n vertices? The subject was initiated by Arthur Cayley in the 1850s.

There is only one tree with one vertex.

Let there be a tree with two vertices u, v. clearly there is only one tree. [Fig 8.13 (a)].

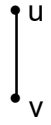


Fig 8.13(a)

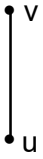
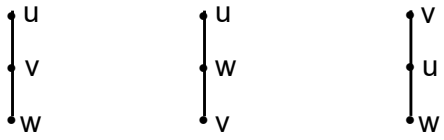


Fig 8.13 (b)

We note that there is another tree given in Fig 8.13 (b). But the tree in Fig 8.13 (b) is the reverse of the tree given in Fig 8.13 (a). Therefore, these two trees are the same. There exists an isomorphism between the two graphs. Here the tree is a path of length one.

Let there be three vertices u, v, w. There will be 3 trees with these 3 vertices. All trees are paths of length two. There are ${}^3C_2$ i.e. 3 possible pairs of endpoints and 1! i.e 1 way to arrange the intermediate vertex within it. The three trees are shown in Fig 8.14.



$$ {}^nC_r = \frac{n!}{r!(n-r)!}, \quad n \geq r $$

Fig 8.14

Let there be 4 vertices u, v, w, x. There are two patterns of trees, – a 'claw' consisting of one vertex linked to each of the others [Fig 8.15 (a)], and a path of length 3 [Fig 8.15 (b)]

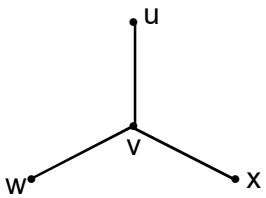


Fig 8.15 (a)

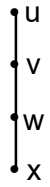


Fig 8.15 (b)

There are 4 'Claws' with each vertex as centre. Again, there are $^4C_2$ x 2 ! i.e. 6 x 2 i.e. 12 paths of length 3. There are $^4C_2$ i.e. 6 pairs of endpoints for the paths and 2! i.e 2 ways to arrange the intermediate vertices within it. Thus, the total number of trees = 4 + 12 = 16.

Let there be 5 vertices u, v, w, x, y. There are three patterns of trees, – a 'claw' consisting of one vertex linked to each of the others [Fig 8.16 (a)], a path of length 4 [Fig 8.16 (b)] and a tree of type shown in fig 8.16(c)

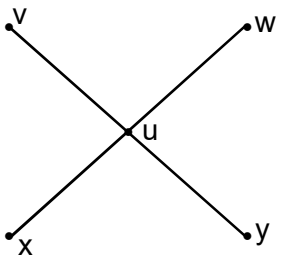


Fig 8.16 (a)



Fig 8.16 (b)

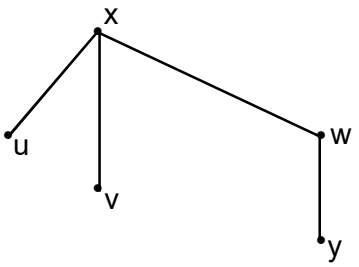


Fig 8.16 (c)

There are 5 'claws' with each vertex as centre. There are $^5C_2$ x 3! i.e. 60 paths of length 4. There are $^5C_2$ i.e. 10 pairs of endpoints for the paths and 3! i.e. 6 ways to arrange the intermediate vertices within it. Again there are $^5C_2$ x 3! i.e. 60 number of the type shown in Fig 8.16 (c) [$^5C_2$ ways to choose the top and the bottom vertices, and 3! ways to arrange the rest].

Thus, the total number of trees = 5 + 60 + 60 = 125

Let the number of trees on n vertices be denoted by F(n). We have seen that

$F(2) = 1 = 2^{2-2}$, $F(3) = 3 = 3^{3-2,}$

$F(4) = 16 = 4^{4-2}$, $F(5) = 125 = 5^{5-2}$,

We state the following theorem, without proof, due to Arthur Cayley.

Theorem 8.6 : (Cayley, 1889) There are n^{n-2} distinct labelled trees on n vertices.



LET US KNOW

A labelled tree is a tree the vertices of which are assigned unique names such as $v_1, v_2, v_3, \ldots$

8.5 SPANNING TREES

If the subgraph T of a connected graph G is a tree containing all the vertices of G, then T is called a spanning tree of G.

If a connected graph G contains n vertices, then any spanning tree of G contains n vertices and (n–1) edges.

Let us consider the connected graph G given in Fig 8.17.

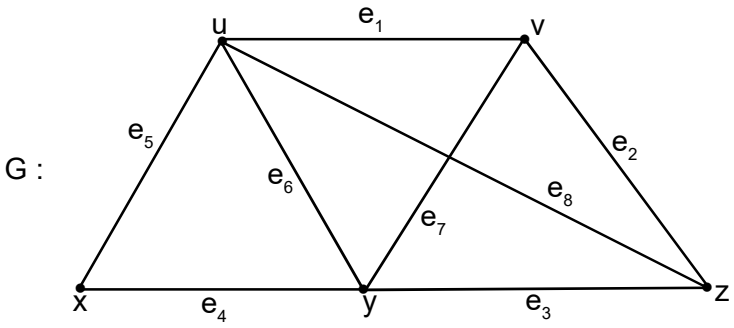


Fig 8.17

The graph G contains 5 vertices. So, any spanning tree of G contains 5 vertices, and 4 edges.

Two spanning trees T_1 and T_2 of G are shown in Fig 8.18 (a) and in Fig 8.18 (b) respectively.

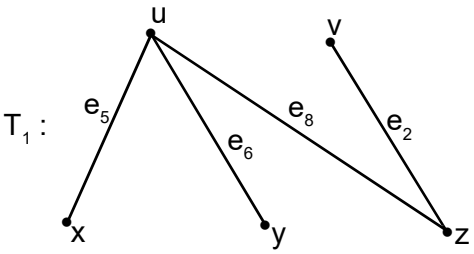


Fig 8.18 (a)

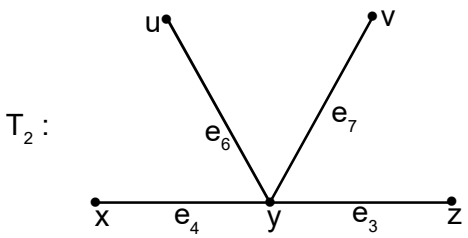


Fig 8.18 (b)

Theorem 8.7 : Every connected graph G has at least one spanning tree.

Proof : Let G be a connected graph.

If G is acyclic, there is nothing to prove. Then G is its own spanning tree.

If G is not acyclic, we remove an edge from the cycle, and the resulting graph remains connected. We repeat this process with one of the remaining cycles. We continue this procedure until there are no cycles left. Thus, we have a tree connecting all the vertices of G, which is the spanning tree of G.

Theorem 8.8 : If a graph G has a spanning tree, it must be connected.

Proof : Let the graph G have a spanning tree T.

Let u, v be any two vertices of G.

$\therefore$ u, v are also 2 vertices of T.

Since T is a tree, there is a path P from u to v in T.

Since T is a subgraph of G, P is a path from u to v in G. Thus, G is connected.

Branch and Chord of a Spanning Tree

Let G be a connected graph and T be a spanning tree of G. An edge of T is called a branch of T while any edge of G that is not contained in T is called a chord of T.

Note : A branch or a chord is defined with respect to a spanning tree. A branch of a spanning tree may be a chord of another spanning tree of a connected graph G, and vice versa.

Let us consider the spanning trees T_1 and T_2 given in Fig 8.18 (a) and in Fig 8,18 (b) respectively of the connected graph G given in Fig 8.17.

e_5 is a branch and e_4 is a chord of the spanning tree T_1, while e_5 is a chord and e_4 is a branch of the spanning tree T_2.



LET US KNOW

Let G be a connected graph with n vertices, and m edges. Then any spanning tree of G contains (n–1) branches, and m–(n–1), i.e., (m–n+1) chords.

We state, without proof, the following result due to cayley.

The number of spanning trees of the complete graph K_n is n^{n-2}, $n \geq 2$.

8.6 FUNDAMENTAL CIRCUITS

Let us consider the graph G given in Fig 8.19

G :

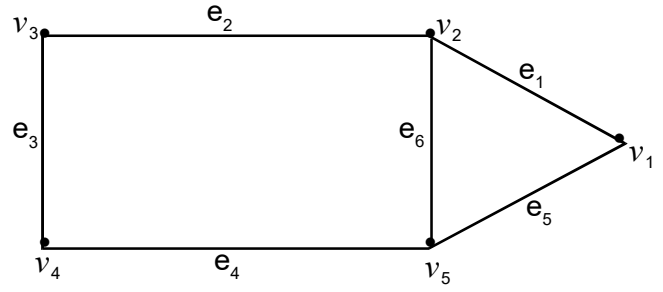


Fig 8.19

A spanning tree T of the above graph is given below.

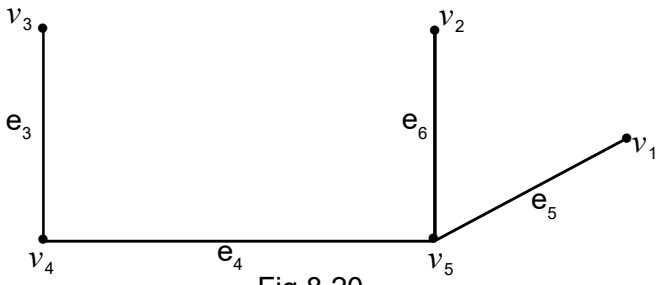


Fig 8.20

The branches of the tree are e_3, e_4, e_5, e_6; whereas the chords are e_1, e_2. If we add e_1 to this spanning tree, we get a circuit $v_1 \rightarrow v_2 \rightarrow v_5 \rightarrow v_1$. Similarly if we add e_2 to this spanning tree, we get one more circuit . $v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_2$. Thus, addition of two chords gives two circuits.

If there are n vertices and m edges in a graph, then there are m–n+1 chords in a spanning tree. Therefore, if we add all the chords to the spanning tree, thee will be m–n+1 circuits.

Let n be the number of vertices, and m the number of edges in a graph G. Then the set of m–n+1 circuits obtained by adding m–n+1 chords to a spanning tree of G is called the **fundamental system of circuits relative to the spanning tree.**

A circuit in the fundamental system is called a **fundamental circuit.**

For example, $v_1 \rightarrow v_2 \rightarrow v_5 \rightarrow v_1$ is the fundamental circuit corresponding to the edge e_1. (Fig 8.20)

Similarly $v_2 \rightarrow v_3 \rightarrow v_4 \rightarrow v_5 \rightarrow v_2$ is the fundamental circuit corresponding to the edge e_2. (Fig 8.20)

8.7 SPANNING TREES IN A WEIGHTED GRAPH

Weighted Graph

A graph is said to be weighted if a number (the weight) is assigned to each edge. Such weights may be costs, lengths or capacities depending on the problem.

Let us consider the graph G given in Fig 8.21.

G :

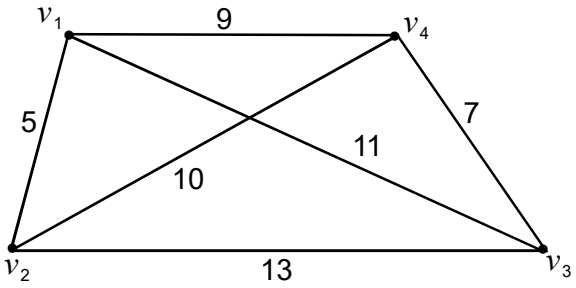


Fig 8.21

Let the vertices v_1, v_2, v_3, v_4 denote the positions of four colleges in a town. The numbers (weights) denote the distances in kilometres between the colleges. Then the graph G is a weighted graph.

Minimum spanning tree

If G is a connected weighted graph, and T is a spanning tree of G, the weight of T is defined as the sum of the weights of all the branches of T.

If G is a connected weighted graph, the spanning tree of G with the smallest total weight is called the minimum spanning tree of G.

Minimum spanning trees have several applications. They can be used for network designs (telephone or cable networks). For example, a cable company wants to lay line to multiple neighbourhoods. By minimising the amount of cable laid, the company will save money. Minimum spanning trees are also used to find approximate solutions for complex mathematical problems.

There are some popular algorithms for finding minimum spanning trees. We will discuss two such algorithms, viz., Kruskal's algorithm, and Prim's algorithm.



LET US KNOW

An algorithm is 'a mathematical procedure or method to obtain a result.' – I Niven and H. S. Zuckerman. [An Introduction to the Theory of Numbers, (1991)]

Kruskal's Algorithm

[This algorithum, due to Joseph Kruskal, first appeared in **Proceedings of the American Mathematical Society** in 1956.]

Let G be a connected weighted graph with n vertices. Any spanning tree of G will contain n vertices and (n–1) edges.

Kruskal's algorithm for obtaining minimum spanning tree is as follows.

Step 1: We list the weights of all the edges of G in order of non-decreasing weight.

Step 2: We choose an edge with minimum weight.

Step 3: Then for each successive step, we choose another edge with smallest weight from the remaining edges in such a way that the chosen edge does not form a circuit with the earlier chosen ones.

Step 4: The process is stopped after (n–1) edges have been chosen.

Note : The weight of a minimum spanning tree is **UNIQUE**. But different minimum spanning trees are possible, as two or more edges can have the same weight.

Example 3 : Find the minimum spanning tree for the weighted graph G shown in Fig 8.21 by using Kruskal's algorithm.

Solution : The weighted graph G has 4 vertices. Therefore, any spanning tree will contain 4 vertices, and (4 – 1), i.e. 3 edges.

For convenience we tabulate the weights of the edges of G in the following table. We assign ∞ as the weight of any non-existing edge.

	v_1	v_2	v_3	v_4
v_1	∞	5	11	9
v_2	5	∞	13	10
v_3	11	13	∞	7
v_4	9	10	7	∞

The weights in non-decreasing order are 5, 7, 9, 10, 11, 13.

The smallest weight is 5 between v_1 and v_2. We choose this edge. The next smallest weight is 7 between v_3 and v_4. We select this edge.

The next smallest weight is 9 between v_1 and v_4. We select this edge.

Thus, three edges have been selected. These three edges will form the minimum spanning tree (Fig 8.22) of G. Total weight = 5+7+9 = 21.



Fig 8.22

Prims' Algorithm

[This algorithm was developed in 1930 by Czech mathematician Vojtech Jarnik and later rediscovered and republished by computer scientists Robert C Prim in 1957, and Edsger W. Dijkstra in 1959.)

We start from one vertex and keep adding edges with the lowest weight until we reach our goal. The steps are given below.

Step 1 : We initialize the minimum spanning tree with a vertex chosen at random.

Step 2 : We find all the edges that connect the tree to new vertices, and find the minimum and add it to the tree.

Step 3 : We keep repeating step 2 until we get a minimum spanning tree.

Example 4 : Find the minimum spanning tree for the weighted graph shown in Fig 8.23 by using Prim's algorithm.

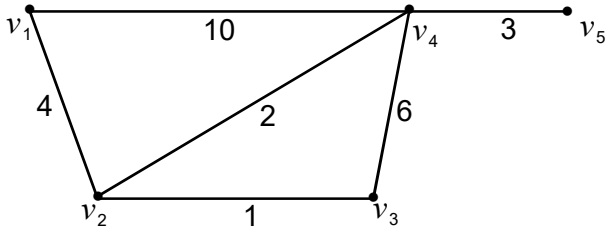


Fig 8.23

Solution : The weighted graph has 5 vertices. Therefore, any tree will contain 5 vertices and (5–1), i.e., 4 edges.

Now we construct a minimum spanning tree using Prim's algorithm.

We choose the vertex v_4.

Next we choose the shortest edge from this vertex and add it ($v_4 v_2$).

Next we choose the edge $v_4 v_5$.

Next we choose $v_2 v_4$.

Thus, 4 edges have been selected. These 4 edges will form the minimum spanning tree : (Fig 8.24). Total weight = 3+2+1+4 = 10.

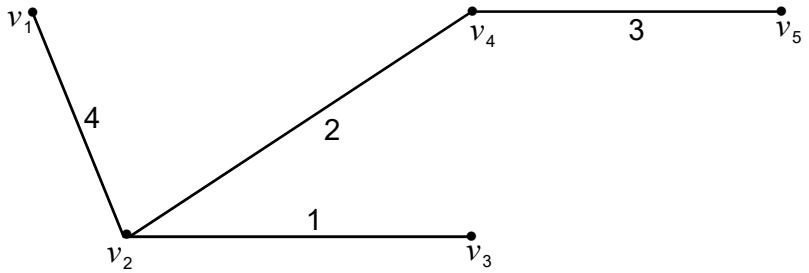


Fig 8.24

8.8 CONNECTIVITY AND SEPARABILITY

8.8.1 Cutset

A cutset S of a connected graph G is a set S of edges having the following properties.

1. The removal of all the edges in S disconnects G.
2. The removal of any proper subset of S will not disconnect G.

Example 5 : Let us consider the graph G given in Fig 8.25. The graph has 8 vertices, and 10 edges.

If we remove the edge e_{10}, the graph becomes disconnected. Therefore $S_1 = \{e_{10}\}$ is a custset of G.

Again, if we remove the edges e_1 and e_2, the graph becomes disconnected. Therefore $S_2 = \{e_1, e_2\}$ is a cutset of G. We note that removal of any proper subset of S_2 will not disconnect G.

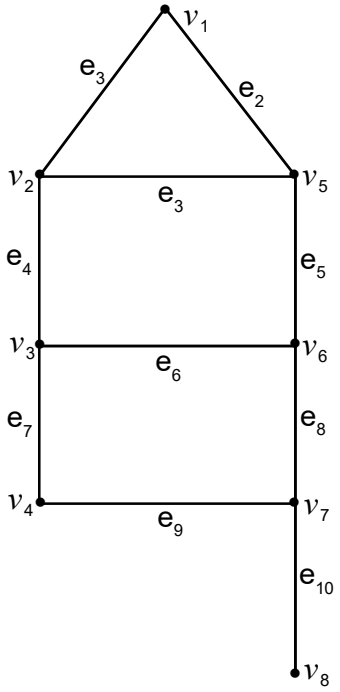


Fig 8.25

Again, if we remove the edges e_5, e_6 and e_8, the graph becomes disconnected. Therefore $S_3 = \{e_5, e_6, e_8\}$ is a cutset of G. We note that removal of any proper subset of S_3 will not disconnect G.

Again, we note that the set $\{e_6, e_7, e_9\}$ is not a cutset since this set has a subset $\{e_7, e_9\}$ whose removal disconnects G.

We note that cutsets of a graph need not have the same number of edges. For example, the cutset S_1 has one element, the cutset S_2 has two elements, and the cutset S_3 has three elements.

Example 6 : Let us consider the complete graph K_4 given in Fig 8.26.

The graph K_4 has 4 vertices and 6 edges.

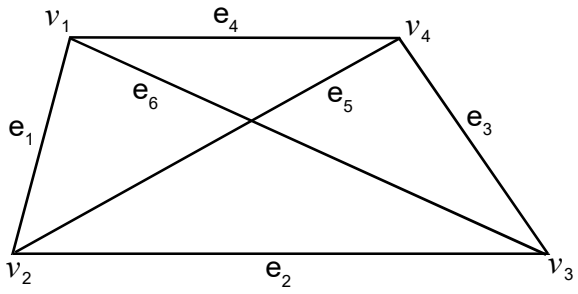


Fig 8.26

If we remove any one edge, say e_4, the graph does not become disconnected. Similarly, if we remove any two edges, say e_1, e_4, the graph does not become disconnected. But if we remove the edges e_1, e_6, e_4; the graph becomes disconnected. Therefore the set $S_1 = \{e_1, e_6, e_4\}$ is a cutset of K_4. We note that removal of any proper subset of S_1 will not disconnect K_4. Similarly, the set $S_2 = \{e_2, e_5, e_3\}$ is a cutset of K_4.

Example 7 : Let us consider the complete bipartite graph $K_{2,3}$ given in Fig 8.27.

$K_{2,3}$:

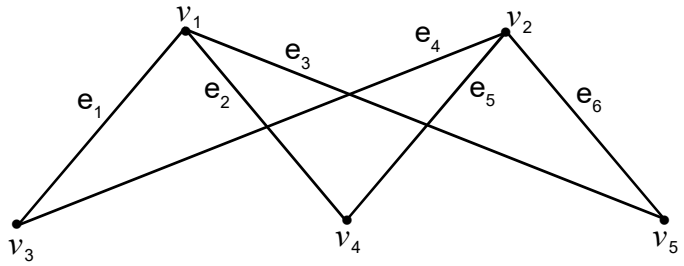


Fig 8.27

The graph $K_{2,3}$ has 5 vertices, and 6 edges.

If we remove any one edge, say e_1, the graph does not disconnected. But if we remove the edges e_1, e_4; the graph becomes disconnected. Therefore, the set $\{e_1, e_4\}$ is a cutset of $K_{2,3}$. Similarly, $\{e_2, e_5\}$, $\{e_3, e_6\}$ are cutsets of $K_{2,3}$.

8.8.2 Edge-Connectivity

The edge-connectivity of a connected graph G is the smallest number of edges whose removal disconnects G.



LET US KNOW

1. The edge-connectivity of a tree is one, because removal of an edge from the tree disconnects the graph.
2. The edge-connectivity of the complete graph K_n with n vertices is n–1.
3. The edge-connectivity of the complete bipartite graph $K_{m,n}$ is the minimum of m and n.

Theorem 8.9 : Every cutset in a connected graph G contains at least one branch of every spanning tree of G.

Proof : Let G be a connected graph.

Let T be any spanning tree of G.

Let S be any cutset of G.

It is required to prove that S contains at least one edge of T.

If possible, suppose S does not contain any edge of T. Then removal of the set S from G, i. e., the graph G–S would not disconnect G, for the graph G–S contains T which is a connected subgraph of G. This is a contradiction to the fact that S is a cutset of G. So, our assumption is wrong. Therefore, S must contain at least one edge of T.

Theorem 8.10 : Any minimal set of edges containing at least one branch of every spanning tree of a connected graph G is a cutset.

Proof : Let G be a connected graph.

Let S be a minimal set of edges containing at least one branch of every spanning tree of G.

Let us consider the subgraph of G after removal of S from G, i.e., G–S.

Since S contains at least one branch of every spanning tree of G, G–S contains no spanning tree of G. Furthermore, the set S is a minimal set of edges such that G–S is disconnected. Hence S is a cutset.

8.8.3 Cut Vertex-Set

A cut vertex-set H of a connected graph G is a set H of vertices having the following properties.

1. The removal of all the vertices in H disconnects G.
2. The removal of any proper subset of H will not disconnect G.

8.8.4 Vertex-Connectivity

The vertex-connectivity of a connected graph G is the smallest number of vertices whose removal disconnects G.



LET US KNOW

If we remove a vertex from a graph, then if there is any edge incident with that vertex, that edge is also removed.

Example 8 : Let us consider the connected graph given in Fig 8.28.

If we remove the vertex v_3, the graph becomes disconnected. Clearly, the vertex-connectivity is one. $\{v_3\}$ is a cut vertex-set.

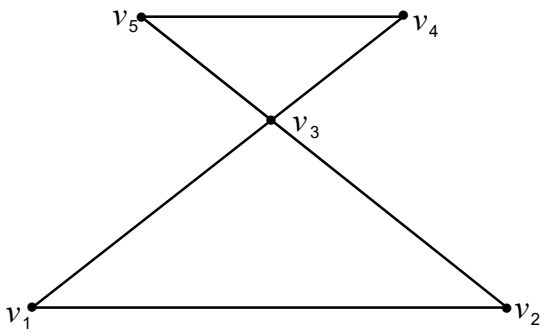


Fig 8.28



LET US KNOW

1. The vertex-connectivity of a tree is one, because removal of a vertex from the tree disconnects the graph.
2. The vertex-connectivity of the complete bipartite graph $K_{m, n}$ is the minimum of m and n.

8.8.5 Separable Graph

A connected graph whose vertex-connectivity is one is called a separable graph.

The graph given in Fig 8.28 is a separable graph.

8.8.6 Cut-Vertex

A cut-vertex is a vertex in a separable graph whose removal disconnects the graph.

v_3 is a cut-vertex in the separable graph given in Fig 8.28.

Example 9 : Show that, in a tree, every vertex of degree greater than one is a cut-vertex.

Solution : Let G be a tree (Fig 8.29). Therefore, it is a connected graph.

Let v be a vertex in G, and d(v) = 2>1.

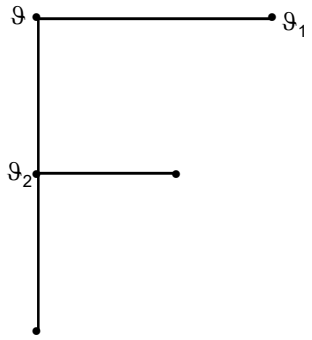


Fig 8.29

Therefore, there are at least two vertices v_1 and v_2 which are adjacent to v. Now if we remove v from the graph, v_1 and v_2 will be in different components because there is no other path between v_1 and v_2. Thus, the graph becomes disconnected. Therefore, v is a cut-vertex.



CHECK YOUR PROGRESS

Q 9: Find the edge-connectivity and the vertex-connectivity of the graph given in Fig 8.30.

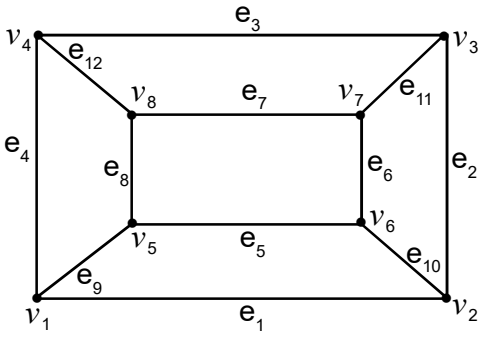


Fig 8.30

8.9 FLOW NETWORK



LET US KNOW

A vertex is considered a source in a graph if it has indegree of zero, and a vertex is considered a sink in a graph if it has outdegree of zero.

A flow network is a directed graph G = (V, E) such that

1. for each edge (u, v) $\in$ E, a nonnegative weight capacity c(u, v) $\geq$ 0 is associated.

   If (u, v) $\notin$ E, we assume that c(u, v) = 0,

2. there are two distinguishing points, the source s, and the sink t.
3. for every vertex $v \in$ V, there is a path from s to t containing v.

Let G = (V, E) be a flow network. Let s be the source, and t be the sink of the network. A flow in G is a real-valued function.

f : V x V $\rightarrow$ $\underline{\underline{R}}$

such that the following properties are satisfied.

1. Capacity constraint

For all u, $v \in$ V, we have f(u, v) $\leq$ c(u, v),

i.e., the flow through each edge is not greater than the capacity.

2. Skew symmetry

For all u, $v \in$ V, we have f(u, v) = –f (u, v),

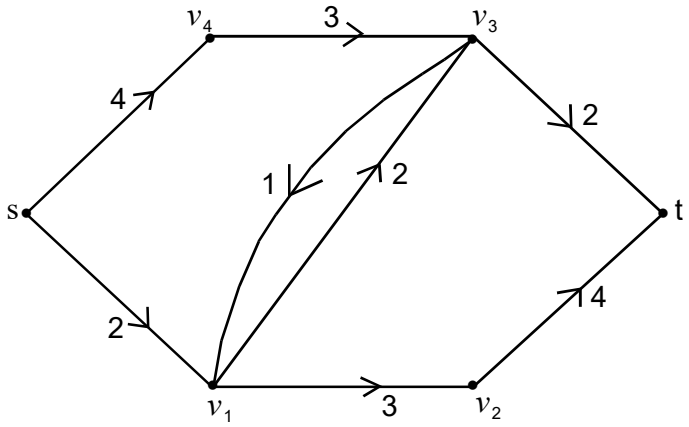
i.e., the flow from u to v is the negative of the flow from v to u.

3. Flow conservation

For all u $\in$ V–{s, t}, we have $\sum_{v \in V} f(u, v) = \sum_{u \in V} f(u, v) = 0$

i.e., the total net flow out of a vertex other than the source or sinkg is zero, i.e., the amount of flow into v is the same as the amount of flow out of v for every vertex $v \in$ V– {s, t}.

The quantity f(u, v), which can be positive or negative, is known as the net flow from the vertex u to the vertex v.



A network flow graph

Fig 8.31

8.10 MATRIX REPRESENTATION OF GRAPHS

A graph can be represented in the form of a matrix. Matrix representation of a graph has several advantages. It is easy to store and manipulate matrices and hence the graphs represented by them can be stored in a computer. Different matrices that can be formed are as follows.

8.10.1 Adjacency Matrix

An adjacency matrix is a square matrix used to represent a finite graph. The elements of the matrix indicate whether pairs of vertices are adjacent or not in the graph.

Let G be a simple graph with n vertices $v_1, v_2, v_3, \ldots, v_n, v_5$. The square matrix A = (a_{ij}) defined by

$$a_{ij} = \begin{cases} 1, \text{if } v_i v_j \text{ is an edge of G} \\ 0, \text{other} \end{cases}$$

is called the adjacency matrix of G.

Example 10 : Find the adjacency matrix of the graph given in Fig 8.32.

Solution : There are 4 vertices. Therefore, the adjacency matrix will be a 4 x 4 square matrix.

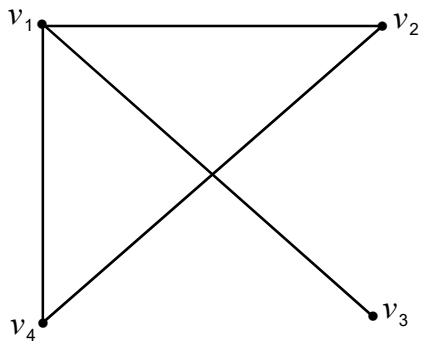


Fig 8.32

Let the adjacency matrix be

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \end{array}$$

There is no edge between v_1, v_1. $\therefore a_{11} = 0$

There is one edge between v_1, v_2. $\therefore a_{12} = 0$

There is no edge between v_1, v_3. $\therefore a_{13} = 0$

There is no edge between v_1, v_4. $\therefore a_{14} = 0$

Similarly $a_{12} = 1, a_{22} = 0, a_{23} = 0, a_{24} = 1$

$a_{31} = 1, a_{32} = 0, a_{33} = 0, a_{34} = 0$

$a_{41} = 1, a_{42} = 0, a_{43} = 0, a_{44} = 0$

$\therefore$ the required adjacency matrix is

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

We note that all the diagonal elements, viz., $a_{11}, a_{23}, a_{33}, a_{44}$ are zero. The remaining elements are either zero or one. Furthermore $a_{12} = a_{21}, a_{13} = a_{31}, a_{14} = a_{41}, a_{23} = a_{32}$, and so on, i.e., $a_{ij} = a_{ji}$. So, the matrix is a symmetric matrix. Also, we note that the number of 1's equal to twice the number of edges (8 = 2 x 4).

Propertics of adjacency matrix of a simple graph

1. The adjaceny matrix of a simple graph with n vertices is an nxn square matrix.
2. We know that a simple graph has no loops. So, the diagonal elements of the adjacency matrix of a simple graph are all zeros.
3. The adjacency matrix of a simple graph is symmetric, viz, $a_{ij} = a_{ji}$, $i \neq j$, since both the entrices are 1 if v_i and v_j are adjacent, otherwise both the entries are 0. Thus, the adjacency matrix is a zero-one matrix. A matrix, which contains entries of only 0 or 1, is called a bit matrix or a Boolean matrix.

   Conversely, let there be a symmetric zero-one matrix A whose diagonal elements are zeros. Then there exists a simple graph G whose adjacency matrix is A.
4. $d(v_i)$ = the number of 'one's' in the i th row or the i th column. Also the number of 1's is twice the number of edges.

Example 11 : Find the graph that have the following adjacency matrix

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Solution : The given matrix is a 4 x 4 zero-one symmetric matrix whose diagonal elements are zero. Therefore the graph is a simple graph with four vertices. Let the vertices be v_1, v_2, v_3, v_4.

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

From the matrix, we see that v_1 is adjacent with each of is v_2, v_3, v_4. v_2 is adjacent with each of v_1, v_3. v_3 is adjacent with each of v_1, v_2, v_4. v_4 is adjacent with each of v_1 and v_3. The graph is as shown below.

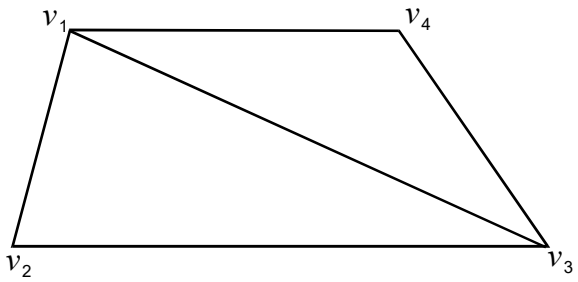


Fig 8.33



LET US KNOW

A graph that contains some parallel edges is called a multigraph.

A graph that contains loops and parallel edges is called a pseudograph.

Note : 1. A pseudograph can also be represented by an adjacency matrix. Here, a loop at the vertex v_i is represented by 1 at the (i, i) th position and the (i. j) th element equals the number of edges that are incident on v_i and v_j .

The adjacency matrix of a pseudograph is also a symmetric matrix, whose diagonal elements are not necessarily zero.

2. A directed simple or multigraph can also be represented by adjacency matrices.

Example 12 : Find the graph that have the following adjacency matrix.

$$A = \begin{pmatrix} 1 & 2 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ 1 & 2 & 1 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix}$$

Solution : The given matrix is a 4 x 4 symmetric matrix. The graph will have 4 vertics. Let the vertices be v_1, v_2, v_3, v_4.

$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{pmatrix} 1 & 2 & 1 & 2 \\ 2 & 0 & 2 & 1 \\ 1 & 2 & 1 & 0 \\ 2 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

We note that there is a loop at v_1 and another loop at v_3. There are parallel edges between v_1, v_2; v_1, v_4; v_2, v_1; v_2, v_3; v_3, v_2; v_4, v_1; There is no loop at v_2, and also at v_4. There is one edge each between v_1, v_3; v_2, v_4; v_3, v_1; v_4, v_2. The graph is shown in Fig 8.34

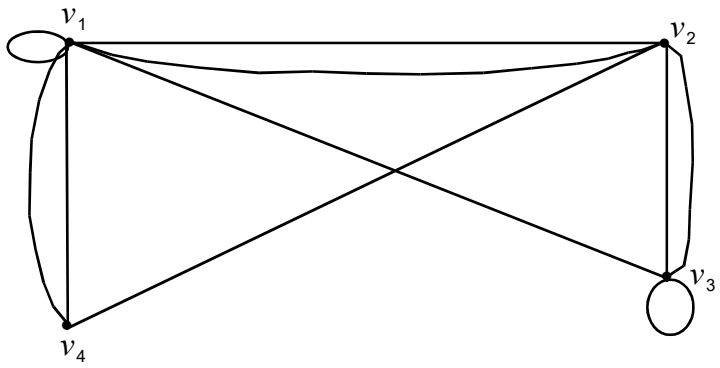


Fig 8.34

Clearly the graph is a pseudograph.

8.10.2 Incidence Matrix

Let G be a simple graph with n vertices $v_1, v_2, v_3, \ldots, v_n$; and m edges $e_1, e_2, e_3, \ldots, e_m$. The n x m matrix B = (b_{ij}) defined by

$$b_{ij} = \begin{cases} 1, \text{ when edge } e_j \text{ is incidenton } v_i \\ 0, \text{ otherwise} \end{cases}$$

is called the incidence matrix of G .

There are n rows corresponding to n vertices, and m columns corresponding to m edges.

Example 13 : Find the incidence matrix of the graph given in Fig 8.35.

Solution : There are 4 vertices and edges. Therefore, the incidence matrix is a 4 x 4 matrix.

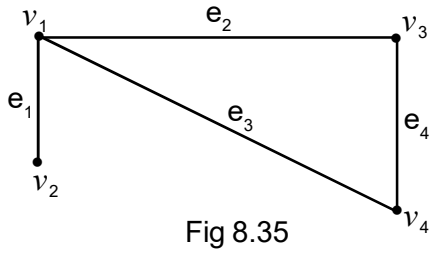


Fig 8.35

The matrix is shown below

$$B = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} e_1 & e_2 & e_3 & e_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

e_1 is incident on v_1. $\therefore$ $b_{11} = 1$

e_2 is incident on v_1. $\therefore$ $b_{12} = 1$

e_3 is incident on v_1. $\therefore$ $b_{13} = 1$

e_4 is not incident on v_1. $\therefore$ $b_{14} = 1$

Similarly $b_{21} = 1$, $b_{22} = 0$, $b_{23} = 0$, $b_{24} = 0$

$b_{31} = 0$, $b_{32} = 1$, $b_{33} = 0$, $b_{34} = 1$

$b_{41} = 0$, $b_{42} = 0$, $b_{43} = 1$, $b_{44} = 1$

We note that each column contains exactly two 1's. We also note that

$d(v_1) = 3$ = the sum of 1's in the first row.

$d(v_2) = 1$ = the sum of 1's in the second row.

$d(v_3) = 2$ = the sum of 1's in the 3rd row.

$d(v_4) = 2$ = the sum of 1's in the fourth row.

Also we note that the second row with single 1 corresponds to the pendent vertex v_2.

Properties of incidence matrix of a simple graph

1. The incidence matrix of a simple graph with n vertices and m edges is an n x m matrix.
2. Each column of the incidence matrix contains exactly two 1's, for each edge is incident exactly on two vertices.
3. A row with all 0's corresponds to an isolated vertex.
4. A row with single 1 corresponds to a pendant vertex.
5. $d(v_i)$ = the number of 1's in the i th row.
6. The incidence matrix is also a zero-one matrix.

Note : A pseudograph can also be represented by an incidence matrix.

Example 14 : Find the incidence matrix of the graph given in Fig 8.36.

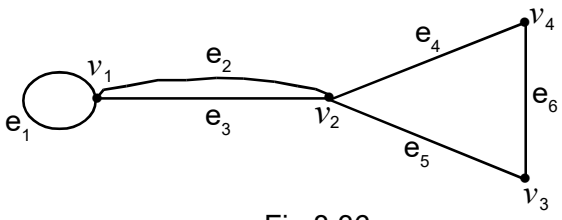


Fig 8.36

Solution : There are 4 vertices and 6 edges. Therefore, the incidence matrix is a 4 x 6 matrix.

e_1 is incident on v_1. $\therefore b_{11} = 1$

e_2 is incident on v_1. $\therefore b_{12} = 1$

e_3 is incident on v_1. $\therefore b_{13} = 1$

e_4 is not incident on v_1. $\therefore b_{14} = 0$

e_5 is not incident on v_1. $\therefore b_{15} = 0$

e_6 is not incident on v_1. $\therefore b_{16} = 0$

Similarly $b_{21} = 0,\ b_{22} = 1,\ b_{23} = 1,\ b_{24} = 1,\ b_{25} = 1,\ b_{26} = 0$

$b_{31} = 0,\ b_{32} = 0,\ b_{33} = 0,\ b_{34} = 0,\ b_{35} = 1,\ b_{36} = 1$

$b_{41} = 0,\ b_{42} = 0,\ b_{43} = 0,\ b_{44} = 1,\ b_{45} = 0,\ b_{46} = 1$

The required incidence matrix is

$$B = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$



LET US KNOW

A submatrix of a matrix is obtained by deleting any collection of rows and/or columns.

Let H be a subgraph of a graph G and let B(H) and B(G) be the incidence matrices of H and G respectively. Then B(H) is a submatrix of B(G), possibly with rows or columns permuted.

8.10.3 Path Matrix

Let G be a graph with m edges, and u and v be any two vertices in G. The path matrix for vertices u and v, denoted by P(u, v) = $(p_{ij})_{nxm}$, where n is the number of different paths between u and v, is defined by

$$p_{ij} = \begin{cases} 1, \text{ if } j\text{th edge lies in the } i\text{th path} \\ 0, \text{ otherwise} \end{cases}$$

Note : 1. A path matrix is a zero-one matrix, i.e., all the entries are either zero or one.

2. A path matrix P(u, v) defined for a particular pair of vertices u and v.
3. The rows in P(u, v) correspond to different paths between u and v.
4. The columns in P(u, v) correspond to different edges in the graph G.

Example 15 : Find the path matrix between the vertices v_1 and v_3 in the graph given in Fig 8.

Solution : The different paths between the vertices v_1 and v_3 are as follows

$p_1 = \{e_2, e_5\}$, $p_2 = \{e_3, e_5\}$, $p_3 = \{e_2, e_4, e_6\}$, $p_4 = \{e_3, e_4, e_6\}$

The path matrix for v_1 and v_3 is given by

$$P(v_1, v_3) = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \end{array} \begin{array}{c} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

We note that the first column containing all zeros correspond to the edge e_1 that does not lie in any path between v_1 and v_3. Also we note that there is no row with all zeros.

Properties of path matrix

1. A column of all zeros corresponds to an edge that does not lie in any path between the two specified vertices.

2. A column of all ones corresponds to an edge that lies in every path between the two specified vertices.
3. There cannot be any row with all zeros.

8.10.4 Cutset Matrix

Let G be a graph with m edges and n cutsets. The cutset matrix of G, denoted by $C = (C_{ij})_{nxm}$, is defined by

$$c_{ij} = \begin{cases} 1, & \text{if } i\text{th cutset contains } j\text{th edge} \\ 0, & \text{otherwise} \end{cases}$$

Note : The cutset matrix is a zero-one matrix, i.e., the entries are either 0 or 1.

Example 16 : Find the cutset matrix of the graph G given in Fig 8.37.

Solution : There are 6 vertices and 7 edges of the graph.

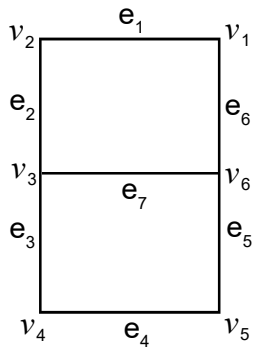


Fig 8.37

If we remove the edges e_1, e_2 ; the graph becomes disconnected. Similarly, if we remove the edges e_3, e_4 ; the graph becomes disconnected. Similarly, if we remove the edges e_1, e_7, e_4; the graph becomes disconnected. There will be altogether.

9 cutsets, viz, $c_1 = \{e_1, e_2\}$, $c_2 = \{e_3, e_4\}$, $c_3 = \{e_4, e_5\}$, $c_4 = \{e_1, e_6\}$, $c_5 = \{e_2, e_6\}$, $c_6 = \{e_3, e_5\}$, $c_7 = \{e_1, e_4, e_7\}$, $c_8 = \{e_2, e_3, e_7\}$, $c_9 = \{e_5, e_6, e_7\}$.

The cutset matrix C is given below-

$$C = \begin{array}{c} \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \\ c_9 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

Properties of cutset matrix

1. Interchange of rows or columns in a cutset matrix corresponds to relabeling of 1.
2. A column with all zeros corresponds to an edge forming a self-loop.
3. Parallel edges form identical columns in the cutset matrix.

8.10.5 Circuit Matrix

Let G be a graph with m edges. Let n be the number of different circuits in G. The circuit matrix of G, denoted by $T = (t_{ij})_{nxm}$, is defined by–

$$t_{ij} = \begin{cases} 1, \text{ if the } i\text{th circuit includes } j\text{th edge} \\ 0, \text{ otherwise} \end{cases}$$

Note : The circuit matrix is a zero-one matrix, i.e., the entries are either 0 or 1.

Example 17 : Find the circuit matrix of the graph G given in Fig 8.38.

Solution : There are 6 vertices, and 8 edges.

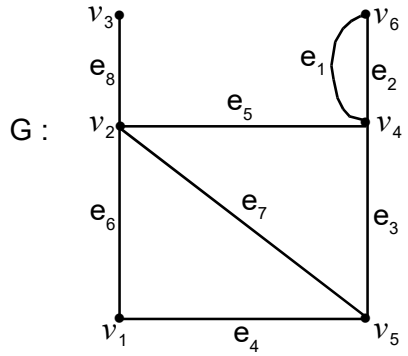


Fig 8.38

The graph has 4 different circuits, viz, $t_1 = \{e_1, e_2\}$, $t_2 = \{e_3, e_5, e_7\}$, $t_3 = \{e_4, e_6, e_7\}$, $t_4 = \{e_3, e_4, e_6, e_5\}$

The circuit matrix B is shown below.

$$C = \begin{array}{c} \\ t_1 \\ t_2 \\ t_3 \\ t_4 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

Properties of circuit matrix

1. The number of ones in a row is equal to the number of edges in the corresponding circuit. For example, there are two ones in the first row of the circuit matrix given in Example 17. The number of edges in the corresponding circuit t_1 is also two.
2. If an edge does not belong to any circuit, then the corresponding column of the circuit matrix contains all zeros. For example, the edge e_8 of the graph given in Example does not belong to any circuit and the corresponding column of the circuit matrix contains all zeros.
3. A circuit matrix is capable of representing a self-loop.



8.11 LET US SUM UP

- A graph having no cycles is called ayclic.
- A tree is a connected ayclic graph.
- A tree with n vertices has (n–1) edges.
- An edge e in a graph G is called a bridge in G if the removal of e disconnects G.
- A tree in which one vertex, called the root is distinguished from all others, is called a root.
- A full binary tree is a tree in which there is exactly one vertex of degree two and each of the remaining vertices is of degree one or three.
- If the subgraph T of a connected graph G is a tree containing all the vertices of G, then T is called a spanning tree of G.

- A graph is said to be weighted if a number (the weight) is assigned to each edge.
- The edge-connectivity of a connected graph G is the smallest number of edges whose removal disconnects G.
- The vertex-connectivity of a connected graph G is the smallest number of vertices whose removal disconnects G.
- A graph can be represented in the form of a matrix. Some of the matrices that can be formed are as follows,– adjacency matrix, incidence matrix, path matrix, cutset matrix, circuit matrix.



8.12 FURTHER READINGS

1) **Graph Theory** by Frank Harary (Naroza Publishing House).

2) **Introduction to Graph Theory** by Robin J. Wilson (Addison Wesley Longman Limited).

3) **Discrete Mathematics with Graph Theory and Combinatorics** by T Veerarajan (Tata McGraw-Hill Publishing Company Limited).



8.13 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: (a) Connected acyclic graph. So, a tree.

(b) not connected. not a tree.

(c) connected acyclic. a tree.

(d) not connected. not a tree.

(e) connected acyclic graph. a tree.

Ans to Q No 2: (a) not a simple graph. not a tree.

(b) not a simple graph. not a tree.

(c) connected acyclic graph. a tree.

Ans to Q No 3: Number of vertices

$= p + 2 + 4 + 3 = p+9$

$\therefore$ number of edges $= p + 9 – 1 = p + 8$

Sum of the degrees of the vertices

$= p \times 1 + 2 \times 2 + 4 \times 3 + 3 \times 4$

$= p + 4 + 12 + 12 = p + 28$

But sum of the degrees of the vertices

$= 2(p + 8) = 2p + 16$

$\therefore$ $2p + 16 = p + 28$

or $2p - p = 28 - 16$

$\therefore$ $p = 12$.

Ans to Q No 4: The graph is connected acyclic. So it is tree. Since it has 11 vertices, the number of edges must be (11–1), i.e., 10.

$\therefore$ a connected acyclic graph cannot contain 11 vertices and 9 edges.

Ans to Q No 5: The graph is connected acyclic. So it is a tree. Therefore, there must be at least 2 vertices with degree 1.

$\therefore$ a connected acyclic graph cannot contain 6 vertices having degrees 1, 3, 4, 4, 6.

Ans to Q No 6: Let there be x vertices of degree 1.

$\therefore$ total number of vertices

$= 2 + 1 + 3 + x = 6 + x$

Sum of the degrees of the vertices

$= 2 \times 2 + 1 \times 3 + 3 \times 4 + xx1=19+x$

Again,sum of degrees of the vertices $=2(6+x-1) = 10 + 2x$

$\therefore$ $19+x=2(x+5)$

or $19+x=2x+10$

or $x=9$

Ans to Q No 7: Number of vertices

$= 2n + 3n + n = 6n$

Sum of the degrees of the vertices

$= 2n \times 1 + 3n \times 2 + n \times 3$

$= 2n + 6n + 3n = 11n$.

Again sum of the degrees of the vertices

$= 2(6n - 1) = 12n - 2$.

$\therefore$ $12n - 2 = 11n$

$\therefore$ $n = 2$

$\therefore$ number of vertices $= 6 \times 2 = 12$, and number of edges $= 12 - 1 = 11$.

Ans to Q No 8: E(v_1)

= max {d(v_1, v_2), d(v_1, v_3), d(v_1, v_4), d(v_1, v_5), d(v_1, v_6), d(v_1, v_7)}

= max {2, 1, 2, 3, 4, 5} = 5

E(v_2) = max {d(v_2, v_1), d(v_2, v_3), d(v_2, v_4), d(v_2, v_5), d(v_2, v_6), d(v_2, v_7)}

= max {2, 1, 2, 3, 4, 5} = 5

E(v_3) = max {d(v_3, v_1), d(v_3, v_2), d(v_3, v_4), d(v_3, v_5), d(v_3, v_6), d(v_3, v_7)}

= max {1, 1, 1, 2, 3, 4} = 4

E(v_4) = max {d(v_4, v_1), d(v_4, v_2), d(v_4, v_3), d(v_4, v_5), d(v_4, v_6), d(v_4, v_7)}

= max {2, 2, 1, 1, 2, 3} = 3

E(v_5) = max {d(v, v_1), d(v_5, v_2), d(v_5, v_3), d(v_5, v_4), d(v_5, v_6), d(v_5, v_7)}

= max {3, 3, 2, 1, 1, 2} = 3

E(v_6) = max {d(v_6, v_1), d(v_6, v_2), d(v_6, v_3), d(v_6, v_4), d(v_6, v_5), d(v_6, v_7)}

= max {4, 4, 3, 2, 1, 1} = 4

E(v_7) = max {d(v_7, v_1), d(v_7, v_2), d(v_7, v_3), d(v_7, v_4), d(v_7, v_5), d(v_7, v_6)}

= max {5, 5, 4, 3, 2, 1} = 5

∴ Thus, there are 2 vertices v_4 and v_5 having the same minimum eccentivity, viz., 3. Therefore, the tree has two centres, viz., v_4 and v_5.

Ans to Q No 9: If we remove any two edges, say e_1 and e_2, the graph does not become disconnected. But if we remove any three edges incident on the same vertex, say e_1, e_2, e_{10}, the graph becomes disconnected. Therefore, the edge-connectivity is three.

Similarly, if we remove any two vertices, say v_2 and v_4, the graph does not become disconnected. But if we remove the vertices v_2, v_4, v_7, the graph becomes disconnected. Therefore, the vertex-connectivity is three.



8.14 MODEL QUESTIONS

Q 1: Define a tree. Prove that a tree with n vertices has (n–1) edges.

Q 2: Define a spanning tree. Draw all the spanning trees of K_3.

Q 3: What is meant by a bridge ? Show that every edge of a tree is a bridge.

Q 4: Show that there must be at least two vertices with degree one in a tree.

Q 5: Prove that every full binary tree has an odd number of vertices.

Q 6: Show that there are sixteen trees with four vertices.

Q 7: Describe Kruskal's algorithm for obtaining minimum spanning tree.

Q 8: What is meant by edge-connectivity? What is the edge connectivity of the graph given below ?

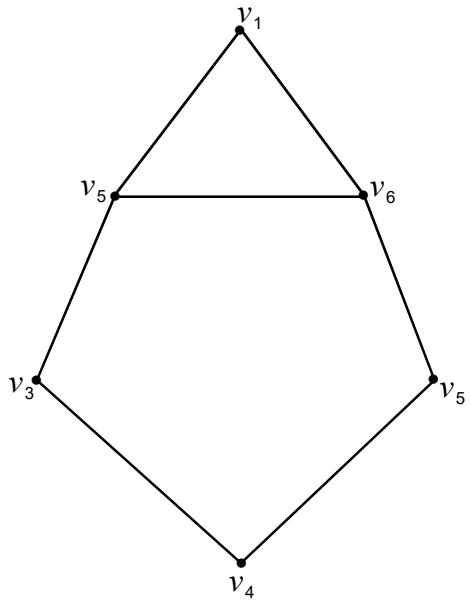


Fig 8.39

Q 9: State the properties of adjacency matrix of a simple graph.

Q 10: State the properties of incidence matrix of a simple graph.

*** ***** ***



REFERENCES

1. Discrete Mathematics with Graph Theory and Combinatorics by T Veerarajan (Tata McGraw-Hill Publishing Company Limited).
2. Balaji, G. *Discrete Mathematics*. Balaji Publishers, 2015.
3. Singaravelu, A. & Jeyaraman, M.P. *Discrete Mathematics*. Meenakshi Agency,2016.
4. Rao, G. S. S. Bhishma. *Discrete Structures and Graph Theory*. SciTech Publications (India) PVT Ltd, 2003
5. *Elements of Discrete Mathematies* by C L Liu, D P Mohapatra (Mc Graw Hill Education (India) Private Limited).
6. *Theory and Problems of Discrete Mathematics* by seymour Lipschutz, Mare Lars Lipson (Tata Mc Graw-Hill Publishing Company Limited).
7. *Introduction to Discrete Mathematies* by M.K Sen, B.C Chakraborty (Books and Allied (P) Ltd.).
8. *Graph Theory* by Frank Harary (Narosa Publishing House)
9. *Graphs and Their Uses* by Oystein Ore (Random House/The L. W. Singer Company)
10. *Discrete Mathematics* by M.K. Gupta (Krishna Prakashan Media (P) Ltd).
11. *A Textbook of Discrete Mathematics* by Swapan Kumar Sarkar (S. Chand & Company Ltd.)
12. Internet.