MCA09

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Housefed Complex, Dispur, Guwahati - 781 006

Master of Computer Applications

DISCRETE MATHEMATICS

CONTENTS

Subject Expert

Prof. Anjana Kakati Mahanta, Deptt. of Computer Science, Gauhati University

Prof. Jatindra Kr. Deka, Deptt. of Computer Science and Engineering, Indian Institute of Technology, Guwahati

Prof. Diganta Goswami, Deptt. of Computer Science and Engineering, Indian Institute of Technology, Guwahati

Course Coordinator

Tapashi Kashyap Das, Assistant Professor, Computer Science, KKHSOU

Arabinda Saikia, Assistant Professor, Computer Science, KKHSOU

SLM Preparation Team

Units	Contributors
1	**Proff. Biswajeet Bhagawati,** Ex-Professor, Head of the Deptt. Mathematics, Cotton College
3,4,5 & 6	**Harekrishna Deka,** Academic Consultant, KKHSOU
7 & 10	**Hitesh Choudhury,** Assistant Professor, Dimoria College
2,8 & 9	**Dr. Dilip Kumar Sarma**, Associate Professor, Cotton College

July 2012

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

The university acknowledges with thanks the financial support provided by the **Distance Education Council, New Delhi**, for the preparation of this study material.

Housefed Complex, Dispur, Guwahati- 781006; Web: www.kkhsou.net

COURSE INTRODUCTION

This course is on ***Discrete Mathematics***. The course is designed to acquaint learners about the ideas and techniques from Discrete Mathematics that are widely used in Computer Science. Discrete Mathematics is the mathematical language of Computer Science and therefore its importance has increased dramatically in recent decades.
The course consists of the following ten units:

Unit 1 is an introductory unit on sets. It includes different types of sets, Venn diagram and various operations associated with sets.
Unit 2 describes relations and functions. Various concepts associcted with relations and functions are discussed in this unit.
Unit 3 and **Unit 4** is on propositional logic. Various concepts like statements, logical connectives, truth tables, tautologies, contradictions, logical equivalence are discussed in this unit.
Unit 5 concentrates on predicate logic.
Unit 6 describes Boolean algebra. Relation of predicate calculus to Boolean algebra are discussed in this unit.
Unit 7 describes counting principles. It includes Pigeonhole principle, permutation and combinations, principles of inclusion etc.
Unit 8 and **Unit 9** are on basic algebraic structure. These two unit describes binary operations, group ring, integral domain, field etc.
Unit 10 concentrates on graph theory.

Each unit of this course includes some along-side boxes to help you know some of the difficult, unseen terms. Some “EXERCISES” have been included to help you apply your own thoughts. 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 make you 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.

MASTER OF COMPUTER APPLICATIONS

Discrete Mathematics

DETAILED SYLLABUS

Unit 1: Sets
Sets – the Empty Set, Finite and Infinite Set, Equal and Equivalent set, Subsets, Power set, Universal set, Venn diagram, Complement of a set, set operations

Unit 2: Relations and Functions
Concept of relation: identity and inverse relation, types of relation, equivalence relation; Concept of function: identity and constant function, types of function

Unit 3: Propositional Logic - I
Statements, logical connectives, truth tables

Unit 4: Propositional Logic - II
Tautologies, contradictions, logical equivalence, Applications to everyday reasoning

Unit 5: Predicate Logic
An axiom system for the Predicate Calculus, Truth tables as an effective procedure for deciding logical validity,

Unit 6: Boolean Algebra
Boolean Algebra, Relation of Predicate Calculus to Boolean algebra

Unit 7: Counting Principles
The Pigeonhole principle -. counting; Permutation and Combination: Definition of Permutation and combination, Simple application of permutation and combination, Principle of Inclusion-Exclusion

Unit 8: Basic Algebraic Structure – I
Binary operations, identity and inverse of an element, group, subgroup, coset, cyclic group, normal subgroup, quotient group

Unit 9: Basic Algebraic Structure – II
Ring, Commutative Ring, Integral domain and Field

Unit 10: Graph Theory
Basic Terminology, Some Special Simple Graphs, Representation of graph and graph isomorphism, Connectivity of a graph, Eulerian and Hamiltonian graph, Trees and its different properties

UNIT-1 : SETS

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to

- describe sets and their representations
- identify empty set, finite and infinite sets
- define subsets, super sets, power sets, universal set
- describe the use of Venn diagram for geometrical discreption of sets
- illustrate the set operations of union, intersection, difference and complement
- know the different algebraic laws of set-operations
- illustrate the application of sets in solving practical problems

1.2 INTRODUCTION

One of the widly used concepts in present day Mathematics is the concept of Sets. It is considered the language of modern Mathematics. The whole structure of Pure or Abstract Mathematics is based on the concept of sets. German mathematician **Georg Cantor** (1845-1918) developed the theory of sets and subsequently many branches of modern Mathematics have been developed based on this theory. In this unit, preliminary concepts of sets, set operations and some ideas on its practical utility will be introduced.

1.3 SETS AND THEIR REPRESENTATION

A set is a collection of well-defined objects. By well-defined, it is meant that given a particular collection of objects as a set and a particular object, it must be possible to determine whether that particular object is a member of the set or not.

The objects forming a set may be of any sort– they may or may not have any common property. Let us consider the following collections :

(i) the collection of the prime numbers less than 15 i.e., 2, 3, 5, 7, 11, 13

(ii) the collection of 0, a, Sachin Tendulkar, the river Brahmaputra

(iii) the collection of the beautiful cities of India

(iv) the collection of great mathematicians.

Clearly the objects in the collections (i) and (ii) are well-defined. For example, 7 is a member of (i), but 20 is not a member of (i). Similarly, 'a' is a member of (ii), but M. S. Dhoni is not a member. So, the collections (i) and (ii) are sets. But the collections (iii) and (iv) are not sets, since the objects in these collections are not well-defined.

The objects forming a set are called **elements** or **members** of the set. Sets are usually denoted by capital letters A, B, C, ...; X, Y, Z, ..., etc., and the elements are denoted by small letters a, b, c, ...; x, y, z, ..., etc.

If ‘a’ is an element of a set A, then we write a $\in$ A which is read as ‘a belongs to the set A’ or in short, ‘a belongs to A’. If ‘a’ is not an element of A, we write a $\notin$ A and we read as ‘a does not belong to A’. For example, let A be the set of prime number less than 15.

Then $2 \in A$, $3 \in A$, $5 \in A$, $7 \in A$, $11 \in A$, $14 \in A$

$1 \notin A$, $4 \notin A$, $17 \notin A$, etc.

Representation of Sets :

Sets are represented in the following two methods :

1. Roster or tabular method
2. Set-builder or Rule method

In the Roseter method, the elements of a set are listed in any order, separated by commas and are enclosed within braces, For example,

A = {2, 3, 5, 7, 11, 13}

B = {0, a Sachin Tendulcar, the river Brahmaputra}

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

In the set C, the elements are all the odd natural numbers. We cannot list all the elements and hence the dots have been used showing that the list continues indefinitely.

In the Rule method, a variable x is used to represent the elements of a set, where the elements satisfy a definite property, say P(x). Symbolically, the set is denoted by {x : P(x)} or {x | p(x)}. For example,

A = {x : x is an odd natural number}

B = {x : x^2–3x+2 = 0}, etc.

If we write these two sets in the Roster method, we get,

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

B = {1, 2}

NOTE

(1) It should be noted that the symbol ‘:’ of ‘|’ stands for the phrase ‘such that’.

(2) While writing a set in Roster method, only distinct elements are listed. For example, if A is the set of the letters of the word MATHEMATICS, then we write A = {A, E, C, M, H, T, S, I} The elements may be listed in any order.

Some Standard Symbols for Sets and Numbers :

The following standard symbols are used to represent different sets of numbers :

N = {1, 2, 3, 4, 5, ...}, the set of natural numbers

Z = {..., –3, –2, –1, 0, 1, 2, 3, ...}, the set of integers

Q = $\{x : x = {}^{p}/_{q};\ p, q \in Z, q \neq 0\}$, the set of rational numbers

R = {x : x is a real number}, the set of real numbers

Z^+, Q^+, R^+ respectively represent the sets of positive integers, positive rational numbers and positive real numbers. Similarly Z^-, Q^-, R^- represent respectively the sets of negative integers, negative rational numbers and negative real numbers. Z^0, Q^0, R^0 represent the sets of non-zero integers, non-zero rational numbers and non-zero real numbers.

ILLUSTRATIVE EXAMPLES

1. Examine which of the following collections are sets and which are not :
   (i) the vowels of the English alphabet
   (ii) the divisors of 56
   (iii) the brilliant degree-course students of Guwahati
   (iv) the renowned cricketers of Assam.

Solution :

(i) It is a set, V = {a, e, i, o, u}
(ii) It is a set, D = {1, 2, 4, 7, 8, 14, 28, 56}
(iii) not a set, elements are not well-defined.
(iv) not a set, elements are not well-defined.

2. Write the following sets in Roster method :
   (i) the set of even natural numbers less than 10
   (ii) the set of the roots of the equation $x^2–5x+6 = 0$
   (iii) the set of the letters of the word EXAMINATION

Solution :

(i) {2, 4, 6, 8}
(ii) {2, 3}
(iii) {E, X, A, M, I, N, T, O}

3. Write the following sets in Rule method :
   (i) $E = \{2, 4, 6, ...\}$
   (ii) $A = \{2, 4, 8, 16, 32\}$
   (iii) $B = \{1, 8, 27, 64, 125, 216\}$

Solution :

(i) $E = \{x : x = 2n, n \in N\}$

(ii) $A = \{x : x = 2^n, n \in N, n < 6\}$

(iii) $B = \{x : x = n^3, n \in N, n \leq 6\}$

CHECK YOUR PROGRESS - 1

1. Express the following sets in Roster method :
   (i) $A = \{x : x$ is a day of the week$\}$
   (ii) $B = \{x : x$ is a month of the year$\}$
   (iii) $C = \{x : x^3 - 1 = 0\}$
   (iv) $D = \{x : x$ is a positive divisor of $100\}$
   (v) $E = \{x : x$ is a letter of the word ALGEBRA$\}$
2. Express the following sets in Set-builder method :
   (i) A = {January, March, May, July, August, October, December}
   (ii) $B = \{0, 3, 8, 15, 24, ...\}$
   (iii) $C = \{0, \pm 5, \pm 10, \pm 15, ...\}$
   (iv) $D = \{a, b, c, ..., x, y, z\}$
3. Write true or false :
   (i) $5 \in N$ (ii) $\frac{1}{2} \in Z$ (iii) $-1 \in Q$
   (iv) $\sqrt{2} \in R$ (v) $\sqrt{-1} \in R$ (vi) $-3 \notin N$

1.4 THE EMPTY SET

Definition : A set which does not contain any element is called an **empty set** or a **null set** or a **void set**. It is denoted by ϕ.

The following sets are some examples of empty sets.

(i) the set $\{x : x^2 = 3 \text{ and } x \in Q\}$

(ii) the set of people in Assam who are older than 500 years

(iii) the set of real roots of the equation $x^2 + 4 = 0$

(iv) the set of Lady President of India born in Assam.

1.5 FINITE AND INFINITE SETS

Let us consider the sets

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

and $B = \{1, 4, 7, 10, 13, ...\}$

If we count the members (all distinct) of these sets, then the counting process comes to an end for the elements of set A, whereas for the elements of B, the counting process does not come to an end. In the first case we say that A is a finite set and in the second case, B is called an infinite set. A has finite number of elements and number of elements in B are infinite.

Definition : A set containing finite number of distinct elements so that the process of counting the elements comes to an end after a definite stage is called a **finite set**; otherwise, a set is called an **infinite set**.

NOTE

A finite set can always be expressed in roster method. But an infinite set cannot be always expressed in roster method as the elements may not follow a definite pattern. For example, the set of real numbers, R cannot be expressed in roster method.

Example : State which of the following sets are finite and which are infinite.

(i) the set of natural numbers N

(ii) the set of male persons of Assam as on January 1, 2009.

(iii) the set of prime numbers less than 20

(iv) the set of concentric circles in a plane

(v) the set of rivers on the earth.

Solution :

(i) $N = \{1, 2, 3, ...\}$ is an infinite set

(ii) it is a finite set

(iii) $\{2, 3, 5, 7, 11, 13, 17, 19\}$ is a finite set

(iv) it is an infinite set

(v) it is a finite set.

1.6 EQUAL SETS

Definition : Two sets A and B are said to be equal sets if every element of A is an element of B and every element of B is also an element of A. In otherwords, A is equal to B, denoted by A = B if A and B have exactly the same elements. If A and B are not equal, we write $A \neq B$.

Let us consider the sets

$A = \{1, 2\}$
$B = \{x : (x-1)(x-2) = 0\}$
$C = \{x : (x-1)(x-2)(x-3) = 0\}$

Clearly $B = \{1, 2\}$, $C = \{1, 2, 3\}$ and hence $A = B$, $A \neq C$, $B \neq C$.

Example : Find the equal and unequal sets :

(i) $A = \{1, 4, 9\}$
(ii) $B = \{1^2, 2^2, 3^3\}$
(iii) C = {x : x is a letter of the word TEAM}
(iv) D = {x : x is a letter of the word MEAT}
(v) $E = \{1, \{4\}, 9\}$

Solution : $A = B$, $C = D$, $A \neq C$, $A \neq D$, $A \neq E$, $B \neq C$, $B \neq D$, $B \neq E$, $C \neq E$, $D \neq E$

NOTE
According to equality of sets discussed above, the sets $A = \{1, 2, 3\}$ and $B = \{1, 2, 2, 2, 3, 1, 3\}$ are equal, since every member of A is a member of B and also every member of B is a member of A. This is why identical elements are taken once only while writing a set in the Roster method.

1.7 SUBSETS, SUPERSETS, PROPER SUBSETS

Let us consider the sets $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4\}$ and $C = \{3, 2, 1\}$. Clearly, every element of A is an element of B, but A is not equal to B. Again, every element of A is an element of C, and also A is equal to C. In both cases, we say that A is a subset of B and C. In particular, we say that A is a proper subset of B, but A is not a proper subset of C.

Definition : If every element of a set A is also an element of another set B, then A is called a **subset** of B, or A is said to be contained in B, and is denoted by $A \subseteq B$. Equivalently, we say that B contains A or B is a **superset** of A and is denoted by $B \supseteq A$. Symbolically, $A \subseteq B$ means that

$$\text{for all } x, \text{ if } x \in A \text{ then } x \in B.$$

If A is a subset of B, but there exists atleast one element in B which is not in A, then A is called a **proper subset** of B, denoted by $A \subset B$. In otherwords,

$$A \subset B \Leftrightarrow (A \subseteq B \text{ and } A \neq B).$$

The symbol '$\Leftrightarrow$' stands for 'logically implies and is implied by' (see unit 5). Some examples of proper subsets are as follows :

$$N \subset Z,\ N \subset Q,\ N \subset R,$$
$$Z \subset Q,\ Z \subset R,\ Q \subset R.$$

It should be noted that any set A is a subset of itself, that is, $A \subseteq A$. Also, the null set ϕ is a subset of every set, that is, $\phi \subseteq A$ for any set A. Because, if $\phi \subseteq A$, then there must exist an element $x \in \phi$ such that $x \notin A$. But $x \notin \phi$, hence we must accept that $\phi \subseteq A$.

Combining the definitions of equality of sets and that of subsets, we get

$$A = B \Leftrightarrow (A \subseteq B \text{ and } B \subseteq A)$$

ILLUSTRATIVE EXAMPLES

1. Write true or false :
   (i) $1 \subset \{1, 2, 3\}$
   (ii) $\{1, 2\} \subseteq \{1, 2, 3\}$
   (iii) $\phi \subseteq \{\{\phi\}\}$
   (iv) $\phi \subseteq \{\phi, \{1\}, \{a\}\}$
   (v) $\{a, \{b\}, c, d\} \subset \{a, b, \{c\}, d\}$

Solution :

(i) False, since $1 \in \{1, 2, 3\}$.
(ii) True, since every element of $\{1, 2\}$ is an element of $\{1, 2, 3\}$.
(iii) False, since ϕ is not an element of $\{\{\phi\}\}$.
(iv) True, since ϕ is subset of every set.
(v) False, since $\{b\} \notin \{a, b, \{c\}, d\}$ and $c \notin \{a, b, \{c\}, d\}$.

1.8 POWER SET

Let us consider a set A = {a, b}. A question automatically comes to our mind– 'What are the subsets of A?' The subsets of A are ϕ, {a}, {b} and A itself.

These subsets, taken as elements, again form a set. Such a set is called the power set of the given set A.

Definition : The set consisting of all the subsets of a given set A as its elements, is called the **power set** of A and is denoted by P(A) or 2^A. Thus,

$$P(A) \text{ or } 2^A = \{X : X \subseteq A\}$$

Clearly,

(i) $P(\phi) = \{\phi\}$

(ii) if A = {1}, then $P^A = \{\phi, \{1\}\}$

(iii) if A = {1, 2}, then $P^A = \{\phi, \{1\}, \{2\}, A\}$

(iv) if A = {1, 2, 3}, then $P^A = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$

From these examples we can conclude that if a set A has n elements, then P(A) has 2^n elements.

1.9 UNIVERSAL SET

A set is called a **Universal Set** or the **Universal discourse** if it contains all the sets under consideration in a particular discussion. A universal set is denoted by U.

Example :

(i) For the sets {1, 2, 3}, {3, 7, 8}, {4, 5, 6, 9}
We can take U = {1, 2, 3, 4, 5, 6, 7, 8, 9}

(ii) In connection with the sets N, Z, Q we can take R as the universal set.

(iii) In connection with the population census in India, the set of all people in India is the universal set, etc.

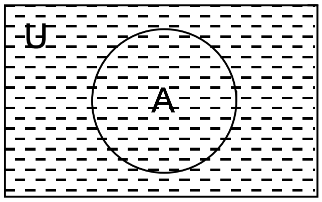
CHECK YOUR PROGRESS - 2

1. Find the empty sets, finite and infinite sets :
   (i) the set of numbers divisible by zero
   (ii) the set of positive integers less than 15 and divisible by 17
   (iii) the set of planets of the solar system
   (iv) the set of positive integers divisible by 4
   (v) the set of coplaner triangles
   (vi) the set of Olympians from Assam participating in 2008, Beijing Olympic.
2. Examine the equality of the following sets :
   (i) $A = \{2, 3\}$, $B = \{x : x^2-5x+6 = 0\}$
   (ii) $A = \{x : x$ is a letter of the word WOLF$\}$
   $B = \{x : x$ is a letter of the word FLOW$\}$
   (iii) $A = \{a, b, c\}$, $B = \{a, \{b, c\}\}$
3. Write true or false :
   (i) $\{1, 3, 5\} \subseteq \{5, 1, 3\}$
   (ii) $\{a\} \subset \{\{a\}, b\}$
   (iii) $\{x : (x-1)(x-2) = 0\} \not\subset \{x : (x^2-3x+2)(x-3) = 0\}$
4. Write down the power sets of the following sets :
   (i) $A = \{1, 2, 3, 4\}$
   (ii) $B = \{1, \{2, 3\}\}$
5. Give examples to show that $(A \subseteq B$ and $B \subseteq C) \Rightarrow A \subseteq C$.

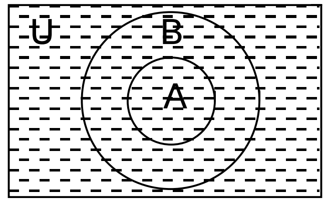
1.10 VENN DIAGRAM

Simple plane geometrical areas are used to represent relationships between sets in meaningful and illustrative ways. These diagrams are called **Venn-Euler** diagrams, or simply the **Venn-diagrams**.

In Venn diagrams, the universal set U is generally represented by a set of points in a rectangular area and the subsets are represented by circular regions within the rectangle, or by any closed curve within the rectangle. As an illustration Venn diagrams of $A \subset U$, $A \subset B \subset U$ are given below :



$A \subset U$



$A \subset B \subset U$

Similar Venn diagrams will be used in subsequent discussions illustrating different algebraic operations on sets.

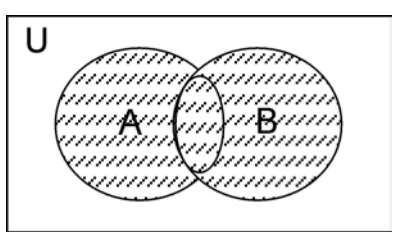
1.11 SET OPERATIONS

We know that given a pair of numbers x and y, we can get new numbers x+y, x–y, xy, $^x/_y$ (with $y \neq 0$) under the operations of addition, subtraction, multiplication and division. Similarly, given the two sets A and B we can form new sets under set operations of **union**, **intersection**, **difference** and **complements**. We will now define these set operations, and the new sets thus obtained will be shown with the help of Venn diagrams.

1.11.1 UNION OF SETS

Definition : The union of two sets A and B is the set of all elements which are members of set A or set B or both. It is denoted by $A \cup B$, read as 'A union B' where '$\cup$' is the symbol for the operation of 'union'. Symbolically we can describe $A \cup B$ as follows :

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



$A \cup B$ (Shaded)

It is obvious that $A \subseteq A \cup B$, $B \subseteq A \cup B$

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

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

Example 2 : Let Q be the set of all rational numbers and K be the set of all irrational numbers and R be the set of all real numbers.

Then $Q \cup K = R$

Identities : If A, B, C be any three sets, then

(i) $A \cup B = B \cup A$

(ii) $A \cup A = A$

(iii) $A \cup \phi = A$

(iv) $A \cup U = U$

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

Proof :

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

(ii) $A \cup A = \{x : x \in A \text{ or } x \in A\} = \{x : x \in A\} = A$

(iii) $A \cup \phi = \{x : x \in A \text{ or } x \in \phi\} = \{x : x \in A\} = A$

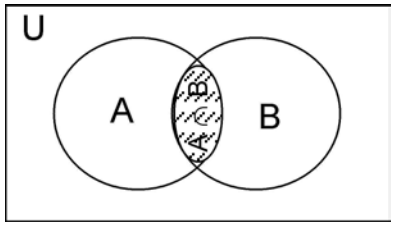
(iv) $A \cup U = \{x : x \in A \text{ or } x \in U\}$
$= \{x : x \in U\}$, since $A \subset U$
$= U$

(v) $(A \cup B) \cup C = \{x : x \in A \cup B \text{ or } x \in C\}$
$= \{x : (x \in A \text{ or } x \in B) \text{ or } x \in C\}$
$= \{x : x \in A \text{ or } (x \in B \text{ or } x \in C\}$
$= \{x : x \in A \text{ or } x \in B \cup C\}$
$= A \cup (B \cup C)$

1.11.2 INTERSECTION OF SETS

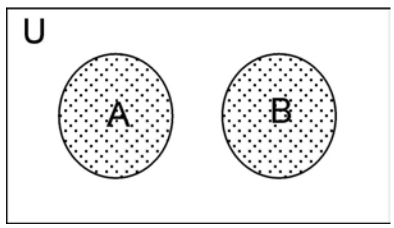
Definition : The intersection of two sets A and B is the set of all elements which are members of both A and B. It is denoted by $A \cap B$, read as 'A intersections B', where '$\cap$' is the symbol for the operation of 'intersection'. Symbolically we can describe it as follows :

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



$A \cap B$ (Shaded)

From definition it is clear that if A and B have no common element, then $A \cap B = \phi$. In this case, the two sets A and B are called **disjoint sets**.



$A \cap B = \phi$

It is obvious that $A \cap B \subseteq A$, $A \cap B \subseteq B$.

Example 1 : Let A = {a, b, c, d}, B = {b, d, 4, 5}

Then $A \cap B = \{b, d\}$

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

Then $A \cap B = \phi$.

Identities :

(i) $A \cap B = B \cap A$

(ii) $A \cap A = A$

(iii) $A \cap \phi = \phi$

(iv) $A \cap U = A$

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

(vi) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

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

Proof :

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

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

$= B \cap A$

(ii) $A \cap A = \{x : x \in A \text{ and } x \in A\}$

$= \{x : x \in A\}$

$= A$

(iii) Since ϕ has no element, so A and ϕ have no common element.

Hence $A \cap \phi = \phi$

(iv) $A \cap U = \{x : x \in A \text{ and } x \in U\}$

$= \{x : x \in A\}$, since $A \subset U$

$= A$

(v) $(A \cap B) \cap C = \{x : x \in A \cap B \text{ and } x \in C\}$

$= \{x : (x \in A \text{ and } x \in B) \text{ and } x \in C\}$

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

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

$= A \cap (B \cap C)$

NOTE

$x \in A \cap B$

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

But, $x \notin A \cap B$

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

Again, $x \in A \cup B$

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

But, $x \notin A \cup B$

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

(vi) $x \in A \cap (B \cup C) \Leftrightarrow x \in A$ and $x \in (B \cup C)$

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

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

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

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

So, $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

and $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Hence, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

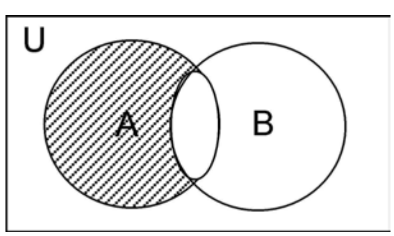
Similarly, it can be proved that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

1.11.3 DIFFERENCE OF SETS

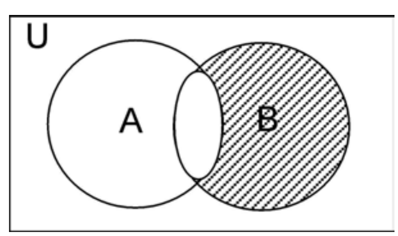
Definition : The difference of two sets A and B is the set of all elements which are members of A, but not of B. It is denoted by A–B.

Symbollically, $A - B = \{x : x \in A \text{ and } x \notin B\}$

Similarly, $B - A = \{x : x \in B \text{ and } x \notin A\}$



A – B (Shaded)



B – A (Shaded)

Example : Let $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 4, 5\}$, $C = \{6, 7, 8\}$

Then $A - B = \{2, 3\}$

$A - C = A$

$B - C = B$

$B - A = \phi$

Properties :

(i) $A - A = \phi$

(ii) $A - B \subseteq A$, $B - A \subseteq B$

(iii) $A - B$, $A \cap B$, $B - A$ are mutually disjoint and

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

(iv) $A - (B \cup C) = (A - B) \cap (A - C)$

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

Proof : We prove (iv), others are left as exercises.

$$\begin{aligned} x \in A - (B \cup C) &\Leftrightarrow x \in A \text{ and } x \notin (B \cup C) \\ &\Leftrightarrow x \in A \text{ and } (x \notin B \text{ and } x \notin C) \\ &\Leftrightarrow (x \in A \text{ and } x \notin B) \text{ and } (x \in A \text{ and } x \notin C) \\ &\Leftrightarrow x \in (A - B) \text{ and } x \in (A - C) \\ &\Leftrightarrow x \in (A - B) \cap (A - C) \end{aligned}$$

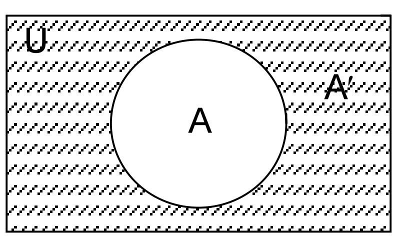
So, $A - (B \cup C) \subseteq (A - B) \cap (A - C)$, $(A - B) \cap (A - C) \subseteq A - (B \cup C)$

Hence, $A - (B \cup C) = (A - B) \cap (A - C)$.

1.11.4 COMPLEMENT OF A SET

Definition : If U be the universal set of a set A, then the set of all those elements in U which are not members of A is called the **Compliment** of A, denoted by A^C or A'.

Symbolically, $A' = \{x : x \in U \text{ and } x \notin A\}$.



A′ (Shaded)

Clearly, $A' = U - A$.

Example : Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $A = \{2, 4, 6, 8\}$

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

Identities :

(i) $U' = \phi$, $\phi' = U$

(ii) $(A')' = A$

(iii) $A \cup A' = U$, $A \cap A' = \phi$

(iv) $A - B = A \cap B'$, $B - A = B \cap A'$

(v) $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$

NOTE

The identities $(A \cup B)' = A' \cap B'$ and $(A \cap B)' = A' \cup B'$ are know as **Derorgan's Laws**.

Proof : We prove $(A \cup B)' = A' \cap B'$. The rest are left as exercises.

$$
\begin{aligned}
(A \cup B)' &= \{x : x \in U \text{ and } x \notin A \cup B\} \\
&= \{x : x \in U \text{ and } (x \notin A \text{ and } x \notin B\} \\
&= \{x : (x \in U \text{ and } x \notin A) \text{ and } (x \in U \text{ and } x \notin B)\} \\
&= \{x : x \in A' \text{ and } x \in B'\} \\
&= A' \cap B'.
\end{aligned}
$$

ILLUSTRATIVE EXAMPLES

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

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

$B = \{3, 6, 9\}$

and $C = \{1, 2, 3, 4, 5\}$, then find

(i) $A \cup B$, (ii) $A \cap C$, (iii) $B \cap C$, (iv) A', (v) $A \cup B'$, (vi) $C' \cap B$, (vii) $A' \cup C'$, (viii) $A - C$, (ix) $A - (B \cup C)'$, (x) $A' \cap B'$.

Solution : (i) $A \cup B = (2, 3, 4, 6, 8, 9, 10\}$

(ii) $A \cap C = \{2, 4\}$

(iii) $B \cap C = \{3\}$

(iv) $A' = \{1, 3, 5, 7, 9\}$

(v) $B' = \{1, 2, 4, 5, 7, 8, 10\}$

So, $A \cup B' = \{1, 2, 4, 5, 6, 7, 8, 10\}$

(vi) $C' = \{6, 7, 8, 9, 10\}$

So, $C' \cap B = \{6, 9\}$

(vii) From (iv) & (vi), $A' \cup C' = \{1, 3, 5, 6, 7, 8, 9, 10\}$

(viii) $A - C = \{6, 8, 10\}$

(ix) $B \cup C = \{1, 2, 3, 4, 5, 6, 9\}$

$(B \cup C)' = \{7, 8, 10\}$

So, $A - (B \cup C)' = \{2, 4, 6\}$

(x) From (iv) & (v), $A' \cap B' = \{1, 5, 7\}$.

2. Verify the identities :

   (i) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

   (ii) $(A \cup B)' = A' \cap B'$

   taking $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, $C = \{3, 4, 5\}$ and $U = \{1, 2, 3, 4, 5, 6\}$.

Solution : (i) $B \cap C = \{3, 4\}$

$A \cup (B \cap C) = \{1, 2, 3, 4\}$ ....(1)

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

$(A \cup B) \cap (A \cup C) = \{1, 2, 3, 4\}$ ....(2)

From (1) & (2), we get

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

(ii) $A' = \{4, 5, 6\}$, $B' = \{1, 5, 6\}$

$A' \cap B' = \{5, 6\}$ ....(3)

$(A \cup B)' = \{1, 2, 3, 4\}' = \{5, 6\}$ ....(4)

From (3) & (4), wet get

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

CHECK YOUR PROGRESS - 3

1. Find the following sets :

   (i) $\phi \cap \{\phi\}$ (ii) $\{\phi\} \cap \{\phi\}$ (iii) $\{\phi, \{\phi\}\} - \{\phi\}$ (iv) $\{\phi, \{\phi\}\} - \{\{\phi\}\}$

2. If $A = \{a, b, c\}$, $B = \{c, d, e\}$, $U = \{a, b, c, d, e, f\}$ then find

   (i) $A \cup B$ (ii) $A \cap B$ (iii) $A - B$ (iv) $B - A$ (v) A'

3. If $A = \{3n : n \in N\}$, $B = \{n : n \in N, n < 20\}$ then find $A \cap B$, $B - A$.

4. If $A = \{x : x \in R, 1 < x \leq 7\}$, $B = \{ x : x \in R, 3 \leq x < 12\}$ then find $A \cup B$, $A \cap B$, $A - B$, $B - A$.

5. Using numerical examples, virify that :

   (i) $A - B = B' - A'$

   (ii) $(A - B) \cup (B - A) = (A \cup B) - (A \cap C)$

   (iii) $A - (B \cap C) = (A - B) \cup (A - C)$

6. Prove that : (i) $B - A \subseteq A'$ (ii) $B - A' = B \cap A$

   (iii) $A \cup B = \phi \Rightarrow A = \phi$ and $B = \phi$.

1.12 LAWS OF THE ALGEBRA OF SETS

In the preceding discussions we have stated and proved various identities under the operations of union, intersection and complement of sets. These identities are considered as **Laws of Algebra of Sets**. These laws can be directly used to prove different propositions on Set Theory. These laws are given below :

1. **Idempotent laws :** $A \cup A = A$, $A \cap A = A$
2. **Commutative laws :** $A \cup B = B \cup A$, $A \cap B = B \cap A$
3. **Associative laws :** $A \cup (B \cup C) = (A \cup B) \cup C$,
   $A \cap (B \cap C) = (A \cap B) \cap C$
4. **Distributive laws :** $A \cup (B \cap C) = (A \cup B) \cap (A \cap C)$,
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. **Identity laws :** $A \cup \phi = A$, $A \cup U = U$
   $A \cap U = A$, $A \cap \phi = \phi$
6. **Complement laws :** $A \cup A' = U$, $A \cap A' = \phi$
   $(A')' = A$, $U' = \phi$, $\phi' = U$
7. **De Morgan's laws :** $(A \cup B)' = A' \cap B'$
   $(A \cap B)' = A' \cup B'$.

Let us illustrate the application of the laws in the following examples :

Example 1 : Prove that $A \cap (A \cup B) = A$

Solution : $A \cap (A \cup B) = (A \cup \phi) \cap (A \cup B)$, using identity law
$= A \cup (\phi \cap B)$, using distributive law
$= A \cup (B \cap \phi)$, using commutative law
$= A \cup \phi$, using identity law
$= A$, again using identity law

Example 2 : Prove that $A \cap (A' \cup B) = A \cap B$

Solution : $A \cap (A' \cup B) = (A \cap A') \cup (A \cap B)$, using distributive law
$= \phi \cup (A \cap B)$, using complement law
$= (A \cap B) \cup \phi$, using commutative law
$= A \cap B$, using identity law

1.13 TOTAL NUMBER OF ELEMENTS IN UNION OF SETS IN TERMS OF ELEMENTS IN INDIVIDUAL SETS AND THEIR INTERSECTIONS

We shall now prove a theorem on the total number of elements in the union of two sets in terms of the number of elements of the two individual sets and the number of elements in their intersection. Its application in solving some practical problems concerning everyday life will be shown in the illustrative examples.

Theorem : If A and B are any two finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$

[The symbol $|S|$ represents total number of elements in a set S]

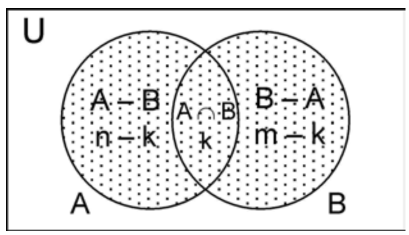
Proof : Let $|A| = n$, $|B| = m$, $|A \cap B| = k$

Then from the Venn diagram, we get $|A - B| = n - k$, $|B - A| = m - k$

We know that $A \cup B = (A - B) \cup (A \cap B) \cup (B - A)$

Where $A - B$, $A \cap B$, $B - A$ are mutually disjoint.

Hence
$$\begin{aligned} |A \cup B| &= |A - B| + |A \cap B| + |B - A| \\ &= (n - k) + k + (m - k) \\ &= n + m - k \\ &= |A| + |B| - |A \cap B| \end{aligned}$$



Deduction :

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

Proof :
$$\begin{aligned} |A \cup B \cup C| &= |(A \cup B) \cup C| \\ &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \\ &= |A| + |B| + |C| - |A \cap B| - \\ &\qquad [|A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)|] \\ &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + \\ &\qquad |A \cap B \cap C| \end{aligned}$$

Corollaries :

(i) If A and B are disjoint, then $A \cap B = \phi$ and so $|A \cap B| = 0$.
Hence $|A \cup B| = |A| + |B|$, which is known as the **Sum Rule of Counting**.

(ii) If A, B and C are mutually disjoint, then as above
$|A \cup B \cup C| = |A| + |B| + |C|$.

ILLUSTRATIVE EXAMPLE

1. In a class of 80 students, everybody can speak either English or Assamese or both. If 39 can speak English, 62 can speak Assamese, how many can speak both the languages?

Solution : Let A, B be the sets of students speaking English and Assamese respectively.

Then $|A \cup B| = 80$, $|A| = 39$, $|B| = 62$.

We are to find $|A \cap B|$.

Now $|A \cup B| = |A| + |B| - |A \cap B|$

So, $|A \cap B| = |A| + |B| - |A \cup B| = 39 + 62 - 80 = 21$.

Hence, 21 students can speak both the languages.

2. Among 60 students in a class, 28 got class I in SEM I and 31 got class I in SEM II. If 20 students did not get class I in either SEMESTERS, how many students got class I in both the SEMESTERS?

Solution : Let A and B be the sets of students who got class I in SEM I and SEM II respectively.

So, $|A| = 28$, $|B| = 31$.

20 students did not get class I in either SEMESTERS out of 60 students in the class.

Hence $|A \cup B| = 60 - 20 = 40$

But $|A \cup B| = |A| + |B| - |A \cap B|$

i.e., $40 = 28 + 31 - |A \cap B|$ So, $|A \cap B| = 19$

Therefore, 19 students did not get class I is both the SEMESTERS.

3. Out of 200 students, 70 play cricket, 60 play football, 25 play hockey, 30 play both cricket and football, 22 play both cricket and hockey, 17 play both football and hockey and 12 play all the three games. How many students do not play any one of the three games?

Solution : Let C, F, H be the sets of students playing cricket, football and hockey respectively. Then

$|C| = 70$, $|F| = 60$, $|H| = 25$,

$|C \cap F| = 30$, $|C \cap H| = 22$, $|F \cap H| = 17$, $|C \cap F \cap H| = 12$.

So, $|C \cup F \cup H| = |C| + |F| + |H| - |C \cap F| - |C \cap H| - |F \cap H| + |C \cap F \cap H|$

$= 70 + 60 + 25 - 30 - 22 - 17 + 12 = 98$

Thus 98 students play atleast one of the three games.

Hence, number of students not playing any one of the three games

$= 200 - 98 = 102.$

EXERCISES

1. Write 'true' or 'false' with proper justification :
   (i) the set of even prime numbers is an empty set
   (ii) $\{x : x+2 = 5, x < 0\}$ is an empty set
   (iii) $\{3\} \subset \{1, 2, 3\}$
   (iv) $x \in \{\{x, y\}\}$
   (v) $\{a, b\} \subseteq \{a, b, \{c\}\}$
   (vi) if A be any set, then $\phi \subseteq A \subseteq U$
2. Which of the following sets are equal?
   $A = \{x : x^2 + x - 2 = 0\}$
   $B = \{x : x^2 - 3x + 2 = 0\}$
   $C = \{x : x \in Z, |x| = 1\}$
   $D = \{-2, 1\}$
   $E = \{1, 2\}$
   $F = \{x : x^2 - 1 = 0\}$
3. Find the sets which are finite and which are infinite :
   (i) the set of natural numbers which are multiple of 7
   (ii) the set of all districts of Assam
   (iii) the set of real numbers between 0 and 1
   (iv) the set of lions in the world.
4. If $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A = \{0, 2, 3, 6\}$, $B = \{1, 2, 6, 8\}$, $C = \{3, 7, 8, 9\}$, then find A', B', C', $(A \cup B) \cap C$, $(A \cup B') \cup C'$, $(A \cap B) \cap C'$, $(A - C) \cup B'$, $(B - A)' \cap C$.
5. If $A \cup B = B$ and $A \cap B = B$, then what is the relation between A and B?

6. Verify the following identities with numerical examples :
   (i) $A - B = B' - A'$
   (ii) $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
   (iii) $A - (B \cap C) = (A - B) \cup (A - C)$
   (iv) $A - (B \cup C) = (A - B) \cap (A - C)$.
7. Write down the power set of the set $A = \{\{\phi\}, a, \{b, c\}\}$.
8. Given $A = \{\{a, b\}, \{c\}, \{d, e, f\}\}$, how many elements are there in $P(A)$?
9. Using numerical examples, show that
   (i) $(A \cap B) \cup (A - B) = A$
   (ii) $A \cup B = A \cup (B - A)$
   (iii) $A \cup B = B \cup (A - B)$
   (iv) $B - A \subseteq A'$
   (v) $B - A' = B \cap A$.
10. Using Venn diagrams show that
    (i) $A \cup B \subset A \cup C$ but $B \not\subset C$
    (ii) $A \cap B \subset A \cap C$ but $B \not\subset C$
    (iii) $A \cup B = A \cup C$ but $B \neq C$.
11. Give numerical examples for the results given in 10.
12. Show that $(A - B) - C = (A - C) - (B - C)$.
13. Out of 100 persons, 45 drink tea and 35 drink coffee. If 10 persons drink both, how many drink neither tea nor coffee?
14. Using sets, find the total number of integers from 1 to 300 which are not divisible by 3, 5 and 7.
15. 90 students in a class appeared in tests for Physics, Chemistry and Mathematics. If 55 passed in Physics, 45 passed in Chemistry, 60 passed in Mathematics, 40 both in Physics and Chemistry, 30 both in Chemistry and Mathematics, 35 both in Physics and Mathematics and 20 passed in all the three subjects, then find the number of students failing in all the three subjects.

1.14 LET US SUM UP

1. A set is a collection of well-defined and distinct objects. The objects are called members or elements of the set.
2. Sets are represented by capital letters and elements by small letters. If 'a' is an element of set A, we write $a \in A$, otherwise $a \notin A$.
3. Sets are represented by (i) Roster or Tabular method and (ii) Rule or Set-builder method.
4. A set having no element is called **empty set** or **null set** or **void set**, denoted by ϕ.
5. A set having a finite number of elements is called a **finite set**, otherwise it is called an **infinite set**.
6. Two sets A and B are equal, i.e. $A = B$ if and only if every element of A is an element of B and also every element of B is an element of A, otherwise $A \neq B$.
7. A is a **subset** of B, denoted by $A \subseteq B$ if every element of A is an element of B and A is a **proper subset** of B if $A \subseteq B$ and $A \neq B$. In this case, we write $A \subset B$.
8. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
9. The set of all the subsets 8 a set A is called the **power set** of A, denoted by P(A) or 2^A. If $|A| = n$, then $|P(A)| = 2^n$.
10. Venn diagrams are plane geometrical diagrams used for representing relationships between sets.
11. The union of two sets A and B is $A \cup B$ which consists of all elements which are either in A or B or in both. $A \cup B = \{x : x \in A \text{ or } x \in B\}$
12. The intersection of two sets A and B is $A \cap B$ which consists of all the elements common to both A and B.
13. For any two sets A and B, the difference set, $A - B$ consists of all elements which are in A, but not in B. $A - B = \{x : x \in A \text{ and } x \notin B\}$
14. The **Universal set U** is that set which contains all the sets under any particular discussion as its subsets.
15. The **complement** of a set A, denoted by A^c or A' is that set which consists of all those elements in U which are not in A.
    $A' = \{x : x \in U \text{ and } x \notin A\} = U - A$
16. Following are the **Laws of Algebra of Sets** :
    $A \cup A = A$, $A \cap A = A$

$A \cup B = B \cup A$, $A \cap B = B \cap A$

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

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

$A \cup \phi = A$, $A \cup U = U$, $A \cap U = A$, $A \cap \phi = \phi$

$A \cup A' = U$, $A \cap A' = \phi$, $(A')' = A$, $U' = \phi$, $\phi' = U$

$(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$.

17. $|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

1.15 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS - 1

1. (i) A = {Monday, Tuesday, Wednessday, Thursday, Friday, Saturday, Sunday}
   (ii) B = {January, February, March, April, May, June, July, August, September, October, November, December}
   (iii) $C = \{1, w, w^2\}$
   (iv) D = {1, 2, 4, 5, 10, 20, 25, 50, 100}
   (v) E = {A, B, E, G, L, R}
2. (i) A = {x : x is a month of the year having 31 days}
   (ii) $B = \{x : x = n^2 - 1, n \in N\}$
   (iii) $C = \{x : x = 5n, n \in Z\}$
   (iv) D = {x : x is a letter of the English Alphabet}
3. (i) True, (ii) False, (iii) True, (iv) True, (v) False, (vi) True.

CHECK YOUR PROGRESS - 2

1. (i) ϕ, (ii) ϕ, (iii) finite, (iv) infinite, (v) infinite, (vi) ϕ.
2. (i) B = {2, 3} = A
   (ii) A = {W, O, L, F}, B = {F, L, O, W} and so, A = B
   (iii) $A \neq B$; since $b \in A$ but $b \notin B$.
3. (i) True
   (ii) False, since $\{a\} \in \{\{a\}, b\}$
   (iii) $\{x : (x-1)(x-2) = 0\} = \{1, 2\}$, $\{x : (x^2-3x+2)(x-3) = 0\} = \{1, 2, 3\}$
   Hence $\{x : (x-1)(x-2) = 0 \subset \{x : (x^2-3x+2)(x-3) = 0\}$ and so, the given result is false.

4. (i) $P(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\},$
$\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, A\}$
(ii) $P(B) = \{\phi, \{1\}, \{\{2, 3\}\}, B\}$

CHECK YOUR PROGRESS - 3

1. (i) ϕ, (ii) $\{\phi\}$, (iii) $\{\{\phi\}\}$, (iv) $\{\phi\}$
2. (i) $A \cap B = \{a, b, c, d, e\}$, (ii) $\{C\}$, (iii) $A - B = \{a, b\}$, (iv) $B - A = \{d, e\}$,
(v) $A' = \{d, e, f\}$
3. $A = \{3, 6, 9, 12, 15, 18, 21, ...\}$, $B = \{1, 2, 3, ..., 18, 19, 20\}$,
Hence $A \cap B = \{3, 6, 9, 12, 15, 18\}$
and $B - A = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19\}$
4. $A \cup B = \{x : 1 < x < 12, x \in R\}$
$A \cap B = \{x : x \in R, 3 \le x \le 7\}$
$A - B = \{x : x \in R, 1 < x < 3\}$
$B - A = \{x : x \in R, 7 < x < 12\}$
5. Take $U = \{p, q, r, s, t, u, v, w, x, y, z\}$, $A = \{p, q, u, v, x, y\}$
$B = \{q, v, y, z\}$ and $C = \{p, s, t, v, x, y\}$
(i) $A - B = \{p, u, x\}$, $A' = \{r, s, t, w, z\}$, $B' = \{p, r, s, t, u, x\}$
$B' - A' = \{p, u, x\}$ and hence, $A - B = B' - A'$
(ii) $B - A = \{z\}$ and so, $(A - B) \cup (B - A) = \{p, u, x, z\}$
Again, $A \cup B = \{p, q, u, v, x, y, z\}$ and $A \cap B = \{q, v, y\}$
So, $(A \cup B) - (A \cap B) = \{p, u, x, z\}$
Thus, $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$
(iii) $A - C = \{q, u\}$ and so, $(A - B) \cup (A - C) = \{p, q, u, x\}$
$B \cap C = \{v, y\}$ and so, $A - (B \cap C) = \{p, q, u, x\}$
Thus $A - (B \cap C) = (A - B) \cup (A - C)$.
6. (i) $x \in B - A \Rightarrow x \in B$ and $x \notin A \Rightarrow x \in U$ and $x \notin A$
$\Rightarrow x \in A'$, Where x is an arbitrary element of $(B - A)$.
Hence $B - A \subseteq A'$
(ii) $x \in B - A' \Leftrightarrow x \in B$ and $x \notin A'$
$\Leftrightarrow x \in B$ and $x \in A \Leftrightarrow x \in B \cap A$
Hence $B - A' \subseteq B \cap A$ and $B \cap A \subseteq B - A'$
Thus, $B - A' = B \cap A$
(iii) $A \subseteq A \cup B \Rightarrow A \subseteq \phi$, as $A \cup B = \phi$ ——(1)
Also $\phi \subseteq A$ ——(2)
From (1) & (2), we get $A = \phi$. Similarly, $B = \phi$.

1.16 FURTHER READINGS

(i) Discrete Mathematics – Semyour Lipschutz & Marc Lipson.

(ii) Discrete Mathematical Structures with Applications to Computer Scinece – J. P. Tremblay & R. Manohar.

1.17 POSSIBLE QUESTIONS

1. Give examples of
   (i) five null sets
   (ii) five finite sets
   (iii) five infinite sets
2. Write donw the following sets in rule method
   (i) $A = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$
   (ii) $B = \left\{\frac{1}{1.2}, \frac{1}{2.3}, \frac{1}{3.4}, \frac{1}{4.5}, \ldots\right\}$
   (iii) $C = \{2, 5, 10, 17, 26, 37, 50\}$
3. Write down the following sets in roster method
   (i) $A = \{x : x \in N, 2 < x < 10\}$
   (ii) $B = \{x : x \in N, 4+x < 15\}$
   (iii) $C = \{x : x \in Z, -5 \leq x \leq 5\}$
4. If $A = \{1, 3\}$, $B = \{1, 3, 5, 9\}$, $C = \{2, 4, 6, 8\}$ and $D = \{1, 3, 5, 7, 9\}$ then fill up the dots by the symbol $\subseteq$ or $\not\subseteq$:
   (i) A ... B, (ii) A ... C, (iii) C ... D, (iv) B ... D
5. Write true or false :
   (i) $4 \in \{1, 2, \{3, 4\}, 5\}$, (ii) $\phi = \{\phi\}$
   (iii) $A = \{2, 3\}$ is a proper subset of $B = \{x : (x-1)(x-2)(x-3) = 0\}$
   (iv) $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$
6. If $U = \{x : x \in N\}$, $A = \{x : x \in N, x \text{ is even}\}$, $B = \{x : x \in N, x < 10\}$
   $C = \{x : x \in N, x \text{ is divisible by } 3\}$, then find (i) $A \cup B$, (ii) $A \cap C$, (iii) $B \cap C$, (iv) A', (v) B', (vi) C'.
7. If $A \cup B = B$ and $B \cup C = C$, then show that $A \subseteq C$.

8. If $U = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$,
   $A = \{-5, -2, 1, 2, 4\}$
   $B = \{-2, -3, 0, 2, 4, 5\}$
   $C = \{1, 0, 2, 3, 4, 5\}$,
   then find (i) $A \cup B$, (ii) $A \cap C$, (iii) $A \cap (B \cup C)$,
   (iv) $B \cap C'$, (v) $A' \cup (B \cap C')$, (vi) $A - C'$, (vii) $A - (B \cup C)'$,
   (viii) $(B \cup C')$, (ix) $A' \cup C'$, (x) $(C' \cup B) - A$.

9. Prove the following :
   (i) If A, B, C are three sets such that $A \subseteq B$, then $A \cup C \subseteq B \cup C$, $A \cap C \subseteq B \cap C$.
   (ii) $A \subseteq B$ if and only if $B' \subseteq A'$.
   (iii) $A \subseteq B$ if and only if $A \cap B = A$.
   (iv) If $A \cap B = \phi$, then $A \subseteq B'$.

10. How many elements are there in P(A) if A has (i) 5 elements, (ii) 2^n elements?

11. Every resident in Guwahati can speak Assamese or English or both. If 80% can speak Assamese and 30% can speak both the language, what percent of residents can speak English?

12. 76% of the students of a college drink tea and 63% drink coffee. Show that a minimum of 39% and a minimum of 63% drink both tea and coffee.

13. In a survey of 100 students it is found that 40 read Readers' Digest, 32 read India Today, 26 read the Outlook, 10 read both Readers' Digest and India Today, 6 read India Today and the Outlook, 7 read Readers' Digest and the Outlook and 5 read all the three. How many read none of the magazines?

14. In an examination 60% students passed in Mathematics, 50% passed in Physics, 40% passed in Computer Science, 20% passed in both Mathematics and Physics, 40% passed in both Physics and Computer Science, 30% passed in both Mathematics and Computer Science and 10% passed in all the three subjects. What percent failed in all the three subjects?

UNIT 2: RELATIONS AND FUNCTIONS

UNIT STRUCTURE

2.1 LEARNING OBJECTIVES

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

- the concept of a relation
- different types of relation
- equivalence relation, equivalence class
- the concept of a function
- different types of function.

2.2 INTRODUCTION

Set theory may be called the language of modern mathematics. We know that a set is a well-defined collection of objects. Also we know the notion of subset of a set. If every element of a set B is in set A, then B is a subset of A. Symbolically we denote it by $B \subseteq A$.

Also we note that if A is a finite set having n elements, the number of subsets of A is 2^n.

Again if A, B are two non-empty sets, the cartesian product of A and B is denoted by A x B and is defined by $A \times B = \{(a, b) : a \in A, b \in B\}$

(a, b) is called an ordered pair.

Let $a \in A$, $c \in A$; $b \in B$, $d \in B$.

$\therefore (a, b) \in A \times B$, $(c, d) \in A \times B$

We know that $(a, b) = (c, d) \Leftrightarrow a=c, b=d$.

Also we know that if A, B are finite and n(A)=x, n(B)= y, then

$$n(A \times B) = n(B \times A) = xy$$

[Here n(A) denotes the number of elements of A]

If one of the sets A and B is infinite, then A x B and B x A are infinite.

In this unit we will study relations and functions which are subsets of cartesian product of two sets.

We will denote the set of natural numbers by 'N', the set of integers by Z, the set of rational numbers by Q, the set of real numbers by IR, the set of complex numbers by C.

2.3 CONCEPT OF RELATION

Let us consider the following sentences.

(1) 11 is greater then 10.

(2) 35 is divisible by 7.

(3) New Delhi is the capital of India.

In each of the sentences there is a relation between two 'objects'.

Now let us see what is meant by relation in set theory.

Definition Let A and B be two non-empty sets. A subset R of A x B is said to be a **relation** from A to B.

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

If $R \subseteq A \times B$, and $(a, b) \in R$; $a \in A$, $b \in B$, it is also written as aRb and is read as 'a is R 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(AxB)=xy. So, the number of subsets of AxB is 2^{xy}.

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

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

B={8, 9}

$\therefore$ A x B ={(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 2 : Let IR be the set of real numbers.

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

$\therefore$ R is a relation of IR.

$\because$ 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 3: Let X be the set of odd integers.

Let R = {(x, y) : 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 X

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

Example 4: 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 the even integers is an even integer.

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

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

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

2.3.1 Identity Relation

Let A be a non-empty set.

$I_A = \{(a, a) : a \in A\} \subseteq A \times A$

I_A is called the identity relation on A.

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

Then $I_A = \{(1, 1), (2, 2), (3, 3), (4, 4)\} \subseteq A \times A$.

Clearly I_A is the identity relation on A.

2.3.2 Inverse Relation

Let A, B be two non-empty sets. Let R be a relation from A to B, i.e. $R \subseteq A\times B$. The inverse relation of R is denoted by R^{-1}, and is defined by $R^{-1}=\{(b, a) : (a, b)\in R\} \subseteq B \times A$

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

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

Example 6: Let A = {1, 2, 3}

B = {5, 6}

$R = \{(1, 5), (2, 6), (3, 5)\} \subseteq A \times B$

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

CHECK YOUR PROGRESS 1

Q 1: Let A, B be two finite sets, and n(A)=4, n(B)=3. How many relations are there from A to B ?

Q 2: Let A be a finite set such that n(A) =5. Write down the number of relations on A.

Q 3: Let IN be the set of natural numbers.

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

Examine if the following ordered pairs belong to R.

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

Q 4: Let E be the set of even integers.

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

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

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

Write down the identity relation on A.

Q 6: 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}.

2.4 TYPES OF RELATION

Let A be a non-empty set, and R be a relation on A, i.e. $R \subseteq A \times A$.

1. R is called reflexive if $(a, a) \in R$, i.e; 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 anti-symmetric 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 7: Let $A = \{1, 2, 3\}$

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

Examine if R is reflexive, symmetric,anti-symmetric, 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 anti-symmetric.

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

$\therefore$ R is transitive.

Example 8: Let Z be the set of integers, and $R = \{(x, y) : x, y \in Z, x \leq y\}$

Examine if R is reflexive, symmetric, anti-symmetric and transitive.

Solution : We have $a \leq a$, $\forall\ a \in Z$

i.e, $(a, a) \in R$, $\forall a \in Z$

$\therefore$ R is reflexive.

Again, if $a \leq b$, $b \not\leq a$

i.e; $(a, b) \in R \not\Rightarrow (b, a) \in R$

$\therefore$ 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 anti-symmetric.

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

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

Let $R = \{(1, 1), (1, 2)\} \subseteq A \times A$

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.

CHECK YOUR PROGRESS 2

Q 1: Let $A = \{1, 2, 3)$ and R be a reflexive relation on A having minimum number of ordered pairs. Write down R.

Q 2: Define a relation on the set

$A = \{1, 2, 3, 4\}$ which is

(i) symmetric, but neither reflexive nor transitive;

(ii) reflexive and transitive, but not symmetric;

(iii) reflexive and symmetric, but not transitive.

2.5 EQUIVALENCE RELATION

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

Example 10: Let Z be the set of integers and

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

Examine if R is an equivalence relation on Z.

Solution : Let $x \in Z$

$\therefore$ $x+x$ is even

$\Rightarrow (x, x) \in R, \forall x \in Z$

$\therefore$ 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

$(x, z) \in R$

$\therefore$ R is transitive

$\therefore$ R is an equivalence relation on Z.

Example 11: 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 : A line cannot be perperdicular to itself, i.e. $x \not\perp x$

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

$\therefore$ R is not reflexive

If a line x is perpendicular to another line y, then y is perpendicular to x, i.e.

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

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

$\therefore$ R is symmetric.

If $x \perp y$, $y \perp z$, then $x \not\perp z$

$\therefore (x, y), (y, z) \in R \not\Rightarrow (x, z) \in R$

If x is perpendicular to y, y is perpendicular to z, then x is parallel to z.

$\therefore$ R is not transitive.

Example 12: Let A be the set of all straight lines in a plane.

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

Examine if R is an equivalence relation on A.

Solution : A line is parallel to itself, i.e. $x \| x \ \forall \ x \in A$

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

$\therefore$ R is reflexive.

$x \| y \Rightarrow y \| x$

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

$\therefore$ R is symmetric.

$x \| y, y \| z \Rightarrow x \| z$

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

$\therefore$ R is transitive

Thus, R is an equivalence relation on A.

Example 13: Let IN be the set of natural numbers. Let a relation R be defined on IN x IN by (a, b) R (c, d) if and only if ad = bc

Show that R is an equivalence relation on IN x IN.

Solution : We have ab = ba

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

$\therefore$ R is reflexive

(a, b) R (c, d) $\Rightarrow$ ad = bc; a, b, c, d, $\in$ IN

$\Rightarrow$ cb = da

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

$\therefore$ R is symmetric

(a, b) R (c, d) and (c, d) R (e, f); a, b, c, d, e, f, $\in$ IN

$\Rightarrow$ 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 IN x IN.

Example 14: (Congruence modulo n)

Let Z be the set of integers, and n be any fixed positive integer.

Let a, b$\in$ Z

a is said to be congruent to b modulo n if and only if a–b is divisible by n.

Symbolically, we write.

a $\equiv$b (mod n)

Show that the relation 'congruence modulo n' is an equivalence relation on Z.

Solution : We know that a–a is divisible by n, i.e., a $\equiv$ a (mod n)

$\therefore$ the relation is reflexive.

Let a $\equiv$b (mod n)

$\Rightarrow$ a–b is divisible by n.

$\Rightarrow$ b–a is divisible by n.

$\Rightarrow$ b$\equiv$a (mod n)

$\therefore$ the relation is symmetric.

Let a $\equiv$b (mod n), b $\equiv$c (mod 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 (mod n)

$\therefore$ the relation is transitive.

Thus, the relation 'congruence modulo n' is an equivalence relation on Z.

We know that 15-3 is divisible by 4.

$\therefore$15 is congruent to 3 modulo 4 i.e.

15 $\equiv$3 (mod 4)

15–3 is not divisible by 7

$\therefore$15 is not congruent to 3 modulo 7

i.e. 15 $\not\equiv$3 (mod 7)

Example 15: Let Z be the set of integers.

Let R = {(a, b) : a, b $\in$ Z, ab$\geq$0}

Examine if R is an equivalence relation on Z.

Solution : We have aa $\geq$0

$\therefore (a, a) \in R, \forall a \in Z$

$\therefore$ 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

$(-2) \times 0 = 0, 0 \times 2 = 0$

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

But $(-2) \times 2 = -4 < 0$

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

$\therefore$ R is not transitive.

Thus, R is not an equivalence relation.

Theorem 1: The inverse of an equivalence relation is also an equivalence relation.

Proof. Let A be a non-empty set. Let R be an equivalence relation on A

R is reflexive.

$\therefore (x, x) \in R, \forall x \in A$

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

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

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

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

$\Rightarrow (x, y) \in R$ [$\therefore$ 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 def^n of R^{-1}]

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

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

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

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

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

Theorem 2: The intersection of two equivalence relations is also an equivalence relation.

Proof. Let A be a non-empty set.

Let R and S be two equivalence relations on A.

R and S are reflexive

$\therefore (x, x) \in R$ and $(x, x) \in S, \forall x \in A$

$\Rightarrow (x, x) \in R \cap S, \forall x \in A$

$\therefore R \cap S$ 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 $(y, x) \in S$ [$\therefore$ R, 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 $(x, z) \in S$ [$\therefore$ R, S are transitive]

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

$\therefore R \cap S$ is transitive.

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

Remarks : 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.

$R \cup S$ = {(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

$\therefore$ $R \cup S$ is not an equivalence relation.

2.5.1 Equivalence Class

Let us consider the set Z of integers

Let R = {(a, b) : a, b $\in$ Z, a–b is divisible by 3}

i.e. R = {(a, b) : a, b$\in$Z, a $\equiv$b (mod 3)}

Clearly R is reflexive, symmetric and transitive.

$\therefore$ R is an equivalence relation on Z.

Let [0] denote the set of integers congruent to 0 modulo 3. Then

[0] = {...., –9, –6, –3, 0, 3, 6, 9, ...}

Let [1] denote the set of integers congruent to 1 modulo 3. Then

[1] = {..., –8, –5, –2, 1, 4, 7, 10, ...}

Let [2] denote the set of integers congruent to 2 modulo 3. Then

[2] = {...., –7, – 4, –1, 2, 5, 8, 11, ...}

We see that

...... = [0] = [3] = [6] =.....

...... = [1] = [4] = [7] =.....

...... = [2] = [5] = [8] =.....

Each of [0], [1], [2] is called an equivalence class. [0] is the equivalence class of 0, [1] is the equivalence class of 1, [2] is the equivalence class of 2.

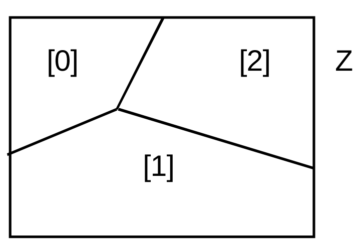
We see that there are 3 distinct equivalence classes, viz, [0], [1], [2].

Also we note that

[0] U [1] U [2] = z

[0] $\cap$ [1] =ϕ , [1] $\cap$ [2] = ϕ [2]$\cap$[0] = ϕ

The set {[0], [1], [2]} is called a partition of Z.



Definition : Let A be a non-empty set and R be a relation on A.

For any a$\in$A, the equivalence class [a] of a is defined by

$[a] = \{x \in A : xRa\}$

i.e. the equivalence class [a] of a is the collection of all those elements of A which are related to a under the relation R.

Note : $[a] \neq \phi$, $\because$ aRa

Definition : Let A be a non-empty set.

The set P of non-empty subsets of A is called a partition of A if

(i) A is the union of all members of P,

(ii) any two distinct members of P are disjoint.

Theorem 3 : Let A be a non-empty set and R be an equivalence relation of A. Let a, b $\in$ A. Then [a] = [b] if and only if (a, b) $\in$R.

Proof. Let [a] = [b]

$\because$ R is reflexive, $\therefore$ aRa

$\therefore$ a $\in$[a]

$\Rightarrow$ a $\in$[b] [$\because$ [a]=[b]]

$\Rightarrow$ aRb

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

Conversely : Let (a, b) $\in$R. $\therefore$ aRb

Let x $\in$ [a]. $\therefore$ xRa

Now, xRa and aRb

$\therefore$ xRb [$\because$ R is transitive]

$\Rightarrow$ x$\in$ [b]

Thus, x $\in$ [a] $\Rightarrow$ x$\in$[b]

$\therefore$[a] $\subseteq$ [b] ... (1)

Again, let y$\in$[b] $\therefore$ yRb

Now, yRb and bRa [$\because$ R is symmetric, aRb $\Rightarrow$ bRa]

$\therefore$ yRa [$\because$ R is transitive]

$\Rightarrow$ y$\in$ [a]

Thus, y$\in$[b] $\Rightarrow$ y$\in$[a]

$\therefore$ [b] $\subseteq$ [a] ... (2)

From (1) and (2), [a] = [b]

Theorem 4 : Two equivalence classes are either equal or disjoint.

Proof. Let A be a non-empty set. Let R be an equivalence relation on A.

If A, B are two non-empty sets, then either $A \cap B \neq \phi$ or $A \cap B = \phi$

Let a, b $\in$ A.

Then [a], [b] are either not disjoint or disjoint.

Let [a], [b] be not disjoint,

i.e. $[a] \cap [b] \neq \phi$.

Let $x \in [a] \cap [b]$

$\Rightarrow x \in [a]$ and $x \in [b]$

$\Rightarrow$ xRa and xRb

$\Rightarrow$ aRx and xRb [$\because$ R is symmetric, xRa $\Rightarrow$ aRx]

$\Rightarrow$ aRb [$\because$ R is transitive]

Let $y \in [a]$

$\Rightarrow$ yRa

Now yRa and aRb

$\therefore$ yRb [$\because$ R is transitive]

$\Rightarrow y \in [b]$

Thus, $y \in [a] \Rightarrow y \in [b]$

$\therefore [a] \subseteq [b]$

Similarly, $[b] \subseteq [a]$

$\therefore [a] = [b]$

So, if [a], [b] are not disjoint, they are equal.

$\therefore$ [a], [b] are either equal or disjoint.

CHECK YOUR PROGRESS 3

Q 1: What is the name of the relation on a set . which is reflexive, symmetric and transitive?

Q 2: Is the relation "<" on the set of narural nimbers IN an equivalence relation? Justify your answer.

Q 3: Let Z be the set of integers.

Let R = {(a, b) : a, b $\in$ Z, a–b is divisible by 5}

Examine if R is an equivalence relation on Z ?

Q 4: Let A be the set of all triangles in a plane.

Let R = {(x, y) : x, y $\in$ A., x is similar to y}

Examine if R is an equivalence relation on A.

Q 5: let Z be the set of integers.

Let R = {(x, y) : x, y $\in$ Z, x–y is even}

Is R an equivalence relation on Z ?

Justify your answer.

2.6 CONCEPT OF FUNCTION

Let A and B be two non-empty sets, and f $\subseteq$ A xB such that

(i) (x, y) $\in$ f, $\forall$ x$\in$A and any y$\in$B

(ii) (x, y) $\in$ f and (x, y$'$)$\in$ f $\Rightarrow$ y=y$'$.

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

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

Example 16 : Let A = {1, 2}, B = {7, 8, 9}

f = {(1, 8), 2, 7)} $\subseteq$ A x B.

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

$\therefore$f is a function from A to B.

Example 17 : Let A = {1, 2}, B = {7, 8, 9}

g = {(1, 7), (1, 9)} $\subseteq$ A x B

Here, two distinct ordered pairs have the same first component.

$\therefore$ f is not a function from A to B.

Example 18 : Let A = {1, 2, 3, 4}, B = {x, y, z, w}

Are the following relations from A to B be functions?

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

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

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

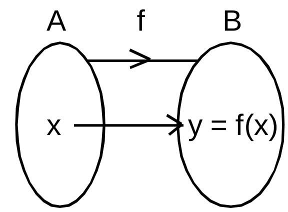
(ii) Yes.

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.

We observe that if A and B are two non-empty 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 the set A to the set B. The rules are denoted by f, g etc. The sets A, B may be the same.



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

$f : A \rightarrow B$. The unique element y of B that is associated with x of A is called the image of x under f. Symbolically we write it as $f = f(x)$. x is called the pre-image of y. The set of all the images under f is called the range of f.

Example 19 : Let IN be the set of natural members, and Z be the set of integer and $f : IN \rightarrow Z$, $f(x) = (-1)^x$; $x \in IN$

Clearly, domain of f = IN

codomain of f = Z

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

$\therefore$ range of f = $\{-1, 1\}$

2.6.1 Identity Function

Let A be a non-empty set and $i : A \rightarrow A$, $i(x) = x$, $\forall x \in A$

i is called the identity function.

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

2.6.2 Constant Function

Let A, B be two non-empty sets and $f : A \rightarrow B$ be a function such that $f(x) = k$, $\forall x \in A$

f is called a constant function.

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

2.7 TYPES OF FUNCTION

Let A, B be two non-empty sets and $f : A \rightarrow B$ be a function.

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 an onto function, range of f=codomain 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?

Let $x_1, x_2, \in A$

If $f(x) = f(x_2) \Rightarrow x_1 = x_2$, then f is one-one.

or,

If $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, then f is one-one.

How to prove that f is onto?

Let $y \in B$ (codomain)

Let $y = f(x)$

We find x in terms of y

If $x \in A$, then f is onto; otherwise not.

Example 20: Let IN be the set of natural numbers,

Let $f : IN \rightarrow IN$, $f(x) = 3x+7$

Examine if f is a bjective function.

Solution : Let $x_1, x_2 \in IN$ (domain)

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

$\Rightarrow 3x_1+7=3x_2+7$

$\Rightarrow x_1 = x_2$

$\therefore$ f is one-one (injection).

Let $y \in IN$ (codomain)

Let $y = f(x)$

$\Rightarrow y = 3x + 7$

$\Rightarrow$ x = $\frac{y-7}{3}$

If y = 1, x = $\frac{1-7}{3}$ = -2 $\notin$ N

$\therefore$ f is not onto

$\therefore$ f is not a bijection.

Example 21: Let X be the set of real numbers excluding 1. Show that the function f : X$\rightarrow$X, f(x)=$\frac{x+1}{x-1}$ is one-one and onto.

Solution: Let $x_1, x_2 \in$ X(domain)

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

$\Rightarrow \frac{x_1+1}{x_1-1} = \frac{x_2+1}{x_2-1}$

$\Rightarrow \frac{(x_1+1)+(x_1-1)}{(x_1+1)-(x_1-1)} = \frac{(x_2+1)+(x_2-1)}{(x_2-1)-(x_2-1)}$ (by componendo and dividendo)

$\Rightarrow \frac{2x_1}{2} = \frac{2x_2}{2}$

$\Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

Let y $\in$ X (codomain)

Let y = f(x)

$\Rightarrow y = \frac{x+1}{x-1}$

$\Rightarrow$ y(x–1) = x+1

$\Rightarrow$ yx–y = x+1

$\Rightarrow$ yx – x = y+1

$\Rightarrow$ x(y–1) = y+1

$\Rightarrow x = \frac{y+1}{y-1}$ $\in$ X (domain)

$\therefore$ f is onto.

Example 22: Let A = {1, 2, 3,}. Write down all the bijective function from A to itself.

Solution :

i : A$\rightarrow$ A, i(1) = 1, i(2) = 2, i(3) = 3

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

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

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

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

$f_5 : A \to A$, $f_5(1) = 3$, $f_5(2) = 1$, $f_5(3) = 2$

Note. There are 6 =3! bijective functions from A = {1, 2, 3} to itself.

If A has n elements, there are n! bijective functions from A to itself.

Theorem 5 : Let A be a finite set, and $f : A \to A$ be onto. Then f is one-one.

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

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

Let $f : A \to A$ be onto.

Now, range of f

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

$\therefore$ f is onto, range of f = codomain of f = A.

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

$\therefore$ A has n elements,

$\therefore f(a_1), f(a_2), ..., f(a_n)$ are distinct.

Thus, distinct elements in A (domain) have distinct images in A (codomain).

$\therefore$ f is one-one.

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

Let IN be the set of natural numbers.

Let $f : IN \to IN$, $f(x) = 1$, if x = 1 and x = 2,

$= x-1$, if $x \geq 3$

Clearly, f is onto, but not one-one.

Theorem 6 : Let A be a finite set, and $f:A \to A$ be one-one. Then f is onto.

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

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

Let $f : A \to A$ be one-one.

$\therefore f(a_1), f(a_2), ..., f(a_n)$ are n distinct elements of A (codomain).

Let $u \in A$ (codomain).

Let $u = f(a_i)$, $1 \leq i \leq n$

$\therefore$ there exists $a_i \in A$ (domain) such that $f(a_i) = u$.

$\therefore$ f is onto.

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

Let IN be the set of natural numbers.

Let f : IN $\rightarrow$IN, f(x) = 5x

Clearly, f is one-one, but not onto.

CHECK YOUR PROGRESS 4

Q 1: Let IN be the set of natural numbers.

Let f : IN $\rightarrow$IN, f(x) = x^2+1

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

Q 2: Let IR be the set of real numbers and

f : IR$\rightarrow$IR be defined by

$$f(x) = \begin{cases} 1, & \text{if} \quad x > 0 \\ 0, & \text{if} \quad x = 0 \\ -1, & \text{if} \quad x < 0 \end{cases}$$

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

Q 3: Let f : IR$\rightarrow$IR be defined by f (x) =|x|

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

$$\left[f(x) = |x| = \begin{cases} x, \text{ if} & x \geq 0 \\ -x, \text{ if} & x < 0 \end{cases} \right]$$

Q 4: If A = {1, 2}, write down all the bijective functions from A to itself.

Q 5: Write down the condition such that a constant function is onto.

Q 6: Write down the condition such that a constant function is one-one.

2.8LET US SUM UP

- If A, B are two non-empty sets, a subset of A x B in said to be a relation from A to B.
- If A, B are two finite sets and n(A) = x, n(B) = y, the number of relations from A to B is 2^{xy}.
- If A is a non-empty set, I_A = {(a, a) : a$\in$A} is called the identity relation on A.

- If A, B are two non-empty and R is a relation from A to B, the inverse relation R^{-1} is defined by
  $R^{-1} = \{(b, a) : (a, b) \in R\}$, which is a relation from B to A.
- A relation R on a non-empty set A is called.
  (i) reflexive if $(a, a) \in R$, for all $a \in A$;
  (ii) symmetric if whenever $(a, b) \in R$, $(b, a) \in R$;
  (iii) anti-symmetric if $(a, b) \in R$, $(b, a) \in R \Rightarrow a = b$;
  (iv) transitive if whenever $(a, b), (b, c) \in R$, then $(a, c) \in R$.
- A relation R on a non-empty set A is called an equivalence relation if it is reflexive, symmetric and transitive.
- The inverse of an equivalence relation is also an equivalence relation.
- The intersection of two equivalence relations is also an equivalence relation.
- If R is a relation on a non-empty set A, then for any $a \in A$; the equivalence class [a] of a is the collection of all those elements of A which are related to a under the relation R.
- Two equivalence classes are either equal or disjoint.
- If A and B are two non-empty 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 a relation, but every relation is not a function.
- If different elements in domain have different images in codomain, then the function is one-one (injective).
- If each element in codomain is the image of at least one element in domain then the function is onto (surjective).
- A function is bijective if it is injective and surjective.
- If A is a finite set and $f : A \rightarrow A$ is onto, then f is one-one.
- If A is a finite set and $f : A \rightarrow A$ is one-one, then f is onto.

2.9 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: 2^{12}

Ans to Q No 2: 2^{25}

Ans to Q No 3: (7, 4), (72, 27) belong to R.

Ans to Q No 4: Yes. The sum of two even integers cannot be odd.

Ans to Q No 5: $I_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$

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

CHECK YOUR PROGRESS – 2

Ans to Q No 1: $R = \{(1, 1), (2, 2), (3, 3)\}$

CHECK YOUR PROGRESS – 3

Ans to Q No 1: Equivalence relation.

Ans to Q No 2: No. Not reflexive and symmetric.

Ans to Q No 3: Equivalence relation.

Ans to Q No 4: Equivalence relation.

Ans to Q No 5: Yes.

CHECK YOUR PROGRESS – 4

Ans to Q No 1: One-one, but not onto.

Ans to Q No 2: Neither one-one nor onto.

Ans to Q No 3: Neither one-one nor onto

Ans to Q No 4: $i : A \to A$, $i(1) = 1$, $i(2) = 2$

$f : A \to A$, $f(1) = 2$, $f(2) = 1$

Ans to Q No 5: Codomain is a singleton set.

Ans to Q No 6: Domain is a singleton set.

2.10 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.

2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).

3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).

4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.

5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

2.11 POSSIBLE QUESTION

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

How many relations are there from A to B ? Write down any four relations from A to B.

Q 2: 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 3: Let Q be the set of rational numbers and f : Q$\rightarrow$Q be a function defined f(x) = 4x+5. Examine if f is bijective

Q 4: Let A be the set of all triangles in a plane.

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

Examine if R is an equivalence relation on A.

Q 5: Let IN be the set of natural numbers. A relation R is defined on IN x IN by (a, b), R (c, d) if and only if a+d = b+c.

Show that R is an equivalence relation on IN x IN.

Q 6: Let A = {1, 2, 3}

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

Show that R is reflexive but neither symmetric nor transitive.

Q 7: Let C be the set of complex numbers and IR be the set of real numbers.

Let $f : C \rightarrow IR$, $f(z) = |z|$, $z \in C$.

Examine if f is (1) one-one, (ii) onto.

Q 8: Let A, B be two non-empty sets.

Let $f : A \times B \rightarrow B \times A$, $f(a, b) = (b, a)$; $(a, b) \in A \times B$

Show that f is bijective.

Q 9: Let f : IN x IN, $f(a, b) = 3^a 4^b$, $(a, b) \in IN \times IN$

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

Q 10: Let $f : Z \times Z \rightarrow Z$, $f(a, b) = ab$, $(a, b) \in Z \times Z$

Examine if f is (i) injective, (ii) surjective.

*** ***** ***

Unit - 3 PROPOSITIONAL LOGIC - 1

UNIT STRUCTURE

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to

- define statements and examples of statements
- define truth tables about different statements
- know about negation of statements
- know about conjuction, disjunction, conditional and bi-conditional of two statements
- Learn about converse, opposite and contrapositive of statement

3.2 INTRODUCTION

Mathematical logic or logic is the discipline that deal with the methods of reasoning . As all of us know that the main asset that makes humans far move superior that other species is the ability of reasoning. Logic provides rules and techniques for determining whether a given argument or mathematical proof or conclusion in a scientific theory is valid or not . Logic is concerned with studying arguments and conclusions. Logic is used in mathematics to prove theories and to draw conclusions from experiments in physical science in our every day life to solve many types of problem . Logic is used in computer science to verify the correctness of programs. The rules of logic or techniques of logic are called rules of inference because the main aim of logic is to draw conclusions inferences from given set of hypothesis. In this unit, we will introduce you to the definition and examples of statements, truth table of different statements. We will allso discuss about the logical connectives. Moreover, we will discuss about the converse, opposite and contrapositive of statements.

3.3 DEFINITION OF STATEMENTS

In logic we communicate our ideas or thoughts with the help of sentences in a particular language. The following types of sentences are normally used in our everyday communication.

Assertive sentence : A sentence that makes an assertion is called an assertive sentence or declerative sentence.
For example , “ Mars supports life .“is an assertive or a declerative sentence .

Imperative sentence : A sentence that expresses a request or a command is called an imperative sentence .
For example , “ please bring me a cup of tea.” is an imperative.

Exclamatory sentence : A sentence that express some strong feeling is called an exclamatory .
For example , “ How big is the whale fish !.”is an exclamatory sentence .

Interrogative sentence : A sentence that asks some questions is called an interrogative .
For example , “What is your age ? “ is an interrogative sentence .
STATEMENT *: A sentence or proposition is an assertive (or decleartive) sentence which is either true or false but not both . A sentence cannot both true and false at the same time .*

3.3.1 Examples of Statements

IllUSTRATION 1 : Consider the following sentences :

i) Washington D .C is not in America.
ii) Every square is a rectangle.
iii) The earth is a planet.
iv) Three plus six is 9.
v) The sun is a star.

Each of sentences (iii) , (iv) & (v) is a true declerative sentence and so each of them is a statement .

Each of sentences (i) & (ii) is a false declerative sentence and so each of them is a statement .

IllUSTRATION 2 : Consider the following sentences :

i) Do your home work.
ii) Give me a glass of water?
iii) How are you ?
iv) Have you ever seen Taj Mahal ?
v) May god bless you !
vi) May you live long !

Sentences (i) & (ii) are imperative sentences . so they are not statements .Each of sentences (iii) & (iv) is asking a question. So they cannot be assigned true or false. Hence they are not statements . Each of sentences (v) & (vi) is an imperative optive. So we cannot assign true or false of them and hence none of them is a statement.

NOTE

To denote statements we use the capital letters P, Q, R, ... etc

CHECK YOUR PROGRESS - 1

1. Find out which of the following sentences are statements and which are not - justify your answer.

   i) Paris is in England.
   ii) May god bless you ?
   iii) 6 has three prime factors .
   iv) 18 is less than 16 .
   v) How far is chennai from here?
   vi) Every rhombus is a square .
   vii) There are 35 days in a month.
   viii) Two plus three is five.
   ix) x +2 = 9
   x) The moon is made of green cheese.

3.4 LOGICAL CONNECTIVES

Till now , we consider primary statements. We often combine simple (primary) statements to form compound statements by using certain connecting words known as logical connectives. Primary statements are combined by means of connectives : *AND , OR, IF---- THEN ,* and *IF AND ONLY IF,* lastly *NOT.*

Now we will discuss in details about logical connectives with their truth tables.

3.4.1 Negation

The denial of a statement P is called its negation and is written as **~** and read as 'not P'. Negation of any statement P is formed by writing " It is not the case that ------- " or " It is false that ------- " before P or inserting in P the word " not ".

Let us consider the statement

P : All integers are rational numbers .

The negation of this statement is :

~ P : It is not the case that all integers are rational numbers.

or

~ P : It is false that all integer is not a rational numbers.

or

~ P : At least one integer is not a rational numbers.

or

~ P : At least one integer is not a rational numbers.

Consider now the statement ,

P : 7> 9

The negation of this statement is

~ P : 7 < 9

or

~ P : 7= 9

TRUTH TABLE OF NEGATION

If the truth value of "P " is T, then the truth value of ~P is F. Also if the truth value of "P " is F, then the truth value of ~p is T .

This definion of the negation is summarized as follows by a table .

The truth table of ~P is :

P	~ P
T	F
F	T

Table 4.1

IIUSTRATION EXAMPLES :

Write the negation of the following statements :

(i) $\sqrt{7}$ is a rational.

(ii) $\sqrt{2}$ is not a complex number.

(iii) Every natural number is greater than zero.

(iv) All primes are odd.

(v) All mathematicians are man .

Solution : (i) Let *r* denotes the given statement i.e

r : $\sqrt{7}$ is a rational.

The negation ~ r of this statement is given by

~ r : It is not the case that $\sqrt{7}$ is a rational.

or

~ r : $\sqrt{7}$ is not a rational.

or

~ r : It is false that $\sqrt{7}$ is rational .

(ii) Let the given statement be denoted by *u* i.e

u : $\sqrt{2}$ is not a complex number.

The negation ~ u of this statement is given by

~u : $\sqrt{2}$ is a complex number.

or

~u : It is false that $\sqrt{2}$ is not a complex number.

(iii) The negation of the given statement is :

It is false that every natural number is greater than 0.

or

There exists a natural number which is not greater than 0.

(iv) The negation of the given statement is

There exists a prime which is not odd.

or

Some primes are not odd.

or

At least one prime is not odd.

(v) The negation of the given statement is :

Some mathematician is not man.

or

There exists a mathematician is not man.

or

At least one mathematician is not man.

or

It is false that all mathematicians are man.

CHECK YOUR PROGRESS - 2

1. Write the negation of the following statements -

   i) Bangalore is the capital of Karnataka.
   ii) The Earth is round.
   iii) The Sun is cold.
   iv) Some even integers are prime.
   v) Both the diagonals of a rectangle have the same length.

3.4.2 Conjunction

The conjunction i.e joining of two statements P and Q is the statement $P \wedge Q$ which is read as "*P and Q*"

IlIUSTRATION EXAMPLES :

(i) The conjunction of the statements :

P : It is raining.

Q : 2+2=4 is $P \wedge Q$.i.e

It is raining and 2+2=4 .

(ii) Consider the statement

P : The Earth is round and the Sun is cold.

Its components are :

Q : The Earth is round.

R : The Sun is cold.

Truth table : The statement $P \wedge Q$ has the truth value T whenever both P and Q have the truth value T ; Other wise it has the truth value F.

The truth table for conjunction as follows :

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Table 4.2

IlIUSTRATION EXAMPLES :

Translate the following statement into symbolic form :

Ramu and Raghu went to school.

Solution : In order to write it as a conjunction of two statements, it is necessary first to paraphrase the statement as Ramu went to school and Raghu went to school.

Now write P : Ramu went to school.

Q : Raghu went to school

Then the given statement can be written in symbolic form as $P \wedge Q$.

3.4.3 Disjunction

The disjunction of the two statements P and Q is the statement $P \vee Q$ which is read as "*P or Q*".

IlUSTRATION 3 :

(i) Consider the compound statement

P : Two lines intersect at a point or they are parallel.

The component statements of this statement are :

Q : Two lines intersect at a point.

R : Two lines are parallel.

(ii) Consider another statement

P : 45 is a multiple of 4 or 6.

Its component statements are :

Q : 45 is a multiple of 4 .

R : 45 is a multiple of 6.

Truth table : The statement P $\vee$ Q has the truth value F only when both P and Q have the truth value F, P $\vee$ Q is true if either P is true or Q is true (or both Pand Q are true). Truth table for disjunction :

P	Q	P $\vee$ Q
T	T	T
T	F	T
F	T	T
F	F	F

NOTE

The connective is not always the same as the word "or " because the fact that the word "or " in English language can be used in two different senses :
i) Inclusive OR (one or the other or both) and
ii) Exclusive OR (one or the other but not both)

CHECK YOUR PROGRESS - 3

1. Write the following statements in symbolic form :
   (i) Pavan is rich and Raghav is not happy.
   (ii) Pavan is not rich and Raghav is happy.
   (iii) Naveen is poor but happy.
   (iv) Naveen is rich or unhappy
   (v) Naveen and Amal are both smart .
   (vi) It is not true that Naveen and Amal are both smart
   (vii) Naveen is poor or he is both rich and unhappy
   (vii) Naveen is neither rich nor happy.

IIIUSTRATION EXAMPLES :

Write the components statements of the following compound statements and check the compound statement is true or false.

(i) 50 is a multiple of both 2and 5.
(ii) All living things have two legs and two eyes .
(iii) Mumbai is the capital of Gujrat or Maharashtra.
(iv) $\sqrt{2}$ is a rational number or an irrational
(v) A rectangle is a quadrilatateral or a 5 sided polygon.

Solution : (i) The components statements of the given statement are

P : 50 is multiple of 2
Q : 50 is multiple of 5

we observe that both P and Q are true statements. Therfore the compound statement is true.

(ii) The component statements of the given statement are

P : All living things have two legs.

Q : All living things have two eyes.

we find that both P and Q are false statements. Therefore, the compound statement is false.

(iii) The components statements of the given statement are

P : Mumbai is the capital of Gujrat.

Q : Mumbai is the capital of Maharashtra.

we find that P is false and Q is true. Therefore, the compound statement is true.

(iv) The components statement are

P : A rectangle is a quadrilaterl.

Q : A rectangle is a 5 sided polygon.

we observe that P and Q is false . Therefore, the compound statement is true.

(v) The compound statement are

P : $\sqrt{2}$ is a rational number.

Q : $\sqrt{2}$ is an irrational number.

clearly P is false and Q is true, therefore the compound statement is true.

CHECK YOUR PROGRESS - 4

1. Write the component statements of the following compound statements and check the compound statement is true or false.
   (i) Delhi is in India and 2+2=4.
   (ii) Delhi is in England and 2+2=4.
   (iii) Delhi is in India and 2+2=5 .
   (iv) Delhi is in England and 2+2=5.
   (v) Square of an integer is positive or negative.
   (vi) The sky is blue and the grass is green .
   (vii) The earth is round or the sun is cold.
   (viiI) All rational numbers are real and all real numbers are complex.
   (ix) 25 is a multiple of 5 and 8.
   (x) 125 is a multiple of 7or 8.

3.4.5 Conditional

If P and Q are any two statements, then the statement $P \rightarrow Q$ read as "*if P , then Q*", is called a conditional statement.

Example   Let   P : Amulya works hard.

Q : Amulya will pass the examination.

Then $P \rightarrow Q$: If Amulya works hard, then he will pass the exam.

The statement P is called the *antecedent* and Q is called the *consequent* in $P \rightarrow Q$. The sign $\rightarrow$ is called the sign of implication.

We will also write $P \rightarrow Q$ for P only if Q.

Truth table for conditional '$P \rightarrow Q$ ' as follows :

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

we will also write $P \rightarrow Q$ for   (i) P only if Q

(ii) Q If P   (iii) Q provided that P,   (iv) P is sufficient for Q,

(v) Q is necessary conditions for P,   (vi) P implies Q,

(vii) Q is implied by P

IllUSTRATION EXAMPLES :

1. Write each of the following statements in the form " If--then"

(i) You get job implies that your credentials are good.

(ii) A quadrilateral is a parallogram if its diagonals bisect each other.

(iii) To get A+ in the class, it is necessary that you do all the excercisesof the book.

Solution :

(i) we know that "If P, then Q" is equivalent to "$P \rightarrow Q$"

Therefore,the given statement can be written as

"If you get a job , then your credentials are good."

(ii) The given statement can be written as-
"If the diagonal of a quadrilateral bisect each other, then it is parallogrm".

(iii) The givenstatement can be written as
"If you get A+ in the class, then you do all the exercise of the books".

2. Write the components statements of each of the following statements. Also check whether the statements are true or not.
   (i) If a triangle ABC is equilateral , then it is isosceles.
   (ii) If a and b are integers , then ab is a rational number.

Solution :

(i) The component statements of the given statement are:

P : The triangle ABC is equilateral.

Q : The triangle ABC is isosceles.

Since an equilateral triangle is isosceles, so the given statement is true.

(ii) The component statements are :

P : a and b are integers.

Q : ab is a rational number.

Since the product of two integers is an integer and therefore a rational number. So, the compound statement is true.

CHECK YOUR PROGRESS - 5

1. Write down the truth value of each of the following implication.

   (i) If 3+2=7, then Paris is the capital of india.
   (ii) If 3+4=7,then 3 〉 7.
   (iii) If 4 〉 5,then 5 〈 6.
   (iv) If 7 〉 3, then 6 〈 14.
   (v) If two integers a and b are such that a>b, then a-b is always a positive integer.

3.4.6 Biconditional (IF AND ONLY IF IMPLICATION)

If P and Q are any two statements , then the statement $P \leftrightarrow Q$ which is read as"P IF and only if Q" and abbreviated as "Piff Q" is called a biconditional.

The following table defines the biconditional :

The statement $P \leftrightarrow Q$ has the truth value T whenever both P and Q have identical truth values.

Truth table for biconditional ($P \leftrightarrow Q$):

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

The biconditional $P \leftrightarrow Q$ is the conjunction of the conditionals $P \to Q$ and $Q \to P$ i.e $(P \to Q) \wedge (Q \to P)$ is an alternate notation for $P \leftrightarrow Q$

Also, truth table for $(P \to Q) \leftrightarrow (Q \to P)$

P	Q	$P \to Q$	$Q \to P$	$(P \to Q) \wedge (Q \to P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Note that both truth tables are identical.

IlIUSTRATION EXAMPLES :

1. Consider the statement :

A triangle is equilateral if and only if it is equiangular.

This is if and only if implication with the component statements:

P : A triangle is equilateral.

Q : A triangle is equiangular.

2. $8 \rangle 4$ if and only if $8 - 4$ is positive.

3. $2+2=4$ if and only if it is raining.

4. Two lines are parallel if and only if they have the same slope.

Biconditional $P \leftrightarrow Q$ may be read by following way :

a. P if and only if Q

b. P is equivalent to Q

c. P is necessary and sufficient condition for Q

d. Q is necessary and sufficient condition for P

IllUSTRATION EXAMPLES :

Write the truth value of each of the following biconditional statements.

(i) $4 \rangle 2$ if and only if $0 \langle 4-2$.

(ii) $3 \langle 2$ if and only if $2 \langle 1$.

(iii) $3+5 \rangle 7$ if and only if $4+6 \langle 10$.

Solution :

(i) Let $P : 4 \rangle 2$

$Q : 0 \langle 4-2$

Then, the given statement is $P \leftrightarrow Q$.

Clearly, P is true and Q is true and therefore, $P \leftrightarrow Q$ is true. Hence, the given statement is true, and its truth value is T.

(ii) Let $P : 3 < 2$

$Q : 2<1$

Then , the given statement is $P \leftrightarrow Q$.

Clearly, P is false and Q is false and therefore, $P \leftrightarrow Q$ is true. Hence , the given statement is true, and its truth value is T.

(iii) Let $P : 3+5 > 7$

$Q : 4+6<10$

Then, the given statement is $P \leftrightarrow Q$

Clearly, P is true and Q is false and therefore, $P \leftrightarrow Q$ is false. Hence , the given statement is false and therefore, its truth value is F.

CHECK YOUR PROGRESS - 6

1. Write down the truth value of each of the following

(i) $3+5=8$ if and only if $4+3=7$.

(ii) 4 is even if and only if 1 is prime.

(iii) 6 is odd if and only if 2 is odd.

(iv) $2+3=5$ if and only if $3>5$.

(v) $4+3=8$ if and only if $5+4=10$.

(vi) $2<3$ if and only if $3<4$.

3.5 CONVERSE, OPPOSITE AND CONTRAPOSITIVE OF AN IMPLICATION

These terms are defined as shown below :

Implication	$P \Rightarrow Q$
(i) Converse	$Q \Rightarrow P$
(ii) opposite	$\sim P \Rightarrow \sim Q$
(iii) contrapositive	$\sim Q \Rightarrow \sim P$

IllUSTRATION EXAMPLES :

1. Write down (i) the converse (ii) the opposite and (iii) the contrapositive of the implication:

If a quadrilateral ABCD is a square, then all the sides of quadrilateral ABCD are equal. Write down the truth value of each resulting statement.

Solution : Implication $P \Rightarrow Q$

If a quadrilateral ABCD is a square, then all sides of quadrilateral are equal. (True)

(i) Converse : $Q \Rightarrow P$

If all the sides of a quadrilateral ABCD are equal , then quad.ABCD is a square.(False)

(ii) Opposite : $\sim P \Rightarrow \sim Q$.

If a quad. ABCD is not a square then all the sides of quad. ABCD are not equal. (False)

(iii) Contrapositive: $\sim Q \Rightarrow \sim P$

If all the sides of a quad. ABCD are not equal then quad. ABCD is not a square. (True)

CHECK YOUR PROGRESS - 7

1. Write down (i) the converse (ii) the opposite and (iii) the contrapositive of the implications:
   - (i) If a triangle is equilateral, it is isosceles.
   - (ii) If x is prime number, then x is odd.
   - (iii) If two lines are parallel,then they donot intersect in the same plane
   - (iv) If a number is divisible by 9, then it is divisible by 3.
   - (v) If a triangle is equilateral,then it is equiangular.

Excercise

1. Find out which of the followig sentences are statements and which are not. Justify your answer.
   (i) Every set is a finite set.
   (ii) Are all circles round?
   (iii) All triangles have three sides.
   (iv) Is the earth round?
   (v) Go !

2. Write the negation of the following statements:
   (i) New Delhi is a city.
   (ii) The number 2 is greater than 7.
   (iii) The sum of 2 and 5 is 9.

3. Find the component statements of the following and check whether they are true or not:
   (i) All integers are positive or negative.
   (ii) All primes are either even or odd.
   (iii) 0 is a positive number or a negative number.
   (iv) 24 is a multiple of 2,4 and 8.
   (v) 0 is less than every positive integer and every negative integer.

4. Write the components statements of each of the following statements.Also , check whether the statements are true or not.
   (i) If a natural number is odd, then its square is also odd.
   (ii) If x =4, then x^2 =16.
   (iii) If ABCD is a parallelogram, then AB=CD.
   (iv) If a number is divisible by 9, then it is divisible by 3.
   (v) If a rectangle is a square , then all its four sides are equal.

5. Write down (i) the converse, (ii) the opposite and (iii) the contrapositive of the implications:
   (i) If Mohan is a poet, then he is poor.
   (ii) If she works, she will earn money.
   (iii) If it snows, then they donot drive the car.
   (iv) If x is less than zero, then x is not positive.
   (v) If it is hot outside, then you feel thirsty.

3.6 LET US SUM UP

1. Mathematical logic is concerned with all kinds of reasoning, whether they be legal arguments or mathematical proofs or conclusions in a scientific theory based upon a set of hypotheses.
2. Sentences are usually classified as declarative, exclamatory,interrogative and imperative. In our study of logic, we will confine ourselves to declarative sentences only i.e. we begin by assuming that the object language contains a set of declarative sentences. A primary statement is a declarative sentence which cannot be further broken down or analyzed into simpler sentences.
3. New statements can be formed from primary statements through the use of sentential connectives.The resulting statements are called *compound statements.*
4. The sentential connectives are called logical connectives.the different types of connectives are: *negation(~), AND(conjunction),OR(disjunction), IF---THEN(conditional),IF AND ONLY IF(Bi-conditional) etc.*
5. Truth tables have already been introduced in the definitions of the connectives Our basic concern is to determine the truth value of a statement formula for each possible combination of the truth values of the component statements. A table showing all such truth values is called the truth table of the formula. we constructed the truth table for ~P, $P \vee Q$, $P \wedge Q$, $P \rightarrow Q$ and $P \leftrightarrow Q$.Observe that if the truth values of the components are known,then the truth value of the resulting statement can be readily determined from the truth table by reading along the row which corresponds to the
   correct truth value of the component statements.
6. The statement P is called the antecedent and Q is called the consequent in $P \rightarrow Q$.
7. If P and Q are two statements , then the converse of the implication "if P, then Q" is "if Q, then P".
   The opposite of the implication "if P, then Q"is "if ~P, then ~Q".
   The contrapositive of the implication "if P, then Q" is "if ~Q, then ~P".

3.7 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS - 1

Statement : (i), (iii), (iv), (vi), (vii), (viii) & (x).

CHECK YOUR PROGRESS - 2

(i) Bangalore is not the capital of Karnataka.

(ii) The earth is not round.

(iii) The sun is not cold.

(iii) No even integer is prime.

(iv) There is at least one rectangle whose both diagonals do not have the same length.

CHECK YOUR PROGRESS - 3

(I) $P \wedge \sim Q$ where P : Pavan is rich

Q : Raghav is happy

(II) $\sim P \wedge Q$

(iii) $\sim R \wedge H$ where R : Naveen is rich

H : Naveen is happy

(iv) $R \vee \sim H$

(v) $P \wedge Q$ where P : Naveen is smart

Q : Amal is smart

(vi) $\sim(P \wedge Q)$

(vii) $\sim R \vee (R \wedge \sim H)$ where R : Naveen is rich

R : Naveen is happy

(viii) $\sim R \wedge \sim H$

CHECK YOUR PROGRESS - 4

(i) P : Delhi is in india

Q : 2+2=4

the compound statement is true

(ii) P : Delhi is in England

Q : 2+2=4

the compound statement is false.

(iii) P : Delhi is in india

Q : 2+2=5

the compound statement is false

(iv) P : Delhi is in England

Q : 2+2=5

the compound statement is false

(v) P : Square of an integer is positive

Q : Square of an integer is negative

the compound statement is false

(vi) P : The sky is blue

Q : The grass is green

The compound statement is true.

(vii) P : The earth is round

Q : The sun is cold

The compound statement is true.

(viii) P : All rational numbers are real

Q : All real numbers are complex.

The compound statement is false.

(ix) P : 25 is a multiple of 5

Q : 25 is a multiple of 8

The compound statement is false.

(x) P : 125 is a multiple of 7

Q : 125 is a multiple of 8

The compound statement is false.

CHECK YOUR PROGRESS - 5

(i) True (ii) False (iii) True (iv) False(v)True

CHECK YOUR PROGRESS - 6

(i) False (ii) False (iii) True (iv) False (v) True (vi) True.

CHECK YOUR PROGRESS - 7

(i) converse : If a triangle is isosceles, then it is equilateral.
opposite : If a triangle is not equilateral, then it is not isosceles.
contrapositive : If a triangle is not isosceles, then it is not equilateral.

(ii) converse : If x is odd, then x is a prime.
opposite : If x is not prime, then x is odd.
contrapositive : If x is not odd, then x is not prime.

(iii) converse : If two lines donot intersect in the same plane, then lines are parallel.
opposite : If two lines are not parallel, then they intersect in the same plane.
contrapositive : If two lines intersect in the same plane, then lines are not parallel.

(iv) converse : If a number is divisible by 3, then it is divisible by 9.
opposite : If a number is not divisible by 9, then it is not divisible by 3.
contrapositive : If a number is not divisible by 3, then it is not divisible by 9.

(v) converse : If a triangle is equiangular, then it is equilateral.
opposite : If a triangle is not equilateral, then it is not equiangular.
contrapositive : If a triangle is not equiangular, then it is not equilateral.

3.8 FURTHER READINGS

(I) Discrete Mathematical Structures with Application to Computer Science, J.P Tremblay & R.Manohar

(ii) Discrete Structures and Graph Theory, G.S.S. Bhishma Rao

3.9 POSSIBLE QUESTIONS

1. Find out which of the following sentences are statements and which are not. Justify your answer.
   - (i) The real number x is less than 2.
   - (ii) All real numbers are complex numbers.
   - (iii) Listen to me, Ravi !

3. Find the component statements of the following and check whether they are true or not:
   - (i) A line is staight and extends indefinitely in both directions.
   - (ii) The sky is blue and the grass is green.
   - (iii) The earth is round or the sun is cold.
   - (iv) All rational numbers are real and all real numbers are complex
   - (v) 25 is a multiple of 5 and 8.

4. Write the component statements of each of the following statements.Also , check whether the statements are true or not.
   - (i) Sets A and B are equal if and only if ($A \subseteq B$ and $B \subseteq A$).
   - (ii) $|a|<2$ if and only if ($a>-2$ and $a<2$)
   - (iii) ΔABC is isosceles if and only if $\angle B = \angle C$.
   - (iv) If 7<5 if and only if 7 is not a prime number.
   - (v) ΔABC is a triangle if and only if AB+BC>AC.

5. Write down (i) the converse, (ii) the opposite and (iii) the contrapositive of the implications:
   - (i) If you live in Delhi, then you have winter cloths.
   - (ii) If a quadrilateral is a parallelogram, then its diagonal bisect each other.
   - (iii) If you access the website, then you pay a subscription fee.
   - (iv) If you log on to the server, then you must have a passport.
   - (v) If all the four sides of a rectangle are equal,then the rectangle is a square.

*****

UNIT - 4 PROPOSITIONAL LOGIC-2

UNIT STRUCTURE

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to

- define well-formed formulas
- define tautology and contradiction for well-formed formulas
- know about logical equivalence of two different statement formulas
- know about some important equivalence formulas
- learn about theory of inference

4.2 INTRODUCTION

The notion of a statement has already been introduced in previous unit. In this unit , we define statement formula and well-formed formula.Also, we define tautology and contradiction of statement formulas. In this unit , we discuss equivalence of two statement formulas. Also we discuss theory of inference of statements.

4.3 STATEMENT FORMULAS

Statements which donot contain any connectives are called simple statements. On the other hand, the statement which contain one or more primary statements and at least one connective are called composite or compound statements.

For example, let P and Q be any two simple statements. some of the compound statements formed by P and Q are:-

$\sim P, P \vee Q$, $(P \wedge Q) \vee (\sim P)$, $P \wedge (\sim P)$, $(P \vee \sim Q) \wedge P$.

The above compound statements are called statement formulas derived from statements variables P and Q. Therefore P and Q are called as components of the statement formulas.

A statement formula alone has no truth value. It has truth value only when the statement variables in the formula are replaced by definite statements and it depends on the truth values of the statements used in replacing in the variables.

The truth table of a statement formula

Truth table already been introduced in the definitions of the connectives. In general, if there are 'n' distinct components in a statement formula . we need to consider 2^n possible combinations of truth values in order to obtain the truth table.

For example, if any statement formula have two component statements namely P and Q, then 2^2 possible combinations of truth values must be considered.

IlIUSTRATION EXAMPLES :

1. Construct the truth table for $P \wedge (\sim P)$

Solution:

P	~P	$P \wedge \sim P$
T	F	F
F	T	F

2. Construct the truth table for $P \vee (\sim P)$

P	~P	$P \vee \sim P$
T	F	T
F	T	T

3. Construct the truth table for $P \rightarrow (Q \rightarrow R)$

Solution : P, Q and R are the three statement variables that occur in this formula $P \rightarrow (Q \rightarrow R)$. There are $2^3 = 8$ different sets of truth value assignments for the variables P, Q and R.

The following table is the truth table for $P \rightarrow (Q \rightarrow R)$.

P	Q	R	$Q \rightarrow P$	$P \rightarrow (Q \rightarrow R)$
T	T	T	T	T
T	T	F	F	F
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	F	T
F	F	T	T	T
F	F	F	T	T

CHECK YOUR PROGRESS - 1

1. Construct the truth tables for the following formulas

(a) $\sim(\sim P \wedge \sim Q)$

(b) $(\sim P \vee Q) \wedge (\sim Q \vee P)$

(c) $(P \wedge Q) \rightarrow (P \vee Q)$

4.4 WELL - FORMED FORMULA

A statement formula is an expression which is a string consisting of variables (capital letters with or without subscripts), parentheses, and connective symbols. Not every string of these symbols is a formula. we shall now give a recursive definition of a statement formula,often called a *well -formed formula* (wff).

A well formed formula can be generated by the following rules :

1. A statement variable standing alone is a well-formed formula.
2. If A is a well formed formula,then ~A is a well-formed formula.
3. If A and B are well-formed formulas,then$(A \vee B)$, $(A \wedge B)$, $(A \rightarrow B)$and$(A \leftrightarrow B)$ are well-formed formulas.

4. A string of symbols containing the statement variables, connectives,and parentheses is a well-formed formula, iff it can be obtained by finitely many application of the rules 1,2 and 3.

According to this definition , the following are well-formed formulas:

$\sim(P \wedge Q)$, $\sim(P \vee Q)$, $(P \rightarrow (P \rightarrow Q))$, $(P \rightarrow (Q \rightarrow R))$, and $(((P \rightarrow Q) \wedge (Q \rightarrow R)) \leftrightarrow (P \rightarrow R)$

The following are not well-formed formulas:

1. $\sim P \wedge Q$. Obviously P and Q are well-formed formulas. A wff would be either $(\sim P \wedge Q)$ or $\sim(P \wedge Q)$.
2. $(P \rightarrow Q) \rightarrow (\wedge Q)$. This is not a wff because $\wedge Q$ is not.
3. $(P \rightarrow Q$. Note that $(P \rightarrow Q)$ is a wff.
4. $(P \rightarrow Q) \rightarrow Q)$. The reason for this not being a wff is that one of the parentheses in the beginning is missing. $(P \rightarrow Q) \rightarrow Q$ is still not a wff.

4.5 TAUTOLOGY

We already defined truth table of a statement formula. In general, the final column of a given formula contains both T and F. There are some formulas whose truth values are always T or always F regardless of the truth value assignments to the variables. This situation occurs because of the special construction of these formulas. we have already seen some examples of such formulas.

Consider for example, the statement formulas $P \vee \sim P$ and $P \wedge \sim P$ in Illustration examples 1 and 2. The truth values of $P \vee \sim P$ and $P \wedge \sim P$ which are T and F respectively, are independent of the statement by which the variable P may be replaced.

***Definition** : A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a tautology or a logical truth.*

We may say that a statement formula which is a tautology is identically true. A straightforward method to determine whether a given formula is a tautology is to constuct its truth table. This process can always be used but often becomes tedious, particularly when the number of distinct variables is large or when the formula is complicated .

A simple fact about tautologies is that the conjunction of two tautologies is also a tautology .Let us denote by A and B two statement formulas which are tautologies.If we assign any truth values of the variables of A and B ,then the truth values of both A and B will be T. Thus the truth value of $A \wedge B$ will be T, so that $A \wedge B$ will be a tutology.

4.4.1 Examples of Tautology

1. Verify whether $P \vee (\sim P)$ is a tautology

Solution:

P	$\sim P$	$P \vee \sim P$
T	F	T
F	T	T

As the entries in the last column are T, the given formula is a tautology.

2. Verify whether $(P \vee Q) \rightarrow P$ is a tautology

Solution:

P	Q	$P \vee Q$	$(P \vee Q) \rightarrow P$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	T

Since the entries in the last column of the truth table $(P \vee Q) \rightarrow P$ contain one false, the formula is not a tautology.

3. Verify whether $(P \wedge (P \leftrightarrow Q) \rightarrow Q)$ is a tautology.

P	Q	$P \leftrightarrow Q$	$P \wedge (P \leftrightarrow Q)$	$(P \wedge (P \leftrightarrow Q)) \rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	F	F	T
F	F	T	F	T

As the entries in the last column are T. The given formula is a tautology.

CHECK YOUR PROGRESS - 2

1. Prove the following are tautologies (using truth tables):
   (a) $\sim(P \vee Q) \vee (\sim P \wedge Q) \vee P$
   (b) $(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$
   (c) $Q \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$

4.6 CONTRADICTION

Definition : A statement formula which is false regardless of the truth values of the statements which replaces the variables in it is called a contradiction .

i.e, if each entry in the final column of the truth table of a statement formula is F alone then it is called as contradiction.

clearly , the negation of a contradiction is a tautology and vice-versa.we may call a statement formula which is a contradiction as identically false.

1. Verify the statement $(P \wedge Q) \wedge \sim(P \vee Q)$

P	Q	$P \wedge Q$	$P \vee Q$	$\sim(P \vee Q)$	$(P \wedge Q) \wedge \sim(P \vee Q)$
T	T	T	T	F	F
T	F	F	T	F	F
F	T	F	T	F	F
F	F	F	F	T	F

Since the truth value of $(P \wedge Q) \wedge \sim(P \vee Q)$ is F, for all values of P and Q, the proposition is a contradiction.

2. Prove that, if P(p,q,-----) is a tautology, then ~P(p,q ,-----) is a contradiction and conversely.

Solution: Since a tautology is always true, the negation of a tautology is always false i.e is a contradiction and vice-versa.

4.7 LOGICAL EQUIVALENCE

Let A and B be two statements formulas and let $P_1, P_2, ---- P_n$ denote all the variables occurring in both A and B. Consider an assignment of truth values to $P_1, P_2, ---- P_n$ and the resulting truth values of A and B. If the truth value of A is equal to the truth value of B for every one of the 2^n possible sets of truth values assigned to $P_1, P_2, ------, P_n$, then A and B are said to be equivalent. Assuming that the variables and assignment of truth values to the variables appear in the same order in the truth tables of A and B,then the final columns in the truth tables for A and B are identical if A and B are equivalent.

$A \Leftrightarrow B$ if and only if the truth values of A and B are the same.

If $A \leftrightarrow B$ is a tautology , we write $A \Leftrightarrow B$

Definition: Two formulas A and B are said to be equivalent to each other if and only if $A \leftrightarrow B$ is a tautology.

TRUTH TABLE METHOD

One method to determine whether any two statement formulas are equivalent is to construct their truth tables.

IIIUSTRATION EXAMPLES :

1. Prove that $P \vee Q \Leftrightarrow \sim(\sim P \wedge \sim Q)$

Solution:

P	Q	$P \vee Q$	~P	~Q	$\sim P \wedge \sim Q$	$\sim(\sim P \wedge \sim Q)$	$P \vee Q \leftrightarrow \sim(\sim P \wedge \sim Q)$
T	T	T	F	F	F	T	T
T	F	T	F	T	F	T	T
F	T	T	T	F	F	T	T
F	F	F	T	T	T	F	T

2. Prove that $P \rightarrow Q \Leftrightarrow (\sim P \vee Q)$

P	Q	$P \rightarrow Q$	~P	$\sim P \vee Q$	$P \rightarrow Q \leftrightarrow \sim P \vee Q$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

As $P \rightarrow Q \leftrightarrow \sim P \vee Q$ is a tautology

Then $P \rightarrow Q \Leftrightarrow \sim P \vee Q$.

CHECK YOUR PROGRESS - 3

1 Show the following equivalences using truth table method:

(a) $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$

(b) $\sim(P \rightarrow Q) \Leftrightarrow P \wedge \sim Q$

(c) $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

(d) $\sim(P \wedge Q) \rightarrow (\sim P \vee (\sim P \vee Q)) \Leftrightarrow (\sim P \vee Q)$

(e) $(P \vee Q) \wedge (\sim P \wedge (\sim P \wedge Q)) \Leftrightarrow (\sim P \wedge \sim Q)$

(f) $P \rightarrow Q \Leftrightarrow \sim Q \rightarrow \sim P$

4.8 EQUIVALENT FORMULAS

(a) Idempotent Laws :

(i) $P \vee P \Leftrightarrow P$ (ii) $P \wedge P \Leftrightarrow P$

(b) Associative Laws :

(i) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$

(ii) $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

(c) Commutative Laws :

(i) $P \vee Q \Leftrightarrow Q \vee P$ (ii) $P \wedge Q \Leftrightarrow Q \wedge P$

(d) Distributive Laws :

(i) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

(ii) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

(e) Absorption Laws :

(i) $P \vee (P \wedge Q) \Leftrightarrow P$ (ii) $P \wedge (P \vee Q) \Leftrightarrow P$

(f) Demorgan's Laws:

(i) $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$ (ii) $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$

Some other important equivalence formulas:

(i) $P \vee F \Leftrightarrow P$ (ii) $P \wedge T \Leftrightarrow P$

(iii) $P \vee T,F \Leftrightarrow T$ (iv) $P \wedge T,F \Leftrightarrow F$

(v) $P \vee \sim P \Leftrightarrow T$ (v) $P \wedge \sim P \Leftrightarrow F$

Check yourself the above formulas as an exercise by truth table technique.

REPLACEMENT PROCESS:

Consider the formula $A : P \rightarrow (Q \rightarrow R)$. The formula $Q \rightarrow R$ is a part of the formula. If we replace $Q \rightarrow R$ by an equivalent formula $\sim Q \vee R$ in A, we get another formula $B : P \rightarrow (\sim Q \vee R)$. we can easily verify that the formulas A and B are equivalent to each other.

This process of obtaining B from A is known as the replacement process.

IIIUSTRATION EXAMPLES :

1. Prove that,

$$P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\sim Q \vee R) \Leftrightarrow (P \wedge Q) \rightarrow R .$$

solution : We know that $Q \rightarrow R \Leftrightarrow \sim Q \vee R$

Replacing $Q \rightarrow R$ by $\sim Q \vee R$, we get $P \rightarrow (\sim Q \vee R)$,

which is equivalent to $\sim P \vee (\sim Q \vee R)$ by the same rule.

Now,

$$\sim P \vee (\sim Q \vee R) \Leftrightarrow (\sim P \vee \sim Q) \vee R \Leftrightarrow \sim(P \wedge Q) \vee R) \Leftrightarrow (P \wedge Q) \rightarrow R$$

by associativity of $\vee$, Demorgan's law and the previously used rule.

2. Prove that,

$$(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q$$

Solution:

$$\begin{aligned} & (P \rightarrow Q) \wedge (R \rightarrow Q) \\ \Leftrightarrow\ & (\sim P \vee Q) \wedge (\sim R \vee Q) \\ \Leftrightarrow\ & (\sim P \wedge \sim R) \vee Q \\ \Leftrightarrow\ & \sim(P \vee R) \vee Q \\ \Leftrightarrow\ & (P \vee R) \rightarrow Q \end{aligned}$$

2. Prove that,

$$(\sim P \wedge (\sim Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R .$$

Solution :

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

$\Leftrightarrow$ $((\sim P \wedge \sim Q) \wedge R) \vee ((Q \vee P) \wedge R)$ (Associative Law & distributive Law)

$\Leftrightarrow (\sim(P \vee Q) \wedge R) \vee ((Q \vee P) \wedge R)$ (Demorgan's Laws)

$\Leftrightarrow (\sim(P \vee Q) \vee (P \vee Q)) \wedge R$ (Distributive Law)

$\Leftrightarrow T \wedge R$ Since $\sim S \vee S \Leftrightarrow T$

$\Leftrightarrow R$ as $T \wedge R \Leftrightarrow R$

CHECK YOUR PROGRESS - 4

1. Prove that
   (a) $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q$
   (b) $P \rightarrow (Q \rightarrow P) \Leftrightarrow \sim P \rightarrow (P \rightarrow Q)$
   (c) $\sim(P \leftrightarrow Q) \Leftrightarrow (P \vee Q) \wedge \sim(P \wedge Q)$
   (d) $\sim(P \leftrightarrow Q) \Leftrightarrow (P \wedge \sim Q) \vee (\sim P \wedge Q)$

2. Show that P is equivalent to the following formulas

   (i) $\sim \sim P$ (ii) $P \wedge P$ (iii) $P \vee P$ (iv) $P \vee (P \wedge Q)$

   (v) $P \wedge (P \vee Q)$ (vi) $(P \wedge Q) \vee (P \wedge \sim Q)$

   (vii) $(P \vee Q) \wedge (P \vee \sim Q)$

4.9 TAUTOLOGICAL IMPLICATIONS

Definition : A statement A is said to tautological imply a statement B if and only if $A \rightarrow B$ is a tautology . In this case,we write $A \Rightarrow B$,read as " A implies B".

LET US KNOW

(i) $\Rightarrow$ is not a connective, $A \Rightarrow B$ is not a statement formula.

(ii) Thus $A \Rightarrow B$ states that $A \to B$ is a tautology or A tautologically implies B.

(iii) Clearly, $A \Rightarrow B$ guarantees that B has the truth value T whenever A has the truth value T.

(iv) By constructing the truth tables of A and B , we can determine whether $A \Rightarrow B$.

(v) In order to show any of the given implications, it is sufficient to show that an assignment of the truth value T to the antecedent of the corresponding conditional leads to the truth value T for the consequent. This procedure ensures that the conditional becomes a tautology, thereby proving the implication.

(vi) Another method to show $A \Rightarrow B$ is to assume that the consequent B has the value F and show that this assumption leads to A's having the value F. Then $A \to B$ must have the value T.

(vii) $A \Leftrightarrow B$ if and only if $A \Rightarrow B$ and $B \Rightarrow A$ i.e, If each of two formulas A and B implies the other, then A and B are equivalent.

(ix) If a formula is equivalent to a tautology then it must be a tautology.

(x) If a formula is implied by a tautology then it is a tautology.

IIIUSTRATION EXAMPLE :

1. Show the following implication using the truth table:

$$(P \to (Q \to R)) \Rightarrow (P \to Q) \to (P \to R)$$

Solution : We prove this by using the truth table for

$$(P \to (Q \to R)) \to (P \to Q) \to (P \to R)$$

P	Q	R	$P \to Q$	$Q \to R$	$P \to R$	$P \to (Q \to R)$	$(P \to Q) \to (P \to R)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	F	T	T	T	T
T	F	F	F	T	F	T	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

As the columns of $P \to (Q \to R)$ and $(P \to Q) \to (P \to R)$ are identical. $(P \to (Q \to R)) \to (P \to Q) \to (P \to R)$ is a tautology.

Therefore $(P \to (Q \to R)) \Rightarrow (P \to Q) \to (P \to R)$.

2. Show the following implication without constructing the truth tables:

$$\sim Q \wedge (P \to Q) \Rightarrow \sim P$$

Solution :

To prove that $\sim Q \wedge (P \to Q) \Rightarrow \sim P$, it is enough to show that the assumption that $\sim Q \wedge (P \to Q)$ has the truth value T guarentees the truth value T for ~P.

Now assume that $\sim Q \wedge (P \to Q)$ has the truth value T. Then both ~Q and $P \to Q$ have the truth value T. Since ~Q has truth value T, Q has the truth value F. As Q has the truth value F and $P \to Q$ has the truth value T, it follows that the truth value of P is F and the truth value of ~P is T.

Thus we have prove that

$$\sim Q \wedge (P \to Q) \Rightarrow \sim P$$

SOME IMPORTANT IMPLICATIONS :

1. $P \wedge Q \Rightarrow P$ 2. $P \wedge Q \Rightarrow Q$
3. $P \Rightarrow P \vee Q$ 4. $\sim P \Rightarrow P \to Q$
6. $Q \Rightarrow P \to Q$ 5. $\sim (P \to Q) \Rightarrow P$
7. $\sim (P \to Q) \Rightarrow \sim Q$ 8. $P \wedge (P \to Q) \Rightarrow Q$
11. $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$
12. $(P \vee Q) \wedge (P \to R) \wedge (Q \to R) \Rightarrow R$

Check yourself the above implications by using the truth table.

CHECK YOUR PROGRESS - 5

1. Show the following implications using the truth table:
   (a) $Q \Rightarrow P \rightarrow R$
   (b) $P \wedge Q \Rightarrow P \rightarrow Q$
2. Show the following implications without constructing the truth tables :
   (a) $(P \vee Q) \wedge (\sim P) \Rightarrow Q$
   (b) $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$
   (c) $(P \rightarrow Q) \rightarrow Q \Rightarrow P \vee Q$
   (d) $((P \vee \sim P) \rightarrow Q) \rightarrow ((P \vee \sim P) \rightarrow R) \Rightarrow (Q \rightarrow R)$
   (e) $(Q \rightarrow (P \wedge \sim P)) \rightarrow (R \rightarrow (P \wedge \sim P)) \Rightarrow (R \rightarrow Q)$

4.10 THEORY OF INFERENCE

The main function of logic is to provide rules of inference,or principles of reasoning . The theory associated with such rules is known as inference theory because it is concerned with the inferring of a conclusion from certain premises. When a conclusion is derived from a set of premises by using the accepted rules of resoning ,then such a process of derivation is called a deduction or a formal proof.

The rules of inference are criteria for determining the validity of an argument . These rules are stated in terms of the forms of the statements (premises and conclusions) involved rather than in terms of the actual statements or their truth values.Therefore , the rules will be given in terms of statement formulas rather than in terms of any specific statements.These rules are not arbitrary in the sense that they allow us to indicate as valid at least those arguments which we would normally expect to be valid.

In any argument , a conclusion is admitted to be true provided that the premises (assumption, axioms ,hypotheses) are accepted as true and the resoning used in deriving the conclusion from the premises follows certain accepted rules of logical inference.

Any conclusion which is arrived at by following these rules is called a valid conclusion ,and the argument is called a valid argument.The actual truth values of the premises donot play any part in the determination of the validity of the argument.

VALIDITY USING TRUTH TABLES

Let A and B be two statement formulas. We say that “ B logically follows from A" or " B is a valid conclusion (consequence) of the premise A" iff $A \rightarrow B$ is a tautology, that is, $A \Rightarrow B$.

This definition can be extended for a set of formulas rather than a single formula, we say that from a set of premises $\{H_1, H_2, -----, H_m\}$ a conclusion C follows logically iff

$H_1 \wedge H_2 \wedge ----- \wedge H_m \Rightarrow C$ .... (i)

Given a set of premises and a conclusion , it is possible to determine whether the conclusion logically follows from the given premises by constructing truth tables as follows:

Let $P_1, P_2, -----, P_n$ be all the variables appearing in the premises $H_1, H_2, -----, H_m$ and the conclusion C. If all possible combinations of the truth values are assigned to $P_1, P_2, -----, P_n$ and if the truth values of $H_1, H_2, -----, H_m$ and C are entered in a table, then it is easy to see from such a table whether (1) is true.

We look for the rows in which all $H_1, H_2, -----, H_m$ have the value T. If ,for every such row, C also has the value T, then(1) holds.

Alternatively, we may look for the rows in which C has the value F. If, in every such row , at least one of the values of $H_1, H_2, -----, H_m$ is F, then (1) holds.We call such a method a " **truth table technique"** for determination of the validity of a conclusion.

IIIUSTRATION EXAMPLE :

1. Determine whether the conclusion C follows logically from the premises H_1 and H_2.

(a) H_1: $P \rightarrow Q$ H_2: P C : Q

(b) H_1: $P \rightarrow Q$ H_2: ~P C: Q

(c) H_1: $P \rightarrow Q$ H_2: ~$(P \wedge Q)$ C : ~P

(d) H_1 :~P H_2: $P \leftrightarrow Q$ C:~$(P \wedge Q)$

(e) H_1: $P \rightarrow Q$ H_2: Q C: P

Solution: We first construct the appropriate truth table as shown in the following table.

P	Q	$P \to Q$	~P	~Q	~($P \wedge Q$)	$P \leftrightarrow Q$
T	T	T	F	F	F	T
T	F	F	F	T	T	F
F	T	T	T	F	T	F
F	F	T	T	T	T	T

For (a) we observe that the first row is the only row in which both the premises have the value T.The conclusion also has the value T in that row. Hence it is valid.

In (b) we observe the third and fourth rows. The conclusion Q is true only in the third row, but not in the fourth , and hence the conclusion is not valid.

Similarly, we can show that the conclusion are valid in (c) and (d) but not in (e).

CHECK YOUR PROGRESS - 6

1. Show that the conclusion C follows from the premises H_1 and in H_2 the following cases.

(a) H_1: $P \to Q$ C: $P \to (P \wedge Q)$

(b) H_1: ~P H_2: $P \vee Q$ C: Q

(c) H_1: ~Q H_2: $P \to Q$ C: ~P

(d) H_1: $P \to Q$ H_2: $Q \to R$ C: $P \to R$

(e) H_1: R H_2: $P \vee$ ~P   C: R

2. Determine whether the conclusion C is valid in the following the premises (By truth table technique).

(a) H_1: $P \to Q$ H_2: ~P   C: Q

(b) H_1: ~Q H_2: $P \to Q$ C: ~P

(c) H_1: R H_2: $P \vee$ ~P   C: R

EXERCISE

1. From the formulas given below indicate which are tautologies or contradictions.
   (a) $P \rightarrow (P \vee Q)$
   (b) $((P \rightarrow \sim P) \rightarrow \sim P)$
   (c) $((\sim Q \wedge P) \wedge Q)$
   (d) $((P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$
   (e) $((\sim P \rightarrow Q) \rightarrow (Q \rightarrow P))$
   (f) $(P \wedge Q) \leftrightarrow P$
2. Show that the truth values of the following formulas is idependent of its components.
   $(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$
3. Show the following implications constrcting truth tables.
   (a) $(P \wedge Q) \Rightarrow (P \rightarrow Q)$
   (b) $P \Rightarrow (Q \rightarrow P)$
   (c) $(P \rightarrow (Q \rightarrow R)) \Rightarrow (P \rightarrow Q) \rightarrow (P \rightarrow R)$
4. Show the following equivalences.
   (a) $P \rightarrow (Q \rightarrow P) \Leftrightarrow \sim P \rightarrow (P \rightarrow Q)$
   (b) $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$
   (c) $(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q$
   (d) $\sim (P \leftrightarrow Q) \Leftrightarrow (P \vee Q) \wedge \sim (P \wedge Q)$
5. Show the following implications without constructing the truth tables.
   (a) $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$
   (b) $(P \rightarrow Q) \rightarrow Q \Rightarrow P \vee Q$
   (c) $((P \vee \sim P) \rightarrow Q) \rightarrow ((P \vee \sim P) \rightarrow R) \Rightarrow (Q \rightarrow R)$
   (d) $(Q \rightarrow (P \wedge \sim P)) \rightarrow (R \rightarrow (P \wedge \sim P)) \Rightarrow (R \rightarrow Q)$
6. Show the following equivalences:
   (a) $\sim (P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$
   (b) $\sim (P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$
   (c) $\sim (P \rightarrow Q) \Leftrightarrow P \wedge \sim Q$

4.11 LET US SUM UP

1. A statement formula is an expression which is a string consisting of (capital letters with or without subscripts), parentheses and connective symbols($\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$,$\sim$), which produces a statement when the variables are replaced by statements.

2. A statement variable standing alone (i.e, a string of length one, consisting of a statement) is a well-formed formula.

3. A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a tautology or a logical truth.
4. A statement formula which is false regardless of the truth values of the statements which replaces the variables in it a contradiction.
5. The statement formulas A and B are equivalent provided $A \leftrightarrow B$ is a tautology ; and conversly , if $A \leftrightarrow B$ is a tautology, then A and B are equivalent. We shall represent the equivalence,say A and B, by writing "$A \Leftrightarrow B$," which is read as "A is equivalent to B."
6. A statement A is said is to tautologically imply a statement a statement B if and only if $A \to B$ is a tautology .We shall denote this idea by $A \Rightarrow B$ which is read as "A implies B".
7. The main aim of logic is to provide rules of inference to infer a conclusion from certain premises. The theory associated with rules of inference is known as inference theory.
8. If a conclusion is derived from a set of premises by using the accepted rules of resoning, then such a process of derivation is called a deduction or a formal proof, and the argument or conclusion is called a valid argument or a valid conclusion.
9. The method to determine whether the conclusion logically follows from the given premises by constructing the relevant truth table is called " **Truth table technique".**
10. Let A and B be two statement formulas ,we say that " B logically follows from A " or " B is a valid conclusion (consequence) of the premise A" iff $A \to B$ is tautology i.e , $A \Rightarrow B$.

    By extending the above definition , we say that from a set of premises $\{H_1, H_2, -----, H_m\}$ a conclusion C follows logically iff $H_1 \wedge H_2 \wedge ----- \wedge H_m \Rightarrow C$.

4.12 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS - 1

1. (a) The variable that occur in the formula are P and Q so we have to consider 2^2=4 possible combinations of truth values of two statements P and Q.

P	Q	~P	~Q	~P $\wedge$ ~Q	~(~P $\wedge$ ~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 $\vee$ Q	~Q $\vee$ P	(~P $\vee$ Q) $\wedge$ (~Q $\vee$ 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 $\wedge$ Q	P $\vee$ Q	(P $\wedge$ Q) $\rightarrow$ (P $\vee$ Q)
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

CHECK YOUR PROGRESS - 2

1. (b)

P	Q	~P	~P $\vee$ Q	P $\rightarrow$ Q	(P $\rightarrow$ Q) $\leftrightarrow$ (~P $\vee$ Q)
T	T	F	T	T	T
T	F	F	T	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 (a) & (c) construct truth tables for all the given formula.

CHECK YOUR PROGRESS - 3

1. (b)

P	Q	~Q	$P \to Q$	$\sim(P \to Q)$	$P \wedge \sim Q$	$\sim(P \to Q) \leftrightarrow (P \wedge \sim Q)$
T	T	F	T	F	F	T
T	F	T	F	T	T	T
F	T	F	T	F	F	T
F	F	T	T	F	F	T

As $\sim(P \to Q) \leftrightarrow (P \wedge \sim Q)$ is a tautology.
Then $\sim(P \to Q) \Leftrightarrow P \wedge \sim Q$

(f)

P	Q	~P	~Q	$P \to Q$	$\sim Q \to \sim P$	$(P \to Q) \leftrightarrow (\sim Q \to \sim P)$
T	T	F	F	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

As $(P \to Q) \leftrightarrow (\sim Q \to \sim P)$ is a tautology.
Then $(P \to Q) \Leftrightarrow (\sim Q \to \sim P)$.
Similarly, you can prove other equivalence by using truth table method.

CHECK YOUR PROGRESS - 4

1. (a) We know that $P \to Q \Leftrightarrow \sim P \vee Q$
   Replacing $R \to Q$ by $\sim R \vee Q$

Now , $(P \to Q) \wedge (R \to Q) \Leftrightarrow (\sim P \vee Q) \wedge (\sim R \vee Q)$

$\Leftrightarrow (\sim P \wedge \sim R) \vee Q$ (By distributive law)
$\Leftrightarrow (\sim(P \vee R)) \vee Q$ (By De Morgan's law0
$\Leftrightarrow (P \vee R) \to Q$.

Similarly ., you can prove (b), (c) & (d) by same process.

2. You can prove by truth table method.

CHECK YOUR PROGRESS - 5

1. (a)

P	Q	$P \to Q$	$Q \to (P \to Q)$
T	T	T	T
T	F	F	T
F	T	T	T
F	F	T	T

Since $Q \to (P \to Q)$ is a tautology , Therefore,$Q \Rightarrow (P \to Q)$.

Similarly, try to prove (b) by same process.

2. (a) To prove that $(P \vee Q) \wedge (\sim P) \Rightarrow Q$, it is enough to show that the assumption that $(P \vee Q) \wedge (\sim P)$ has the truth value T guarantees the truth value T for Q.
Now, assume that $(P \vee Q) \wedge (\sim P)$ has the truth value T. Then both $(P \vee Q)$ and $\sim P$ have the truth value T. Since $\sim P$ has truth value T, so P has truth value F. it follows the truth value of Q is F.
Thus we prove that $(P \vee Q) \wedge (\sim P) \Rightarrow Q$.

Similarly , Try to prove (b) , (c) , (d) & (e) by same process.

CHECK YOUR PROGRESS - 6

1.(a)

P	Q	$\sim P$	$\sim Q$	$P \vee Q$	$P \wedge Q$	$P \to Q$	$P \to P \wedge Q$
T	T	F	F	T	T	T	T
T	F	F	T	T	F	F	F
F	T	T	F	T	F	T	T
F	F	T	T	F	F	T	T

We first construct the appropriate truth table as shown above

For (a) we observe that in the first , third and fourth row ,the premise has the value T. The conclusion also has the value T in that rows. Hence, the conclusion C follows from the premise.

For (b) we observe that the third row is the only row in which both the premises have the value T. The conclusion also has the value T in that row. Hence , the conclusion C follows from the premise.

For (c) we observe that the fourth row is the only row in which both the premises have the value T.The conclusion also has the value T in that row. Hence , the conclusion C follows from the premise.

Similarly , try to prove (d) & (e) by constucting the appropriate truth table as shown in the above.

2. We first constuct the appropriate truth table as shown in the following table :

P	Q	$\sim P$	$\sim Q$	$P \to Q$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

For (a) we observe the third and fourth rows. The conclusion Q is true only in the third row, but not in the fourth , and hence the conclusion is not valid.

For (b) we observe that the fourth row is the only row in which both the premises have the value T. The conclusion also has the value T in that row. Hence it is valid.

For (c)

P	R	~ P	P $\vee$ ~ P
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	T

We observe that in the first and third rows, both the premises have the value T. The conclusion also has the value T in that rows. Hence it is valid.

4.13 FURTHER READINGS

(i) Discrete Mathematical Structures with Application to Computer Science by J.P Tremblay & R. Manohar

(ii) Discrete Structures and Graph Theory by G.S.S. Bhishma Rao

4.14 POSSIBLE QUESTIONS

1. Construct the truth value for each of the following:

   (i) $(P \wedge Q) \rightarrow (P \vee Q)$ (ii) $(P \wedge Q) \rightarrow \sim P$

   (iii) $(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$

2. With the help of truth tables, prove the following :

   (i) $(P \rightarrow Q) \Leftrightarrow (\sim P \vee Q)$ (ii) $(P \rightarrow Q) \Leftrightarrow (\sim Q \rightarrow \sim P)$

   (iii) $(P \leftrightarrow Q) \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

3. Show that the truth values of the following formulas are independent of their components .

   (a) $(P \wedge (P \rightarrow Q)) \rightarrow Q$

   (b) $(P \rightarrow Q) \leftrightarrow (\sim P \vee Q)$

   (c) $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R)$

   (d) $(P \leftrightarrow Q) \leftrightarrow ((P \wedge Q) \vee (\sim P \wedge \sim Q))$

4. Given the truth values of P and Q as T and those of R and S as F, find the truth values of the following:

(a) $(\sim(P \wedge Q) \vee \sim R) \vee ((Q \leftrightarrow \sim P) \rightarrow (R \vee \sim S))$

(b) $(P \leftrightarrow R) \wedge (\sim Q \rightarrow S)$

(c) $(P \vee (Q \rightarrow (R \wedge \sim P))) \leftrightarrow (Q \vee \sim S)$

5. Determine whether the conclusion C is valid in the following , when H_1 and in H_2 are premises.

(a) H_1: $P \rightarrow Q$ $\quad H_2$: $\sim Q$ $\quad$ C: P

(b) H_1: $P \rightarrow (Q \rightarrow R)$ $\quad H_2$: $P \wedge Q$ $\quad$ C: R

(c) H_1: $P \rightarrow (Q \rightarrow R)$ $\quad H_2$: R $\quad$ C: P

(d) H_1: $\sim P$ $\quad H_2$: $P \vee Q$ $\quad$ C: $P \wedge Q$

*****

Unit - 5 PREDICATE LOGIC

UNIT STRUCTURE

5.1 LEARNING OBJECTIVES

After going through this unit, you will be able to

- define Predicate
- know about statement functions,variables & Quantifiers
- know about predicate formula
- learn about free and bound variables of statement formula
- learn about different valid formula and equivalence
- know about theory of inference in predicate calculus

5.2 INTRODUCTION

In previous units, our discussion has been limited to the consideration of statements and statement formulas. The inference theory was also restricted in the sense that the premises and conclusions were all statements.The symbols P , Q , R,........... , were used for statements or statements variables. The statements were taken as basic units of statement calculus , only compound were analyzed, and this analysis was done by studying the forms of the compound formulas, i.e. , the connections between the constituent primary statements. It was not possible to express the fact that any two primary statements have some features in common. In order to investigate questions of this nature, we introduce the concept of a predicate in a primary statement . The logic based upon the analysis of predicates in any statement is called predicate logic.

5.3 PREDICATES

Let us first consider the two statements

John is a bachelor

Smith is a bachelor

Obviously , if we express these statements by symbols, we require two different symbols to denote them. Such symbols do not reveal the common features of these two statement viz., both are statements about two different individuals who are bachelors. If we introduce some symbols to denote " is a bachelor " and a method to join it with symbols denoting the names of individuals, then we will have a symbolism to denote statements about any individual 's being a bachelor. The part " is a bachelor " is called a predicate.

We shall symbolize a predicate by a capital letter and the names of individuals or objects in general by small letters. We shall soon see that using capital letters to symbolize statements as well as predicates will not lead to any confusion. Every predicate describes something about one or more objects (the word "object " is being used in a very general sense to include individuals as well). Therefore , a statement could be written symbolically in terms of the predicate letter followed by the name or names of the objects to which the predicate is applied.

We again consider the statements

(1) John is a bachelor

(2) Smith is a bachelor

Denote the predicate " is a bachelor " symbolically by the predicate letter B, " John " by j , and " Smith " by s . Then statements (1) and (2) can be written as B(j) and B(s) respectively .

In general, any statement of the type " p is Q" where Q is a predicate and p is the subject can be denoted by Q(p).

consider another statement

(3) This painting is red

Let R denote the predicate "is red " and let p denote " This painting."

Then the above statement can be symbolized by R(p).

Further, the connective described earlier can now be used to form compound statements such as "John is a bachelor and this painting is red", which can be written as $B(j) \wedge R(p)$.

Other connectives can be also used to form statements such as

$B(j) \vee R(p)$, $\sim R(p)$, $B(j) \rightarrow R(p)$ etc.

A predicate requiring m(m>0) names or object is called an m-place predicate. consider the examples

(4) Amulya is a student

The predicate S : *is a student* is a 1-place predicate because it is related to one object : Amulya .

(5) Naveen is taller than Amal

The predicate T : "is taller than " is a 2-place predicate .

(6) Canada is to the north of the United states

If we denote the predicate N : "is to the north of," c: canada , and s: united states , the statement can be symbolized as N(c,s). The predicate N : "is to the north of ", is a 2-place predicate .

Examples of 3-place predicates and 4-place predicates are :

(7) Susan sits between Ralph and Bill.

(8) Green and Miller played bridge against Johnston and Smith .

The above statements can be represented as S(s, r , b) and B(g,m,j,s). Note that the order in which the names or objects appear in the statement as well as in the predicate is important.

In general, an n-place predicate require n names of object to be inserted in fixed positions in order to obtain a statement . The position of these names is important. If S is an n-place letter and $a_1, a_2, \ldots\ldots\ldots, a_n$ are the names of objects, then S($a_1, a_2, \ldots\ldots\ldots, a_n$).

If we write S(x) for " x is a student", then S(a) , S(b) , S(c) and others having the same form can be obtained from S(x), by replacing x by an appropriate name. Note that S(x) is not a statement, but it results in a statement when x is replaced by the name of an object. The letter x used here is a place holder. We use small letter as individual or object variables as well as names of object .

A simple statement function of one variale is defined to be an expression consisting of a predicate symbol and an individual variable. Such a statement function becomes a statement when the variable is replaced by the name of any object. We can form compound statement functions by combining one or more simple statement functions and logical connectives.

IllUSTRATION EXAMPLE :

1. G(x ,y) : x is greater than y, if both x and y are replaced by the names of objects, we get a statement.

If x=3 , y =2 , then , G (3 ,2) : 3 is greater than 2.

Some restriction can be introduced by limiting the class of objects under consideration. This limitation means that the variables which are mentioned stand for only those objects which are members of a

particular set or class. such a restricted class is called the **universe of discourse** or the **domain** of individuals or simply the **universe.** If the discussion refers to human beings only, then the universe of discourse is the class of human beings. In elemantary algebra or number thoery, the universe of discourse could be number.
The universe of discourse, if any, must be explicitly stated, because the truth value of a statement depends upon it.

2. Consider the statement "Given any positive integer, there is a greater positive integer'. In this case the universe of discourse is the set of positive integer'.

5.4 STATEMENT FUNCTIONS AND VARIABLES

Let H be the predicate "is a mortal" b the name "Mr. Brown" c " canada," and s "a shirt". Then H(b), H(c) , and H(s) all denote statements. In fact, these statements have a common form. If we write H(x) for " x is mortal," then H(b), H(c) , H(s) , and others having the same form can be obtained from H(x) by replacing x by an appropriate name. Note that H(x) is not a statement , but it results in a statement when x is replaced by the name of an object.The letter *x* used here is a placeholder.
A simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable. Such a statement function becomes a statement when the variable is replaced by the name of any object. The statement resulting from a replacement is called a substitution instance of the statement function and is a formula of statement calculus.
For example , if we let M(x) be "x is a man " and H(x) be "x is mortal", then we can have compound satement functions such as

$$M(x) \wedge H(x) \quad , \quad M(x) \rightarrow H(x) \quad , \quad \sim H(x) \quad , \quad M(x) \vee \sim H(x) \quad etc.$$

An extension of this idea to the statement functions of two or more variables is straightforward.
Consider for example, the statement function of two variables :

1. G(x,y) : x is taller than y

If both x and y are replaced by the names of objects, we get a statement. If m represents Mr. Miller and j represents Mr. James, then we have G(m,j) : Mr. Miller is taller than Mr. James
and G(j,m) : Mr. James is taller than Mr. Miller

It is possible to form statement functions of two variable by using statement functions of one variable .

For example , given M(X) : x is a man.

H(y) : y is a mortal.

Then we may write

M(x) $\wedge$ H(x) : x is a man and y is a mortal.

It is not possible, however, to write every statement function of two variables using statement functions of one variable. One way of obtaining statements from any statement function is to replace the variables by the names of object.

5.5 QUANTIFIERS

Let us first consider the following statements. Each one is a statement about all individual or objects belonging to a certain set.

1. All man are mortal.
2. Every apple is red.
3. Any integer is either positive or negative.

Let us paraphrase these in the following manner.

1a. For all x , if x is a man, then x is a mortal.

2a. For all x , if x is an apple, then x is red.

3a. For all x , if x is an integer , then x is either positive or negative.

We have already shown how statement functions such as "x is a man", "x is an apple," or " x is red" can be written by using predicate symbols. If we introduce a symbol to denote the phrase "For all x," then it would be possible to symbolize statements (1a),(2a) and (3a).

UNIVERSAL QUANTIFIERS :

We symbolize " For all x" by the symbol "($\forall x$) " or by "(x)" with an understanding that this symbol be placed before the statement function to which this phrase is applied.using

M(x) : x is man . H(x) : x is a mortal .

A(x) : x is an apple. R(x) : x is red.

N(x) : x is an integer. P(x) : x is either positive or negative.

We write (1a),(2a) and (3a) as

1b. $(\forall x)\ (M(x) \rightarrow H(x))$

2b. $(\forall x)$ $(A(x) \rightarrow R(x))$

3b. $(\forall x)$ $(N(x) \rightarrow P(x))$

Sometimes $(\forall x)(M(x) \rightarrow H(x))$ is also written as $(x)(M(x) \rightarrow H(x))$. The symbols $(\forall x)$ or (x) are called ***universal quantifiers*.** The quantification symbol is "( )" or "($\forall$)" and it contains the variable which is to be quantified. It is now possible for us to quantify any statement function of one variable to obtain a statement.

Thus $(\forall x)$ M(x) is a statement which can be translated as

4. For all x , x is a man

4a. For every x, x is a man

4b. Everything is a man

Note that the particular variable appearing in the statements involving a quanifier is not important because the statements remain unchanged if x is replaced by y throughout. Thus, the statements

$$(\forall x)(M(x) \rightarrow H(x)) \text{ and } (\forall y)(M(y) \rightarrow H(y))$$

are equivalent. Sometimes it is necessary to use more than one universal quantifier in a statement.

For example consider , G(x,y) : x is taller than y.

we can state that " For any x and any y , if x is taller than y, than y is not taller than x" or " For any x and y , if x is taller than y, then it is not true that y is taller than x."

This statement can now be symbolized as

$$(\forall x)(\forall y)(G(x,y) \rightarrow \sim G(y,x))$$

In order to determine the truth values of any one of these statements involving a universal quantifier, one may be tempted to consider the truth values of the statement function which is quantified.

The universal quantifier is used to translate expressions such as *"for all," " every " , and "for any* ".

EXISTENTIAL QUANTIFIER :

Another quantifier will now be introduced to symbolize expressions such as " for some" , "there is at least one" or " there exists some" ("some " is used in the sense of " at least one").

Consider the following sdtatrements :

1. There exists a man.
2. Some men are clever.

3. Some real numbers are rational.

The first statement can be expressed in various ways, two such ways being

1a. There exists an x such that x is a man.

1b. There is at least one x such that x is a man.

similarly , (2) can be written as

2a. There exists an x such that x is a man and x is clever.

2b. There exists at least one x such that x is a man and x is clever.

Such a rephrasing allows us to introduce the symbol "$(\exists x)$,"called the **existential quantifier,** which symbolizes expressions such as " there is at least one x such that" or " there exists an x such that"or " for some x."

Writing M(x) : x is a man.

C(x) : x is clever.

R_1(x) : x is a real number.

R_2(x) : x is rational.

and using the existential quantifier, we can write the statements(1) to (3) as

1c. $(\exists x)$ (M(x))

2c. $(\exists x)$ (M(x) $\wedge$ C(x))

3c. $(\exists x)$ (R_1(x) $\wedge$ R_2(x))

It may be noted that a conjunction has been used in writing the statements of the form "Some A are B," while a conditional was used in writing of the form" All A are B."

IIIUSTRATION EXAMPLE :

1. Write the following statements in symbolic form :

(a) Something is good.

(b) Everything is good.

(c) Nothing is good.

(d) Something is not good.

Solution : Statement (a) means " there is at least one x such that x is good."

statement (b) means " for all x , x is good."

statement (c) means " for all x, x is not good."

statement (d) means " there is at least one x such that x is not good."

Thus if G(x) : x is good, then

Statement (a) can be denoted by $(\exists x)$ (G(x))
Statement (b) can be denoted by $(\forall x)$ (G(x))
Statement (c) can be denoted by $(\forall x)$ (~ G(x))
Statement (d) can be denoted by $(\exists x)$ (~ G(x))

2. Write the following in the symbolic form :

(a) All monkeys have tails.
(b) No monkey has a tail.
(c) Some monkeys have tails.
(d) Some monkeys have no tails.
(e) Some people who trust others one rewarded.
(f) He is ambitious or no one is ambitious.
(g) It is not true that all roads leads to Rome.

Solution : Let M(x): x is a monkey
and P(x) : x has a tail.

The statement (a) can be rephrased as follows:
" For all x , if x is a monkey , then x has a tail" and it can be written as

$$(\forall x)\ [\ M(x) \to P(x)]$$

The statement (b) means " for all x , if x is a monkey , then x has no tail " and it can be written as

$$(\forall x)\ [\ M(x) \to \sim P(x)]$$

The statement (c) means " there is an x such that x is a monkey and x has a tail" and can be written as

$$(\exists x)\ (\ M(x) \wedge P(x))$$

The statement (d) means " there is an x such that x is a monkey and x has no tail" and can be written as

$$(\exists x)\ (M(x) \wedge \sim P(x))$$

(e) Let P(x) : x is a person
T(x) : x trusts others
R(x) : x is rewarded

Then, " some people who trust others one rewarded" can be rephrased as " There is one x such that x is a preson,x trusts others and x is rewarded".

Symbolic form : $(\exists x)\ [\ P(x) \wedge T(x) \wedge R(x)]$

(f) Let P(x) : x is a person
A(x) : x is ambitious

'He' represents a particular person. Let that person be y. So the statement is ' y is ambitious or for all x, if x is a person then x is not ambitious'.

So Symbolic form : $A(y) \vee (\ (\forall x)\ [\ P(x) \to \sim A(x)]$

(g) Let $S(x)$: x is a road

$L(x)$: x lead to Rome.

The statement can be written as

$$\sim (\forall x)[S(x) \rightarrow L(x)]$$

or $$(\exists x)[S(x) \wedge \sim L(x)]$$

3. Identify the quantifier in each of the following statements :

(i) For every real number x, x+4 is greater than x.

(ii) There exists a real number which is twice of itself.

(iii) There exists a (living) person who is 200 years old.

(iv) For every $x \in N$, $x+1>x$.

Solution : (i) For every ($(\forall x)$) Universal quantifier

(ii) There exists ($(\exists x)$) Existential quantifier

(iii) There exists ($(\exists x)$) Existential quantifier

(iv) For every ($(\forall x)$) Universal quantifier

4. Write the negation of the following statements :

(i) For all positive integers x, we have x+2 >8.

(ii) Every living person is not 150 years old.

(iii) All students living in the dormitories.

(iv) Some students are 25(years) or older.

(v) For every real number x, x+0=x = 0+x.

(vi) For every real number x, x is less than x+1.

(vii)There exists a capital for every state in India.

(viii) There exists a number which is equal to its square.

Solution:

(i) There exists a positive integer x such that x+2=8.

or

There exists a positive integer x such that $x+2 \leq 8$.

(ii) There exists a (living) person who is 150 years old.

(iii) Some students do not live in the dormitories.

or

At least one student does not live in the dormitories.

or

There exists a student who does not live in the dormitories.

(iv) None of the students is 25 or older.

or

All the students are under 25.

(v) There exists a real number x such that $x+o \neq x=0+x$.

(vi) There exists a real number x such that x is not less than x+1.

(vii) There exists a state in India which doesnot have its capital.

(viii) For every real number x, $x^2 \neq x$.

CHECK YOUR PROGRESS - 1

1. Write the following statements in the symbolic form:

    (a) All men are good
    (b) No men are good
    (c) Some men are good
    (d) Some men are not good
    (e) If any one is good then John is good.
    (f) Some one is teasing.

2. Write the negation of each of the following statements:

    (i) For every $x \in N$, $x+3< 10$.
    (ii) There exists $x \in N$, $x+3= 10$.
    (iii) All the students completed their homework.
    (iv) There exists a number which is equal to its cube.

THE TRUTH VALUE OF A QUANTIFIED STATEMENT :

We have two ways of obtaining statements with truth values from a statement function like G(x).

1. by replacing each symbol by an object which it represents or
2. by prefixing either the existential quantifier or the universal quantifier.

The truth value of a quantified statement depends upon the universe of that statement.

IllUSTRATION EXAMPLE :

1. Let Q(x) : x is greater than 10

Consider the following universes for this statement :

(a) { 11, 15, 20 , 25 , 30 }
(b) { 5, 15 , 20 , 25 , 30 }
(c) { 5 , 7 , 8 , 9 }

With universe (a), we can produce the statement

Q(11) : 11 is greater than 10.
Q(15) : 15 is greater than 10.

Similarly we can produce Q(20), Q(25) and Q(30).

All theses statements are true. Therefore, $(\forall x)$ (Q(x)) is a true statement in this universe. There does not exist a number in this universe which is not greater than 10. So $(\exists x)$ (~ Q(x)) is false. The negation of this statement is ~ $(\exists x)$ (~ Q(x)). We observe that $(\forall x)$ (Q(x)) and ~ $(\exists x)$ (~ Q(x)) make the same assertion.

With universe (b), Q(5) is false statement , while Q(15), Q(20), Q(25) and Q(30) are true statements. So with universe (b) $(\exists x)$(Q(x)) is a true statement , while $(\forall x)$ (Q(x)) is a false statement. $(\forall x)$ (Q(x)) is false means $(\exists x)$ (~ Q(x) is a true statement.

With universe (c), all the statements Q(5), Q(7) , Q(8) and Q(9) are false and hence $(\forall x)$ (~ Q(x)) is true. It follows that ~$(\exists x)$(Q(x)) is true.

The above example also illustrates that

(i) ' all true' means the same as ' none false'

(ii) ' all false' means the same as 'none true'

(iii) ' not all true' means the same as 'atleast one false'

(iv) ' not all true ' means the same as ' atleast one true'

Infact , the following quantified statements are equivalences:

$$(\forall x)\,(P(x) \Leftrightarrow \sim (\exists x)\,(\sim P(x))$$
$$(\forall x)(\sim P(x)) \Leftrightarrow \sim (\exists x)\,(P(x))$$
$$\sim (\forall x)\,(P(x) \Leftrightarrow (\exists x)\,(\sim P(x))$$
$$\sim (\forall x)\,(\sim P(x)) \Leftrightarrow (\exists x)\,(P(x))$$

The rule for negating a statement covered by one quantifier :

To negate a statement covered by one quantifier , change the quantifier from universal to existential or from existential to universal and negate the statement which it quantifies.

Statement	Its Negation
$(\forall x)$ (P(x)	$(\exists x)$ (~P(x))
$(\exists x)$ (P(x))	$(\forall x)$(~ P(x))

STATEMENT FORMULAS IN PREDICATE CALCULUS :

In secs 6.3 and 6.4 the capital letters were introduced as definite predicates. It was suggested that a superscript n be used along with the capital letters in order to indicate that the capital letter is used as an n-placed predicate. However, this notation was not necessary because an n-place predicate symbol must be followed by n objects variables. Such variable are called object or individual variables and are denoted by lowercase letters. When used as an n-placed predicate, the capital letter is followed by n -individual variables which are enclosed in parentheses and separated by commas. For example , P$(x_1, x_2, \ldots\ldots\ldots, x_n)$ denotes an n-place predicate formula in which the letter P is an n-place predicate and $x_1, x_2, \ldots\ldots\ldots, x_n$ are individual variables. In general, P($x_1, x_2, \ldots\ldots\ldots, x_n$) will be called an atomic formula of predicate calculus.The following are some examples of atomic formulas :

R Q(x) P(x,y) A(x,y,z) P(a,y) and A(x,a,z)

A well-formed formula of predicate calculus is obtained by using the following rules.

1. An atomic formula is well-formed formula.
2. If A is a well-formed formula,then ~ A is a well-formed formula.
3. If A and B are well-formed formulas, then (A $\wedge$ B), (A $\vee$ B), (A $\rightarrow$ B) and (A $\leftrightarrow$ B) are also well-formed formulas.
4. If A is well-formed formula and x is any variable, then ($\forall x$) A and ($\exists x$) A are well-formed formulas.
5. Only those formulas obtained by using rules (1) to (4) are well-formed formulas.

5.6 FREE AND BOUND VARIABLES OF STATEMENT FORMULA

Given a formula containing a part of the form ($\forall x$) P(x) or ($\exists x$)P(x), such a part is called an x-bound part of the formula.Any occurrence of x in an x-bound part of a formula is called a bound occurrence of x, while any occurrence of x or of any variable that is not a bound occurrence is called a free occurrence.

Further, the formula P(x) either in ($\forall x$) P(x) or in ($\exists x$)P(x) is described as the scope of the quantifier. In other words, the scope of a quantifier is the formula immediately following the quantifier.If the scope is an atomic formula, then no parentheses are used to enclose the formula; otherwise parentheses are needed.

IlIUSTRATION EXAMPLE :

Consider the following formulas :

(1) ($\forall x$) P(x ,y)

(2) ($\forall x$) (P(x) $\rightarrow$ Q(x))

(3) ($\forall x$) (P(x) $\rightarrow$ (($\exists y$) R(x,y))

(4) ($\forall x$) (P(x) $\rightarrow$ R(x)) $\vee$ ($\forall x$) (P(x) $\rightarrow$ Q(x))

(5) ($\exists x$) (P(x) $\wedge$ Q(x))

(6) ($\exists x$) P(x) $\wedge$ Q(x)

In (1), P(x,y) is the scope of the quantifier , and both occurrence of x are bound occurrence , while the occurrence of y is a free occurrence.

In (2), the scope of the universal quantifier is $P(x) \rightarrow Q(x)$, and all occurrence of x are bound. In (3), the scope Of $(\forall x)$ is $P(x) \rightarrow ((\exists y)$ $R(x,y)$, while the scope of $(\exists y)$ is $R(x,y)$. All occurrence of both x and y are bound occurrences. In (4), the scope of the first quantifier is $P(x) \rightarrow R(x)$, and the scope of the second is $P(x) \rightarrow Q(x)$. All occurrence of x are bound occurrences. In (5), the scope of $(\exists x)$ is $P(x) \wedge Q(x)$. However, in (6) the scope of $(\exists x)$ is $P(x)$, and the last occurrence of x in $Q(x)$ is free.

Note that in the bound occurrence of a variable, the letter which is used to represent the variable is not important. Infact , any other letter can be used as a variable without affecting the formula , provided that the new letter is not used elsewhere in the formula.

Thus the formulas

$(\forall x)\ P(x,y)$ and $(\forall z)\ P(z,y)$ are the same.

Further, the bound occurrence of a variable cannot be substituted by a constant ; only a free occurrence of a variable can be. For example, $(\forall x)\ P(x) \wedge Q(a)$ is a substitution instance of $(\forall x)\ P(x) \wedge Q(y)$. Infact , $(\forall x)\ P(x) \wedge Q(a)$ can be expressed in English as " Every x has the property P , and a has the property Q."

A change of variables in the bound occurrence is not a substitution instance. Sometimes ,it is useful to change the variables in order to avoid confusion. It is better to write $(\forall y)\ P(y) \wedge Q(x)$ instead of $(\forall x)\ P(x) \wedge Q(x)$, so as to separate the free and bound occurrences of variables. Finally, it may be mentioned that in a statement every occurrence of a variable must be bound, and no variable should a free occurrence . In the case where a free variable occurs in a formula, then we have a statement function.

IIIUSTRATION EXAMPLE :

1. Let $P(x)$: x is a person.
   $F(x,y)$: x is the father of y.
   $M(x,y)$: x is the mother of y.

   Write the predicate " x is the father of the mother of y."

Solution : In order to symbolize the predicate, we name a person called z as the mother of y. Obviously we want to say that x is the father of z and z the mother of y. It is assumed that such a person z exists. We symbolize the predicate as :

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

2. Symbolize the expression

" All the world loves a lover."

Solution :

First note that the quotation really means that everybody loves a lover. Now let

P(x) : x is a person.

L(x) : x is a lover.

R(x,y) : x loves y.

The required expression is

$$(\forall x)(P(x) \rightarrow (\forall y)(P(y) \wedge L(y) \rightarrow R(x,y)))$$

CHECK YOUR PROGRESS - 2

1. Indicate the variables that are free and bound. Also show the scope of the quantifiers.

   (a) $(\forall x)(P(x) \rightarrow R(x)) \rightarrow (\forall x)P(x) \wedge Q(x)$

   (b) $(\forall x)(P(x) \wedge (\exists x) Q(x)) \vee ((\forall x) P(x) \rightarrow Q(x))$

   (c) $(\forall x)(P(x) \leftrightarrow Q(x) \wedge (\exists x) R(x)) \wedge S(x)$

5.7 UNIVERSE OF DISCOURSE

The process of symbolizing a statement in predicate calculus can be quite complicated. However, some simplification can be introduced by limiting the class of individuals or objects under consideration.This limitation means that the variables which are quantified stand for only those objects which are members of a particular set or class.Such a restricted class is called the universe of discourse or the domain of individuals or simply the universe. If the discussion refers to human being only, then the universe of discourse is the class of human beings. In elementary or number theory, the universe of discourse could be numbers(real , complex , rational ,etc.)

The universe of discourse , if any , must be explicitly stated,because the truth value of a statement depends upon it.

1. For instance , consider the predicate

Q(x) : x is less than 5.

and the statements $(\forall x)$ Q(x) and $(\exists x)$ Q(x). If the universe of discourse is given by the sets

1. { -1 , 0 , 1 , 2 , 4}
2. { 3, -2 , 7 , 8 , -2}
3. { 15 , 20 , 24 }

Then ($\exists x$) Q(x) is true for the universe of the discourse (1) and false for (2) and (3). The statement ($\exists x$) Q(x) is true for both (1) and (2) , but false for (3).

2. Consider the statement - All cats are animals

which is true for any universe of discourse. In particular, let the universe of discourse E be { cuddle, Ginger , 0 ,1}, where the first two elements are the names of cats . Obviously statement (1) is true over E. Now consider the statements ($\forall x$)(C(x) $\rightarrow$ A(x)) and ($\forall x$) (C(x) $\wedge$ A(x)) , where C(x) ; x is a cat , and A(x): x is an animal. In C(x) $\rightarrow$ A(x) , if x is replaced by any of the elements of E, then we get a true statement; hence($\forall x$) (C(x) $\wedge$ A(x)) is true over E.

On the other hand , ($\forall x$) (C(x) $\wedge$ A(x)) is false over E because (C(x) $\wedge$ A(x)) assumes the value false when x is replaced by 0 or 1. This means that statement (2) cannot be symbolized as

($\forall x$)(C(x) $\wedge$ A(x))

3. Consider the statement , Some cats are black.

Let E be as above with the understaning thatr both cuddle and Ginger are white cats, and let B(x) : x is black. In this case there is no black cat in the universe E, and (2) is false. The statement ($\exists x$) (C(x) $\wedge$ B(x)) is also over E because there is no black cat in E.On the other hand , ($\exists x$) (C(x) $\rightarrow$ B(x)) is true when is true x is replaced by 0 or 1.

INFERENCE THEORY OF THE PREDICATE CALCULUS :

We first generalize the concept of equivalence and implication to formulas of the predicate calculus. we shall use the same terminology and symbolism as that used for the statement calculus. After defining the concept of validity involving predicate formulas , we derive several valid formulas which will be useful in the inference theory of predicate logic.

5.8 VALID FORMULA AND EQUIVALENCE

The formulas of the predicate calculus are assumed to contain statement variables, predicates, and object variables.The object variables are assumed to belong to a set called the universe of discourse or the domain of the object variable. Such a universe may be finite or infinite. In a predicate formula, when all the object variables are replaced by a definite names of objects and the statement variables by statements , we obtain a statement which has a truth value T or F.

Let A and B be any two predicate formulae defined over a common universe E. If, for ever assignment of object names from the universe E to each of the variables appearing in A and B, the resulting statement have the same truth values, then the predicate formulae A and B are said to be equivalent to each other over E.

This idea is symbolized by writing $A \Leftrightarrow B$ over E. If E is arbitrary ,we say A and B are equivalent and write $A \Leftrightarrow B$.

Similarly , a formula A is said to be valid in E if, for every assignment of objects names from E to the corresponding variables in A and for every assignment of statements to statement variables, the resulting statements have the truth value T.

We write $\mapsto A$ in E. If A is valid for an arbitrary E, then we write $\mapsto A$.

SEVERAL VALID FORMULAE

Now we derive several valid formula, which will be useful in the inference theory of predicate logic. Formulae of predicate calculus that involve quantifiers and no free variables are also formula of the statement calculus.Therefore substitution instances of all the tautologies by these formulae yield any number of special tautologies. For example , if in the tautology $P \rightarrow Q \Leftrightarrow \sim P \vee Q$, we substitute the formulae $(\forall x)$ R(x) and $(\exists x)$ S(x) for P and Q respectively , the following tautology is obtained.

$$((\forall x)\, R(x)) \rightarrow ((\exists x)\, S(x)) \Leftrightarrow \sim ((\forall x)\, R(x)) \vee ((\exists x)\, S(x))$$

Now, we consider the substitution R(x) and S(x) for P and Q in $P \rightarrow Q \Leftrightarrow \sim P \vee Q$, let b be an object in the universe. When b replaces x in the statement $(R(x) \rightarrow S(x)) \leftrightarrow (\sim R(x) \vee S(x))$, the statement $(R(b) \rightarrow S(b)) \leftrightarrow (\sim R(b) \vee S(b))$ is obtained . Clearly , it is a true statement.

Since $P \rightarrow Q \Leftrightarrow \sim P \vee Q$ is a tautology. This general argument shows that $(P(x) \rightarrow Q(x)) \leftrightarrow (\sim P(x) \vee Q(x))$ is always a true statement regardless of what open statements P(x) and Q(x) represent and regardless of what universe is involved.

We therefore conclude that $(P(x) \rightarrow Q(x)) \leftrightarrow (\sim P(x) \vee Q(x))$ is a logically valid statement.

Actually our argument was general enough for us to conclude that if elementary statements such as P, Q, R of a tautology are replaced by predicate statements, then the resulting formula is logically valid. Thus from a tautology (of statement calculus) we can derive a lot of logically valid (predicate) formula.

We have already got the validity of the following formule

$$(\forall x)\,(P(x) \;\leftrightarrow \sim (\exists x)\,(\sim P(x))$$
$$(\forall x)(\sim P(x)) \leftrightarrow \sim (\exists x)\,(P(x))$$
$$\sim (\forall x)\,(P(x) \leftrightarrow (\exists x)\,(\sim P(x))$$
$$\sim (\forall x)\,(\sim P(x)) \leftrightarrow (\exists x)\,(P(x))$$

In addition to the implications and equivalence of statement formulas. we give some more identities

E_{23} $(\exists x)\,(A(x) \vee B(x)) \Leftrightarrow (\exists x)\,A(x) \vee (\exists x)\,B(x)$

E_{24} $(\forall x)\,(A(x) \wedge B(x)) \Leftrightarrow (\forall x)\,A(x) \wedge (\forall x)\,B(x)$

E_{25} $\sim (\exists x)\,A(x) \Leftrightarrow (\forall x) \sim A(x)$

E_{26} $\sim (\forall x)\,A(x) \Leftrightarrow (\exists x) \sim A(x)$

E_{27} $(\forall x)\;(A \vee B(x)) \Leftrightarrow A \vee (\forall x)\;B(x)$

E_{28} $(\exists x)\;(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)\;(A(x) \rightarrow B)$

E_{29} $(\forall x)\,A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$

E_{30} $(\exists x)\;A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$

E_{31} $A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$

E_{32} $A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)\;(A \rightarrow B(x))$

I_{15} $(\forall x)\;A(x) \vee (\forall x)\;B(x) \Leftrightarrow (\forall x)\;(A(x) \vee B(x))$

I_{16} $(\exists x)\;(A(x) \wedge B(x)) \Leftrightarrow (\exists x)A(x) \wedge (\exists x)\;B(x)$

IIIUSTRATION EXAMPLE :

1. Show that, $(\forall x)\,(P(x)) \rightarrow (\exists x)(P(x))$ is logically valid.

Solution : If $(\forall x)\,(P(x))$ is true in some particular universe , then the universe has atleast one object t in it and P(t) is a true statement for every t in the universe . In particular P(t) must be true.Thus $(\exists x)\,(P(x))$ is true. Therefore

$(\forall x)\,(P(x)) \rightarrow (\exists x)(P(x))$ is a valid statement.

2. Show that ,

$$(\forall x)(P(x) \wedge Q(x)) \leftrightarrow ((\forall x)(P(x) \wedge (\forall x)(Q(x))$$

is a logically valid statement.

Solution : If $(\forall x)(P(x) \wedge Q(x))$ is true , then for every t in the universe, $P(t) \wedge Q(t)$ is true. Therefore, for each t, P(t) is true and , for each t , Q(t) is true. Thus $(\forall x)(P(x) \wedge Q(x))$ is true .

This show that $(\forall x)(P(x) \wedge Q(x)) \rightarrow ((\forall x)P(x) \wedge (\forall x)(Q(x))$ is valid.

Conversely, if $(\forall x)(P(x) \wedge Q(x))$ is true, then for each t in the universe P(t) is true; and for each t in the universe,Q(t) is true.

Therefore $P(t) \wedge Q(t)$ is true for each object t in the universe.Thus

$(\forall x)(P(x) \wedge Q(x))$ is true and

$((\forall x)P(x) \wedge (\forall x)(Q(x)) \rightarrow (\forall x)(P(x) \wedge Q(x))$ is valid and hence

$((\forall x)P(x) \wedge (\forall x)(Q(x)) \rightarrow (\forall x)(P(x) \wedge Q(x))$ is logically valid statement.

3. Prove that the statements

(a) $(\forall x)(P(x)) \rightarrow P(y)$

(b) $P(y) \rightarrow (\exists x)(P(x))$ are valid statements

(y represents any one of the objects in the given universe)

Solution: (a)The logical ability of the first statement follows immediately from the fact that if $(\forall x)P(x)$ is true, then P(t) is true for every t in the universe and hence it is true for any specific object 'y' in the universe.

(b) The logical validity of the second statement is a consequence of the meaning of the existential quantifier . The statement $(\exists x)(P(x))$ is true if and only if there exists atleast one object in the universe for which P(x) is true.

Therefore if P(y) is true , then $(\exists x)(P(x))$ is true.

CHECK YOUR PROGRESS - 3

1. Show that the following statements are logically valid statements :

(a) $(\exists x)(P(x) \vee Q(x)) \leftrightarrow (\exists x)P(x) \vee (\exists x)Q(x)$

(b) $(\exists x)(P(x) \wedge Q(x)) \rightarrow ((\exists x)P(x) \wedge (\exists x)Q(x))$

(c) $(\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)P(x) \rightarrow (\forall x)Q(x))$

(d) $\sim (P(x) \vee Q(x)) \leftrightarrow (\sim P(x) \wedge \sim Q(x))$

(e) $(P(x) \rightarrow Q(y)) \leftrightarrow (\sim P(x) \vee Q(y))$

(f) $(P(x) \wedge Q(y)) \rightarrow (P(x) \rightarrow Q(y))$

5.9 THEORY OF INFERENCE

The method of derivation involving predicate formulas uses the rules of inference given for the statement calculus and also certain additional rules which are required to deal with the formulas involving quantifiers. In order to draw conclusion from quantified premises, we need to know how to remove the quantifiers properly,argue with the resulting statements and then properly prefix or add the correct quantifiers.

The rules P and T , regarding the introduction of a premises at any stage of derivation and the introduction of any formula which follows logically from the formulas already introduced ,remains the same.If the conclusion is given in the form of a conditional proof called CP.

The equivalences and implications of the statement calculus can be used in the process of derivation as before,except that the formulas involved are generalized to predicates.But these formulas donot have any quantifiers in them , while some of the premises or conclusion may be quantified.In order to use the equivalences and implications, we need some rules on how to eliminate quantifiers during the course of action.The elimination is done by *rules of specification* called rules **US** and **ES** .

Once the quantifiers are eliminated , the derivation proceeds as in the case of the statement calculus, and the conclusion is reached . It may happen that the desired conclusion is quantified. In this case, we need *rules of generalization* called rules **UG** and **EG,** Which can be used to attach a quantifier.

Now we give the rules of generalization and specification.

RULE US : (Universal Specification)

If a statement of the form $(\forall x)(P(x))$ is assumed to be true, then the universal quantifier can be dropped to obtain P(t) is true for an arbitrary object ' t ' in the universe.

In Symbols , this rule is :

$$\frac{(\forall x)(P(x))}{\therefore \ P(t) \text{ for all } t}$$

RULE UG : (Universal Generalization)

If a statement P(t) is true for each element t of the universe , then the universal quantifier may be prefixed to obtain $(\forall x)(P(x))$.

In Symbols , this rule is :

$$\frac{P(t) \text{ for all } t}{(\forall x)(P(x))}$$

This rule holds , provided we know P(t) is true for each element t in the universe.

RULE ES : (Existential Specification)

If $(\exists x)(P(x))$ is assumed to be true , then there is an element t in the universe such that P(t) is true.
In Symbols , this rule is :

$$\frac{(\exists x)(P(x))}{\therefore \quad P(t) \text{ for some } t}$$

It follows from the truth of $(\exists x)(P(x))$ that at least one such element must exist , but nothing more is guaranteed .

RULE EG : (Existential Generalization)

If P(t) is true for some element t in the universe , then $(\exists x)$, $P(x)$ is true.
In Symbols , this rule is :

$$\frac{P(t) \text{ for some } t}{\therefore \quad (\exists x)(P(x))}$$

IIIUSTRATION EXAMPLE :

1. Verify the validity of the following arguement.

Every living thing is a planet or an animal. John's gold fish is alive and it is not a planet . All animals have hearts. Therefore John 's gold has a heart.

Solution : Let the Universe consist of all living things.

Let P(x) : x is a planet
A(x) : x is an animal
H(x) : x has a heart
g : John's gold fish

Then the inference pattern is

$$\begin{array}{c} (\forall x)(P(x) \vee A(x)) \\ \sim P(g) \\ (\forall x)(A(x) \rightarrow H(x)) \\ \hline H(g) \end{array}$$

Argument :

$[1]$	(1)	$(\forall x)\,(P(x) \vee A(x))$	Rule P
$[2]$	(2)	$\sim P(g)$	Rule P
$[1]$	(3)	$P(g) \vee A(g)$	Rule US , (1)
$[1,2]$	(4)	$A(g)$	Rule T, (2), (3)
$[5]$	(5)	$(\forall x)\,(A(x) \rightarrow H(x))$	Rule P
$[5]$	(6)	$A(g) \rightarrow H(g)$	Rule US, (5)
$[1,2,5]$	(7)	$H(g)$	Rule T, (4), (6)

Thus the conclusion is valid.

2. Given an arguement which will establish the validity of the following inference :

All integers are rational numbers

Some integers are powers of 3

Therefore , some rational numbers are powers of 3.

Solution :

Let $P(x)$: x is an integer

$R(x)$: x is a rational number

$S(x)$: x is a power of 3

The the given inference pattern is

$$(\forall x)\ (P(x) \rightarrow R(x))$$
$$(\exists x)\ (P(x) \wedge S(x))$$
$$\overline{\therefore\ (\exists x)\ (R(x) \wedge S(x))}$$

Arguement :

$[1]$	(1)	$(\exists x)\ (P(x) \wedge S(x))$	Rule P
$[1]$	(2)	$P(b) \wedge S(b)$	Rule ES, (1)
$[1]$	(3)	$P(b)$	Rule T , (2)
$[1]$	(4)	$S(b)$	Rule T , (2)
$[2]$	(5)	$(\forall x)\ (P(x) \rightarrow R(x))$	Rule P
$[2]$	(6)	$P(b) \rightarrow R(b)$	Rule US , (5)
$[1,2]$	(7)	$R(b)$	Rule T , (3) , (6)
$[1,2]$	(8)	$R(b) \wedge S(b)$	Rule T , (7) , (4)
$[1,2]$	(9)	$(\exists x)\ (R(x) \wedge S(x))$	Rule EG , (8)

3. Show that

$$(\forall x)(P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)(P(x) \rightarrow R(x))$$

Solution :

$[1]$	(1)	$(\forall x)(P(x) \rightarrow Q(x))$	Rule P
$[1]$	(2)	$P(y) \rightarrow Q(y)$	Rule US , (1)
$[3]$	(3)	$(\forall x)(Q(x) \rightarrow R(x))$	Rule P
$[3]$	(4)	$Q(y) \rightarrow R(y)$	Rule US , (3)
$[1,3]$	(5)	$P(y) \rightarrow R(y)$	Rule T, (2) , (4) , I_{13}
$[1,3]$	(6)	$(\forall x)\ (P(x) \rightarrow R(x))$	Rule UG , (5)

4. Show that $(\exists x)\ M(x)$ follows logically from the premises

$(\forall x)\ (H(x) \rightarrow M(x))$ and $(\exists x)\ H(x)$

Solution :

$[1]$	(1)	$(\exists x)\ H(x)$	
$[1]$	(2)	$H(y)$	Rule ES , (1)
$[3]$	(3)	$(\forall x)\ (H(x) \rightarrow M(x))$	Rule P
$[3]$	(4)	$H(y) \rightarrow M(y)$	Rule US , (3)
$[1,3]$	(5)	$M(y)$	Rule T , (2) , (4) , I_{11}
$[1,3]$	(6)	$(\exists x)\ M(x)$	Rule EG , (5)

CHECK YOUR PROGRESS - 4

1. Verify the validity of the following arguement.

   All men are mortal.

   Socrates is a man.

   Therefore Socrates is a mortal.

2. Verify the validity of the following arguement.

   Tigers are dangerous animals.

   There are Tigers.

   Therefore there are dangerous animals.

3. Examine the validity of the argument $(S_1, S_2 ; S)$, where

   S_1 : If Hema is not in team A, then Rita is in team B.

   S_2 : If Rita is not in team B, then Mamta is in team A.

   S : Mamta is in the team A or Rita is not in team B.

EXERCISE

1. Which of the following are statements ?

    (a) $(\forall x)\,(P(x) \vee Q(x)) \wedge R$

    (b) $(\forall x)(P(x) \wedge Q(x)) \wedge (\exists x)S(x)$

    (c) $(\forall x)(P(x) \wedge Q(x)) \wedge S(x)$

2. Find the truth values of

(a) $(\forall x)\,(P(x) \vee Q(x))$, where P(x) :x=1, Q(x) :x=2 , and the universe of discourse is { 1, 2 } .

(b) $(\forall x)\,(P \rightarrow Q(x)) \vee R(a)$,where P:2>1, Q(x) : $x \leq 3$; $x > 5$ and a : 5 with the universe being { -2 , 3 , 6 }

(c) $(\exists x)\,(P(x) \rightarrow Q(x)) \wedge T$, where $P(x) : x > 2$, $Q(x) : x = 0$ and T is any tautology , with the universe of discourse as { 1 }.

3. Show that each of the following statements is logically valid.

a) $(R(x) \wedge S(x)) \rightarrow R(x)$, and $(\exists x)(P(x))$

(b) $(\forall x)\,(P(x) \vee Q(x))$, $(\forall x) \sim P(x) \Rightarrow (\forall x)\,(Q(x))$

(c) $(\forall x)\,(P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)\,(P(x) \rightarrow R(x))$

(d) $P \rightarrow (\exists x)Q(x) \Leftrightarrow (\exists x)\,(P(x) \rightarrow Q(x))$

(e) $(\forall x)\,(P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)\,(P(x) \rightarrow R(x))$

4. Is the following conclusion validly derivable from the premises given ?

    If $(\forall x)\,(P(x) \rightarrow Q(x))$; $(\exists y)P(y)$, then $(\exists z)\,Q(z)$.

5.10 LET US SUM UP

1. The logic based upon the analysis of predicates in any statement is called predicate logic.
2. A predicate requiring m(m>0) names or objects is called an m-placed predicate.
3. Certain statements involve words that indicate quantity such as ‘all’, ‘some’, ‘none’, or ‘one’.They answer the question ‘How many?’.

    Since such words indicate quantity they are called Quantifiers. The quantifier ‘ all ‘ is the Universal quantifier. We denote it by the symbol ‘ $(\forall x)$ ’ . The quantifier ‘ some ‘ is existential quantifier. We denote it by the symbol ‘ $(\exists x)$ ’.

4. Generally predicate formulas contain a part of the form $(\forall x)$ P(x) or $(\exists x)$ P(x). Such a part is called x-bound part of the formula. Any variable appearing in an x bound part of the formula is called bound variable. Otherwise it is called free variable. The smallest formula immediately following $(\forall x)$ or $(\exists x)$ is called the scope of the quantifier.
5. Let A and B be any two predicate formulae defined over a common universe E. If, for ever assignment of object names from the universe E to each of the variables appearing in A and B, the resulting statements have the same truth values, then the predicate formulae A and B are said to be equivalent to each other over E. This idea is symbolized by writing $A \Leftrightarrow B$ over E. Similarly , a formula A is said to be valid in E if , for every assignment of object names from E to the corresponding variables in A and for every assignment of statements to statement variables, the resulting statements have the truth value T.
6. In order to draw conclusions from quantified premises,we need to know how to remove the quantifiers properly ,argue with the resulting statements and then properly prefix or add the correct quantifiers. The elimination of quantifiers can be done by rules of specification called US and ES. To prefix the correct quantifier , we need the rules of generalization called UG and EG.

   The rules of specification and generalization as follows:

   Rule US : If a statement of the form $(\forall x)(P(x))$ is assumed to be true, then the universal quantifier can be dropped to obtain P(t) is true for an arbitrary 't' in the universe.

   Rule UG : If a statement P(t) is true for each element t of the universe,then the universal quantifier may be prefixed to obtain $(\forall x)(P(x))$.

   Rule ES : If $(\exists x)(P(x))$ is assumed to be true, then there is an element t in the universe such that P(t) is true.

   Rule EG : If P(t) is true for some element t in the universe, then $(\exists x)(P(x))$ is true.

5.11 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS -1

1. Let M(x) : x is a man and G(x) : x is good

(a) $(\forall x)[M(x) \to G(x)]$

(b) $(\forall x)[M(x) \to \sim G(x)]$

(c) $(\exists x)(M(x) \wedge G(x))$

(d) $(\exists x)(M(x) \wedge \sim G(x))$

(e) Let P(x) : x is a person G(x) : x is good

$(\exists x)[P(x) \wedge G(x)] \to G(\text{John})$.

(f) Let P(x) : x is a person Q(x) : x is teasing

$(\exists x)[P(x) \wedge Q(x)]$

2. (i) There exists $x \in N$ such that $x + 3 \geq 10$.

(ii) For every $x \in N$, $x + 3 \neq 10$.

(iii) Some of the students did not complete their home work.

or

There exists a student who did not complete his home work.

(iv) For every real number x, $x^2 = x$.

CHECK YOUR PROGRESS - 2

1.(a) Occurrences in P(x) and R(x) are bound.But occurrence in Q(x) is free. Scopes of $(\forall x)$ are $(P(x) \wedge R(x))$ and $P(x)$.

(b) Occurrences in P(x) and Q(x) are bound . But last occurrence in Q(x) is free. Scopes of $(\forall x)$ are $P(x) \wedge (\exists x)Q(x)$ and $P(x)$. Scope of $(\exists x)$ is Q(x).

(c) Occurrences in P(x) , Q(x) and R(x) are bound. But occurrence in S(x) is free.Scope of $(\forall x)$ is $P(x) \leftrightarrow Q(x) \wedge (\exists x)R(x)$ and scope of $(\exists x)$ is R(x).

CHECK YOUR PROGRESS - 3

1.(a) It can be proved by considering the negations of the two statements involved. We know that

$(\forall x)(P(x) \wedge Q(x)) \leftrightarrow (\forall x)(P(x)) \wedge (\forall x)(Q(x))$ is a valid statement (Illustration examples -6(2)).

Hence, $(\forall x)(\sim P(x) \wedge \sim Q(x)) \leftrightarrow (\forall x)(\sim P(x)) \wedge (\forall x)(\sim Q(x))$ is valid.

If two statements always have the same truth value then their negations always have the same truth value.

Hence $\sim (\forall x)(\sim P(x) \wedge \sim Q(x)) \leftrightarrow \sim ((\forall x)(\sim P(x)) \wedge (\forall x)(\sim Q(x)))$ is valid.

i.e., $(\exists x)(P(x) \vee Q(x)) \leftrightarrow \sim (\forall x)(\sim P(x)) \wedge \sim (\forall x)(\sim Q(x))$

i.e., $(\exists x)(P(x) \vee Q(x)) \leftrightarrow (\exists x)P(x) \vee (\exists x)Q(x)$ is a valid statement.

(e) Consider the case when $(P(x) \wedge Q(y))$ is true. so both P(x) and Q(x) must be true.Hence , $(P(x) \rightarrow Q(y))$ is true. Therefore ,$(P(x) \wedge Q(y)) \rightarrow (P(x) \rightarrow Q(y))$ is logically valid statement.

Similarly , try to prove (b) , (c) , (d) & (f) .

CHECK YOUR PROGRESS - 4

1.We denote

H(x) : x is a man.

M(x) : x is a mortal.

S : Socrates

We need to show $(\forall x)(H(x) \rightarrow M(x)) \wedge H(s) \Rightarrow M(s)$

Arguement :

[1]	(1)	$(\forall x)(H(x) \rightarrow M(x))$	Rule P
[2]	(2)	$H(s) \rightarrow M(s)$	Rule US , (1)
[3]	(3)	H(s)	Rule P
[1,3]	(4)	M(s)	Rule T , (2) , (3) , I_{11}

Thus the inference is valid.

2. The inference is valid.
3. The given arguement is invalid.

5.12 FURTHER READINGS

(I) Discrete Mathematical Structures with Application to Computer Science by J.P Tremblay & R. Manohar

(ii) Discrete Structures and Graph Theory by G.S.S. Bhishma Rao

5.13 POSSIBLE QUESTIONS

1. Write the following statements in symbolic form :

(a) John is a bachelor.

(b) Smith is a bachelor.

(c) This painting is red.

(d) Susan sits between Ralph and Bill.

(e) Green and Miller played bridge against Johnston and Smith.

2. Are the following conclusions validly derivable from the premises given.

(a) $(\forall x)\,(P(x) \rightarrow Q(x))$, $(\exists y)\,P(y)$ C : $(\exists z)Q(z)$

(b) $(\exists x)\,(P(x) \wedge Q(x))$ C : $(\forall x)\,P(x)$

(c) $(\exists x)\,P(x)$, $(\exists x)\,Q(x)$ C : $(\exists x)\,(P(x) \wedge Q(x))$

(d) $(\forall x)\,(P(x) \rightarrow Q(x))$, $\sim Q(a)$ C : $(\forall x) \sim P(x)$

3. Examine the validity of the argument (S_1, S_2, S_3), where

S_1 : All scholars are absent minded.
S_2 : John is a scholar.
S_3 : John is absent minded.

*****

Unit - 6 BOOLEAN ALGEBRA

UNIT STRUCTURE

6.1 LEARNING OBJECTIVES

After going through this unit, you will be able to

- define algebraic structure and Boolean algebra.
- know about duality of Boolean algebra and principle of duality.
- define Boolean function.
- learn about application of Boolean algebra.

6.2 INTRODUCTION

George Boole(1815-1864) a logician, developed an algebra,known as Boolean algebra to examine a given set of propositions(statements) with a view to checking their logical consistency and simplifying them by removing redundant statements or clauses.He used symbols to represent simple propositions. compound propositions were expressed in terms of these symbols and connectives. For example,'Ram is intelligent and he does well in examinations', is a compound propositions consisting of two simple ones connected by the connective ' AND'.

Let the proposition ' Ram is intelligent ' is represented by the symbols A and let the symbol B represent the proposition ' Ram does well in examinations'. A symbolic way of representing the whole statement will be A and B. similarly the proposition,'My friend gives me a box of sweets or a greeting card for my birthday 'contains the connective' OR'. Once again , representing the individual propositions by the smbols C and D we can write ' C or D' to refer to the whole statement. In 1938 shannon discovered that a simplified version of Boolean algebra can be used in analysis and synthesis of telephone switching network where a large number of electro-mechanical relays and switches were used.

Now, Boolean algebra is widely used in designing computers. We shall introduce Boolean algebra as an algebraic structure and discuss its application to switching circuits.In this unit we will define an abstract mathematical structure called Boolean Algebra named after George Boole . There are three basic operations in the Boolean Algebra,namely,AND,OR and NOT. These operations were symbolised by $\cap$ $\cup$ and or $(\ )^c$ repectively in the case of theory of sets and by $\wedge$ $\vee$ and ~ in the case of mathematical logic.In this unit , we will be using more common symbols dot(.) , plus(+) and prime(') for AND, OR and NOT respectively.

6.3 SOME USEFUL OPERATIONS

In this section we will discuss some results which will be very helpful to understand various concepts of Boolean algebra.

BINARY OPERATION : A binary operation ' $*$ ' on a non-empty set S associates any two elements a and b to a unique element a $*$ b in S. For example, addition and multiplication are binary operations on the set N of all natural numbers, but subtraction is not a binary operation on N. However , addition , multiplication and subtraction are binary operations on the set Z of all integers.

UNARY OPERATION: A unary operation on a set S associates every element of the set to some element of the set S. For example complement (') is a unary operation on the powerset P(A) of A.

COMMUTATIVE BINARY OPERATION : A binary operation ' $*$ ' on a non-empty set S is said to be a commutative binary operation, if

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

For example, union ($\cup$) and intersection ($\cap$) are commutative binary operation on the power set P(S) of a given set.

Similarly,conjunction ($\wedge$) and disjunction ($\vee$) are commutative binary operations on the set of all propositions.

ASSOCIATIVE BINARY OPERATION : A binary operation ' $*$ ' on a set S is said to be an associative binary operation, if

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

For example, union ($\cup$) and intersection ($\cap$) are associative binary operation on the power set P(S) of a given a set S.Also,conjunction ($\wedge$) and disjunction ($\vee$) are associative binary operations on the set of all propositions.

DISTRIBUTIVE BINARY OPERATION : Let S be a non empty set and($*$) and (.) be binary operations. Then, $*$ is said to be distributive over (.) ,if

$$a * (b. c) = (a* b) . (a* c)$$

and $$(b.c)* a = (b* a) . (c* a) \text{ for all } a ,b, c\in S .$$

If S be a non empty set, then union $\cup$ is distributive over intersection $\cap$ on P(S) , because

$$A\cup(B\cap C) = (A\cup B) \cap(A\cup C) \text{ for all } A,B, C\in P(S).$$

Also , intersection $\cap$ is distributive over union $\cup$ on P(S).

IDENTITY ELEMENT : Let S be a non empty set with a binary operation $*$ on S. An element $e\in S$ is the identity element, if

$$e * a = a * e \text{ for all } a \in S$$

Clearly 0 and 1 are identity elements for addition and multiplication on the set Z of integers. The identity elements for $\cup$ and $\cap$ on the power set P(S) of a non empty set S are Φ and S respectively. The identity elements for the conjunction($\wedge$) and disjunction($\vee$) on the set of all propositions are contradiction c and tautology t respectively.

INVERSE OF AN ELEMENT : Let S be a non empty set with a binary operation $*$ on S. let e be the identity element in S for the binary operation $*$ on S. An element $b\in S$ is called the inverse of an element $a \in S$, if $a* b=e=b* a$.

ALGEBRAIC STRUCTURE : A non empty set with a number of operations defined on it is said to form an algebraic structure.

For example, (N , +) , (Z, x), (Z, +, x) are algebraic structures If S is a non empty set, then $\cup$ and $\cap$ are binary operations on the power set P(S) of set S. Therefore, (P(S), $\cup$, $\cap$) is an algebraic structure. If P denotes the set of all propositions , then conjunction($\wedge$) and disjunction($\vee$) are binary operations on P and ~(negation) is a unary operation on P. Therefore , (P, $\wedge$, $\vee$,~) forms an algebraic structure.

6.4 DEFINITION OF BOOLEAN ALGEBRA

In 1854 George Boole introduced a systematic treatment of logic and developed for this purpose an algebraic structure now called Boolean algebra which may be defined as follows :

Definition : Let B be a non-empty set with two binary operations + and $*$ and a unary operation denoted by / .Then , < B , + , $*$, ' >is called a Boolean algebra if the following axioms hold :

B1 : *Commutative laws* :

For all a , b $\in$ B , we have

(i) $a + b = b + a$

(ii) $a * b = b * a$

B2 : *Distributive laws* :

For all a , b $\in$ B , we have

(i) $a + (b * c) = (a+b) * (a+c)$

(ii) $a * (b+c) = (a * b) + (a * c)$

B3 : *Identity laws* :

There exist two elements 0 and 1 in B such that

(i) $a + 0 = a$ for all $a \in B$

(ii) $a * 1 = a$ for all $a \in B$

The element 0 is called the zero element and the element 1 is called the unit element .

B4 : *Complement laws* :

For each $a \in B$, there exists $a' \in B$ such that

(i) $a + a' = 1$ (ii) $a * a' = 0$

The element a' is known as the complement of element a.

B5 : *Associative laws* :

(i) $(a + b) + c = a + (b+c)$

(ii) $(a * b) * c = a * (b * c)$

REMARK 1 : In the Boolean algebra < B , + , $*$, ' >, the operations + , $*$, and ' are called sum , product and complement respectively .

REMARK 2 : In the Boolean algebra < B , + , $*$, ' > is usually denoted by B alone when the operations are understood.

REMARK 3 : In the further discussion ,we will drop the symbol $*$ and use juxtaposition instead. Then , the axiom B2 is written as

(i) $a + bc = (a+b)(a+c)$

(ii) $a(b+c) = ab + ac$

IIIUSTRATION EXAMPLES :

1. Let P(S) be the set of all subsets of a non-empty set S i.e. power set of sets. Let the operations sum(+), product (.) and complement (‘) be defined on P(S) as follows :

$A + B = A \cup B$

$A . B = A \cap B$

and $A' = S - A$ for all $A , B \in P(S)$.

Show that (P(S) , + , . , ‘) is a Boolean algebra .

Solution : Let $A , B \in P(S)$. Then

$A , B \subset S$

$\Rightarrow A \cup B \subset S , A \cap B \subset S$ and $S - A \subset S$

$\Rightarrow A \cup B \in P(S) , A \cap B \in P(S)$ and $S - A \in P(S)$

$\Rightarrow A+B \in P(S), A . B \in P(S)$ and $A' \in P(S)$

Thus , ‘+’ and ‘.’ are binary operations on P(S) and ‘ . ‘ is a unary operation on P(S).

We observe the following properties :

Commutative Laws : Let $A , B \in P(S)$

$A , B \in P(S) \Rightarrow A , B \subset S$

$\Rightarrow A \cup B = B \cup A$ and $A \cap B = B \cap A$(Using theory of sets)

$\Rightarrow A+B = B + A$ and $A . B = B . A$

Thus $A+B = B + A$ and $A . B = B . A$ for all $A , B \in P(S)$. i.e . ‘ +’ and ‘ . ‘ are commutative binary operations on P(S).

Distributive Laws : Let $A , B ,C \in P(S)$. Then

$A , B ,C \in P(S) \Rightarrow A , B, C \subset S$

$\Rightarrow A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Using algebra of sets)

and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$\Rightarrow A + (B . C) = (A + B) . (A + C)$

and $A . (B + C) = (A . B) + (A . C)$

Thus $A + (B . C) = (A + B) . (A + C)$ and $A . (B + C) = (A . B) + (A . C)$ for all $A , B ,C \in P(S)$. i. e ‘ + ‘ and ‘ . ‘ are distributive over ‘ . ‘ and ‘ + ‘ respectively.

Existence of identity elements : For any $A \in P(S)$ i .e . for any subsets of S , we have

$A \cup \Phi = A = \Phi \cup A$ and $A \cap S = A = S \cap A$

$\Rightarrow A + \Phi = A = \Phi + A$ and $A .S = A = S.A$

$\Rightarrow \Phi$ and S are identity elements for ‘ +’ and ‘ . ‘ respectively.

Existence of inverse element : For each A $\in$ P(S) i .e for each A $\subset$ S there exists A' = S - A $\subset$ S such that

$A \cup A' = S$ and $A \cap A' = \Phi$

$\Rightarrow A + A' = S$ and $A . A' = \Phi$

Hence (P(S) , + , . , ') is a boolean algebra.

2. Let B be the set of all logical statements . Let the operations sum (+), product (.) and complement (') be defined on B as follows :

$p + q = p \vee q$

$p . q = p \wedge q$

$p' = \sim p$ for all p , q $\in$ B

where $\vee$, $\wedge$ and ~ has usual meaning in mathematical logic. Show that (B, + , . , ') is a Boolean algebra.

Solution : Let p , q $\in$ B . Then

p and q are logical statements

$\Rightarrow$ $p \vee q, p \wedge q$ and ~ p are logical statements

$\Rightarrow$ p+ q , p . q and p' are logical statements

$\Rightarrow$ + and . are binary operations and ' is a unary operation on B.

We observe the following properties :

Commutative Laws : For any two logical statements p and q i.e .for any p , q $\in$ B, we have

$p \vee q = q \vee p$ and $p \wedge q = q \wedge p$

$\Rightarrow$ p + q = q +p and p . q = q . p

$\Rightarrow$ + and . are commutative binary operations on B.

Distributive Laws : For any three logical statements p, q , r i.e for any p, q , r $\in$ B , we have

$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ and $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

$\Rightarrow$ p+(q.r) = (p+q).(p+r) and p.(q+r) = (p.q) + (p .r)

$\Rightarrow$ + and . are distributive over . and + respectively.

Existence of identity elements : We know that contradiction c and tautology t are logical statements such that for any logical statement p, we have

$p \vee c = p = c \vee p$ and $p \wedge t = p = t \wedge p$

$\Rightarrow$ p +c = p = c+p and p . t = p = t .p

$\Rightarrow$ c and t are the identity elements for + and . respectively. Thus , c and t are respectively the zero and unity elements.

Existence of complement : For each logical statement p i.e for each p $\in$ B , we have ~ p such that

$p \vee \sim p = t$ and $p \wedge \sim p = c$

3. Let D_6 ={ 1 , 2 , 3 , 6 } . Define ' + ' , ' . ' , and ' ' ' in D_6 by

a + b = L C M of a and b
a . b = G C D of a and b

$$a' = \frac{6}{a} \quad \text{for all } a , b \in D_6$$

Show that (D_6 , ' + ' , ' . ' , ' ' ') is a Boolean algebra.

Solution : We prepare the following tables for the operations

' + ' , ' . ' , and ' ' '.

Table for operation ' + '

+	1	2	3	6
1	1	2	3	6
2	2	2	6	6
3	3	6	3	6
6	6	6	6	6

Table for operation ' . '

.	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Table for operation ' ' '

'	1	2	3	6
	6	3	2	1

`

we observe that all the entries in the tables are element of D_6. Therefore ' +' and ' ' ' are binary operations on set D_6. Also , ' ' ' is a unary operation on D_6.

we observe the following properties .

Commutativity : The entries in the composition tables for + and . are symmetric about the diagonal starting from the upper left corner. Therefore, + and . are commutative binary operations on D_6.

Distributivity : From the composition tables of + and . , we have

1 + (2 . 3) = 1 + 1 = 1 and (1+ 2) . (1 +3) = 2 . 3 =1

$\therefore$ 1 + (2 . 3) = (1+ 2) . (1 +3)

Similarly , we have 1 + (2.6) = (1 +2). (1+6)

1 + (3.6) = (1+3) . (1+6)

2+ (3.6)= (2+3). (2+6) etc

Thus , ' + ' is distributive over ' . ' .

Also , we have

1 . (2+3) = 1 .6 =1 and (1.2) + (1.3) = 1 +1 = 1

$\Rightarrow$ 1 . (2+3) = (1.2) + (1.3)

Similarly , 1 . (2+6) = (1. 2) + (1.6)

1 . (3 +6) = (1.3) +(1.6)

2 . (3 +6) = (2.3) + (2.6) etc.

so , ' . ' is distributive over ' +'.

Existence of identity elements : For binary operation ' +' , we observe that the first row of the composition table coincides with the top most row and the first column coincides with the left most column.These two intersect at 1. so, 1 is the identity element for ' +' . Similarly, 6 is the identity element for ' . '.

Thus, 1 and 6 are respectively the zero and unit elements.

Complement laws : we have,

$1+1'$ =1 +6 = 6, 2 + $2'$ = 2 +3 = 6, 3+$3'$ = 3+2 =6, 6+$6'$ =6+1=6

1.$1'$=1.6=1, 2.$2'$=2.3=1, 3.$3'$=3.2=1, 6.$6'$=6.1=1

$$\therefore\ 1' = \frac{6}{1} = 6,\quad 2' = \frac{6}{2} = 3,\quad 3' = \frac{6}{3} = 2,\quad 6' = \frac{6}{6} = 1$$

Thus , the set D_6 with the given binary operations and a unary operation satisfies all the axioms of Boolean algebra.

Hence , (D_6, ' + ' , '.' , ' ' ') is a Boolean algebra .

CHECK YOUR PROGRESS - 1

1. Let D_{30} = { 1 , 2 , 3 , 5 , 6 , 10 , 15 , 30 } be the set of all divisors of 30 and let + and . be two operations on B as defined below :

   a + b = L C M of a and b

   a . b = GCD of a and b

   Also , for each a $\in$ B , let us defined

   $$a' = \frac{30}{a}$$

   Then , show that (D_{30} , +, ., ') is a Boolean algebra.

2. Let D_8 = { 1 , 2 , 4 , 8 } , be the of all divisors of 8 and let + and. be two operations be defined on D_8 as follows :

   a + b = L C M of a and b

   a .b = GCD of a and b

   $$a' = \frac{8}{a}$$

   show that (D_8 , + ,., ') is not a Boolean algebra

3. Let B = { Φ , {1}, {2} , { 1,2} } = power set of set{1,2}. show that (B, $\cup$, $\cap$, ') is a boolean algebra.

4. Let B={ Φ , {1}, {2}, {3} , { 1,2} , { 1,3} , {2,3} , {1,2,3} }= power set of set {1,2,3} . show that(B, $\cup$, $\cap$, ') is a boolean algebra.

6.5 BASIC THEOREMS OF BOOLEAN ALGEBRA

Theorem 1 (*Idempotent laws*) Let B be a Boolean algebra, Then

(i) a + a = a for all a $\in$ B

(ii) a. a = a for all a $\in$ B .

Proof : (i) we have

a + a = (a + a) .1 [By axiom B3 (ii)]

= (a + a) (a+ a') [By axiom B4(i)]

= a + a a' [By axiom B2(i)]

= a + 0 [By axiom B4(ii)]

= a [By axiom B3(i)]

(ii) We have

a.a = a. a + 0 [By axiom B3 (i)]

= a.a +a . a' [By axiom B4(ii)]

= a(a + a') [By axiom B2(ii)]

= a . 1 [By axiom B4(i)]

= a [By axiom B3(ii)]

Theorem 2 (*Boundedness laws*) Let B be a Boolean algebra.

Then, (i) $a + 1 = 1$ for all $a \in B$

(ii) $a . 0 = 0$ for all $a \in B$

Proof : (i) We have

$$\begin{aligned}
a + 1 &= (a+1) . 1 && \text{[By axiom B3 (iii)]}\\
&= 1 . (a+1) && \text{[By commutativity of '.']}\\
&= (a + a')(a+1) && \text{[By axiom B4(i)]}\\
&= a + a'.1 && \text{[By axiom B3(i)]}\\
&= a + a' && \text{[By axiom B3(ii)]}\\
&= 1 && \text{[By axiom B4(i)]}
\end{aligned}$$

(ii) We have

$$\begin{aligned}
a . 0 &= a . 0 + 0 && \text{[By axiom B3(i)]}\\
&= a . 0 + a . a' && \text{[By axiom B4(ii)]}\\
&= a(0 + a') && \text{[By axiom B2(ii)]}\\
&= a(a' + 0) && \text{[By commutativity of '+']}\\
&= a a' && \text{[By axiom B3(i)]}\\
&= 0 && \text{[By axiom B4(ii)]}
\end{aligned}$$

Theorem 3 (*Absorption laws*) Let B be a Boolean algebra.

Then , (i) $a + ab = a$ for all $a \in B$

(ii) $a(a+b) = a$ for all $a \in B$

Proof : (i) we have

$$\begin{aligned}
a + ab &= a . 1 + ab && \text{[By axiom B3(ii)]}\\
&= a(1+b) && \text{[By axiom B2(ii)]}\\
&= a(b+1) && \text{[By commutativity of '+']}\\
&= a.1 && \text{[By Theoerm 2 (i)]}\\
&= a && \text{[By axiom B3(ii)]}
\end{aligned}$$

(ii) We have

$$\begin{aligned}
a(a+b) &= (a+0)(a+b) && \text{[By axiom B3(i)]}\\
&= a + (0.b) && \text{[By axiom B2(i)]}\\
&= a + (b.0) && \text{[By commutativity]}\\
&= a + 0 && \text{[ByTheoerm 3(i)]}\\
&= a && \text{[By axiom B3(i)]}
\end{aligned}$$

Theorem 4 : (*Uniqueness of complement*)

Let a be any element in a Boolean algebra B, then

$$a + x = 1 \quad \text{and} \quad ax = 0 \Rightarrow x = a'$$

Proof : We have

$$\begin{aligned}
a' &= a' + 0 && \text{[By axiom B3(i)]}\\
&= a' + ax && [\ \therefore ax=0 \text{ (Given)}]\\
&= (a' + a)(a' + x) && \text{[By axiom B2(i)]}\\
&= 1.(a' + x) && \text{[By axiom B4(i)]}\\
&= (a' + x) && \text{[By axiom B3(ii)]}
\end{aligned}$$

Also,

$$\begin{aligned}
x &= x + 0 && \text{[By axiom B3(i)]}\\
&= x + a a' && [\ \therefore a a' = 0]\\
&= (x+a)(x+a') && \text{[By axiom B2(i)]}
\end{aligned}$$

$=1.(x + a')$ [x+a=1]

$= x + a'$ [By axiom B3(ii)]

$= a' + x$ [By commutativity]

Hence , $a' = (a' + x) = x$

Theorem 5 : (*Involution laws*)

Let a be any element in a Boolean algebra B, then $(a')' = a$

Proof : By the definition of complement we have,

$a + a' = 1$ and $a a' = 0$

$\Rightarrow$ $a' + a = 1$ and $a' a = 0$ [By commutativity]

$\Rightarrow$ a is the complement of a' i.e., $a = (a')'$.

Theorem 6 : In a Boolean algebra B, prove that

(i) $0' = 1$ (ii) $1' = 0$.

Proof : For any $a \in B$, we have

$a.1 = a$ [By axiom B3(ii)]

and $a+1 = 1$ [By theoerm 2(i)]

$\Rightarrow$ $0.1 = 0$ and $0+1=1$ [Replacing a by 0]

$\Rightarrow$ 1 is complement of 0 i.e

$0' = 1$ [$a' a=0$ and $a' + a = 1$]

Now, $0' = 1$ $\Rightarrow$ $(0')' = 1'$ $\Rightarrow$ $0 = 1'$ [$(a')' = a$]

Hence , $0' = 1$ and $1' = 0$.

Theorem 7 : (*De Morgan's laws*)

Let B be a Boolean algebra. Then,

(i) $(a + b)' = a' b'$ for all $a , b \in B$

i.e., complement of a+b is $a' b'$

(ii) $(a b)' = a' + b'$ for all $a , b \in B$

i.e., complement of ab is $a' + b'$

Proof : (i) In order to prove that $(a + b)' = a' b'$ i.e., $a' b'$ is the complement of a+b , it is sufficient to show that

$(a+b) + (a' b') = 1$ and $(a+b) (a' b') = 0$

We have,

$(a+b) + (a' b') = (b + a) + (a' b')$ [a +b = b+a by axiom B1(i)]

$= b + (a + a' b')$ [by associativity law of +]

$= b + (a + a') (a + b')$ [By distributive of + over .]

$= b + 1.(a + b')$ [$\because$ $a + a' = 1$]

$= b + (a + b')$ [$\because$ 1.a =a]

$= b + (b' + a)$ [$\because$ $a + b' = b' + a$]

$= (b + b') + a$ [by associativity law of +]

$= 1 + a \quad [\because\ b + b' = 1]$
$= 1 \quad [\because\ 1 + a = 1]$

and ,

$(a+b)\,(a'b') = ((a+b)a')b'$ [by associativity law of .]
$= (aa' + ba')b'$ [by distributive of . over +]
$= (0 + ba')b'$ $[\because\ aa' = 0]$
$= (ba')b'$ $[\because\ 0 + ba' = ba']$
$= (a'b)b'$ $[\because\ ba' = a'b]$
$= a'(b\,b')$ [by associativity law of .]
$= a'0$ $[\because\ b\,b' = 0]$
$= 0$

Thus, we have

$(a+b) + (a'b') = 1$ and $(a+b)\,(a'b') = 0$

$\Rightarrow a'b'$ is the complement of a+b

$\Rightarrow (a+b)' = a'b'$.

(ii) In order to prove that $(a\,b)' = a' + b'$, it is sufficient to show that

ab +($a' + b'$) = 1 and ab ($a' + b'$) = 0.

We have,

$ab + (a' + b') = (ab + a') + b'$ [by associativity law of +]
$= ((a + a')(b + a')) + b'$ [by distributive of + over .]
$= (1.(b + a')) + b'$ $[\because\ a + a' = 1]$
$= (b + a') + b'$ $[\because\ 1.x = x]$
$= b' + (b + a')$ [by commutativity of +]
$= (b' + b) + a'$ [by associativity of +]
$= 1 + a$ $[\because\ b' + b = b + b' = 1]$
$= 1$ $[\because\ 1 + a = 1]$

and ,

$ab\,(a' + b') = (ba)\,(a' + b')$ $[\because\ ab = ba]$
$= b(a\,(a' + b'))$ [by associativity of.]
$= b(aa' + ab')$ [by distributive of . over +]
$= b(0 + ab')$ $[\because\ aa' = 0]$
$= b(ab')$ $[\because\ 0 + x = x]$
$= (ab')b$ [by commutativity]
$= a(b'b)$ [by associativity]
$= a.0$ $[\because\ b'b = bb' = 0]$
$= 0$

Hence , $(a\,b)' = a' + b'$

6.6 DUALITY IN BOOLEAN ALGEBRA

Definition : The dual of any statements is the statement obtained by interchanging the operations + and . , and interchanging the corresponding identity elements 0 and 1 , in the original statement.

For example, the dual of the statement

$(1+a)\ (b+0)=b$ is the $(0.a) + (b.1) = b$.

IIIUSTRATION EXAMPLES :

1. Write the dual of each of the following Boolean equations:

(i) $(a . 1)\ (0 + a') = 0$

(ii) $a + a'b = a + b$

Solution : In order to write the duals of the given Boolean equations, we interchange + and . , and interchange 0 and 1.

Thus , the duals are

(i) $(a+o) + (1 . a') = 1$

(ii) $a\ (a' + b) = ab$.

2. Write the dual of each of the following Boolean equations:

(i) $a\ (a' + b) = ab$.

(ii) $(a + 1)\ (a+0) = a$

(iii) $(a + b)\ (b+c) = ac + b$

Solution : In order to write the duals of the given Boolean equations, we interchange + and . , and interchange 0 and 1. Thus , the duals are :

(i) $a + a'b = ab$

(ii) $a . 0 + a . 1 = a$

(iii) $ab + bc = (a+c)\ b$.

PRINCIPLE OF DUALITY : The dual of any theoerm in a Boolean algebra B is also a theoerm.

IIIUSTRATION EXAMPLES :

1 . For all a , b in a Boolean algebra B , prove that

(i) $a + a'b = a + b$

(ii) $a\ (a' + b) = ab$

Solution : (i) We have ,

$a + a'b = (a + a')\ (a + b)$ [by distributive of + over .]

$= 1 . (a + b)$ [$\because$ $a + a' = 1$]

$= (a+b).1$ [by commutativity]

$= a+b$ [$\because$ $a . 1 = a$]

(ii) Since $a + a'b = a + b$ holds for all $a, b \in B$. Therefore, its dual also holds .

Hence , $a\ (a' + b) = ab$ for all $a, b \in B$

2. For all a , b in a Boolean algebra B , prove that

(i) $(a+b) . (a+1) = a + a . b + b$

(ii) $(a' + b')' = a . b$

(iii) $a + a . (b+1) = a$

Solution:

(i) We have ,

$$\begin{aligned}
\text{LHS} &= (a+b) . (a+1) \\
&= a .(a+1) + b .(a+1) && \text{[By distributive of . over +]} \\
&= a . 1 + b . a + b .1 && \text{[a+1 = 1 and . is distributive over +]} \\
&= a + a. b + b && [\because \text{ a.1=a and b.1=b]} \\
&= \text{RHS.}
\end{aligned}$$

(ii) We have ,

$$\begin{aligned}
(a' + b')' &= (a')' . (b')' && \text{[Using De' Morgan's laws]} \\
&= a . b && [\because (a')' = a \text{ and } (b')' = b]
\end{aligned}$$

(iii) We have ,

$$\begin{aligned}
\text{LHS} &= a + a . (b+1) \\
&= a + a . 1 && [\because b + 1 = 1] \\
&= a + a && [\because a .1 = a] \\
&= a && [\because a + a = a]
\end{aligned}$$

3. For all a , b , c in a Boolean algebra B, prove that

(i) ($a+c= b+c$ and $a+c' = b+c'$) $\Rightarrow a = b$

(ii) ($ac = bc$ and $a c' = b c'$) $\Rightarrow a=b$.

Solution :

(i) We have

$$\begin{aligned}
a &= a + 0 && [\because a = a + 0] \\
&= a + c c' && [\because c c' = 0] \\
&= (a + c)(a + c') && \text{[By distributive of + over .]} \\
&= (b+c) (b+ c') && [\because a+c= b+c \text{ and } a+c' = b+c'] \\
&= b + c c' && \text{[By distributive of . over +]} \\
&= b && [\because c c' = 0]
\end{aligned}$$

Thus, ($a+c= b+c$ and $a+c' = b+c'$) $\Rightarrow a = b$.

(ii) We have ,

$a+c= b+c$ and $a+c' = b+c' \Rightarrow a = b$

Taking its dual , we have

$ac = bc$ and $a c' = b c' \Rightarrow a = b$

By the principle of duality this must also be true .

4. Prove the following Boolean identity :

$$ab + a b' c = ab + ac$$

Solution : We have,

$$\begin{aligned}
ab + a b' c &= a (b + b' c) && \text{[By distributive of . over +]} \\
&= a\{(b + b') (b+c)\} && \text{[By distributive of + over .]} \\
&= a\{ 1 . (b+c)\} && [\because b + b' = 1] \\
&= a(b+c) && [\because 1. x = x .1 = x] \\
&= ab + ac
\end{aligned}$$

5. In a Boolean algebra B, prove that ,

$$(a+b)'(a'+b') = a'b' \quad \text{for all} \quad a, b \in B$$

Solution : We have

$(a+b)'(a'+b') = (a'b')(a'+b')$ [By De Morgan's law]

$= (a'b')a' + (a'b')b'$ [By distributive of . over +]

$= a'(a'b') + (a'b')b'$

$= (a'a')b' + a'(a'b')$ [By associativity of .]

$= a'b' + a'b'$ [$\because$ x . x =x for all x $\in$ B]

$= a'b'$

6. In a Boolean algebra B, for all x , y , z x $\in$ B , prove that

$$x.y + y.z + y.z' = y$$

Solution : we have

$x.y + y.z + y.z'$

$= x.y + y.(z + z')$ [By distributive of . over +]

$= x.y + y.1$ [$\because$ $z + z' = 1$]

$= y.x + y.1$ [by commutativity of .]

$= y.(x+1)$ [By distributive of . over +]

$= y.1$ [$\because$ x +1=1]

$= y$ [$\because$ y . 1 = y]

Hence , $x.y + y.z + y.z' = y$

CHECK YOUR PROGRESS - 2

1. write the dual of each of the following :
   - (i) $a a' = 0$
   - (ii) $a + 0 = a$
   - (iii) $(a+b)(a'+c')(b+c)$
   - (iv) $a + b'$
   - (v) $ab + ab' + a'b$
   - (vi) $a.b' = 0$ if and only if $a.b = a$
   - (vii) If $a+b = 0$, then $a = 0 = b$
   - (viii) $a=0$ if and only if $b = a.b' + a'.b$ for all b.
2. Let B be a Boolean algebra and a, b $\in$ B. Then, prove the following :
   - (i) $a(a+b) = a + ab$
   - (ii) $a + a'b = a + b$
   - (iii) $(a+b)' = a'b'$
   - (iv) $(ab)' = a' + b'$

6.7 DEFINITION OF BOOLEAN FUNCTIONS

In a Boolean algebra B, by a constant we shall mean any symbol representing a specified element such as 0 and 1, and by a variable we shall mean a symbol representing an arbitrary element of B.

Definition : *An expression consisting of combinations of binary operations + and . , unary operation , ' and a finite number of elements of a Boolean algebra is called a Boolean function.*

For example If a, b, c $\in$ B, then a + b', a + a' b , a' bc + a b' c are Boolean functions.

The terms of a Boolean function are separated by a + sign only.

Monomials : Any Boolean function which does not involve the operation + is called a monomial .

Thus, x , (y.z), (x.y. z') , etc ., etc are monomials.

Polynomials : A Boolean function which consists of the sum of two or more monomials is called a Boolean Polynomial.

Example f(x,y)= x.y + $x'.y'$ is a Boolean polynomial in x and y and it has two terms, namely x.y and $x'.y'$.

IllUSTRATION EXAMPLES :

1. Simplify each of the following Boolean functions :

(i) ab + ac + bd + cd

(ii) $a'b'$cd + a'bcd + a$b'c'$d

Solution : (i) We have ,

ab + ac + bd + cd

= (ab + ac) + (bd +cd) [By associativity of +]

= a(b+c) + (b+c)d [By distributivity of . over +]

= a(b+c) + d(b+c) [By commutativity of .]

= (a +d) (b+c) [By distributivity of . over +]

(ii) We have,

$a'b'$cd + a'bcd + a$b'c'$d

= a'(b' + b) cd +a$b'c'$d [By distributivity of . over +]

= (a'.1) cd + a$b'c'$d [$\because$ b'+b = b+b'=1]

= a'cd + a$b'c'$d

2 . Simplify the following Boolean expression :

a { b + c($(ab+ac)'$ }

Solution : We have,

a { b + c($(ab+ac)'$ }

= a { b + c($((ab)'\,(ac)')$} [By De Morgan's Law]

= ab + ac ($(ab)'\,(ac)'$)

$= ab + ((ab)' (ac)\ (ac)')$ [By associativity of .]

$= ab + (ab)' .0$

$= ab + 0$

$= ab$

3. Simplify each of the following Boolean functions :

(i) $x' + (x'. y)$

(ii) $(x.y) + (y.z) + (y.z')$

Solution : We have,

(i) $x' + (x'. y)$

$= x'.1 + (x'.y)$ [$\because$ $x'.1 = x'$]

$= x'.(1 + y)$ [by distributive law]

$= x'.1$ [1+y =1]

$= x'$ [$x'.1$=1]

(ii) We have

$(x.y) + (y.z) + (y.z')$

= x .y + y . (z + z') [by distributive law]

= x .y + y .1 [$\because$ z + z'=1]

= y . x + y .1 [$\because$ x.y = y.x]

= y . (x +1) [by distributive law]

= y .1 [$\because$ x+1=1]

=y [$\because$ y.1=y]

CHECK YOUR PROGRESS - 3

1 . Simplify the following Boolean functions :

(i) abbccc

(ii) $abd + abd' + a'c + a'bc + abc$

(iii) $ab' + a'b + ab + a'b'$

2. Simplify the following Boolean functions :

(i) $a'b' + ab' + a'b$

(ii) $a + ab' + a'b$

(iii) $ab' + abc + a'c$

6.8 APPLICATION OF BOOLEAN ALGEBRA

Boolean algebra is useful in designing switching circuits . Subsequently we will use Boolean algebra to design logic circuits for logical and arithmetic operations performed by processors.

Boolean Algebra of Switching circuits :

Let B={ 0 ,1}, where 0 and 1 denote the two mutully exclusive states , off and on, of a switch respectively .

Let the operations of connecting the switches in parallel and connecting the switches in series be denoted by + and . respectively.

Let $0'$ =1 and $1'$ =0.

Then, [B , + , . , ‘] is a Boolean algebra, known as the Boolean algebra of switching circuits.

The composition tables for the above operations are given below

+	0	1
0	0	1
1	1	1

.	0	1
0	0	0
1	0	1

'	
0	1
1	0

Boolean switching circuit : An arrangement of wires and switches formed by the repeated use of a combination of switches in parallel and series is called a Boolean switching circuit .

Equivalent switching circuits : Two switching circuits A and B, are said to be equivalent , denoted by A ~B if both are in the same state for the same states of their constituent switches.

Thus, two switching circuits are said to be equivalent if and only if their corresponding Boolean functions are equal . This happens when their Boolean function have the same value , o or 1, for every possible assignment of the values o and 1 to their variables.

EXERCISE

1. Let B ={ 0 , 1 } and let the operations + and . on B be defined as $x + y = \max\{x, y\}$ and $x . y = \min\{x, y\}$ and , let $0' = 1$ and $1' = 0$.
show that [B, + , . , '] is a Boolean algebra.
2. Let B= { 1 , 2 , 3 , 6 , 7 , 14, 21 , 42}
for all x, y $\in$ B , define

$x + y = \text{LCM}\{x,y\}$, $x.y = \text{HCF}\{x,y\}$ and $x' = \dfrac{42}{x}$

Show that [B, + , . , '] is a Boolean algebra.
3. Let B= { 1,2,4} and for all x ,y $\in$ B , Let

$x + y = \text{LCM}\{x,y\}$, $x.y = \text{HCF}\{x,y\}$ and $x' = \dfrac{4}{x}$

Show that [B, + , . , '] is a Boolean algebra.

4. Write the dual statement of each of the following :

(i) $x . x' = 0$ (ii) $x + 0 = x$
(iii) $x + 1 = 1$ (iv) $x.y' + y = x + y$
(v) $(x + y)' = x' . y'$ (vi) $(x' + y')' = x.y$

(vii) $x + [x . (y + 1)]$ (viii) $(x + y) . (x + 1) = x + (x . . y) + y$
(ix) $[(x' + y) . (y' + z)] . (x' + z)' = 0$
(x) $(x' + y) . (x + y') = (x' . y') + (x.y)$
(xi) $x + [(y' + x) . y]' = 1$
(xii) $(x . 1) . (0 + x') = 0$
(xiii) $x . y' + y . x' = 0$ if and only if $x = y$
(xiv) $x . y = 1$ if and only if $x = 1$ and $y = 1$
(xv) $x . y' = 0$ if and only if $x' + y = 1$

5. In a Boolean algebra B , for all x , y , z $\in$ B, Prove the followings:
i) $x' + x . y = x' + y$ (ii) $(x + y)' . (y + z)' = x' . y' . z'$
(iii) $x . y + x . y' . z = x . y + x . z$
(iv) $x + x . y' + x' . y = x + y$
(v) $x' . y' + x . y' + x' . y = x' + y'$
(vi) $x + x' . (x + y) + y.z = x + y$
(vii) $(x + y') . (x' + y) . (x' + y') = x' . y'$

6 . Simplify the folloowing Boolean function:
$$(x.y) + [z . (x' + y')]$$

6.9 LET US SUM UP

1. George Boole a mathematician developed an algebra known as Boolean algebra. Shannon discovered that Boolean algebra can be used to design switching circuits. As computer circuits also use a combination of switches which can be in one of two states " open " or "closed " . Boolean algebra is useful in designing these circuits.
2. In a Boolean algebra B, for all x,y $\in$ B , we have

   I Identity laws

   (i) $x + 0 = x$ (ii) $x . 1 = x$

   II Complement laws

   (i) $x + x' = 1$ (ii) $x . x' = 0$

   III Idempotent laws

   (i) $x + x = x$ (ii) $x . x = x$

   IV Boundedness laws

   (i) $x + 1 = 1$ (ii) $x . 0 = 0$

   V Absorption laws

   (i) $x + (x . y) = x$ (ii) $x . (x + y) = x$

   VI Involution law

   $(x')' = x$

   VII Complementary law

   (i) $0' = 1$ (ii) $1' = 0$

   VIII De Morgan's laws

   (i) $(x + y)' = x'.y'$ (ii) $(x . y)' = (x' + y')$

3. A set of axioms or postulates is first stated in Boolean algebra. These postulates define the valid symbols in this algebra , which are 0 and 1. The valid operators which operate on these two symbols are next defined . These are the AND , OR AND NOT operators.
4. Boolean variables connected with Boolean operators form Boolean expressions. A set of theoerms is derived using postulates of Boolean algebra. These are useful to manipulate Boolean expression.
5. In a Boolean algebra [B , + , . , '] , the dual of any statement is the statement obtained by interchanging + and . and simultanously interchanging the elements 0 and 1 in the original statement.
6. Boolean algebra can be used in designing switching circuits.

6.10 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS - 1

1. The given operations on D_{30} satisfy the following properties:

I. Closure properties

Let a and b be any two arbitrary elements of D_{30}.

Then, each one of a and b is a divisor of 30.

$\Rightarrow$ LCM of a and b is a divisor of 30 and HCFof a and b is a divisor of 30.

$\Rightarrow$ (a+b) $\in D_{30}$ and (a . b) $\in D_{30}$.

So , D_{30} is closed for each of the operations + and . .

II . Commutative laws :

Let a and b be any two arbitrary elements of D_{30}. Then ,

LCM of a and b= LCM of b and a $\Rightarrow$ a+b = b+a, and

HCFof a and b=HCFof b and a $\Rightarrow$ a.b = b.a .

(i)a+b = b+a for all a,b $\in D_{30}$

(ii)a.b = b.a for all a,b $\in D_{30}$

III. Associative laws :

Let a , b , c be arbitrary elements of B.

(i) LCM[{LCM(a,b)} and c] = LCM[a and { LCM(b,c)}]

$\Rightarrow$ (a+b)+c = a+(b+c) for all a, b , c $\in D_{30}$.

(ii) HCF[{HCF(a,b)} and c] = HCF[a and {HCF(b,c)}]

$\Rightarrow$ (a.b).c =a.(b.c) for all a, b , c $\in D_{30}$.

IV. Distributive laws :

Let a and b be any two arbitrary elements of D_{30}.

Then, We know that HCF is distributive over LCM , and LCM is distributive over HCF.

(i) a.(b+c) = (a.b) +(a.c) for all a, b , c $\in D_{30}$.

[distributive law of HCF over LCM]

(ii) a+(b.c) = (a+b).(a+c)

[distributive law of LCM over HCF]

V. Existence of identity elements

Clearly, 1 $\in D_{30}$ and 30 $\in D_{30}$ such that

(i) a+1 = LCM(a and 1)= a for all a $\in D_{30}$.

(ii) a .30=HCF(a and 30)=a for all $\in D_{30}$

This shows that 1 is the identity element for + and 30is the identity element for . .

VI. Existence of complement

For each a $\in D_{30}$, let us define its complement by $a' = \frac{30}{a}$.

Then , we have (i) (a+a')=LCM(a, $\frac{30}{a}$)=30 (ii) a.a'=HCF(a, $\frac{30}{a}$)=1

$$\therefore \quad \{1' = 30 \text{ and } 30' = 1\};\{2' = 15 \text{ and } 15' = 2\};$$
$$\{3' = 10 \text{ and } 10' = 3\};\{5' = 6 \text{ and } 6' = 5\}.$$

Thus, each a$\in D_{30}$ has its complement a' in B.

Hence, (D_{30} , +, . , ' ,) is a Boolean algebra.

Similarly, try to prove (2), (3) &(4).

CHECK YOUR PROGRESS - 2

1. (i) $a + a' = 1$

(ii) $a \, . 1 = a$

(iii) $ab + a'c' + bc$

(iv) ab'

(v) $(a + b)\,(a + b')\,(a' + b)$

(vi) $a + b' = 1$ if and only if $a + b = a$

(vii) If $a \, . \, b = 1$, then $a = 1 = b$

(viii) $a = 1$ if and only if $b = (a + b') \, . \, (a' + b)$

2. (i) we have LHS = a(a+b) = a.a +a.b

= a +a.b [a.a=a]

= a +ab

=RHS

(ii)we have LHS = $a + a'b = (a + ab) + a'b$ $[\because a = a + ab]$

$= a + (ab + a'b)$

$= a + (a + a')b$

$= a + 1.b$

$= a + b.$

=RHS

For (iii) & (iv) , See Theorem 7.

CHECK YOUR PROGRESS - 3

1. (i) abc (ii) $ab + a'c + bc$ (iii) $a + b$.
2. (i) $a' + b'$ (ii) $a + b$ (iii) $ab' + c$

6.11 FURTHER READINGS

(I) Discrete Mathematical Structures with Application to Computer Science by J.P Tremblay & R. Manohar

(ii) Discrete Structures and Graph Theory by G.S.S. Bhishma Rao

(iii) Fumdamentals of Computer, by Rajaraman

6.12 POSSIBLE QUESTIONS

1. write the dual of each of the following boolean function:

   (i) $ac + a + bc$

   (ii) $ab + a'b'$

   (iii) $a'b' + b'c + bc'$

   (iv) $a'(b' + c') + a'(b + c)$

2. If a, b, c ......are elements of a Boolean algebra, simplify

   (i) $(a + bc)(a + b'c)$

   (ii) $a(ab + c)'$

3. If a, b, c are elements of a Boolean algebra, Prove that

   $(ab' + a'b)(a + c) = (a + b)(a' + b')(a + c)$

4. In a Boolean algebra B, for all $x, y \in B$, prove that

   (i) $(x' + y')' = x . y$ (ii) $(x + y). x'. y' = 0$

   (iii) $(x + y)' + (x + y')' = x'$ (iv) $(x + y + z)' = x'. y'.z'$

*****

UNIT 7 : COUNTING PRINCIPLES

UNIT STRUCTURE

7.1 LEARNING OBJECTIVES

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

- learn about pigeonhole principle and its generalized form
- describe the sum and product rule of counting
- describe permutation and combinations
- learn about the principle of inclusion-exclusion

7.2 INTRODUCTION

In our day to day life, it is often necessary to select certain things or arrange some objects from a group of objects. In this unit, you will learn some basic counting techniques which will be useful in determining the number of different ways of arranging objects.

7.3 FUNDAMENTAL PRINCIPLE OF COUNTING

The fundamental counting principle can be used to determine the number of possible outcomes for compound events. First we discuss to basic counting principles.

i) **The product rule :** If an event can occur in m different ways and if following it, another event can occur in n different ways, then in the given order, both the events can occur in the given order, both the events can occur in the m × n, i.e. mn ways. This principle can be generalised to any finite number of events. If we have a procedure consisting of seqeuntial events E_1, E_2, ... E_n that can be happen in m_1, m_2, ... m_n ways respectively, then there are $m_1.m_2. ... ... .m_n$ ways to carry out the procedure.

   The product rule can be phrased in terms of set theory.

   Let $A_1, A_2, ..., A_n$ be finite sets, then the number of ways to choose one element from set in the order $A_1, A_2, ... A_n$ is,

   $|A_1 \times A_2 \times ... ... \times A_n| = |A_1| \times |A_2| \times ... ... \times |A_n|$

   where, $|A_i|$ (i = 1, 2, ... n) denotes the number of elements in the set A_i.

ii) **The sum rule :** If an event can occur in m different ways and another event can occur in n different ways and if these two events can not be done at the same time i.e they are independent, then either of the two events can occur in (m + n) ways.

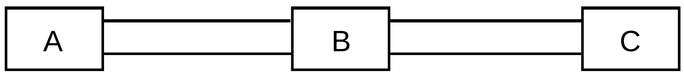
   The Sum rule of counting can also be generalised to any number of finite events. That is, if we have events E_1, E_2 ... ..., E_n, that can occur in m_1, m_2, ... m_n ways respectively and no of two of these events can be done at the same time, then there are $m_1+m_2+... ... ... + m_n$ ways to do one of these events.

   The sum rule can also be phrased in terms of set theory.

   Let $A_1, A_2, ..., A_n$ be disjoint sets, then the number of ways to choose any element from one of these sets is

   $|A_1 \cup A_2 \cup ... ... \cup A_n| = |A_1| + |A_2| + ... + |A_n|$

Example 1 : The following diagram represents the route connecting to 3 locations A, B and C. How many possible roots are there to go from location A to C? Write all possible routes.



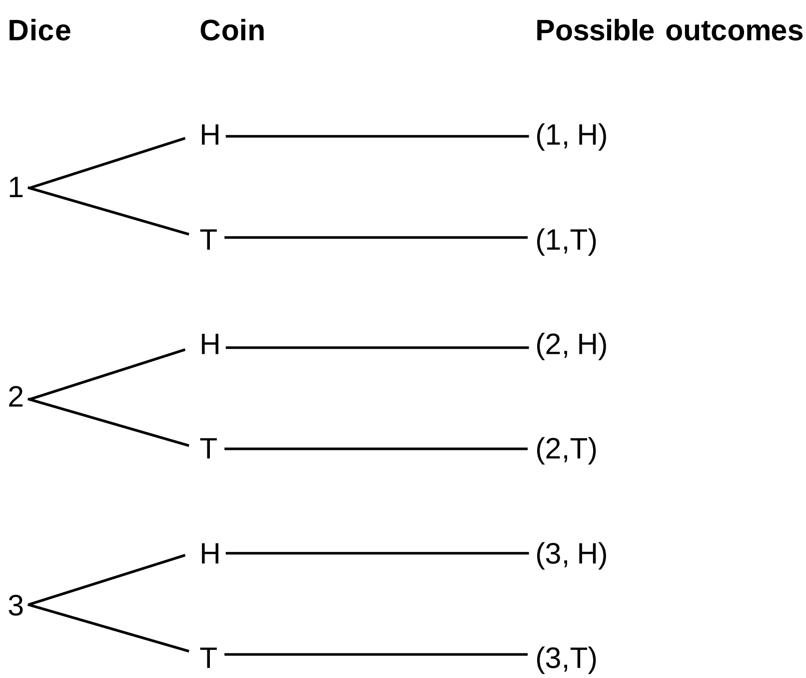
Solution : The number of routes from location A to B is 2 and from location B to C is 3.

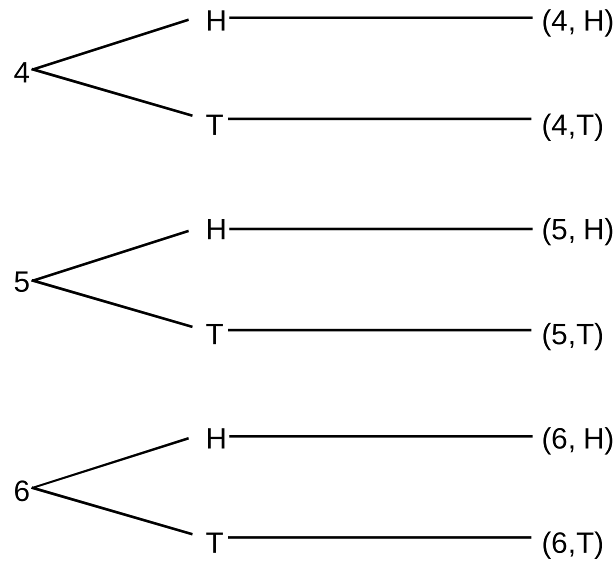
By fundamental principle of counting the number of possible routes to go from location A to C is $2 \times 3 = 6$. All the possible routes are r_1R_1, r_1R_2, r_1R_3, r_2R_1, r_2R_2, r_3R_3

Example 2 : A person throws a dice and then tosses a coin. The combined outcomes of the dice and the coin are recorded. How many such possible outcomes are there? Write all such possible outcomes.

Solution : When a dice is thrown, there are 6 possible outcomes viz. 1, 2, 3, 4, 5, 6. Again when a coin is tossed, there are 2 possible outcomes namely head (H) and tail (T).

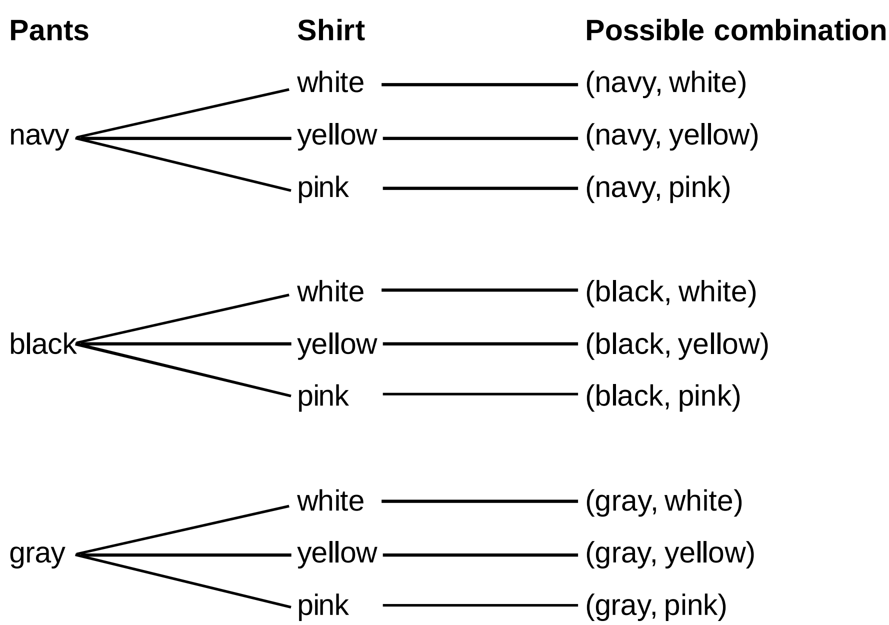
By fundamental principle of counting, the number of possible outcome of a dice and a coin are $6 \times 2 = 12$





Example 3 : Pranjal has 3 pairs of different coloured pants : navy, black and gray. He also has 3 different coloured shirts : white, yellow and pink. In how many ways can pranjal get dressed in pant and a shirt? Write all possible combination of dress code.

Solution : Pranjal has 3 pairs of different coloured pants and 3 different coloured shirts. Hence by fundamental principle of counting, the number of possible dress code for him is 3×3 = 9 ways. All possible combination of dress code are given by the following diagram.



Example 4 : An apartment complex apartments with 3 different options, designated by A through C

A : first floor, second floor

B : one bedroom, two bedroom, three bedroom

C : one bathroom, two bathrooms

How many apartment options are available? Describe all such options.

Solution : Here A has 2 options, B has 3 options and C has 2 options. Hence by fundamental principle of counting, there are 2.3.2 = 12 possible options.

All such possible options are listed bellow :

1.	1^{st} floor	one bedroom	one bathroom
2.	1^{st} floor	one bedroom	two bathrooms
3.	1^{st} floor	two bedrooms	one bathroom
4.	1^{st} floor	two bedrooms	one bathroom
5.	1^{st} floor	three bedroom	one bathroom
6.	1^{st} floor	three bedroom	two bathrooms
7.	2^{nd} floor	one bedroom	one bathroom
8.	2^{nd} floor	one bedroom	two bathrooms
9.	2^{nd} floor	two bedroom	one bathroom
10.	2^{nd} floor	two bedrooms	two bathrooms
11.	2^{nd} floor	three bedroom	one bathroom
12.	2^{nd} floor	three bedroom	two bathroom

Example 5 : A coin is tossed three times and the outcomes are recorded. How many possible outcomes are there? How many possible outcomes if the coin is tossed 5 times and n times?

Solution : In a single toss of a coin, there are 2 possible outcomes, either head (H) or Tail (T). Therefore, when a coin is tossed three times, the number of possible outcomes are 2×2×2 = 8 and all possible outcomes are (HHH), (HHT), (HTH). (HTT). (THH), (THT), (TTH), (TTT).

Similarly when a coin is tossed 5 times, the number of possible outcomes are 2×2×2×2×2 = 32

Again, when a coin is tossed n-times, the number of possible outcomes are $\underbrace{2\times2\times\ldots\ \ldots\ \ldots\times2} = 2^n$

Example 6 : A person wants is make a time table for 4 periods. He was to give one period each to english, mathematics, physics and chemistry. How many different time table can he make?

Solution : First period can be allowed to any of the four subjects. The person can do this in 4 ways. After allotting one subject to first period, he can give any of the remainig 3 subjects to second period. It can be done in 3 ways. Third period can be allotted to the remaining two subjects in 2 ways. The remaing fourth subjects, then can be allotted to the fourth period in 1 way.

Hence, by fundamental principle of counting, the number of different time tables = $4\times3\times2\times1 = 24$.

Example 7 : The teacher in class will award a prize to either a girl or a boy. How many different choices are there, if there are 110 girls and 85 boys in the class.

Solution : By fundamental principle of counting there are $110 + 85 = 195$ choices.

Example 8 : How many 2-digit even numbers can be formed from the digits 3, 4, 5, 6 and 7, if

i) repetition of digits is not allowed.

ii) repetition of digits is allowed.

Solution :

i) An even number will be formed when units place is filled with either 4 or 6 i.e there are 2 possible choices for filling up the units place.

Since repetition of digits is not allowed, therefore there are only 4 possible choices to fill up the ten's place. Hence by counting principle, total number of the possible even numbers of two digits $= 2\times4 = 8$

ii) Here units place can be filled up with either by 4 or 6 i.e by 2 ways and since repetition of digits is allowed, therefore thereare 5 possible choices to fill up the tens place.

Hence, by fundamental principle of counting, the number of possible even numbers of two digits = 2×5 = 10.

7.4 THE PIGEONHOLE PRINCIPLE

Statement : If there are n+1 objects and n boxes, then there is at least one box with two or more objects.

Proof : We can prove the principle by contradiction.

Assume that we have n+1 objects and every boxes has at most one object. Then the total number of objects is n, which is a contradiction because there are n+1 objects. Hence if n+1 objects are placed into n boxes, then there is at least one box containing two or more objects.

Example 1 : Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

Example 2 : Among 13 people, there are 2 who have their birthday in the same months.

The generalised pigeonhole principle states that "If N objects are placed into K boxes, then there is at least one box containing at least $\lceil N/K \rceil$ objects."

Note : [n] denotes the smallest integer greater than or equal to n.

Example 3 : Assume there there are 100 people. can you tell something about the number of people born in the same months.

Solution : Yes, there exists a month in which at least $\lceil 100/12 \rceil$ = $\lceil 8.3 \rceil$ = 9 people were born.

CHECK YOUR PROGRESS

Q.1. What is the sum rule for counting?

Q.2. There are 3 questions in a question paper. If the questions have 4, 3, 2 sloutions, find the total number of possible solutions.

Q.3. Give the statement of the pigeon hole principle.

7.5 MEANING OF FACTORIAL NOTATION

There are occasions when we wish to consider the product of first n natural numbers which is denoted by $\lfloor n$ or n! and call it as n-factorial, where n is a whole number.

$n! = n\,(n-1)\,(n-2)\ \ldots\ \ldots\ \ldots\ 3.2.1$

$\therefore\ 1! = 1$

$2! = 2.1 = 2$

$3! = 3.2.1 = 6$

$4! = 4.3.2.1 = 24$ and so on.

Also $0! = 1$

Note : It should be kept in mind that factorial notation is used only for whole numbers and not for negative integers or fractions.

7.6 PERMUTATIONS

While arranging the words with different letters, the order of letters plays an important part. Similarly, forming a number, the individual digits plays a significant role. Such situations in which order of occurence of events is important give rise to permutations.

The different arrangments that can be made with a given number of things taking some or all of them of a time are called permulation.

For example, the permulation of the letters a, b, c taken two at a time are ab, ba, ac, ca, bc, cb.

The symbol ${}^nP_r$ or P (n, r) is used to denote the number of permulations of n distinct things taken r at a time.

Permutation of n-distinct objects:

Theorem : The number of different permutations of n- distinct objects taken r at a time is given by ${}^np_r = n\,(n-1)\,(n-2)\ \ldots\ \ldots\ \ldots\ [n-(r-2)]$

$$= \frac{n!}{(n-r)!} \qquad [r \le n]$$

Note : 1) $n! = n\,(n-1)!$
$= n\,(n-1)(n-2)!$
$= n\,(n-1)(n-2)(n-3)!$ etc.

2) In the above repetition was not allowed. So that if we could fill the first place in n ways the second could be filled in (n–1) ways, third in (n–2) ways and finally rth in [n–(r–1)] ways.

Hence, ${}^{n}p_{r} = n(n-1)(n-2).........[n-(r-1)]$

3) If repetition is allowed, then each of the r-place can be filled in n ways.

Hence all the r-places can be filled in $\underbrace{n.n.n\ldots\ \ldots\ \ldots\ n}_{\text{r-times}} = n^r$ ways.

4) The number of permutation of n things taken all at a time is n!

By definition, ${}^{n}p_{n} = n(n-1)(n-2)\ldots\ \ldots\ \ldots\ 2.1$

$= n!$

5) We have, ${}^{n}p_{r} = \dfrac{n!}{(n-r)!}$

put r = n, ${}^{n}p_{n} = \dfrac{n!}{(n-n)!}$

$= \dfrac{n!}{0!}$

or $n! = \dfrac{n!}{0!}$

$\therefore\ 0! = \dfrac{n!}{n!} = 1$

Thus, 0! = 1

Example 1 : Prove the following relations

i) ${}^{n}p_{n} = n.{}^{n-1}p_{n-1}$

ii) $(n+1)\,{}^{n}p_{r} = (n-r+1)\,{}^{n+1}p_{r}$

iii) ${}^{n}p_{r} = {}^{n-1}p_{r} + r.\,{}^{n-1}p_{r-1}$

iv) $1+1.\,{}^{1}p_{1}+2.\,{}^{2}p_{2}+3.\,{}^{3}p_{3}+\ldots\ \ldots\ \ldots\ +n.{}^{n}p_{n} = {}^{n+1}p_{n+1}$

Solution :

i) By definition

$$^{n}p_{n} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!\left[\because 0! = 1\right]$$

Again $n.^{n-1}p_{n-1} = n\frac{(n-1)!}{[(n-1)-(n-1)]!}$

$$= n\frac{(n-1)!}{0!}$$

$$= n(n-1)! = n!$$

Hence, $^{n}p_{n} = n.\,^{n-1}p_{n-1}$

ii) We have

$$(n+1)^{n}p_{r} = (n+1)\frac{n!}{(n-r)!} = \frac{(n+1)!}{(n-r)!}$$

Again $(n-r+1)^{n+1}p_{r} = (n-r+1) = \frac{(n+1)!}{[(n+1)-r]!}$

$$= (n-r+1)\frac{(n+1)!}{[(n+1)-r]!}$$

$$= \frac{(n+1)!}{(n-r)!}$$

Hence, $(n+1)^{n}p_{r} = (n-r+1)^{n+1}p_{r}$

iii) We have,

$$^{n-1}p_{r} + r^{n-1}p_{r-1} = \frac{(n-1)!}{(n-1-r)!} + r\frac{(n-1)!}{[(n-1)-(r-1)]!}$$

$$= \frac{(n-1)!}{(n-1-r)!} + r\frac{(n-1)!}{(n-r)!}$$

$$= (n-1)!\left[\frac{1}{(n-r-1)!} + \frac{r}{(n-r)!}\right]$$

$$= (n-1)!\left[\frac{(n-r)}{(n-r)(n-r-1)!} + \frac{r}{(n-r)!}\right]$$

$$= (n-1)!\left[\frac{(n-r)}{(n-r)!} + \frac{r}{(n-r)!}\right]$$

$$= (n-1)!\left[\frac{n-r+r}{(n-r)!}\right]$$

$= \dfrac{n(n-1)!}{(n-r)!}$

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

$= {}^np_r$

iv) We have,

$1 + 1.{}^1p_1 + 2.{}^2p_2 + 3.\ {}^3p_3 + \ldots\ldots\ldots + n.{}^np_n$

$= 1 + 1.1! + 2.2! + 3.3! + \ldots\ldots\ldots + n.n!$

$= 1 + (2–1)! + (3–1)\ 2! + (4–1)\ 3! + \ldots\ldots\ldots\ [n + 1–1]n!$

$= 1! + (2!–1!) + (4!–3!) + \ldots\ldots\ldots + [(n + 1)–n!]$

$= (n + 1)!$

$= {}^{n+1}p_{n+1}$

Example 2 : How many words with or without meaning can be formed using all the letters of the word EQUATION, using each each letter exactly once

Solution : The word 'EQUATION' contains 8 letters which are all different. We are to use all the 8 letters and each letter is to used only once.

$\therefore$ The required number of words $= {}^8p_8$

$= \dfrac{8!}{(8-8)!}$

$= \dfrac{8!}{0!} = \dfrac{8!}{1}$

$= 8\times7\times6\times5\times4\times3\times2\times1$

$= 40320$

Example 3 : How many arrangements of the letters of the word 'BENGALI' can be made

i) if the vowels are to occupy only odd places

ii) if the vowels are never separate

iii) the relative positions of vowels and consonants are not changed.

Solution :

i) There are 4 odd places and 3 even places. The 3 vowels can occupy odd places in ${}^4p_3$ ways and consonants can be arranged in ${}^4p_4$ ways.

$\therefore$ Number of words $= {}^4p_3 \times {}^4p_4$

$$= \frac{4!}{(4-3)!} \times \frac{4!}{(4-4)!}$$

$$= \frac{4!}{1!} \times \frac{4!}{0!}$$

$= 4! \times 4!$

$= 24 \times 24 = 576$

ii) Regarding vowels A, E, I as one letter, we can arrange 5 letters in 5! ways in each of which vowels are together. These 3 vowels can be arranged themselves in 3! ways.

$\therefore$ Total number of words $= 5! \times 3!$

$= 120 \times 6$

$= 720$

iii) As the vowels and consonants are to retain their relative places. 3 vowels can be arranged in 3! ways and 4 consonants in 4! ways.

$\therefore$ Number of words $= 3! \times 4!$

$= 6 \times 24$

$= 144$

Example 4 : How many four digit numbers can be formed with the digit 1, 2, 3, 4 which are i) even, ii) odd

Solution :

i) To be an even number, the units place can be filled with either 2 or 4 i.e. c in 2 ways. The remaining three digits can be arranged in 3 places in ${}^3p_3$ ways.

Hence, the required number of numbers $= 2 \times {}^3p_3$

$= 2 \times 3!$

$= 2 \times 6 = 12$

ii) To be an odd number, the units place can be filled with 1 or 3 i.e. in 2 ways. The remaining 3 digits can be arranged in three places in ${}^3p_3$ ways.

Hence, the required number of numbers $= 2 \times {}^3p_3$

$= 2 \times 3!$

$= 2 \times 6 = 12$

Example 5 : How many four digits numbers can be formed with the digit 1, 2, 3, 4 which are

i) greater than 3000

ii) lying between 1000 and 3000

iii) divisible by 4

Solution :

i) To be a number greater than 3000, the thousands place can be filled by 3 or 4 i.e. in 2 ways. The remaining 3 digits can be arranged in 3 places (units, tens and thousands) in ${}^3p_3 = 3! = 6$ ways.

$\therefore$ Required number of numbers $= 2\times6$

$= 12$

ii) To be a number between 1000 and 3000, the thousands place can be filled with 1 or 2 i.e. in 2 ways. The remaining 3 digits can be arranged in three places in ${}^3p_3 = 3! = 6$ ways.

$\therefore$ Required number of numbers $= 2\times6$

$= 12$

ii) To be a number between 1000 and 3000, the thousands place can be filled with 1 or 2 i.e. in 2 ways. The remaining 3 digits can be arranged in three places in ${}^3p_3 = 3! = 6$ days.

$\therefore$ Required number of numbers $= 2\times6 = 12$

iii) We know that a number is divisible by 4 if the two digit number formed by the digits in its tens and units places is divisible by 4.

The two digit number in the tns and units places can be 12, 24 or 32 i.e. tens and units places can be filled in 3 ways. The remaining 2 digits can be arranged in other two places in ${}^2p_2 = 2! = 2$ ways.

Hence required number of numbers $= 3\times2 = 6$

Permutations when all the objects are not distinct : In the previous section we studied the permutations of distinct objects. Sometimes repetitions are allowed in the arrangement. For instance, let us consider the different permutations of the digits of the number 112. It is a 3 digit number when there are two 1's and one 2's. The total number of permutation of there 3 elements is not definitely ${}^3p_3 = 3!$ because here two digits are indentical. To find the number of permutations when some of the objects are alike, we must consider the follwoing theorem.

Theroem : The number of permutations of n objects of which m are of one kind and (n–m) of another kind, taken all at a time is $\frac{n!}{m!(n-m)!}$

Note : The number of permutations of n objects of which p are of one kind, q are of another kind and the remaining (n–p–q) of third kind is

$$\frac{n!}{p!\,q!\,(n-p-q)!}$$

Example 1 : Find the number of permutations that can be made out of the letters of the word 'MATHEMATICS'

Solution : Number of letters in the word 'MATHEMATICS' is 11 of which 2 are A's, 2 are T's, 2 are M's and the remaining are different.

$$\therefore \text{ Required number of permutations } = \frac{11!}{2!2!2!}$$

$$= \frac{11.10.9.8.7.6.5.4.3.2.1}{2.2.2}$$

$$= 4989600$$

Example 2 :

i) How many different permutations can be formed from the letters of the word 'EXAMINATION'?

ii) How many of them begin with A?

iii) In how many of them the vowels occur together?

Solution :

i) The total number of letters in the word 'EXAMINATION' is 11, of which 2 are A's, 2 are I's, 2 are N's.

$$\therefore \text{ The total number of permutation } = \frac{11!}{2!2!2!} = 4989600$$

ii) For the words begining with A, there are 1- letters for other places of which 2 are I's and 2 are N's

$$\therefore \text{ Total permutation } = 1 \times \frac{10!}{2!\,2!}$$

$$= \frac{10.9.8.7.6.5.4.3.2.1}{2.2} = 907,200$$

iii) If the vowels are kept together, then these 6 vowels can be considered as one unit, then the number of letters reduces to 6 of which 2 are N's. So number of permutation of these 6 letter word

$$= \frac{6!}{2!} = \frac{6.5.4.3.2}{2}$$

$$= 360$$

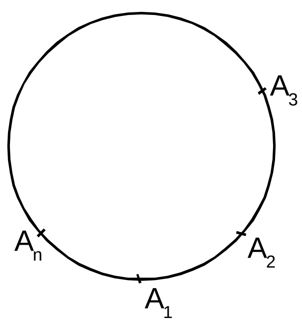
But the vowels can be arranged themselves. There are 6 vowels out of which 2 are A's and 2 are I's. So vowels can be arranged in

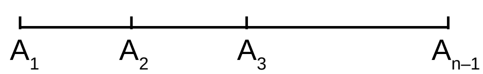
$$\frac{6!}{2!2!} \text{ ways } = \frac{6.5.4.3.2}{2.2}$$

$$= 180$$

$\therefore$ Total permutation = 360 × 180 = 64,800

Circular Permutations : Circular permutations are the permutations of objects along the circumference of a circle. In a circular permutation there is neither a begining nor an end.

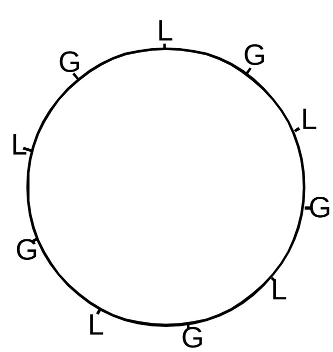




Here having fixed one object the remaining (n–1) objects can be arranged round in table in (n–1)! ways.

Example 1 : In how many ways can 5 gents and 4 ladies dine at a round table if no two ladies are to sit together.

Solution : Since the ladies are not to sit together, so 5 gents can have (5–1)! circular permutation.



$\therefore$ number of permutations in which gents can take their seats 4! = 24

Now there are 5 seats for ladies.

So 4 ladies occupy 5 seats in $^5p_4$ ways $= \frac{5!}{(5-4)!} = 120$

$\therefore$ Required no. of arrangement $= 24 \times 120$
$= 2880$

7.6 COMBINATIONS

Each of the different selections or groups that can be made by taking some or all of them (irrespective of order) is called a combination.

The number of combinations of n diffenent things taken r at a time ($r \leq n$) is denoted by ^nc_r and is defined by $^nc_r = \frac{n!}{r!(n-r)!}$

Thus the number combination of three letters a, b, c taken two at a time are $^3c_2 = \frac{3!}{2!\,(3-2)!} = 3$ which are ab, bc, ca.

Note :

i) The number of combinations of n things taken all at a time is given by $^nc_n = \frac{n!}{n!\,(n-n)!} = \frac{n!}{n!\,0!} = 1$

ii) The number of combinations of n things taking none at a time is given by $^nc_0 = \frac{n!}{0!\,(n-0)!} = 1$

iii) The number of combinations of n different things taken r at a time is equal to the number of combinations of n different things taken (n–r) at a time.

$$\therefore\ ^nc_r = {}^nc_{n-r}$$

Example 1 : If n and r are natural numbers and $r \leq n$, then prove that

$$^nc_r + {}^nc_{r-1} = {}^{n+1}c_r$$

Solution : By definition, we have

$$^nc_r + {}^nc_{r-1} = \frac{n!}{r!\,(n-r)!} + \frac{n!}{(r-1)!\,[(n-r+1)]!}$$

$$= \frac{n!}{r(r-1)!\,(n-r)!} + \frac{n!}{(r-1)!\,(n-r+1)(n-r)!}$$

$$= \frac{n!}{(r-1)!\,(n-r)!} + \left[\frac{1}{r} + \frac{1}{n-r+1}\right]$$

$$= \frac{n!}{(r-1)!\,(n-r)!} + \left[\frac{n-r+1+r}{r(n-r+1)}\right]$$

$$= \frac{(n+1)n!}{r(r-1)!\,(n-r+1)!\,(n-r)!}$$

$$= \frac{(n+1)!}{r!\,[(n+1)-r]!}$$

$$= {}^{n+1}c_r$$

Example 2 : A student has to answer 10 questions, choosing at least 4 from each of part A and part B. If there are 6 questions in part A and 7 in part B in how many ways can the student choose 10 questions?

Solution : The student has to answer 10 questions choosing at least 4 from each part A and B.

$\therefore$ The different possibilities are

i) 4 questions from A and 6 questions from B

ii) 5 questions from A and 5 questions from B

iii) 6 questions from A and 4 questions from B

$\therefore$ selection i) can be done in ${}^6c_4 \times {}^7c_6$ ways = 15 × 7 = 105

selection ii) can be done in ${}^6c_5 \times {}^7c_5$ ways = 6 × 21 = 126

selection iii) can be done in ${}^6c_6 \times {}^7c_4$ ways = 1 × 35 = 35

$\therefore$ Total number of selection = 105 + 126 +35 = 266

Example 3 : A polygon has 44 diagonals. Find the number of sides.

Solution : Let the number of sides of the polygon = n

$\therefore$ The number of angular points = n

The number of lines joining any two of these non-colinear n points = ${}^nc_2$

$\therefore$ Number of diagonals = ${}^nc_2 - n$

$\Rightarrow 44 = {}^nc_2 - n$

$$\Rightarrow \frac{n!}{2!(n-2)!} - n = 44$$

$$\Rightarrow \frac{n(n-1)}{2} - n = 44$$

$\Rightarrow n^2 - n - 2n = 88$

$\Rightarrow$ $n^2 - 3n - 88 = 0$

$\Rightarrow$ $(n + 8)(n - 11) = 0$

$\Rightarrow$ $n = -8, 11$

But $n \neq -8$, $\therefore$ $n = 11$

Hence the required number of sides = 11.

Example 4 : How many words of 5 letters can be constructed using 2 vowels and 3 consonants of the letter of word 'INVOLUTE'

Solution : There are 4 vowels viz I, O, U, E and 4 consonants viz. N, V, L, T. Out of four, 2 vowels can be selected in ${}^4c_2$ ways. Again out of four consonants, 3 can be selected in ${}^4c_3$ ways.

Both the operations, i.e 2 vowels and 3 consonants can be selected in ${}^4c_2 \times {}^4c_3$ ways.

Each combination contains 5 letters. These 5 letters can be arranged in 5! ways.

Total number of words $= {}^4c_2 \times {}^4c_3 \times 5!$

$$= \frac{4 \times 3}{2 \times 2} \times 4 \times 5 \times 4 \times 3 \times 2 \times 1 = 2880$$

7.8 PRINCIPLE OF INCLUSION - EXCLUSION

The principle of inclusion-exclusion is an important technique used in the art of enumeration. When two tasks can be done at the same time, we can not use the sum rule to count the number of ways to do one of the two tasks. Adding the number of ways to do each tasks leads to an overcount, since the ways to do both tasks are counted twice. To correctly count the number of ways to do one of the two tasks, we add the number of ways to do each of the two tasks and then subtract in number of ways to do both tasks. This technique is called the principle of inclusion-exclusion.

We can phrase this counting principle interms of sets. Let A_1 and A_2 be sets and let T_1 be the task of chosing an element from A_1 and T_2 the task of choosing an element from A_2. There are $|A_1|$ ways to do T_1 and $|A_2|$ ways to do T_2. The number of ways to do either T_1 or T_2 is the sum of the number of ways to do T_1 and the number of ways to do T_2, minus the number of ways to do both T_1 and T_2. Since there are $|A_1 \cup A_2|$ ways to do either T_1 or T_2 and $|A_1 \cap A_2|$ ways to do both T_1 and T_2. We have

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

Example : A discrete mathematics class contains 30 students majoring in computer science, 20 students majoring in mathematics and 8 joins in mathematics and computer science majors. How many students are in this class, if every student is majoring in mathematics, or computer science or both.

Solution :

Let A = The set of students majoring in computer science.

B = The set of students majoring in mathematics.

Then $A \cap B$ = the set of students who joins mathematics and compter science majors.

and $A \cup B$ = the set of students majoring in mathematics or computer science or both.

Hence $|A| = 30$, $|B| = 20$, $|A \cap B| = 8$

$$\therefore |A \cup B| = |A| + |B| - |A \cap B|$$

$$= |\, 30 + 20 - 8 \quad = 42$$

Therefore, there are 42 students in the class.

Similarly, the formula for the number of elements in the union of there sets A, B, C, we have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A|$$

The principle of inclusion-exclusion can be generalized to find the number of ways to do one of n different tasks or equivalently, to find the number of elements in the union of n sets A_1 A_2 ... ... A_n, we have

$$|A_1 \cup A_2 \cup \ldots\ldots\ldots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i \le j \le n} |A_i \cap A_j|$$

$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \ldots\ldots\ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots\ldots\ldots \cap A_n|$$

Example : In a survey of 60 people, it was found that 25 people read newspaper H, 26 read newspaper T and 26 read newspaper I, 9 read both H and I, 11 read both H and T, 7 read both T and I, 3 read all three newspapers, Find

The number of people who read at least one of the newspapers.

Solution : We have,

$| H | = 25. | T | = 26, | T | = 26, | H \cap I | = 9, |H \cap T | = 11,$

$| T \cap I | = 8, | H \cap T \cap I | = 3$

The number of people who read at least one of the newspapers

$= |H \cup T \cup I |$

Now, $|H \cup T \cup I | = | H | + | T | + | I | - | H \cap T | - | T \cap I |$

$- | I \cap H | + | H \cap T \cap I |$

$= 25 + 26 + 26 + - 11 - 9 - 8 + 3 = 52$

CHECK YOUR PROGRESS

Q.4. How many 5 digits telephone numbers can be formed from the digits 1, 2, 3, 4, 5, 6, 7 if no digit is repeated.

Q.5. Find the number of permutations which can be made with the letters of the word 'ENGINEERING'

Q.6. How many arrangments of the letters of the word 'BENGALI' can be made

i) if the vowels are never separate

ii) if the vowels are to occupy only odd places

Q.7. Show that the number of ways in which n different books can be arranged on a self. So that two particular books are not together is (n-2) × (n–1)!

Q.8. From the digits 1, 2, 3, 4, 5, 6, 7, 8 how many 3 digit odd numbers can be formed when

i) repetition of digits is allowed?

ii) repetition of digits is not allowed.

Q.9. There are 6 boys and 3 girls in a class. An entertainment committee of 6 persons is to be selected such that there are 4 boys and 2 girls in the committee. In how many ways can the committee be selected.

Q.10. An examination paper consists of 12 questions divided into parts A and B. Part A contains 7 questions and part B contains

5 questions selecting at least 3 from each part. In how many ways can the candidate select the questions.

Q.11. A polygon has 35 diagonals. Find the number of sides.

Q.12. Prove that ${}^{n}c_{r-1} + {}^{n}C_{r} = {}^{n+1}C_{r}$

Q.13. In a class of 35 students, 15 study economics, 22 study physics and 14 study chemistry. If 11 students study both economics and physics, 8 study physics and chemistry and 5 study economics and chemistry and if 3 study all the three subjects. Find how many students of the class are not taking any of these subjects.

7.9 LET US SUM UP

- If an event can occur in m different ways and if following it, another event can occur in n different ways, then in the given order, both the events can occur in m×n ways.
- It an event can occur in m different ways and another event can occur in n different ways and if these two events can not be done at the same time, i.e they are independent, then either of the two events can occur in (m + n) ways.
- If there are n + 1 objects and n boxes then there is at least one box with two or more objects.
- The number of different permutations of n distinct objects taken r at a time is given by ${}^{n}p_{r} = \frac{n!}{(n-r)!}$
- The number of permutations of n objects of which m are of one kind and (n–m) of another kind, taken all at a time is $\frac{(n+1)\,!}{r!(n-r+1)!}$
- Circular permutations are the permutations of objects along the circumference of a circle. In a circular permutation there is neither a begining nor an end.

- The number of combinations of n different things taken r at a time ($r \leq n$) is denoted by $^nc_r = \dfrac{n!}{r!(n-r)!}$
- The number of combinations of n different things taken r at a time is equal to the number of combinations of n different things taken (n-r) at a time i.e $^nc_r = {}^nc_{n-r}$

7.10 FURTHER READING

- *Robsen Kennth H. 2003.* Discrete Mathematics and its Application, 3rd edition. New Delhi : Tata Mc Graw - Hill Publishing Company Limited.
- *Sharma, J. K. 2007.* Discrete Mathematics, 2nd edition. New Delhi : Macmillan
- *Tyengar, N. Ch. S. N., V. M. Chandrasekran, K. A Venkatesh and P. S. Arunachalam, 2008.* Discrete Mathematics, New Delhi : Vikas Publishing House Pvt. Ltd.
- *Mott, J. L. 2007.* Discrete Mathematics for Computer Scientists, 2nd edition, New Delhi : Prentice-Hall of Indian Pvt. Ltd.

7.11 ANSWER TO CHECK YOUR PROGRESS

Ans. to Q. No. 1 : If an event can occur in m different ways and another event can occur in n different ways and if these two events are independent, then either of the two events can occur in (m+n) ways.

Ans. to Q. No. 2 : Question 1 has 4 solutions, question 2 has 3 solutions, question 3 has 2 solution. So by multiplication principle, the total number of solutions = $4 \times 3 \times 2 = 24$

Ans. to Q. No. 3 : If n+1 objects are put into n boxes, then there must be at least one box containing two or more objects.

Ans. to Q. No. 4 : We have 7 digits and 5 are to be selected

$\therefore$ Number of telephone numbers $= {}^7p_5$

$$= \frac{7!}{(7-5)!}$$

$$= 7\times6\times5\times4\times3$$

$$= 2520$$

Ans. to Q. No. 5 : The word 'ENGINEERING' consist of 11 letters of which there are 3 E's, 3 N's, 2 G's, 2 I's and rest all are different. Thus the possible permutation of the word are

$$= \frac{11!}{3!\times3!\times2!\times2!} = 2{,}77{,}200$$

Ans. to Q. No. 6 : There are 7 letters in the word 'BENGALI' of which 3 are vowels and 4 consonants.

i) Regarding vowels a, e, i as one letter, we can arrange 5 letters in 5! ways in each of which vowels are together. These 3 vowels can be arrange themselves in 3! ways.

$\therefore$ Total number of words $= {}^5p_5 \times {}^3p_3 = 720$

ii) There are 4 odd places and 3 even places. The 3 vowels can occupy odd places in ${}^4p_3$ ways and consonants can be arranged in ${}^4p_4$ ways.

$\therefore$ Total number of words $= {}^4p_3\times{}^4p_4 = 24\times24 = 576$

Ans. to Q. No. 7 : n books can be arranged in n! ways. Treating the two particular books to be one. We have n-1 books which can be arranged in ${}^{n-1}p_{n-1} = (n-1)!$ ways. Corresponding to each arrangement 2 books can be arranged among themselves in ${}^2p_2 = 2$ ways.

$\therefore$ The two books are together in $2\times(n-1)!$ arrangements.

$\therefore$ The number of arrangements in which they are not together $= (n!) - 2\times(n-1)!$

$$= n(n-1)! - 2\times(n-1)!$$

$$= (n-2)\times(n-1)!$$

Ans. to Q. No. 8 : We have 4 even numbers and 4 odd numbers.

i) The unit's place can be filled in from the digits 1, 3, 5, 7 in 4 ways. The ten's place can be filled 8 ways. The hundred's place can be filled in 8 ways.

∴ Total number of 3 digit odd numbers $= 8 \times 8 \times 4$

$= 256$

ii) The unit's place can be filled in 4 ways. After filling in the unit's place, we are left with 7 digits.

∴ The ten's place can be filled in 7 ways. Similarly, hundred's place can be filled in 6 ways.

∴ Total number of 3 digit odd numbers $= 6 \times 7 \times 4$

$= 168$

Ans. to Q. No. 9 : 4 boys can be selected from 6 boys in ${}^6c_4$ ways and 2 girls can be selected from 3 girls in ${}^3c_2$ ways.

∴ Required number of ways in which committee can be selected $= {}^6c_4 \times {}^3c_2$

$$= \frac{6!}{4!2!} \times \frac{3!}{2!1!} = 15 \times 3 = 45$$

Ans. to Q. No. 10 : The different choices are:

i) 3 questions from part A and 5 question from part B

ii) 4 questions from part A and 4 questions from part B

iii) 5 questions from part A and 3 questions from part B

Requird number of ways

$$= {}^7c_3 \times {}^5c_5 + {}^7c_4 \times {}^5c_4 + {}^7c_5 \times {}^5c_3$$

$$= 35 \times 1 + 35 \times 5 + 21 \times 10$$

$$= 420$$

Ans. to Q. No. 11 : Let the number of sides = n

∴ Number of angular points = n

Number of lines joining any two of these n non-coliner points $= {}^nc_2$

Number of diagonals $= {}^nc_2 - n \Rightarrow {}^nc_2 - n = 35$

$$\Rightarrow \frac{n(n-1)}{2} - n = 35$$

$\Rightarrow n^2 – n – 2n = 70$

$\Rightarrow n^2 – 3n – 70 = 0$

$\Rightarrow n^2 – 10n + 7n – 70 = 0$

$\Rightarrow (n – 10) + 7 (n – 10) = 0$

$\Rightarrow (n – 10)(n + 7) = 0$

$\Rightarrow n = 10, –7$

But $n \neq –7$

Hence, the required numbr of sides are 10

Ans. to Q. No. 12 : LHS $= {}^nc_{r–1} + {}^nc_r$

$$= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!}$$

$$= \frac{n!}{(r-1)!(n-r+1)(n-r)!} + \frac{n!}{r(r-1)!(n-r)!}$$

$$= \frac{n!}{(r-1)!\,(n-r)!}\left[\frac{1}{n-r-1} + \frac{1}{r}\right]$$

$$= \frac{n!}{(r-1)!\,(n-r)!}\left[\frac{r+n-r+1}{r(n-r+1)}\right]$$

$$= \frac{(n+1)\,n!}{r(r-1)!(n-r+1)(n-r)!}$$

$$= \frac{(n+1)\,!}{r!(n-r+1)!} = {}^{n+1}c_r = \text{RHS}$$

Ans. to Q. No. 13 : Let A, B, C be the set of students who study economics, physics and chemistry respectvely, then we have,

$|A| = 15$ $|B| = 22$ $|C| = 14$

$|A \cap B| = 11$ $|B \cap C| = 8$ $|A \cap C| = 5$

and $|A \cap B \cap C| = 3$

We know that ,

$|A \cap B \cap C| = |A| + |B| + |C| – |A \cap B| – |B \cap C|$

$– |A \cap C| + |A \cap B \cap C|$

$= 15 + 22 + 14 – 118 – 5 + 3 = 30$

$\therefore$ Number of students who do not study any of these subjects $= |A \cup B \cup C|$

$= 35 – 30 = 5$

7.12 MODEL QUESTIONS

Short-answer questions

Q.1. What is the product rule for counting?

Q.2. What is meant by ${}^{n}p_{r}$ and ${}^{n}c_{r}$?

Q.3. Prove that 0! = 1

Q.4. Define circular permutation.?

Q.5. Give the statement of Generalized pigeon hole principle.

Q.6. How many different words containing all the letters of the word ‘TRIANGLE’ can be formed so that consonants are never separated?

Q.7. What is the number of combinations of n objects taken r at a time in which p particular objects never occur?

Q.8. Give an example of the application of pigeonhole principle.

Q.9. How many positive integers between 100 and 999 inclusive are divisible by 7?

Q.10. State the principle of inclusion and exclusion.

Long answer questions

Q.1. How many 4 digit numbers greater than 10,000 can be formed from the digits 1, 2, 3, 4 and 5?

Q.2. How many four digit numbers can be formed with the digit 1, 2, 3 and 4 which are i) odd, ii) even?

Q.3. How many different ords can be formed with the letters of the word ‘ALGEBRA’?

Q.4. How many different words can be formed with the letters of the word ‘COMPUTER’? How many of them

i) will begin with C and with R?

ii) will not have T and R together?

Q.5. How many positive integers less than 1000

i) are divisible by 6?

ii) are divisible by 6 but not 8?

iii) are divisible by both 6 and 8?

Q.6. In how many ways can the letters of the word 'PERMUTATIONS' be arranged if the

i) vowels are all together?

ii) there are always 4 letters between P and S

Q.7. There are 3 prizes to be distributed among 5 students. In how many ways it can be done when

i) no students gets more than one prize

ii) no student gets all the prizes.

Q.8. In an election, a voter may vote for any number of candidates but not greater than the number to be chose. There are 7 candidates and 4 are to be chosen. In how many possible ways can a person vote?

Q.9. Out of 6 boys and 4 girls, a group of 7 is to formed. In how many ways can this be done if the group is to have a majority of boys?

Q.10. A committee of 5 is to be selected from among 6 boys and 5 girls. Determine the number of ways of selecting the committee if it is to consist of at least 1 boy and 1 girl.

Q.11. A committee of 5 is formed from 7 boys and 4 girls. In how many ways can this be done when the committee consists of

i) exactly 3 girls ii) at least 3 girls

Q.12. The Indian Cricket team consists of 18 players. It includes 2 wicket keepers and 5 bowlers. In how many ways can a cricket eleven be selected if we have to select 1 wicket-keeper and at least 3 bowlers?

Q.13. In how many ways can 5 Doctor and 3 Enginneer sit around a table. So that no two enginneers are together?

Q.14. Show that the total number of combination which can be made of n different objects taken some or all at a time is 2^n-1

Q.15. How many combinations of the letters of the word 'NUMBERS' taken 3 at a time

i) contain M? ii) donot contain M?

iii) contain M and R iv) contain neither M nor R?

Q.16. Of the members of three athletic teams in a certain school, 21 are on basketball team, 26 on the hockey team, and 29 on the football team, 14 play hockey and basketball, 15 play hockey and football and 12 play football and basketball, 8 are on all the three teams. How many members are there together?

Q.17. State and prove the principle of inclusion and exclusion for three sets.

UNIT 8:BASIC ALGEBRAIC STRUCTURE -I

UNIT STRUCTURE

8.1 LEARNING OBJECTIVES

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

- binary operation on a set
- groups
- subgroups and cosets
- cyclic groups
- normal subgroups
- quotient groups.

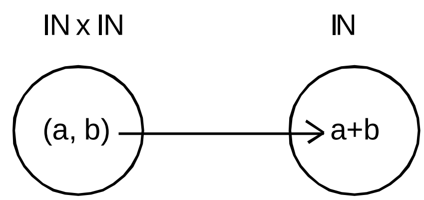
8.2 INTRODUCTION

In unit-1, we have studied relations and functions. In this unit we will introduce the notion of groups. Group is an algebraic structure, i.e, a non-empty set equipped with a binary operation satisfying certain postulates. Group theory occupies an important position in the study of abstract algebra.

8.3 BINARY OPERATION

Let us consider the set IN of natural numbers.

For every ordered pair $(a, b) \in$ IN x IN, we get a unique $a+b \in$ IN. So we can define a funtion f : IN x IN $\rightarrow$ IN, $f(a, b) = a+b$.

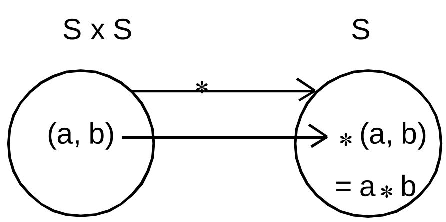


This function is known as a binary operation on IN. Thus, addition is a binary operation on IN.

Similarly, multiplication is a binary operation on IN; for every ordered pair $(a, b) \in$ IN x IN. We get a unique $ab \in$ IN. But subtraction is not a binary operation on IN; for every ordered pair $(a, b) \in$ IN x IN, we do not get $a-b \in$ IN. We have $(2, 3) \in$ IN x IN, but $2-3 = -1 \notin$ IN.

Definition: A binary operation $*$ on a non-empty set S is a function from S x S to S, i.e.

$* : S \times S \rightarrow S$



Here the image of $(a, b) \in S \times S$ under the function $*$, i.e $*(a, b)$ is denoted by $a * b$.

Thus, $*$ is a binary operation on S if $a * b \in S$, for all $a, b \in S$.

Definition: Let $*$ be a binary operation on a non-empty set S and H be a subset of S. H is said to be closed under $*$ if for all a, b $\in$ H, we have $a * b \in H$.

Number of Binary operations on a finite set

Let A, B be two finite sets, and n (A) = m and n (B) = n.

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 in n ways and lastly, the m th element can be associated in n ways.

$\therefore$ the number of functions

$= n. n \ldots \ldots n$ (m factors) $= n^m$]

We know that n (A x A) = 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 IN.
2. Subtraction is not a binary operation on IN.
3. Multiplication is a binary operation on IN.
4. Addition is a binary operation on Z.
5. Addition is not a binary operation on the set S = Z – {0} of non–zero integers, for $3 \in S$, $-3 \in S$, but $3+(-3) = 0 \notin S$.
6. Subtraction is a binary operation on 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 matrex.
8. Let M_{mxn} be the collection of all m x n real matrices. Matrix addition is a binary operation on M_{mxn}.
9. Let M_{nxn} be the collection of all nxn real matrices. Matric multiplication is a binary operation on M_{nxn}.
10. Addition (also multiplication) is a binary operation on the set C of complex numbers.

Example 1: Is $*$ defined by $a * b = a-b+10$ a binary operation on Z ?

Solution: Let a, b $\in$ Z

Clearly $a-b+10 \in Z, \forall\ a, b \in Z$

i.e., $a * b \in Z, \forall a, b \in Z$

$\therefore *$ is a binary operation on Z

Example 2: Is $*$ defined by $a * b = \frac{ab}{5}$ a binary operation on Q ?

Solution: Let $a, b \in Q$

$\therefore ab \in Q$ (the product of two rational numbers is a rational number)

$\therefore \frac{ab}{5} \in Q$

i.e. $a * b \in Q, \forall a, b \in Q$

$\therefore *$ is a binary operation on Q

Example 3: Let P be the set of all subsets of a non-empty 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, as follows.

Let $A = \{a_1, a_2, a_3\}$.

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 x a_j (i = 1, 2, 3; j = 1, 2, 3) in the (i, j) th cell as shown in Table 2.1. Each of the 9 entries belongs to A, since $*$ is a binary operation on A.

$*$	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 2.1

Example 4: Is multiplication a binary operation on {–1, 0, 1} ?

x	–1	0	1
–1	1	0	–1
0	0	0	0
1	–1	0	1

Table 2.2

Solution: Each of the 9 entries belongs to A

$\therefore$ multiplication is a binary operation on {–1, 0, 1}.

Example 5: Is addition a binary operation on {–1, 0, 1} ?

Solution: $-2 \notin \{-1, 0, 1\}$

$2 \notin \{-1, 0, 1\}$

$\therefore$ addition is not a binary operation on {–1, 0, 1}.

+	–1	0	1
–1	–2	–1	0
0	–1	0	1
1	0	1	2

Table 2.3

Example 6: Is $*$ defined by $a * b = |a-b|$ a binary operation on {0, 1, 2} ?

Solution: $0 * 0 = |0-0| = 0$,

$0 * 1 = |0-1| = 1$,

$0 * 2 = |0-2| = 2$;

$1 * 0 = |1-0| = 1$, $1 * 1 = |1-1| = 0$,

$1 * 2 = |1-2| = 1$;

$2 * 0 = |2-0| = 2$, $2 * 1 = |2-1| = 1$, $2 * 2 = |2-2| = 0$,

$*$	0	1	2
0	0	1	2
1	1	0	1
2	2	1	0

Table 2.4

From the table we see that $*$ is a binary operation on {0, 1, 2}.

8.3.1 Commutative Binary Operation

A binary operation $*$ on a non-empty set S is commutative if $a * b = b * a$, $\forall a, b \in S$.

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 2.4 are symmetric with respect to the principal diagonal 0, 0, 0. Therefore, $*$, defined in Example 6, is commutative on {0, 1, 2}.

Example 7: Is the binary operation $*$ defined by $a * b = a-b+5$ commutative on Z ?

Solution: We have $a * b = a-b+5$

$b * a = b-a+5$, $\forall a, b \in Z$

Clearly $a * b \neq b * a$

$\therefore *$ is not commutative on Z.

Example 8: Let Q be the set of rational numbers. Let $*$ be a binary operation on Q defined by $a * b = ab^2$, $\forall a, b \in Q$. Is $*$ commutative?

Solution: $a * b = ab^2$, $b * a = ba^2$, $\forall a, b \in Q$

$\therefore a * b \neq b * a$

$\therefore *$ is not commutative.

8.3.2 Associative Binary Operation

A binary operation $*$ on a non-empty set S is associative if $(a * b) * c = a * (b * c)$, $\forall a, b, c \in S$.

Example 9: Is the binary operation $*$ defined by $a * b = a–b+5$ associative on Z ?

Solution: Let $a, b, c \in Z$.

$(a * b) * c = (a–b+5) * c$

$= (a–b+5) – c+5$

$= a–b–c+10$

$a * (b * c) = a * (b–c+5)$

$= a – (b–c+5)+ 5$

$= a – b + c – 5 + 5$

$= a – b + c$

$\therefore (a * b) * c \neq a * (b * c)$

$\therefore *$ is not associative.

Example 10: Let X be the set of rational numbers excluding 1. We define $*$ on X as follows.

$a * b = a + b – ab$, $\forall a, b \in X$.

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. $a-1=0,\ 1-b=0$

i.e. $a = 1,\ b = 1$, which is a contradiction.

$\therefore a+b-ab \in X$

i.e $a * b \in X,\ \forall a, b \in X$

$\therefore *$ is a binary operation on X

Second Part

$a * b = a+b-ab$

$= b+a-ba$

$= b * a$

$\therefore *$ is commutative on X.

Again $(a * b) * c$

$= (a+b-ab) * c$

$= (a+b-ab) + c - (a+b-ab)c$

$= a+b-ab+c - ac-bc+abc$

$= a+b+c-ab-bc-ca+abc$

$a * (b * c) = a * (b+c-bc)$

$= a+(b+c-bc) - a(b+c-bc)$

$= a+b+c-ab-bc-ca+abc$

$\therefore (a * b) * c = a * (b * c)$

$\therefore *$ is associative.

8.3.3 Identity Element

Let S be a non-empty set equipped with a binary operation $*$. An element $e \in S$ is called an identity element for $*$ if

$$a * e = a = e * a,\ \forall a \in S.$$

Note: Identity element for a binary operation if it exists, is unique.

Examples

1. Multiplication is a binary operation on IN. There exists $1 \in$ IN such that

$$a * 1 = a = 1 * a,\ \forall\ a \in \text{IN}$$

$\therefore$ 1 is the identity for multiplication in IN.

2. Addition is a binary operation on Z.

There exists $0 \in Z$ such that

$$a + 0 = a = 0+a, \ \forall\, a \in Z$$

$\therefore$ 0 is the identity for addition in Z.

3. Addition is a binary operation on IN. But there does not exist identity element for addition in IN.

4. Matrix addition is a binary operation on M_{mxn}, the set of all m x n real matrices. The m x n null matrix 0 is the identity for matrix addition in M_{mxn}.

8.3.4 Inverse of an Element

Let S be a non-empty 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}. 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 IN and $1 \in$ IN is the identity for multiplication. But no element of IN, except 1, possesses inverse under multiplication in IN.

2. Addition is a binary operation on Z and $0 \in Z$ is the identity for addition. For every $a \in Z$, there exists $-a \in Z$ such that

$$a+(-a) = 0=(-a) + a.$$

$\therefore$ –a is the inverse of a under addition.

8.4 GROUP

A non-empty set G, equipped with a binary operation $*$, is called a group if the following postulates are satisfied.

(i) Associativity

$(a * b) * c = a * (b * c), \forall a, b, c \in G$

(ii) Existence of Identity

There exists $e \in G$ such that

$a * e = a = e * a, \forall a \in G$.

e is called identity.

(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.

Furthermore, if $*$ is commutative, G is called an Abelian group, after the name of the celebrated Norwegian mathematician Niels Heurik Abel (1802–1829).

Note : 1. In order to be a group, there must be a non-empty 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.
3. A non-empty set G equipped with a binary operation is called a semigroup if the binary operation is associative.

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.

(ii) We know that multiplication of real numbers is associative.

(iii) 1 is the identity under multiplication.

(iv) Every element G possesses inverse in G.

1 is the inverse of 1,

–1 is the inverse of –1.

*	–1	1
–1	1	–1
1	–1	1

Table 2.5

$\therefore$ G is a group under multiplication.

(v) Moreover, multiplication of real numbers is commutative.

$\therefore$ G is an Abelian group.

Example 13: Let G = {z : z is complex and z^n=1}, i.e. G is the set consisting of the n the roots of unity. ($n \in$ IN)

(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 numbers is associative.

(iii) There exists $1 \in$ G such that

$1z = z = z1, \ \forall z \in G$

$\therefore$1 is the identity element.

(iv) Let $z \in$ G. $\therefore z^n = 1$

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 the 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.

Note : We have seen that, for every positive integer n, there exists an Abelian group of order n.

Example 14: Let Z be the set of integers

(i) Let a, b $\in$ Z

$\therefore$ a+b $\in$ Z, $\forall$ a, b $\in$ Z

i.e. addition is a binary operation on Z.

(ii) We know that multiplication of integers is associative.

(iii) We have 0$\in$ Z and a+0 = a = 0+a, $\forall$ a$\in$ Z

$\therefore$ 0 is the identity.

(iv) For every a $\in$ Z, there exists –a$\in$ Z such that a+(–a) = 0 = (–a) +a.

$\therefore$ Z is a group under addition.

(v) Moreover, addition of real numbers is commutative.

$\therefore$ Z is an Abelian group under addition.

Note : Z is an infinite group.

Some other examples are the following.

- Q is an Abelian group under addition.
- IR is an Abelian group under addition.
- Q_0, the set of non-zero rational numbers is an Abelian group under multiplication.
- IR_0, the set of non-zero real numbers is an Abelian group under multiplication.
- C is an Abelian group under addition.
- C_0, the set of non-zero complex numbers is an Abelian group under multiplication.

Example 15: Let G = $\left\{\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} : \alpha \in IR\right\}$

(i) Let $A_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in G,$

$$A_\beta = \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix} \in G; \quad \alpha, \beta \in IR$$

Now $A_\alpha A_\beta = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{pmatrix}$

$$= \begin{pmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix} = A_{\alpha+\beta} \in G$$

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 $A_\alpha I = A_\alpha = IA_\alpha, \forall A_\alpha \in G$.

$\therefore$ I is the identity element

(iv) We have $|A_\alpha| = \begin{vmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{vmatrix}$

$$= \cos^2\alpha + \sin^2\alpha = 1 \neq 0$$

$\therefore A_\alpha^{-1}$ exists.

$\therefore \operatorname{adj} A_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$

$\therefore A_\alpha^{-1} = \dfrac{1}{|A_\alpha|} adj \ A_\alpha$

$$= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} = \begin{pmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{pmatrix} \in G$$

$\therefore$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 = $\left\{ \begin{pmatrix} x & x \\ x & x \end{pmatrix} : x \in IR, \ x \neq 0 \right\}$

(i) Let $\begin{pmatrix} x & x \\ x & x \end{pmatrix} \in G, \ \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in G$

x, y $\in$ IR, $x \neq 0$, $y \neq 0$

Now $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} y & y \\ y & y \end{pmatrix} = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in G,$ xy $\in$ IR, 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 $\begin{pmatrix} x & x \\ x & x \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \\ \frac{x}{2}+\frac{x}{2} & \frac{x}{2}+\frac{x}{2} \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

$\therefore \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ 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.

Note : In the above example, 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.

$$a * b = a+b-ab, \ \forall \ a, b \in G$$

(i) $*$ is a binary operation on G

[Ref : Example 10]

(ii) $*$ is associative on G

[Ref : 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.

$$a * \frac{a}{a-1} = 0 = \frac{a}{a-1} * a$$

$\therefore \frac{a}{a-1}$ is the inverse of a under x.

$\therefore$ G is a group commutative.

[Ref : Example 10]

$\therefore$ G is an Abelian group.

Theorem 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]

Again $ef = f = fe$ [$\because$ 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 the identity}

$= b(ac)$ [$\because e = ac$]

$= (ba)c$ [by associativity]

$= ec$ [$\because$ e is the identity]

$= c$

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 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$

$= a\,e\,a^{-1}$

$= aa^{-1}$

$= e$

$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b$

$= b^{-1}\,eb$

$= b^{-1}\,b$

$= e$

$\therefore b^{-1}a^{-1}$ is the inverse of ab, i.e. $(ab)^{-1} = b^{-1}a^{-1}$

(v) We have $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b=(a^{-1}a)c$, [by associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$, [$\because$ e is the identity]

Again $ba = ca$

$\Rightarrow (ba)a^{-1} = (ca)\,a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$ [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 $\in$ G

$\therefore$ $a^{-1} = a$, $b^{-1} = b$ (given)

Now $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ [Theorem 1 (iv)]

$\therefore$ 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 $\in$ G.

Solution: $(ab)^2 = a^2 b^2$

$\Leftrightarrow$ (ab) (ab) = (aa) (bb)

$\Leftrightarrow$ a(ba)b = a(ab)b

$\Leftrightarrow$ (ba)b = (ab)b, [by left cancellation law]

$\Leftrightarrow$ ba = ab, [by right cancellation law]

$\Leftrightarrow$ G is Abelian.

CHECK YOUR PROGRESS 1

Q 1: Let A be a finite set having 4 elements. What is the number of binary operations on A?

Q 2: Is $*$ defined by $a * b = \frac{a}{b}$, a binary operation on IR ?

Q 3: Is multiplication a binary operation on {–1, 1, i, –i} ? where $i = \sqrt{-1}$.

Q 4: Let Q be the set of rational numbers. Show that $*$ defined by

$a * b = a + ab$, is a binary operation on Q.

Examine if $*$ is (i) commutative, (ii) associative.

Q 5: Show that the set G = {1, ω, ω^2} consisting of the cube roots of unity is a group under usual multiplication. (ω is a complex cube root of unity).

Q 6: Show that the set G consisting of all 2 x 2 non-singular matrices over reals is a group under matrix multiplication.

Q 7: Let G = $\left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} : x \in IR,\ x \neq 0 \right\}$

Show that G is an Abelian group under matrix multiplication.

Q 8: If for every element a in a group G, $a^2 = e$; prove that G is Abelian. (e is the identity of G).

8.5 SUBGROUP

Let us consider the set Z of integers.

We know that Z is a group under addition.

Let 2Z = {0, ± 2, ± 4, ...} be the set of even integers.

Clearly 2Z is a non-empty subset of Z.

Moreover, 2Z is also a group under addition.

In this case, 2Z is said to be a subgroup of Z.

Definition : A non-empty 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 are nontrivial.

(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)]

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 group under multiplication

$\therefore H \leq G$.

The set of real numbers IR is a group under addition. The set IR_+ of positive real numbers is a group under multiplication. IR_+ is a subset of IR, but not a subgroup of IR. Binary operations are different.

Theorem 2: Let H be a subgroup of a group G. Then

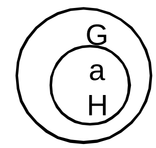
(i) the identity element of H is the identity element of G;

(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 be the inverse of a in H, and c be the inverse of a in G.

$\therefore$ ab = e = ba

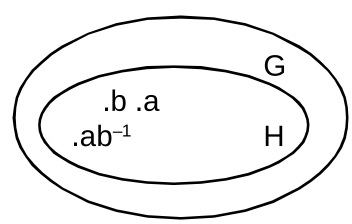
ac = e = ca

$\therefore$ 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 can conclude that there cannot be two disjoint subgroups of a group.

Theorem 3 : A non-empty 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) $e \in H, a \in H \Rightarrow ea^{-1} \in H$

$\Rightarrow a^{-1} \in H$

$\therefore$ 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 $\Rightarrow$ $a(b^{-1})^{-1}\in H$ (Since $(b^{-1})^{-1}\in H$)

$\Rightarrow$ ab $\in$ H

(iv) The binary operation is associative in H as it is associative in G.

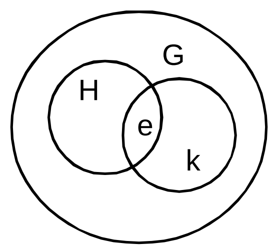
$\therefore$ H is a group under the same binary operation in G. Also H $\subseteq$ G.

$\therefore$ H $\leq$ G.

Note : If G is an additive group, i.e., if G is a group under addition, then a non-empty subset H of G is a subgroup of G if and only if a, b $\in$ H $\Rightarrow$ a–b$\in$ H.

Theorem 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 $\neq \phi$,

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. $\therefore ab^{-1} \in H$

a, b $\in$ K and K $\leq$ G. $\therefore ab^{-1}\in K$

$ab^{-1}\in H$ 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 necessarity a subgroup.

Let Z = {0, $\pm$1, $\pm$2, $\pm$3, ...} be the additive group of integers.

Let 2Z = {0, $\pm$2, $\pm$4, $\pm$6,.....}

3Z = {0, $\pm$3, $\pm$6, $\pm$9,.....}

Clearly 2Z $\leq$Z, 3 Z $\leq$ Z

Now 2$\in$ 2 Z $\cup$3 Z, 3 $\in$ 2 Z $\cup$ 3 Z

But 2+3 = 5 $\notin$ 2 Z $\cup$ 3 Z

$\therefore$ addition is not a binary operation on 2Z $\cup$ 3 Z.

$\therefore$ 2 Z $\cup$ 3 Z cannot be a group.

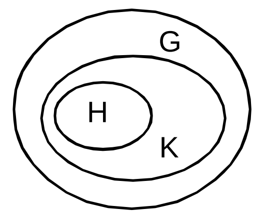
Theorem 5 : The union of two subgroups is a subgroup if and only if one of them is contained in the other.

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 $ab \in K$, $b \in K \Rightarrow (ab)b^{-1} \in K$

$\Rightarrow a(bb^{-1}) \in K$

$\Rightarrow ae \in K$

$\Rightarrow a \in K$

which is a contradiction.

So, our assumption is wrong.

$\therefore$ either $H \subseteq K$ or $K \subseteq H$.

8.6 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 $aH = \{ah : h \in H\}$ is called a left coset of H in G.

Note : (1) Right (or left) coset cannot be empty we have $e \in H$

$\therefore ea = a \in H a \qquad \therefore Ha \neq \phi$

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 $a+H=\{a+h : h \in H\}$

Example : Let us consider the additive group of integers Z.

We know that $2Z = \{0, \pm 2, \pm 4, \pm 6, ...\} \leq Z$

We have

$0+2Z = \{0, \pm 2, \pm 4, \pm 6, ...\} = 2Z$

$1+2Z = \{\pm 1, \pm 3, \pm 5, \pm 7, ...\}$

$2+2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}$

$3+2Z = \{\pm 1, \pm 3, \pm 5, \pm 7, ...\}$ and so on.

Thus, we see that

$2Z = 2+2Z = 4+2Z = ...$

$1+2Z = 3+2Z = 5+2Z = ...$

$\therefore$ 2Z has two distinct left cosets viz. 2Z and 1+2Z such that

$$2Z \cup (1+2Z) = Z$$

$$2Z \cap (1+2Z) = \phi$$

Similarly, 2Z has two distinct right cosets 2Z and 2Z + 1 such that

$$2Z \cup (2Z+1) = Z$$

$$2Z \cap (2Z+1) = \phi$$

Theorem 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) $aH = bH \Leftrightarrow a^{-1}b \in H$; $Ha = Hb \Leftrightarrow ab^{-1} \in H$, where $a, b \in G$

Proof : (i) Let $aH = H$

We have $ae \in aH$, e is the identity of G

$\Rightarrow ae \in H \qquad [\because aH = H]$

$\Rightarrow a \in H$

Conversely, let $a \in H$

Let $x \in aH$

This $\Rightarrow$ x = ah, for some $h \in H$

Now $a \in H$, $h \in H$ $\therefore ah \in H \Rightarrow x \in H$

Thus, $x \in aH \Rightarrow x \in H$

$\therefore aH \subseteq H$ ...(1)

Again, let $y \in H$

$\therefore a \in H$, $\therefore a^{-1} \in H$

$\therefore a^{-1}y \in H$

$\Rightarrow a^{-1}y = h_1$, for some $h_1 \in H$

$\Rightarrow a(a^{-1}y) = ah_1$

$\Rightarrow (aa^{-1})y = ah_1$

$\Rightarrow ey = ah_1$

$\Rightarrow y = ah_1 \in aH$

Thus, $y \in H \Rightarrow y \in aH$

$\therefore H \subseteq aH$ ...(2)

From (1) and (2), aH = H

Similarly $Ha = H \Leftrightarrow a \in H$.

(ii) aH = bH

$\Leftrightarrow a^{-1}(aH) = a^{-1}(bH)$

$\Leftrightarrow (a^{-1}a)H = (a^{-1}b)H$

$\Leftrightarrow eH = (a^{-1}b)H$

$\Leftrightarrow H = (a^{-1}b)H$

$\Leftrightarrow a^{-1}b \in H$ (using (1))

Similarly, $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Theorem 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 $h_2 \in H$

$\therefore ah_1 = bh_2$

$\Rightarrow (ah_1)h_1^{-1} = (bh_2)h_1^{-1}$

$\Rightarrow a\, h_1h_1^{-1} = b\, h_2h_1^{-1}$

$\Rightarrow ae = bh_2h_1^{-1}$, where e is the identity of G

$\Rightarrow a = bh_2h_1^{-1}$

Similarly $b = ah_1h_2^{-1}$

Let $p \in aH \Rightarrow p = ah_3$ for some $h_3 \in H$

$= bh_2h_1^{-1}h_3$

$\in bH, \because h_2h_1^{-1}h_3 \in H$

Thus, $p \in aH \Rightarrow p \in bH$ $\quad \therefore aH \subseteq bH$ $\quad$ (1)

Again, let $q \in bH \Rightarrow q = bh_4$ for some $h_4 \in H$

$\Rightarrow q = ah_1h_2^{-1}h_4$

$\in aH, \quad \because h_1h_2^{-1}h_4 \in H$

Thus $q \in bH \Rightarrow q \in aH$ $\quad \therefore bH \subseteq aH$ $\quad$ (2)

From (1) and (2), $aH = bH$

Thus, aH, bH are either disjoint or identical.

Theorem 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 $O(G) = n$ and $H \leq G$.

Let e be the identity of G.

Case 1 : Let $H = \{e\}$,

There is nothing to prove. $O(H) = 1$, and 1 divides n.

Case 2 : Let $H = G$. Hence $O(H) = O(G)$.

There is nothing to prove.

Case 3 : Let $H \neq \{e\}$, $H \neq G$.

Let $O(H) = m$, $m < n$.

Let $H = \{h_1, h_2, h_3, \ldots h_m\}$, where the 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 $ah_i = ah_j$, $1 \leq i \leq m$, $1 \leq$

$j \le m$, $i \ne j$ then $h_i = h_j$, (by left cancellation law), which is a contradiction.

Again, no element of H is equal to any element of aH, for if $h_i = ah_j$, then $h_i\, h_j^{-1}$ i.e. $h_i\, h_j^{-1} = a$ 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 $bH = \{bh_1, bh_2, ..., bh_m\}$

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 $ah_i = bh_j$, then $ah_i h_j^{-1} = bh_j h_j^{-1}$ i.e $ah_i h_j^{-1} = b$ 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 2

Q 1: Is the multiplicative group IR_+ of positive real numbers a subgroup of the additive group IR of real numbers? Justify your answer.

Q 2: Can there be two disjoint subgroups of a group? Justify your answer.

Q 3: Can an Abelian group have a non-Abelian subgroup ?

Q 4: Let Z be the additive group of integers. Let m be a fixed integer. Show that the set.

$mZ = \{0, \pm m, \pm 2m, \pm 3m, ...\}$ is a subgroup of Z.

Q 5: Let G be the group consisting of all 2 x 2 non-singular real matrices under matrix multiplication. Let

H = $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in IR \text{ and } ad - bc = 1 \right\}$

Show that H is a subgroup of G.

Q 6: Give an example to show that a group cannot be expressed as the union of two of its proper subgroups.

8.7 CYCLIC GROUPS

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, $n \in Z$. 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.

Examples

(1) We know that G = {–1, 1} is a group under multiplication.

We have $(-1)^1 = -1$, $(-1)^2 = 1$

$\because$ G is a cyclic group generated by –1, i.e. G = <–1>

(2) We know that G = {1, ω , ω^2} is a group under multiplication ; ω is a complex cube root of unity.

We have, $\omega^1 = \omega$, $\omega^2 = \omega^2$, $\omega^3 = 1$

.. G is cyclic group generated by ω i.e., G = $<\omega>$

Similarly G = $<\omega^2>$

(3) We know that G = {–1, 1, –i, i} is a group under multiplication.

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 >

(4) Let Z be the additive group of integers.

Let x $\in$ Z Then x = 1x

$\therefore$ G is a cyclic group generated by 1, i.e. G = < 1 >

Similarly G = < –1 >.

Theorem 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 10 : If a is a generator of a cyclic group G, a^{-1} is also a generator of G.

Proof : Let $G = < a >$ be a cyclic group.

Let $x, y \in G$.

Then there exists integer m such that $x = a^m$

$= (a^{-1})^{-m}$

$\therefore G = < a^{-1} >$.

Division Algorithm for 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 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 Algerithm, 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.

$\therefore p = mq$

$\Rightarrow x = a^p = a^{mq} = (a^m)^q$

$\therefore H = \langle a^m \rangle$ is a cyclic group.

Theorem 12 : A group of prime order is cyclic.

Proof : Let G be a finite group, and O (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.

$\therefore$ by Lagrange's subgroup order theorem,

O (H) divides O (G)

i.e. O(H) divides p

This $\Rightarrow$ O(H) = 1 or p

But $O(H) \neq 1$, $\because a \neq e$.

$\therefore$ O (H) = p = O(G)

$\therefore$ H = G

$\therefore$ G is a cyclic group generated by a.

Example 21: Prove that a group of order ≤ 5 is Abelian.

Solution: Obviously, a group of order one is Abelian. We know that every group of prime order is cyclic and every cyclic group is Abelian.

$\therefore$ groups of orders 2, 3, 5 are Abelian.

Let us consider group of order 4.

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. Similarly 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

.	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 2.6

$\because a^{-1} = a$ $\therefore aa = e$

Again, each element of G must appear exactly once in every row or column of the operation table.

$\therefore$ 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

$\therefore$ 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.

8.8 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 Δ 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 : 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 Δ 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.

Theorem 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 ia Abelian]

$= Ha$

$\therefore H \Delta G$.

Theorem 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 $H \Delta G$.

$\therefore aH = Ha$, 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]

$\Rightarrow gh = h_1g$, for some $h_1 \in H$

$\Rightarrow ghg^{-1} = h_1 gg^{-1}$

$\Rightarrow ghg^{-1} = h_1 \in H$

i.e. $ghg^{-1} \in H$

Conversely, let $H \leq G$ such that $ghg^{-1} \in H$, for all $g \in G$, $h \in H$.

Let $a \in G$ $\therefore ah \in aH$

$\therefore aha^{-1} \in H$, by the given condition

$\Rightarrow (aha^{-1})a \in Ha$

$\Rightarrow ah(a^{-1}a) \in Ha$

$\Rightarrow ah \in Ha$

$\therefore aH \subseteq Ha$ (1)

Now $ha \in Ha$.

We take $a^{-1} = b$.

$\therefore bhb^{-1} \in H$

$\Rightarrow a^{-1}h(a^{-1})^{-1} \in H$

$\Rightarrow a^{-1}ha \in H$

$\Rightarrow a(a^{-1}ha) \in aH$

$\Rightarrow (aa^{-1}) ha \in aH$

$\Rightarrow ha \in aH$

$\therefore Ha \subseteq aH$ (2)

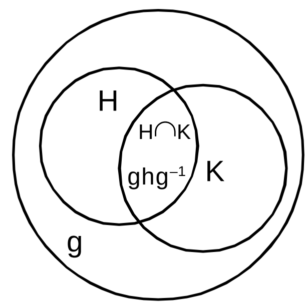
From (1) and (2), $aH = Ha$

$\therefore H \Delta G$.

Theorem 15 : The intersection of any two normal subgroup of a group is again a normal subgroup of the group.

Proof : Let G be a group, an $H \Delta G$, $K \Delta G$.

$\therefore H \leq G$, $K \leq G$ 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 $H \Delta G$

$\therefore ghg^{-1} \in H$

Again $g \in G$, $h \in K$ and $K \Delta G$

$\therefore ghg^{-1} \in K$

Thus, $ghg^{-1} \in H$ and $ghg^{-1} \in K$.

$\therefore ghg^{-1} \in H \cap K$

$\therefore H \cap K \Delta G$.

Note : The union of two normal subgroups is not necessarily a normal subgroup.

8.9 QUOTIENT GROUPS

Let G be a group and H be a normal subgroup 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 collection of all cosets of H in G.

Let $a, b \in G$ $\therefore aH, bH \in G/H$.

We define a binary operation in G/H by the rule $(aH)(bH) = abH$, $ab \in G$.

We show that the binary operation is well defined.

Let $aH = cH$,

$bH = dH$; $a, b, c, d \in H$.

Now $aH = cH \Rightarrow a^{-1}(aH) = a^{-1}(cH)$

$\Rightarrow (a^{-1}a)H = a^{-1}cH$

$\Rightarrow H = a^{-1}cH$

$\Rightarrow a^{-1}c \in H$ [Theorem 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 $(ab)^{-1}(cd) = (b^{-1}a^{-1})(cd)$

$= b^{-1}(a^{-1}c)d$

$= b^{-1}h_1 d$

$= b^{-1}dh_1$ [$\because dH = Hd$]

$= h_2 h_1 \in H$

$\therefore (ab)^{-1}(cd)H = H$

$\Rightarrow abH = cdH$

Thus, $\left.\begin{matrix} aH = cH \\ bH = dH \end{matrix}\right\} \Rightarrow abH = cdH$

$\therefore$ the binary operation defined above is well defined.

Theorem 16 : Let G be a group and H be a normal subgroup 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 $(aH)(bH) = abH$; $a, b \in G$

(ii) Let $a, b, c \in G$

$\therefore aH, bH, cH \in G/H$

Now $((aH)(bH))(cH) = (abH)(cH)$

$= (ab)c\,H$

$= a(bc)H$ [$\because$G is a group, $(ab)c = a(bc)$]

$= (aH)((bc)H)$

$= (aH)((bH)(cH))$

$\therefore$ 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 : This group is known as the quotient group (or factor group) is known as the quotient group (or factor group) of G by H.

Theorem 17 : Every quotient group of an Abelian group is Abelian.

Proof : Let G be an Abelian group, and $H \leq G$.

$\therefore$ 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 $(aH)(bH) = abH$

$= baH$ [$\because$ G ia Abelian, $ab = ba$]

$= (bH)(aH)$

$\therefore$ G/H is Abelian.

Theorem 18 : Every quotient group of a cyclic group is cyclic.

Proof : Let $G = \langle a \rangle$ be a cyclic group.

Let $H \leq G$

$\because$ G is cyclic, $\therefore$ G is Abelian and, therefore, H is normal in G.

So, we can construct the quotient group G/H.

Let $x \in G$, $\therefore$ $xH \in G/H$.

Now $x = a^m$ for some integer m.

Let $m > 0$

Now $xH = a^mH$

$= (a\, a\, a \ldots a)H$

$= (aH)(aH)(aH)\ldots(aH)$

$= (aH)^m$

$\therefore$ G/H is a cyclic group generated by aH.

We can prove the result immediately for $m = 0$ or $m < 0$.

CHECK YOUR PROGRESS 3

Q 1: Can a non-Abelian group be cyclic?

Q 2: Show that a non-Abelian group must contain at least six elements.

Q 3: Let G = {1, ω , ω^2} be the multiplicative group; ω being a complex cube root of unity. Is the group simple?

Q 4: Can a group of order seven be non-Abelian?

Q 5: Let Z be the additive group of integers. The set 3 Z = {0, $\pm$ 3, $\pm$ 6, ...} is a subgroup of Z. Write down the number of elements of the quotient group $Z/3Z$.

8.10 LET US SUM UP

- A binary operation $*$ on a non-empty 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 non-empty set S is commutative if a $*$ b = b $*$ a, $\forall$ a, b$\in$S.
- A binary operation $*$ on a non-empty set S is associative if (a $*$ b) $*$ c = a $*$ (b $*$ c), $\forall$ a, b, c $\in$ S
- An element e in a non-empty set S equipped with a binary operation $*$ is called an identity element for x if a $*$ e = a = e $*$ a, $\forall$ a $\in$ S.
- An element b in a non-empty 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 non-empty set equipped with a binary operation satisfying certain postulates.
- A non-empty subset H of a group G is a subgroup of G if H is also a group under the same binary operation of G.

- If H is a subgroup of a group G, the set $Ha = \{ha : h \in H\}$, $a \in G$, is called a right coset of H in G. Similarly, a left coset is defined.
- 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; $n \in Z$
- A subgroup H of a group G is a normal subgroup of G if $aH = Ha$, for all $a \in G$.
- If G is a group and H is a normal subgroup of G, the set G/H consisting of all the cosets of H in G is a group, called the quotient group (or the factor group).

8.11 ANSWERS TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS – 1

Ans to Q No 1: $4^{4^2} = 4^{16}$

Ans to Q No 2: No.

Ans to Q No 3: Yes

Ans to Q No 4: not commutative, not associative.

CHECK YOUR PROGRESS – 2

Ans to Q No 1: No,Binary operations are different.

Ans to Q No 2: No. Two subgroups of a group have at least one common element, viz., the identity element.

Ans to Q No 3: No.

Ans to Q No 6: $Z = \{0, \pm 1, \pm 2, \pm 3, ...\}$ is an additive group.

$2Z = \{0, \pm 2, \pm 4, \pm 6, ...\}$

and $3Z = \{0, \pm 3, \pm 6, \pm 9, ...\}$

are two subgroups of Z

$Z \neq 2Z \cup 3Z$.

CHECK YOUR PROGRESS – 3

Ans to Q No 1: Every cyclic group is Abelian. Therefore, every non-Abelian group is non-cyclic.

Ans to Q No 3: Yes. It has no normal subgroups other than G, {1}.

Ans to Q No 4: No. Every group of prime order is cyclic and every cyclic group is Abelian.

Ans to Q No 5: Three.

8.12 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

8.13 POSSIBLE QUESTION

Q 1: Let IR be the set of real numbers. Examine if the binary operation $*$ defined by $a * b = a+5b$; $a, b \in$ IR is (i) commutative, (ii) associative.

Q 2: Let S be a set having 3 elements. How many binary operations can be defined on S?

Q 3: 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 group under $*$.

Q 4: Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$, for all $a, b \in G$.

Q 5: Let G be an Abelian group. Prove that the set H = $\{x \in G : x = x^{-1}\}$ is a sub group of G.

Q 6: Show that a group of order 4 is always Abelian.

Q 7: Let g be a group and e be the identity of G. Prove that G is Abelian if $b^{-1}a^{-1}ba = e$, for all a, b $\in$ G.

Q 8: Let G be a group and H be a subgroup of G. Let a, b $\in$ G. Show that the two right cosets Ha, Hb are equal if and only if the two left cosets $a^{-1}H$, $b^{-1}H$ are equal.

Q 9: <u>Index of a subgroup.</u> Let G be a group and H be a subgroup of G. The number of distinct left (or right) cosets of H in G is called the index of H in G. Generally it is denoted by [G : H]

If G is a finite group, show that [G : H] = $\dfrac{o(G)}{o(H)}$.

Q 10: Let G = $\left\{\begin{pmatrix} a & b \\ o & d \end{pmatrix} : a, b, d \in IR \text{ and } ad \neq 0\right\}$

Show that G is a non-Abelian group under matrix multiplication.

Let H = $\left\{\begin{pmatrix} 1 & b \\ o & 1 \end{pmatrix} : b \in IR\right\}$

Show that H is a normal subgroup of G.

Q 11: Show that a group of prime order is simple.

*** ***** ***

UNIT 9: BASIC ALGEBRAIC STRUCTURE -II

UNIT STRUCTURE

9.1 LEARNING OBJECTIVES

After going through this unit you will be able to know

- ring and its properties
- integral domain, field and their properties.

9.2 INTRODUCTION

In Unit 2, we have discussed group and its various properties, sub group, coset, cyclic group, normal sub groups and quotient group. In this unit we will study ring. Group is an algebraic structure, i.e., a non empty set equipped with a binary operation and satisfying certain postulates. Ring is also an algebraic structure, i,e., a non-empty set equipped with two binary operations and satisfying certain postulates.

9.3 RING

A non-empty set R, equipped with two binary operations, called addition (+) and multiplication (·) is called a ring if the following postulates are satisfied.

(1) R is an additive Abelian group,

(2) R is an multiplicative semigroup

(3) 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

Note : 1. In order to be a ring, there must be a non-empty set equipped with two binary operations, viz, + and . , satisfying the postulates 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 . may not be own 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.

4. If a , b $\in$ R, then - b $\in$ R ($\therefore$ R is an additive group). 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 (or identity) if there exists an element e $\in$ R such that

ae = a = ea, for all a $\in$ R.

Note 1. A ring may or may not have a unity.

2. If R is a ring with unity, unity may be same as the zero element. For example, {0} is a commutative ring with unity . Here 0 is the additive as well as the multiplicative identity. It is known as the zero ring.

Theorem 3.1 : 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 identities of R.

ef = e = fe [$\because$ f is unity]

ef = f = fe [$\because$ e is unity]

$\therefore$ e = f

Note: In view of the above theorem, we write ''the unity''.

Example 1. Let R = {$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$: a, b are integers}

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 $\in$ Z

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 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(iv) For every $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in$ R, we have $\begin{pmatrix} -a & -b \\ 0 & 0 \end{pmatrix} \in$ 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 additive 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.

The two distributive laws are satisfied.

$\therefore$ 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 non- commutative ring.

Again, there does not exist any element X $\in$ G such that

$$x\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}x \text{, for all } \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in \text{R}$$

$\therefore$ R is a ring without unity.

Example 2 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 non-commutative ring.

We have I = $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$, and

AI = A = IA, for all A $\in$ R.

$\therefore$ R is a ring with unity.

Example 3: Let 2Z be the set of all even integers

I. 2Z is an Abelian group under usual addition.

II. 2Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ 2Z is a ring under usual addition and multiplication.

Moreover, 2Z is a commutative ring.

2Z is a ring without unity, for 1 $\notin$ 2Z.

Example 4: Let Z be the set of integers.

I. Z is an Abelian group under usual addition.

II. Z is a multiplicative semigroup.

III. The two distributive laws are satisfied.

$\therefore$ Z is a ring under usual addition and scalar multiplication.

Moreover, Z is a commutative ring . It is also a ring with unity, 1 $\in$ Z.

Other examples of commutative rings with unity are

☐ the ring Q of rational numbers

☐ the ring IR of real numbers.

☐ the ring C of complex numbers.

Example 5 Let C [a, b] denote the set of all real-valued continuous functions defined on [a, b] ; a, b $\in$ R

Let f, g $\in$ C [a, b]

We define (f + g) (x)= f (x) + g (x)

(fg) (x) = f (x) g (x), x $\in$ [a, b]

I. (i) We have (f + g) (x) = f(x) + g (x) $\in$ R

Also, the sum of two continuous functions is continuous.

$\therefore$ f + g is continuous and so f + g $\in$ C [a, b]

$\therefore$ addition of functions is a binary operation on C [a, b].

(ii) Let f, g, h $\in$ C [a, b], x $\in$ [a, b]

$$\begin{aligned}((f+g)+h)(x) &= (f+g)(x)+h(x)\\ &= (f(x)+g(x))+h(x)\\ &= f(x)+(g(x)+h(x))\\ &= f(x)+(g+h)(x)\\ &= (f+(g+h))(x), \forall x \in [a,b]\end{aligned}$$

$\therefore$ (f + g) + h = f + (g + h)

(iii) We have 0 : [a, b] $\to$ 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] $\to$ 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)

= (g + f) (x), $\forall$ 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 continous 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)

= f (x) (gh) (x)

= (f (gh)) (x), $\forall x \in [a, b]$

$\therefore$ (fg)h = f (gh)

$\therefore$ 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)

= (f h) (x) + (gh) (x)

= (fh + gh)(x)

$\therefore$ (f + g) h = fh + gh

Similarly f (g + h) = fg + fh

$\therefore$ C [a , b] is a ring under addition and multiplication of functions.

CHECK YOUR PROGRESS - 1

1. Give an example of a commutative ring with unity having only one element.
2. Give an example of a non-commutative ring without unity.
3. Give an example of a commutative ring without unity.
4. Give an example of a non-commutative ring with unity.
5. Give an example of an infinite commutative ring with unity.
6. Let IR^2 = {(a, b) : a, b are reals}

We define

(a, b) + (c, d) = (a + c, b + d),

(a, b) (c, d) = (ac, bd);

a, b, c, d are reals.

Show that IR^2 is a commutative ring with unity.

Theorem 2

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 $a0 = 0$

Similarly $0a = 0$

(ii) We have $a0 = 0$

This $\Rightarrow a((-b) + b) = 0$, $[\therefore (-b) + b = 0]$

$\Rightarrow a(-b) + ab = 0$, by left distributive law

$\Rightarrow a(-b)$ is the additive inverse of ab

$\therefore$ i.e., $a(-b) = -(ab)$

Similarly $(-a)b = -(ab)$

(iii) We have $(-a)(-b) = l(-b)$, taking $l = -a$

$= -(lb)$, 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)

Boolean Ring: Let R be a ring and $a \in R$.

a is called an idempotent element of R if $a^2 = a$.

A ring R is called a Boolean ring, if every element of it is idempotent.

Note: George Boole (1815-1864) of the nineteenth century was ‘‘an essentially self-taught Britisher’’. He is famous for his epoch - making book <u>The Laws of Thought.</u>

Theroem 3: Let R be a Boolean ring. Then

(i) $a + a = 0$, for all $a \in R$

i. e. every element of R is its own additive inverse

(ii) $a + b = 0 \Rightarrow a = b$, for all $a, b \in R$

(iii) R is a commutative ring.

Proof : (i) Let $a \in R$. $\therefore$ $a^2 = a$

Also $a + a \in R$

$\therefore$ $(a + a)^2 = a + a$ [$\therefore$ R is a Boolean ring]

$\Rightarrow$ $(a + a)(a + a) = a + a$

$\Rightarrow$ $(a + a) a + (a + a)a = a + a$, By left distributive law

$\Rightarrow$ $(a^2 + a^2) + (a^2 + a^2) = a + a$, by right distributive law

$\Rightarrow$ $(a + a) + (a + a) = (a + a) + 0$

$\Rightarrow$ $a + a = 0$, by left cancellation law in the additive group R

(ii) We have $a + a = 0$

$\therefore$ $a + b = a + a$, by (i)

$\Rightarrow$ $b = a$, by left cancellation law in the additive group R

i.e. $a = b$

(iii) Let $a, b \in R$ $\therefore$ $a^2 = a, b^2 = b$

Also $a + b \in R$

$\therefore$ $(a + b)^2 = a + b$

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

$\Rightarrow$ $(a + b)a + (a + b)b = a + b$, by left distributive law

$\Rightarrow$ $(a^2 + ba) + (ab + b^2) = a + b$

$\Rightarrow$ $(a + ba) + (ab + b) = a + b$

$\Rightarrow$ $(a + b) + ba + ab = (a + b) + 0$, by associatively and commutative of addition.

$\Rightarrow$ $ba + ab = 0$, by left cancellation law in the additive group R.

$\Rightarrow$ $ab = ba$, by (ii)

$\therefore$ R is a commutative ring.

9.4 INTEGRAL DOMAIN, 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 = O.

Again, let us consider the ring Z of integers. If a, $b \in Z$ 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 divisors whereas the ring Z of integers has no zero divisors, for if $a \in Z$, $b \in Z$, $a \neq 0$, $b \neq 0$, then $ab \neq 0$, $ba \neq 0$.

Concellation 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 multiplication laws (cancellation of non zero 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 4: 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 $a \neq 0$, ab = 0 ,ab = a0 $\Rightarrow$ b = 0, by cancellation law.

Similarly, if $b \neq 0$, ab = 0 $\Rightarrow$ ab = 0b $\Rightarrow$ a = 0.

So there can be no zero divisor.

Conversely, let there be no zero divisors in R.

Let a, b, c $\in$R and ab = ac, a $\neq$0

$\therefore$ ab – ac = 0

a (b – c) = 0

$\therefore$ 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 in the ring Z of integers, It is a commutative ring, has unity and is without zero divisors.

Note: An integral domain may be considered as a generalisation of Z.

Example 6: Let us consider the set R = {a + bi : a, b are integers, $i = \sqrt{-1}$ } of Gaussian integers, after the name of C. F. Gauss (1777-1855).

I. (i) Let a + bi, c + di$\in$R,

a, b, c, d are integers, i = $\sqrt{-1}$

(a + bi) + (c + di) = (a + c) + (b + d)i$\in$R

(ii) Addition of complex numbers is associative.

(iii) We have 0 = 0 + 0i$\in$R

and 0 + (a + bi) = a + bi = (a + bi) + 0

(iv) For every a + bi$\in$ R, we have (–a) + (–b)i $\in$ R such that

(a + bi) + ((–a) + (–b)i) = 0 =((–a) + (–b)i) + (a + bi)

(v) Addition of complex numbers is commutative.

$\therefore$R is an Abelian group under addition of complex numbers.

II. (i) (a + bi) (c + di) = (ac – bd) + (ad + bc)i $\in$R

(ii) Multiplication of complex numbers is associative

$\therefore$R is a semigroup under multiplication of complex numbers.

III. Clearly the two distributive laws hold good.

$\therefore$R is a ring

Furthermore, multiplication of complex numbers is commutative.

$\therefore$ R is a commutative ring.

Also R possesses 1 (1=1 + oi)

$\therefore$ R is a ring with unity.

Again we know that the product of two non-zero complex numbers cannot be zero.

$\therefore$ R is without zero divisors.

Thus, R is an integral domain.

Definition: Let R be a ring with unity e $\neq$ 0. If every non-zero element of R has multiplicative inverse in R, then R is called a Division Ring (or a <u>Skew Field</u>).

A commutative division ring is called a field.

The simplest example of a field is the ring IR of real numbers.

It is commutative, has unity and every non-zero element has multiplicative inverse in IR.

Therefore, IR is a field.

Similarly, the ring C of complex numbers is also a field.

Note: The ring z of integers is not a field. (why?)

Example 7: Examine if the ring

R = {a + bi : a, b, are integers, i = $\sqrt{-1}$ }

of Gaussian integers is a field.

Solution: We know that R is a commutative ring with unity.

(Ref. Example 6)

Let a + bi $\in$ R such that a + bi $\neq$ 0

Now the multiplicative inverse of a + bi is $\frac{a}{a^2+b^2}+\left(-\frac{b}{a^2+b^2}\right)i$ which is not an element of R.

$\therefore$ R is not a field.

Theorem 5: 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

$\therefore$ a $\neq$ 0, $a^{-1} \in$ F (F is a field)

Now ab = 0

$\Rightarrow$ a^{-1} (ab) = a^{-1} 0

$\Rightarrow (a^{-1} a) b = 0$

$\Rightarrow b = 0$

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 and 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 Z of integers. We know that Z is an integral domain. But only two elements, viz, –1 and 1 have multiplicative inverses in Z. $\therefore$ Z is not a field.

However we have the following

Theorem 6: A non-zero finite integral domain is a field.

Proof: Let R = $\{a_1, a_2, a_3, \dots\ a_n\}$ be a finite non-zero integral domain, where all the a_i's are distinct.

Let a_1 be the zero element of R.

Let us consider the non zero elements $a_2, a_3, \dots, a_n$.

Let a_p be not the unity of R ($p \neq 1$)

Let us consider the products

$a_p a_2,\ a_p a_3, \dots,\ a_p a_n$

All these elements belong to R. Also all the elements are distinct, for if

$a_p a_i = a_p a_j$, $2 \leq i \leq n$, $2 \leq j \leq n$, $i \neq j$

then $a_p a_i - a_p a_j = 0$

$\Rightarrow a_p (a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$, [$\because a_p \neq 0$ and R is without zero divisors]

$\Rightarrow a_i = a_j$, which is a contradiction

Now one of $a_p a_2, a_p a_3, \dots, a_p a_n$ 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 non-zero element of R has multiplicative inverse in R.

$\therefore$ R is a field.

Theorem 7: A division ring has no zero divisors.

Proof: Let R be a division ring.

Let a, b $\in$ R such that $a \neq 0$ and ab=0

$\therefore a \neq 0, a^{-1} \in R$ ($\because$ R is a division ring)

Now ab = 0

$\Rightarrow a^{-1} (ab) = a^{-1} 0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow b = 0$

Similarly, if $b \neq 0$ and ab = 0, then a = 0.

$\therefore$ R is without zero divisors

CHECK YOUR PROGRESS - 2

1. Does the ring Q of rational numbers contain zero divisors?
2. Let R be the ring of all 2 x 2 matrices over integers, Does the cancellation laws hold good in R?
3. Is the ring 2Z of even integers an integral domain?
4. Give an example of an integral domain which is not a field.
5. If in a ring R, $a^2 = a$ for all $a \in R$, show that $2a = 0$ and $a + b = 0 \Rightarrow a = b$
6. Does the ring $IR^2 = \{(a, b) : a, b \in IR\}$ contain zero divisions?

9.5 LET US SUM UP

- A non-empty 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

- 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 (or identity) 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 element 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 non-zero 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.
- Every field is an integral domain, but every integral domain is not a field.
- A non-zero finite integral domain is a field.

9.6 ANSWERS TO "CHECK YOUR PROGRESS"

CHECK YOUR PROGRESS-1

1. {0} is a commutative ring with unity. It should be noted that, in this ring, 0 is the additive as well as the multiplicative identity.
2. The ring R = $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right.$: a, b are integers} is a non-commutative ring without unity.
3. The ring 2Z of even integers is a commutative ring without unity.

4. The ring R of all 2 x 2 matrices over integers is a non-commutative ring with unity.

5. The ring Z of integers is an infinite commutative ring with unity.

6. $IR^2 = \{(a, b) : a, b \text{ are reals}\}$

I. (i) Let $(a, b), (c, d) \in IR^2$, where a, b, c, d are reals

Now $(a, b) + (c, d) = (a + c, b + d) \in IR^2$

(ii) Let $(a, b), (c, d), (e, f) \in IR^2$

$$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f)$$
$$= ((a + c) + e, (b + d) + f)$$
$$= (a + (c + e), b + (d + f))$$
$$= (a, b) + (c + e, d + f)$$
$$= (a, b) + ((c, d) + (e, f))$$

$\therefore$ addition is associative.

(iii) We have $(0, 0) \in IR^2$,

and $(0, 0) + (a, b) = (a, b) = (a, b) + (0, 0)$

$\therefore$ (0, 0) is the additive identity.

(iv) For every $(a, b) \in IR^2$, we have $(-a, -b) \in IR^2$ such that $(a, b) + (-a, -b) = (0, 0) = (-a, -b) + (a, b)$

$\therefore$ (–a, – b) is the additive inverse of (a, b).

(v) $(a, b) + (c, d) = (a + c, b + d)$
$$= (c + a, d + b)$$
$$= (c, d) + (a, b)$$

$\therefore$ addition is commutative.

$\therefore IR^2$ is an additive Abelian group.

II. (i) $(a, b)(c, d) = (ac, bd) \in IR^2$

(ii) $((a, b)(c, d))(e, f) = (ac, bd)(e, f)$
$$= ((ac)e, (bd)f)$$
$$= (a(ce), b(df))$$
$$= (a, b)(ce, df)$$
$$= (a, b)((c, d)(e, f))$$

$\therefore$ multiplication is associative.

$\therefore IR^2$ is a multiplicative semigroup.

III. $(a, b)((c, d) + (e, f)) = (a, b)(c + e, d + f)$

$= (a(c+e), b(d+f))$

$= (ac + ae, bd + bf)$

$= (ac, bd) + (ae, bf)$

$= (a, b)(c, d) + (a, b)(e, f)$

Similarly $((a, b) + (c, d))(e, f) = (a, b)(e, f) + (c, d)(e, f)$

$\therefore IR^2$ is a ring

Furthermore, $(a, b)(c, d) = (ac, bd)$

$= (ca, db)$

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

$\therefore$ IR^2 is a commutative ring.

Again, $(1, 1) \in IR^2$, and

$(a, b)(1, 1) = (a1, b1) = (a, b) = (1, 1)(a, b)$

$\therefore (1, 1)$ is the unity.

$\therefore$ IR^2 is a ring with unity.

Thus, IR^2 is a commutative ring with unity

CHECK YOUR PROGRESS - 2

1. No. If $a, b \in Q$ and $a \neq 0, b \neq 0$, then $ab \neq 0$
2. No. Cancellation laws hold good in a ring if and only if it has no zero divisors. The ring of all 2 x 2 matrices over integers contains zero divisors. So cancellation laws do not hold good in the ring of all 2 x 2 matrices over integers.

For example

$$\begin{pmatrix} 1 & 3 \\ 3 & 9 \end{pmatrix}\begin{pmatrix} 3 & 3 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 18 & 24 \\ 54 & 72 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 3 \\ 3 & 9 \end{pmatrix}\begin{pmatrix} 6 & 9 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 18 & 24 \\ 54 & 72 \end{pmatrix}$$

i. e. $\begin{pmatrix} 1 & 3 \\ 3 & 9 \end{pmatrix}\begin{pmatrix} 3 & 3 \\ 5 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 9 \end{pmatrix}\begin{pmatrix} 6 & 9 \\ 4 & 5 \end{pmatrix}$,

i. e. $AB = AC$, but $B \neq C$,

where $A = \begin{pmatrix} 1 & 3 \\ 3 & 9 \end{pmatrix}, B = \begin{pmatrix} 3 & 3 \\ 5 & 7 \end{pmatrix}, C = \begin{pmatrix} 6 & 9 \\ 4 & 5 \end{pmatrix}$

3. The ring 2Z of even integers is not an integral domain, since it does not contain the multiplicative identity.

4. The ring Z of integers is an integral domain, but not a field. Only –1 and 1 have multiplicative inverses in Z,
5. Ref Theorem 3 ((i), (ii))
6. Yes.

   $(7, 0) \in IR^2$, $(0, 13) \in IR^2$ $(7, 0) \neq (0, 0)$, $(0, 13) \neq (0, 0)$.

   But $(7, 0)(0, 13) = (0, 0)$.

9.7 FURTHER READINGS

1) Lanski, Charles : *Concepts in Abstract Algebra*, (First Indian edition, 2010) American Mathematical Society.
2) Vasistha, A. R. : *Modern Algebra (Abstract algebra),* Krishna Prakashan Media (p) Ltd. Meerut-250001 (U. P).
3) Vinberg, E. B. : *A course in Algebra* (First Indian edition, 2009), American Mathematical Society).
4) Vatsa, B. S. and Vatsa, Suchi : *Modern Algebra*, New Age International (p) Ltd., New Delhi-110002.
5) Sen, M. K, Ghosh, Shamik and Mukhopadhyay, Parthasarthi : *Topics in Abstract Algebra,* Universities Press (India) Pvt. Ltd., Hyderabad, 500029.

9.8 PROBABLE QUESTIONS

Q 1: Let Z be the set of integers, We define (+) and (·) on Z as follows

$a (+) b = a + b - 1$,

$a (\cdot) b = a + b - ab$, for all $a, b \in Z$

Examine Z is a commutative ring with unity under (+), (·).

Q 2: Let R = {(a, b) : a, b are reals}. We define

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

$(a, b)(c, d) = (ac - bd. bc + ad)$

Prove that R is a field.

Q 3: Let R = $\{a + b\sqrt{2}$: a, b are rational numbers$\}$. show that R is a field under usual addition and multiplication.

Q 4: Prove that a ring R is commutative if and only if

$(a + b)^2 = a^2 + 2ab + b^2$, for all $a, b \in R$

[Here a^2 means aa]

Q 5: Let R be a commutative ring with unity and is without zero divisors. Show that the only idempotent elements are the zero element and the unity element.

*** ***** ***

UNIT 10 : GRAPH THEORY

UNIT STRUCTURE

10.1 LEARNING OBJECTIVES

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

- definition of different types of graphs
- graph representation in computer memory
- graph traversing technique
- trees and its different properties
- hamiltonian and Eulerian graph

10.2 INTRODUCTION

Graph theory has a wide range of applications in physical science and all Engineering branches. It also has uses in social sciences, chemical sciences, information retrieval systems, linguistics even in economics also. Graph are discrete structures consisting of vertices and edges that connects these vertices. There are several different types of graphs that differ with respect to the kind and number of edges that can a connect a pair of vertices. Problems in almost every conceivable discipline can be solved using graph models.

10.3 BASIC TERMINOLOGY

A graph G = (V,E) is a pair of sets, where V = {v_1, v_2 ... ...} is a set of vertices and E = {e_1, e_2 ... ...} is a set of edges connecting pair of vertices.

In other words, in a graph there is a mapping from the set of edges E to the set of vertices V such that each $e \in E$ is associated with ordered or unordered pair of elements of V. The most common representation of a graph is by means of a diagram in which the vertices are represented as points and each edge as a line segment joining its end vertices. Fig. 10.1 provides an example of a graph with vertices V = {v_1, v_2, v_3, v_4, v_5, v_6} and edges E = {e_1, e_2, e_3, e_4, e_5, e_6, e_7}

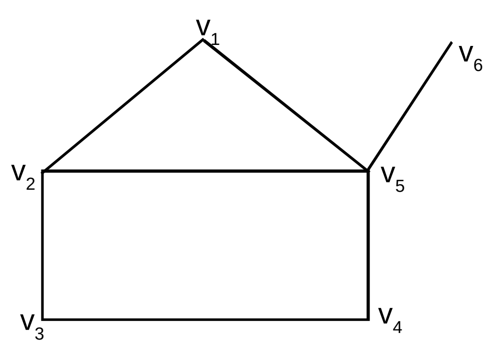


fig. 10.1

A graph is said to be an undirected graph if edges are unordered pairs of distinct vertices. Fig. 10.1 is an example of undirected graph. In an undirected graph we can refer to an arc joining the vertex pair u and v as either (u, v) or (v, u).

A graph is said to be the directed graph or digraph if the edges are ordered pairs of vertices. In this case an edge (u, v) is said to be from u to v and to join u to v.

Fig. 10.2 provides an example of a directed graph on

V = {v_1, v_2, v_3, v_4, v_5} with

E = (v_1, v_2), (v_2, v_3), (v_3, v_4), (v_5, v_4), (v_3, v_5), (v_2, v_5), (v_1, v_5)

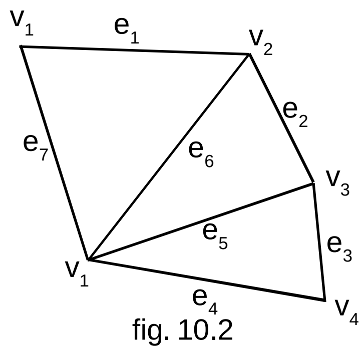


fig. 10.2

The direction of an edge is shown by placing a directed arrow on the edge.

Degree of a vertex : The degree of a vertex v in a graph G, denoted by d (v) or deg (v) is the number of edges incident with v.

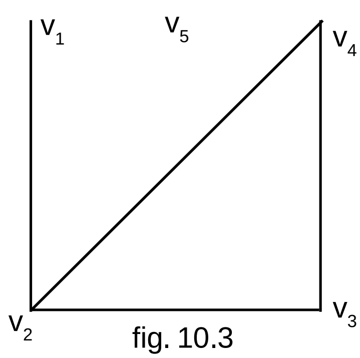


fig. 10.3

For example the graph in fig. 10.3 we have $d(v_1) = 1$, $d(v_2) = 3$, $d(v_3) = 2$, $d(v_4) = 2$, $d(v_5) = 0$

Indegree : The indegree of a vertex v a directed graph is the number of edges ending at it and is denoted by indeg (v)

In fig. 10.2 the indegree of various vertices are as follows :

vertex :	v_1	v_2	v_3	v_4	v_5
indegree :	0	1	1	2	3

Outdegree : The outdegree of a vertex v in a directed graph is the number of edges begining from it and is denoted by outdeg (v).

In fig. 10.2 the outdegree of various vertices are as follows :

vertex :	v_1	v_2	v_3	v_4	v_5
indegree :	2	2	2	0	1

Pendant vertex, isolated vertex : A vertex of degree one is called a pendant vertex. In fig. 10.3 v_1 is a pendant vertex. Again a vertex of degree zero or having no incident edges is called an isolated vertex. In fig. 10.3 v_5 is an isolated vertex.

Loop paralled edges, simple graph,multigraph : A loop is on edge from a vertex to itself. i,e a loop is an edge between a vertex. A loop contributes 2 to the degree of a vertex. In fig. 10.4 edge e_2 from vertex v_2 forms a loop.

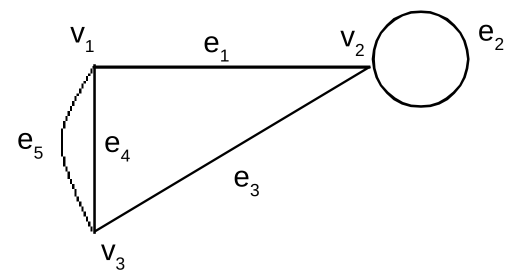


fig. 10.4

If there is more than one edge between a pair of vertices in a graph, then these edges are called paralled edges. In fig. 10.4 e_4 and e_5 are called paralled edges.

A graph with no loops and parallel edges is called a simple graph. The graph is fig. 10.3 is a simple graph.

Again a graph with loops and paralled edges is called a multigraph. The graph in fig. 10.4 is a multigraph.

Theorem 10.1 : Prove that the sum of the degrees of the vertices in a graph G is equal to twice the number of edges in G. i.e. for a graph G with n vertices and edges, then $\sum_{i=1}^{n} d(vi) = 2e$

Proof : Let G be a graph with n vertices and e edges. Since each degree contributes a count one to the degree of each of the two vertices on which the edge is incident i.e. every edge contributes degree 2 to the sum

$$\therefore \sum_{i=1}^{n} d(vi) = 2e$$

Even and odd vertices : A vertex is said to be an even or odd vertices according as its degree is an even or odd number. In fig. 10.3, v_3, v_4 are even vertices and v_1, v_2 are odd vertices.

Theorem 10.2 : Prove that the number of vertices of odd degree in a graph is always even.

Proof : We have that for a graph G of n vertices and e edges, the sum of degrees of all vertices is twice the number of edges i,e

$$\sum_{i=1}^{n} d(vi) = 2e \quad \text{... ... ... (10.1)}$$

Among all n vertices, some are even vertices and some are odd vertices.

$$\therefore \sum_{i=1}^{n} d(v_i) = \sum_{even} d(v_j) + \sum_{odd} d(v_k) \quad \text{... ... ... (10.2)}$$

From (1) and (2), we have

$$\sum_{even} d(v_j) + \sum_{odd} d(v_k) = 2e$$

$$\Rightarrow \sum_{odd} d(v_k) = 2e - \sum_{odd} d(v_j) \quad \text{... ... ... (10.3)}$$

Since every term in the R.H.S of equation (10.3) is even, then the sum on the left side must contain an even number of terms.

Hence, the number of odd vertices in a graph is even.

Remark : In fig. 10.3

i) Sum of degree of all vertices $= d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5)$

$= 1+ 3 + 2 + 2 + 0$

$= 8$, which seven

and equal to twice number of edges.

ii) The number of vertices of odd degrees are v_1 and v_2 which is even.

Adjacent vertices : Two vertices are said to be adjacent if they are connected by an edge if there is an edge e = (u, v) connecting vertices u and v, then u and v are called adjacent to each other.

Example 1 : Consider the graph as shown in the fig. 11.5 Determine

a) pendent vertices

b) odd vertices

c)even vertices

d) adjacent vartices

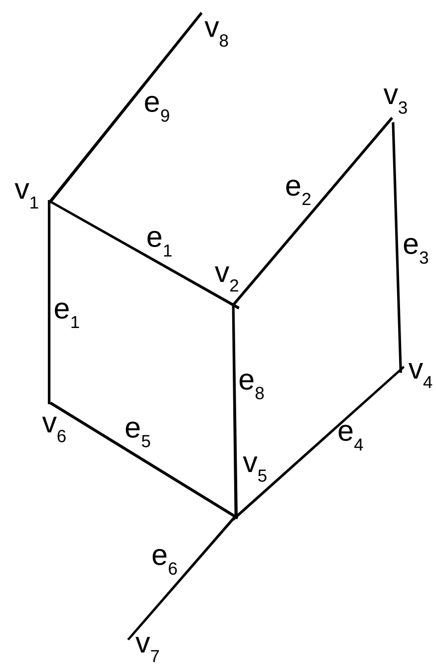


fig. 10.5

Solution :

a) Since vertex v_7 and v_8 is of degree one therefore v_7 and v_8 are pendent vertices

b) Vertices having odd degree are v_1, and v_2. These two vertices are odd vertices.

c) Vertices having even degrees are v_3, v_4, v_5 and v_6. These vertices are even vertices.

d) Vertex v_1 is adjacent to v_2, v_6 and v_8

Vertex v_2 is adjacent to v_1, v_3 and v_5

Vertex v_3 is adjacent to v_2 and v_4

Vertex v_4 is adjacent to v_3 and v_5

Vertex v_5 is adjacent to v_2, v_4, v_6 and v_7

Vertex v_6 is adjacent to v_1 and v_5

Vertex v_7 is adjacent to v_5

Vertex v_8 is adjacent to v_1

10.4 SOME SPECIAL SIMPLE GRAPHS

Few important types of simple graphs are discusssed here which are frequently used in graph theory.

Complete graph : A simple graph is in which there exists an edge between every pair of vertices is called a complete graph. A complete graph on n vertices may be denoted by the symbol k_n. since every vertex is joined with every other vertex through one edge. The degree of every vertex is n–1 in a complete graph of n vertices. Also, a complete graph on n vertices has ${}^nc_2 = \frac{n(n-1)}{2}$ edges. The graphs k_n, for n = 1, 2, 3, 4, 5, 6 are displayed in fig. 10.7

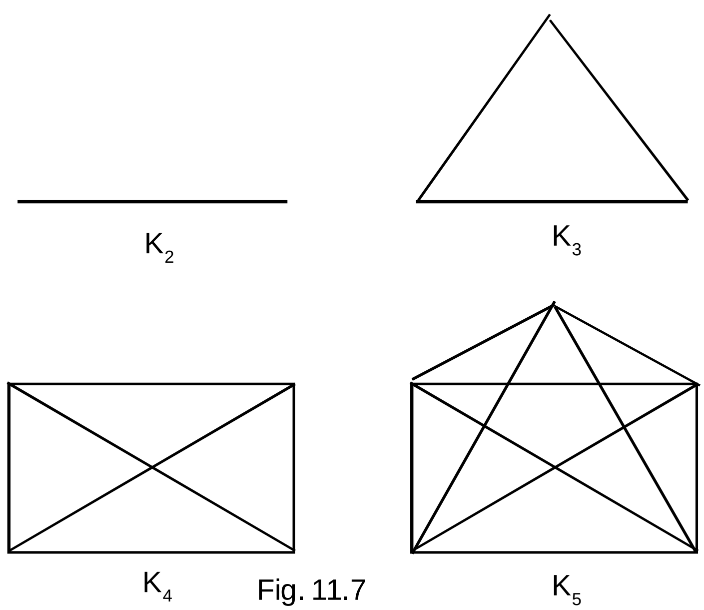


Fig. 11.7

Regular Graph : A graph in which every vertex has the same degree is called a regular graph. If every vertex has degree K, then the graph is called a k-regular or regular graph of degree K.

Note :

i) A graph is called a rull graph is every vertex in the graph is an isolated vertex i.e every rull graph is regular of degree zero.

ii) A complete graph k_n is regular of degree n–1

iii) If a graph has n vertices and is regular of degree k, then it has $\frac{kn}{2}$ edges.

Complementary graph : The complementary graph $\overline{G}$ of a simple graph G has the same vertices as G. Two vertices are adjacent in G. That is vertices which are adjacent in G are not adjacent in $\overline{G}$ and vice versa. If G is a loop free undirected graph with n-vertices and if G= k_n, then $\overline{G}$ is a graph consisting of n vertices and no edges. Fig. 10.8(a) shows an undirected graph with 6 vertices. Its complement is shown in fig. 10.8(b)

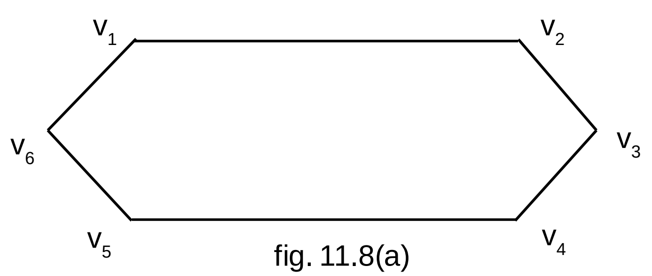


fig. 11.8(a)

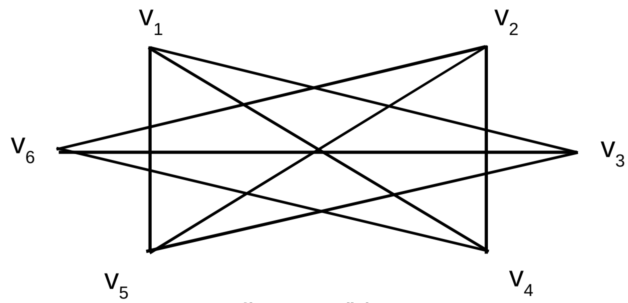


fig. 11.8(b)

Bipartite graph : A simple graph is called bipartite if its vertex set V can be partitioned into two disjoint sets v_1 and v_2 such that every edge in the graph connects a vertex in v_1 and a vertex in v_2. In other words a graph G is called bipartite graph when $V = v_1 U v_2$ and $v_1 \cap v_2 = \phi$ and every edge of G is of the form (v_i, v_j) with $v_i \in v_1$ and $v_j \in v_2$

A complete bipartite graph is a bipartite graph in which every vertex of v_1 is adjacen to every vertex of v_2. If number of vertices in v_1 are m and number of vertices in v_2 are n, then the complete bipartite graph is denoted by Km,n. A complete bipartite graph km, n has m + n vertices and mn edges. The complete bipartite graph $k_{3.3}$ and $k_{3,4}$ are displayed in fig. 10.9

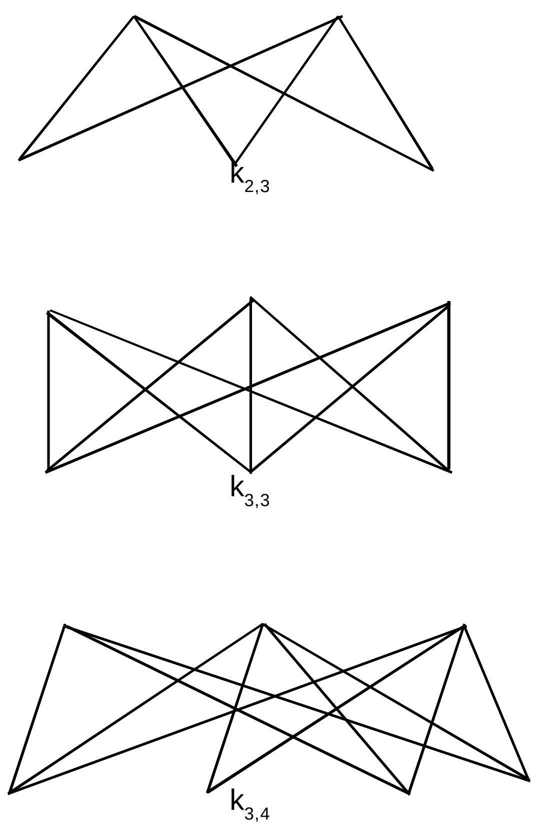


fig. 10.9

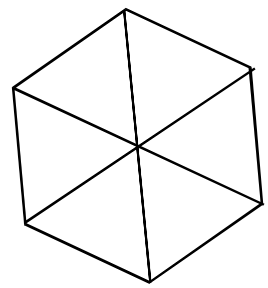
Example 3 : Draw the following graphs

1) 3-regular but not complete

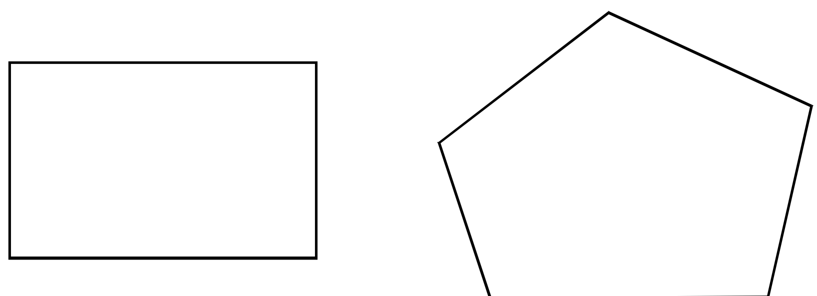
2) 2-regular but not complete

3) A complete bipartite graph having 2 vertices in one partite set and 4 vertices in the other partite set.

Solution : 1) The required graph of 3-regular but not complete is shown in fig.



2) The required graph of 2-regular but not complete is shown in fig.



3) A complete bipartite graph having 2 vertices in one partite set and 4 vertices in other partite set is shown in fig

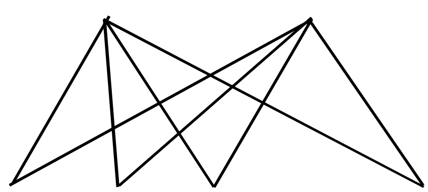


fig. 10.10

Example 4 :

a) Find the number of edges in the graph K_{12}

b) Find the number of vertices of a complete graph of 105 edges.

Solution :

a) We have that the number of edges in a complete graph K_n is ${}^{n}c_2$ = $\frac{n(n-1)}{2}$ edges

$\therefore$ Number of edges in K_{12} = $\frac{12(12-1)}{2}$

= 66

b) Let the number of vertices be n.

$\therefore$ number of edges in k_n = $\frac{n(n-1)}{2}$

$\Rightarrow$ 105 = $\frac{n(n-1)}{2}$

$\Rightarrow$ n(n-1) = 210

$\Rightarrow$ n^2–n–210 = 0

$\Rightarrow$ n^2–15n + 14n–210 = 0

$\Rightarrow$ n(n–15) + 14 (n–15) = 0

$\Rightarrow$ (n–15) (n + 14) = 0

$\Rightarrow$ n = 15, –14

Since $n \neq -14$. so, number of vertices of the complete graph with 105 edges be 15

Example 5 : Can you construct a regular graph of degree 3 with nine vertices.

Solution : Since, in a regular graph every vertex has the same degree, so the total number of degrees of the regular graph of degrees 3 with nine vertices = 3×9 = 27

Again, we know that in a graph G

$\sum d(v_i) = 2e$, when e is the number of edges

$\Rightarrow$ 27 = 2e

$\Rightarrow$ $e = \frac{27}{2}$, which is not possible.

Hence, we can not construct a regular graph of degree 3 with nine vertices.

Remark : The maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$, when it is graph is complete

CHECK YOUR PROGRESS - 1

1. What is a simple graph?
2. Define degree of a vertex.
3. Define pendant and isolated vertex.
4. When a vertex is said to be an even or odd?
5. What do you mean by complete graph and regular graph.

10.5 REPRESENTATION OF GRAPHS AND GRAPH ISOMORPHISM

There are many useful ways to represent graphs. A matrix is a convenient and wueful way of representing a graph to a computer. The following representation are most commonly used to represent a graph in computer memory.

1. Adjacency matrix (vertex-vertex adjacency matrix)

2. Incidence matrix (vertex-edge incidence matrix)

1. **Adjacency matrix :** Suppose that G = (V,E) is a simple undirected graph with n vertices. Suppose that the vertices of G are listed arbitrarily as $v_1, v_2, \dots \dots \dots, v_n$. The adjacency matrix denoted by A(G) of G with respect to this listing of the vertices is a n X n matrix (a_{ij}) defined as :

$$[a_{is}] = \begin{cases} 1, \text{ if vertex } v_i \text{ is adjacent to vertex } v_j. \text{ i.e. there is an edge} \\ \quad \text{between } v_i \text{ and } v_j \\ 0 \text{ , otherwise.} \end{cases}$$

The adjacency matrix A(G) for the graph consisting 5 vertices, shown in fig. 11.14

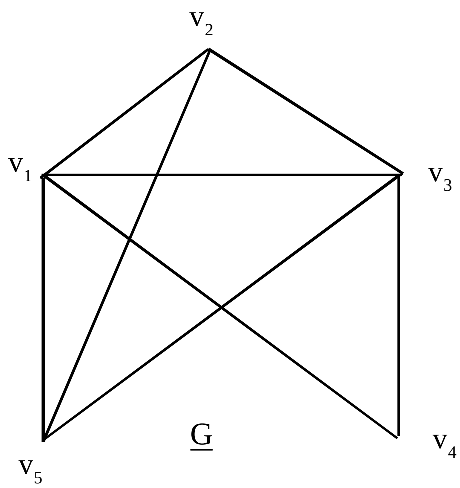


fig. 10.11

λ

$$A(G) = \begin{array}{c|ccccc} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \hline v_1 & 0 & 1 & 1 & 1 & 1 \\ v_2 & 1 & 0 & 1 & 0 & 1 \\ v_3 & 1 & 1 & 0 & 1 & 1 \\ v_4 & 1 & 0 & 1 & 0 & 0 \\ v_5 & 1 & 1 & 1 & 0 & 0 \end{array}$$

Since an adjacency matrix of a graph is based on the ordering chosen for the vertices. Hence, there are as many as n! different adjacency matrices for a graph with n vertices. because there are n! different orderings of n vertices.

Following observations can be made about the adjacency matrix A(G) of a graph G are

a) The entries along the principal diagonal of A(G) are all o's if and only if the graph has no self loops.

b) The adjacency matrix A(G) = [aij] is symmetric. i,e aij = aji, for all i,j

c) A graph G is connected graph if and only if the matrix B = A(G) + $[a(G)]^2 + ... + [A(G)]^{n-1}$ has no zero entries of the main diagonal, where A(G) is the adjacency matrix of G with n vertices.

d) The number of non-zero elements in the adjacency matrix of a graph is equal to the sum of degress of all vertices of the graph.

Adjacency matrices can also be used to represent directed graph. For a divected graph G consists of n vertices, an nxn adjacency matrix A(G) = $[a_{ij}]$ is defined as :

a_{ij} = 1. if edges begining at vertex v_i and ending at v_j

2. otherwise

The adjacency matrix A(G) of the directed graph G in fig. 10.12 is shown bellow.

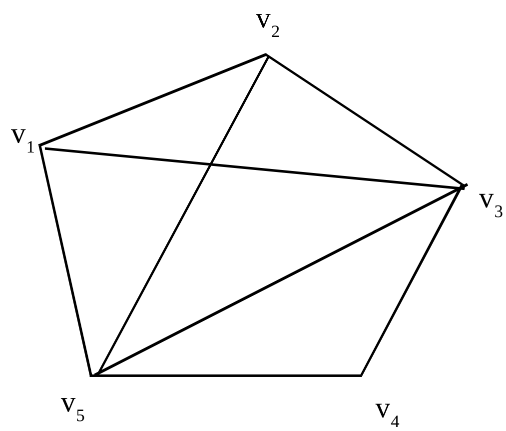


fig. 10.12

$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \left[\begin{array}{ccccc} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{array}\right] \end{array}$$

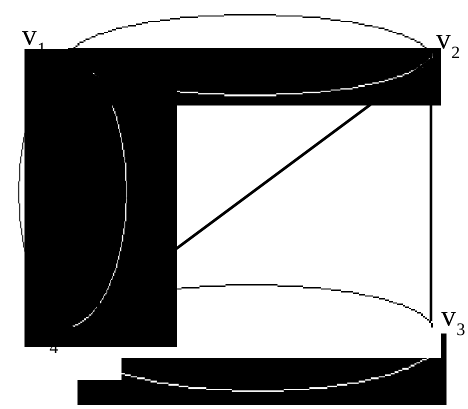
A(G)

Note : The non-zero elements in the adjacency matrix is equal to the number of edges in the directed graph.

When the graph G is a multi-graph i,e an undirected graph with loops and multiple (perallel) edges, then it can also be represented by an adjacency matrix. A loop at the vertex v_i is represented by a 1 at the (i,i)th position of the adjacency matrix. When multiple edges are present, then the value of the (i, j)th entry of the adjacency matrix equals to the number of edges that are associated to (v_i, v_j). i.e.

$$a_{ij} = \begin{cases} m. & \text{if there are one or more edges between vertex } v_i \\ & \text{and } v_j;\ m = \text{number of edges} \\ 0. & \text{otherwise} \end{cases}$$

The adjacency matrix A(G) to represent the multigraph show in fig. 10.13 is given bellow.



G

fig. 10.13

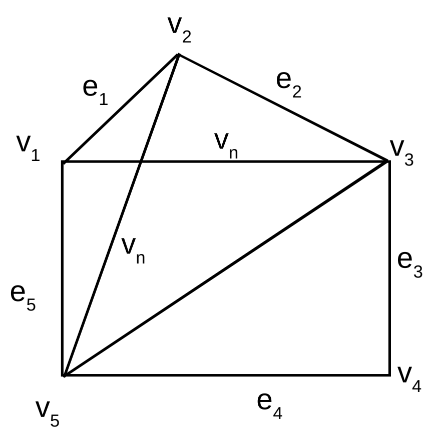
$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \left|\begin{array}{cccc} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 0 & 1 & 0 \end{array}\right| \end{array}$$

2) **Incidence matrix :** Let G = (v, E) be an undirected simple graph. Suppose that $v_1, v_2, \ldots \ldots \ldots, v_n$ are n vertices and $e_1, e_2, \ldots \ldots \ldots, e_m$ are m edges of G. Then incidence matrix of G denoted by I (G) is an n×m matrix

[mij] defined by

$$I(G) = [m_{ij}]$$
$$= 1 \quad \text{if vertex } v_i \text{ is incident with } e,i$$
$$0 \quad \text{otherwise}$$

The incidence matrix I(G) for the graph in fig 10.14 is shown bellow.



G

fig. 10.14

$$\begin{array}{c|ccccccc|}
 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\
v_1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
v_2 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
v_3 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
v_4 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
v_5 & 0 & 0 & 0 & 1 & 1 & 1 & 0
\end{array}$$

I(G)

The following observations can be made about the incidence matrix I(G) of the graph

a) Each column of the matrix contains exactly two unit elements.

b) The number of unit elements in row i represents the degree of the vertex v_i

c) A row with a single unit element corresponds to a pendant vertex.

d) A row with all zero elements corresponds to an isolated vertex.

Again for a directed graph G consisting of n vertices an m edges, an n×m incidence matrix

$I(G) = [M_{ij}]$ is defined as

$$M_{ij} = \begin{cases} 1, & \text{if } v_i \text{ is initial vertex of edge } e_j \\ -1, & \text{if } v_i \text{ is end vertex of edge } e_j \\ 0, & \text{if } v_i \text{ is not incident on } e_j \end{cases}$$

The following 5×7 incidence matrix representation for the directed graph in fig. 10.15

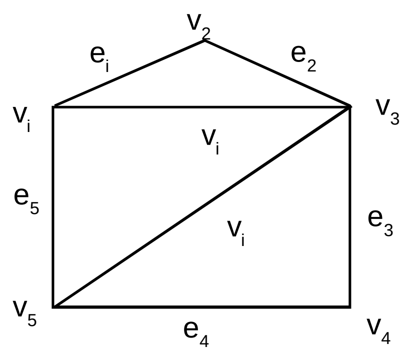
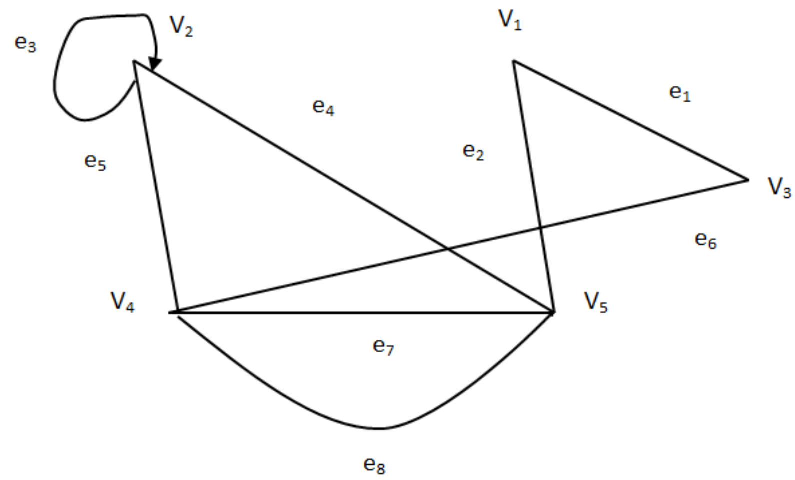


fig. 10.15

$$\begin{array}{c|ccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ \hline v_1 & 1 & 0 & 0 & 0 & -1 & 0 & 1 \\ v_2 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ v_3 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \\ v_4 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ v_5 & 0 & 0 & 0 & 1 & 1 & -1 & 0 \end{array}$$

I(G)

Example 6 : Find the adjacency matrix and incidence matrix of the multigraph G shown in fig. 10.16



(G)

fig. 10.16

Solution : The adjacency matri for the graph G is

$$A(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{ccccc} v_1 & v_2 & v_3 & v_4 & v_5 \end{array} \\ \left|\begin{array}{ccccc} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{array}\right| \end{array}$$

A(G)

Again the incidence matrix for the given graph G is

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \left|\begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right| \end{array}$$

I(G)

Example : Is the graph G, with the following adjacency matrix, a connected graph?

$$A(G) = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Sojution : Here number of vertices = 5

Let B = A(G) + $[A(G)^2 + \{A(G)]^3 + [A(G)]^4$

$$\text{Now, } [A(G)]^2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 3 & 2 & 2 & 3 \\ 4 & 4 & 2 & 2 & 3 \\ 4 & 3 & 3 & 3 & 2 \\ 3 & 2 & 2 & 3 & 1 \\ 3 & 3 & 1 & 1 & 3 \end{bmatrix}$$

$$[A(G)]^2 = \begin{bmatrix} 4 & 3 & 2 & 2 & 3 \\ 4 & 4 & 2 & 2 & 3 \\ 4 & 3 & 3 & 3 & 2 \\ 3 & 2 & 2 & 3 & 1 \\ 3 & 3 & 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 12 & 7 & 8 & 10 \\ 15 & 13 & 8 & 8 & 11 \\ 15 & 12 & 9 & 10 & 9 \\ 11 & 8 & 7 & 8 & 6 \\ 11 & 10 & 5 & 5 & 9 \end{bmatrix}$$

$[A(G)]^4 = [A(G)]^3 . A(G)$

$$= \begin{bmatrix} 51 & 43 & 27 & 29 & 26 \\ 55 & 47 & 29 & 31 & 39 \\ 55 & 45 & 31 & 34 & 36 \\ 40 & 32 & 23 & 26 & 25 \\ 40 & 35 & 20 & 21 & 30 \end{bmatrix}$$

Now $B = A(G) + [A(G)]^2 + [A(G)]^3 + [A(G)]^4$

$$= \begin{bmatrix} 70 & 59 & 36 & 40 & 50 \\ 75 & 65 & 40 & 41 & 54 \\ 75 & 61 & 44 & 48 & 47 \\ 55 & 42 & 33 & 38 & 32 \\ 55 & 49 & 26 & 27 & 43 \end{bmatrix}$$

Since B has no zero entry on the main diagonal.

$\therefore$ The given graph is connected.

Isomorphism of graphs : Two graphs are said to be isomorphic it they have identical behaviour in terms of graph-theoretic properties. More precisely :

Let $G_1 (V_1, E_1)$ and $G_2 (V_2, E_2)$ be two simple undirected graphs. A function $f: V_1 \rightarrow V_2$ is called a graph isomorphism if

i) f is one-one and onto, i.e there exists a one-to-one correspondance between their vertices as well as edges (both the graphs have equal number of vertices and edges, however, vertices may have different levels.)

ii) for all $u,v \in V_1$, $\{u,v\} \in E_1$ if and only if $\{f(u), f(v)\} \in E_2$

If such a function exists, then the graphs G_1 and G_2 are called isomorphic graphs.

For example, we can verify that the graph G and H in fig 11.20 are isomorphic

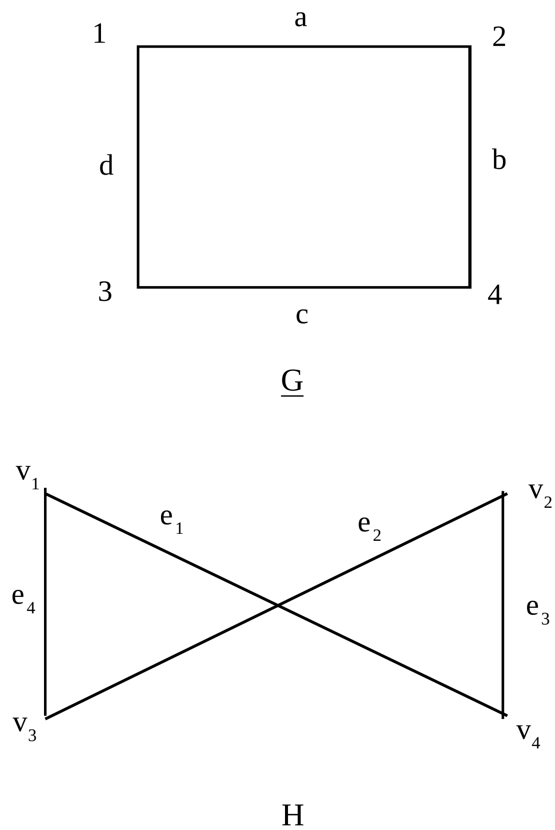


fig. 10.17

The correspondance between the two graphs is as follows : The vertices 1, 2, 3 and 4 in G is corresponds to v_1, v_4, v_3 and v_2 respectively in H. The edges a, b, c, d in G corresponds to e_1, e_3, e_2, e_4 respectively.

Note : i) Two isomorphic graphs have equal number of vertices and edges.

ii) Two isomorphic graphs have equal number of vertices with same degree.

Example 8 : Show that the graph displayed in fg 10.18 are not isomorphic

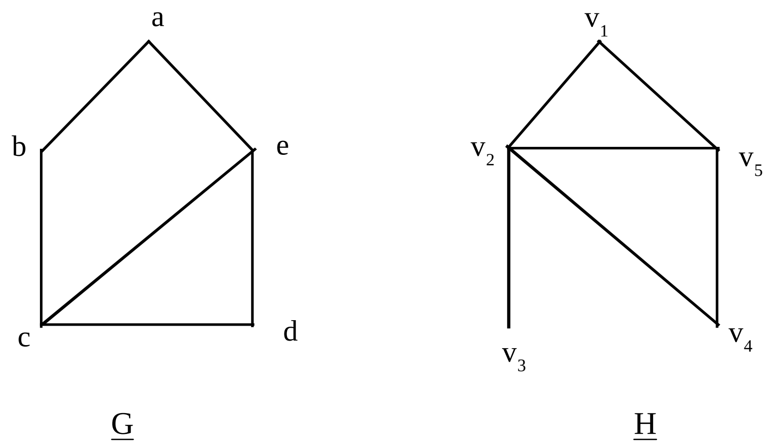


fig. 10.19

Solution : The graph G and H both have five vertices and six edges. However the graph H has a vertex of degree one namely v_3. Where as G has no vertices of egree one. Hence G and H are not isomorphic.

Example : Show that the simple graphs with the following adjacency matrices are isomorphic.

$$, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Solution : Since the given adjacency matrices are of order three each, so its graph has three vertices namely v_1, v_2, v_3 and u_1, u_2, u_3 respectivety.

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \end{array} \qquad \begin{array}{c} \\ u_1 \\ u_2 \\ u_3 \end{array} \begin{array}{c} \begin{array}{ccc} u_1 & u_2 & u_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Their corresponding graphs are shown in fig. 10.20

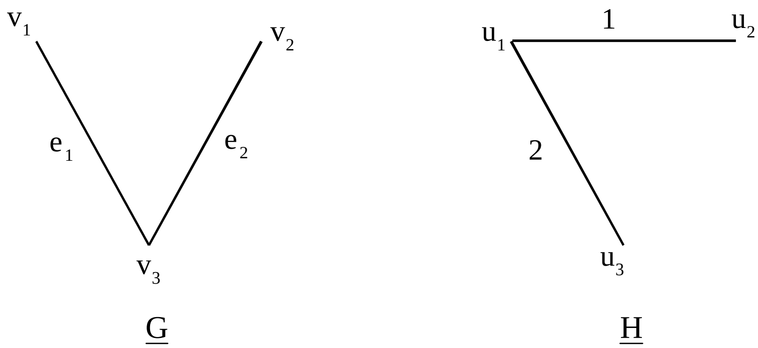


fig. 10.20

There is a one-to-one correspondance between the vertices and edges of the graph G and H. Both the graph has there vertices and 3 edges each. Two vertices of the graph G has degree one and one vertex has degree two. Again two veftces of the graph H has degree one and one vertex has degree two. The vertices v_1, v_2 and v_3 in G corresponds to u_2, u_3 and u_1 in H respectively. The edges e_1 and e_2 in G corresponds to 1 and 2 in H respectively.

Hence both the graph are isomorphic.

10.6 CONNECTIVITY OF A GRAPH

Walk : A walk is defined as a finite alternating requence of vertices and edges, begining and ending with vertices, such that each edge is incident with the vertices preceding and following it. Let u, v be any two vertices in an undirected graph G. Then a walk u-v in G is finite alternating sequence u-v_1 e_1 v_2 e_2 ... ... e_n v_n = V of vertices and edges.

Vertices with which a walk begins and ends are called ternimal vertices.

Open and colsed walk : A walk is said to be closed walk if it is possible that a walk begins and end at the same vertex.

A walk that is not closed is called an open walk.

Path : An open walk in which no vertex appears more than once is called a path. The number of edges in a path is called the length of the path. An edge which is not a loop is s path of length one. A loop can be included in a walk but not in a path.

Circuits : A circuit is a closed walk of non-zero length that contains no repeated edges except the initial and end vertex where intial and end vertex. That is, a circuit is a closed, nontersecting walk. A circuit is also called elementary cycle, circular path and polygon.

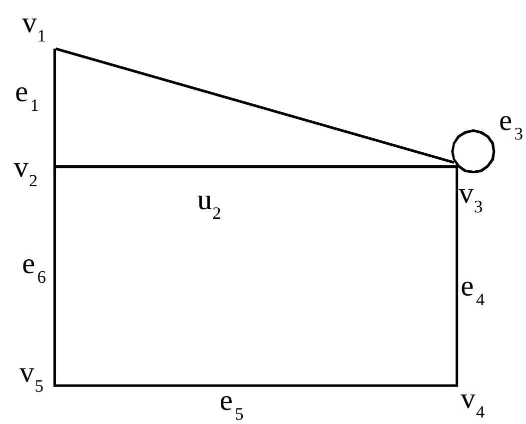


fig. 10.21

In figure 11.23, examples of walk, path and circuits are given bellow.

Walk : v_1 e_1 v_2 e_2 v_3 e_3 v_3 e_4 v_4 etc

Path : v_1 e_1 v_2 e_2 v_3 e_4 v_4 etc

Circuit : v_2 e_1 v_3 e_4 v_9 e_5 v_5 e_6 v_2 etc

Connected graphs : A graph is said to be connected if we can reach any vertex from any other vertex by traveling along th edges. More formally : A graph is said to be connected if there exists at least one path between every pair of its vertices, otherwise, the graph is disconnected. That is a graph G is connected if give any vertices u and v, it is possible to travel from u to v along a sequence of adjacent edges fig. 10.21 is connected graph but in fig. 10.21 is a disconnected graph.

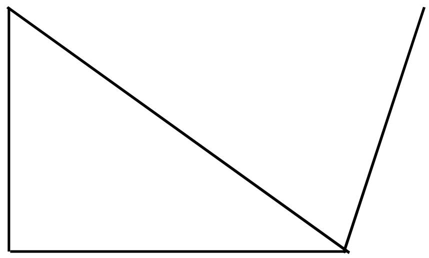


fig. 10.22

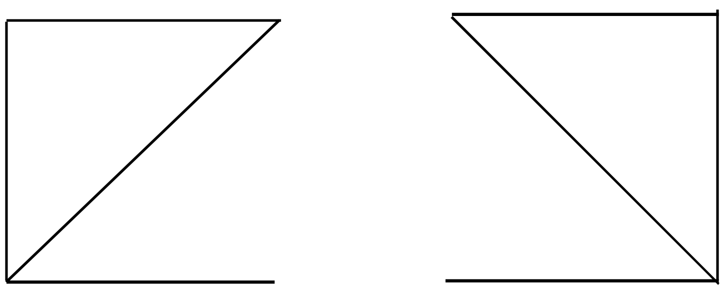


fig. 10.23

A disconnected graph consists of two or more connected graphs. Each of these connected subgroups is called a component. fig.11.25 is a disconnected graph with two components.

Cut points and Bridges : Vertex v in a connected graph G is called a cutpoint if G-v is disconnected, where G-v is the graph obtained from G by deleting the vertex v and all the edges connecting v. In fig. 11.26(a), vertex v_4 is the cutpoint

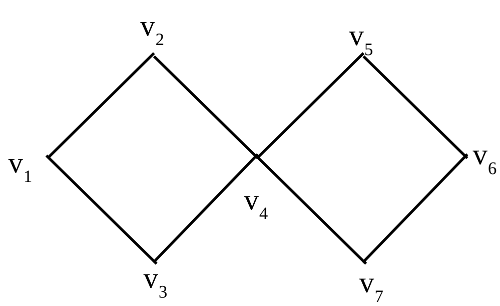


fig. 10.24(a)

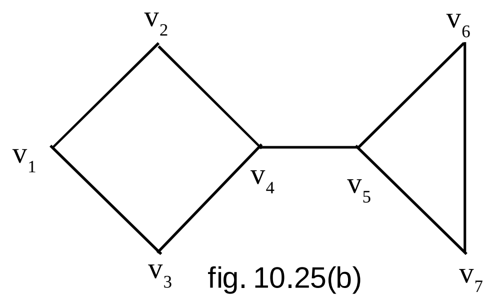


fig. 10.25(b)

An edge e of a connected graph G is called a bridge or cut edge if G-e is disconnected. In fig. 11.25(b), the edge (v_4, v_5) is a bridge.

Theorem 11.3 : A simple graph G with n vertices and k components can have at most $\frac{1}{2}$ (n–k) (n–k+1) edges.

Solution : Let the number of vertices in each of the K components of a graph G be $n_1, n_2, \ldots \ldots \ldots n_k$. Then the sum of all vertices in each k components must be equal to the number of vertices in G. i.e

$$n_1 + n_2 + \ldots \ldots \ldots n_k = n$$

$$\Rightarrow \sum_{i=1}^{k} n_i = n$$

Any component with n_i vertices ($1 \leq i \leq k$) will have maximum possible number of edges = $\frac{1}{2} n_i (n_i - 1)$, when it is complete.

Hence the maximum number of edges in G are

$$\Rightarrow \frac{1}{2}\sum_{i=1}^{k} n_i (n_i - 1)$$

$$= \frac{1}{2}\sum_{i=1}^{k} n_i^2 - \frac{1}{2}\sum_{i=1}^{k} n_i$$

$$\leq \frac{1}{2}\left[n^2 - (k-1)(2n-k)\right] - \frac{1}{2} n$$

$$= \frac{1}{2}\left[n^2 - 2nk + k^2 + n - k\right]$$

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

Connectivity of a graph :

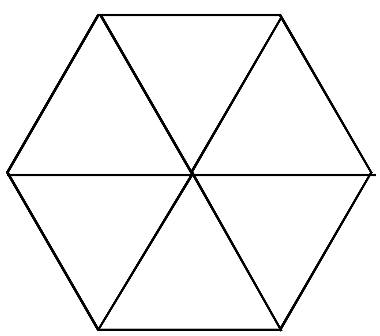
Edge connectivity : Each cut-set of a connected graph G consists of a certain number of edges. The number of edges in the smallest cut-set (i,e cut-set with fewest number of edges) is defined as the edge connectivity of G.

Equivaluntly the edge connectivity λ (G) of a connected graph can be defined as the minimum number of edges whose removal reduces the graph disconnected. If G is a tree, then λ (G) = 1, became removel of any one edges reduces the the tree disconnected.

λ (G)=2

fig. 10.26

Vertex connectivity : The vertex connectivity K(G) of a connected graph G is defined as the minimum number of vertices whose removal from G leaves the graph disconnected. If G is a tree then K(G) = 1



K(G) = 3

fig. 10.27

10.7 EULERIAN AND HAMILTONIAN GRAPH

Eulerian graph :

A undirected graph with no isolated vertices is said to have an Euler circuit if there is a circuit in G that traverses every edge of the graph exactly once. If there is an open trail from vertex u to v in G and this trail traverses each edge in G exactly once, the trail is called Euler trail. [A trail from a vertex u to v is a path that doesnot involve a repeated edge] An eulerian tour is a closed walk that starts at some vertex, passes through each edge exactly once and returns to the starting vertex.

Since any closed walk in an undirected graph enters and leaves any vertex the same number of times, the subgraph composed of the edges in any closed walk is even. Thus, if the graph contains a closed walk passing through each edge exactly once, the graph must be even, conversely, if the graph is even, then it contains an Euler tour,

A path that passes through each edge exactly once but vertices may be repeated is called Euler path.

A graph that contains an Euler tour or Euler circuit is called an Eulerian graph.

Note : i) If a graph G has a vertex of odd degree, then there can be no Euler circuit in G.

ii) if a graph G is connected and each vertex has even degree, then there is an Euler circuit.

For example the graph in fig 11.29(a) in an Eulerian graph because all the vertices are of even degree, so it has an Eluerian circuit $v_1 \rightarrow v_2 \rightarrow v_3 \rightarrow v_5 \rightarrow v_4 \rightarrow v_3 \rightarrow v_1$

But the graph G in fig.11.29(b) is not an Eulerian graph because all the vertices of G are not even degrees, so there doesnot have any Euler circuit.

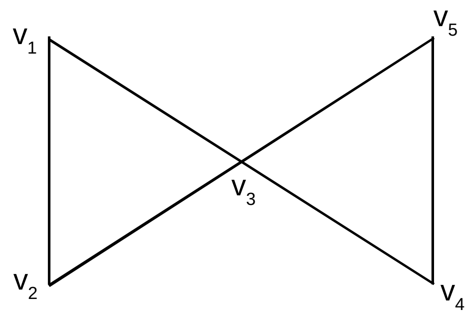


fig. 11.28(a)

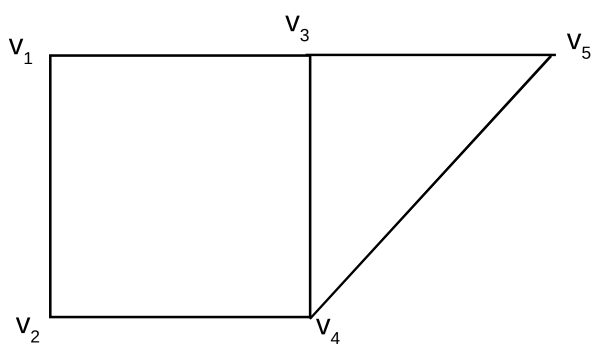


fig. 11.28(b)

Hamiltonian graph : Let G be a connected graph with more than two vertices. If there is a path in G that uses each vertex of the graph exactly once, then such a path is called Hamiltonian path. If the path is a circuit that contains each vertex in G exactly once, except the initial vertex, then such a path is called a Hamiltonian circuit.

A graph that contains an Hamiltonian circuit is called a Hamiltonian graph.

Note : i) The complete bipartite graph $k_{m,n}$ is Hamiltonian if m = n and m>1.

ii) Eulerian circuit uses every edge exactly once but many repeat vertices, while Hamiltonian circuit uses each vertex exactly once except for the first and last vertex.

For example, the graph in fig. 11.30 is Hamiltonian because there is an Hamiltonian circuit shown by the arrow symbols.

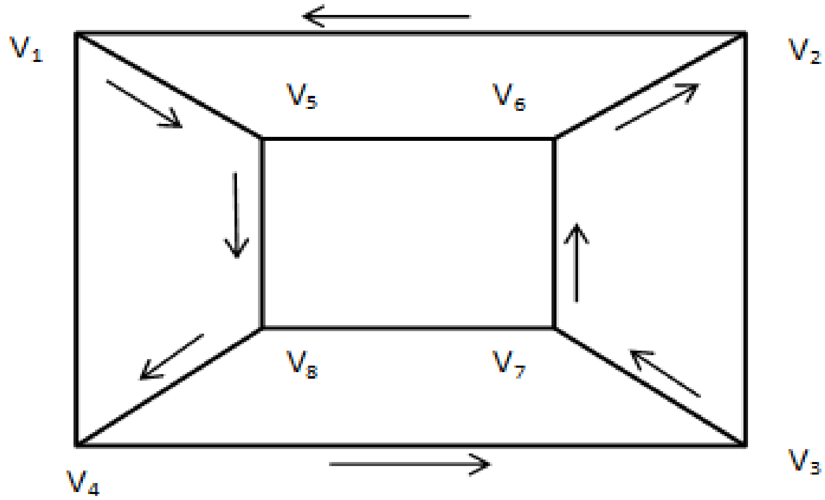


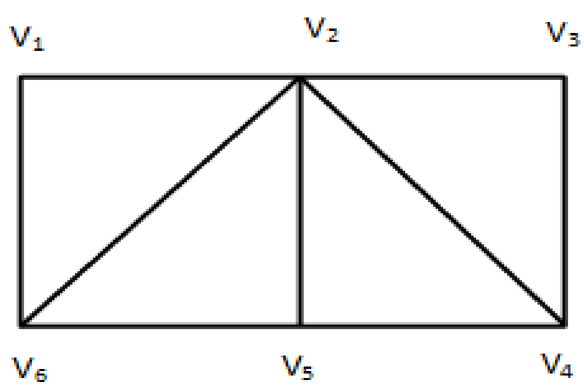
fig. 10.29

Example : Draw three graph which are

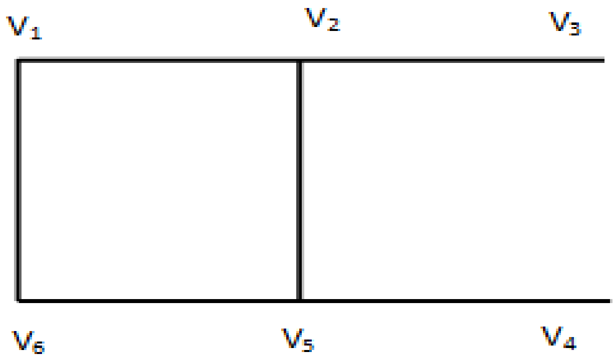
i) Hamiltonian but not an Eulerian

ii) Neither Eulerian nor Hamiltonian

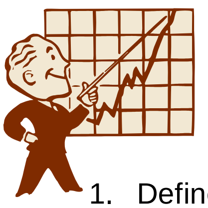
Soln.



) Hamiltonian but not an Eulerian



iii) Neither Eulerian nor Hamiltonian



CHECK YOUR PROGRESS-2

1. Define adjacency matrix of undirected graph
2. When two graphs are said to be isomorphic?
3. Define cutpoint and bridge of a connected graph.
4. What is vertex connectivity.
5. Define Eulerian path and circuits

10.8 TREES AND ITS DIFFERENT PROPERTIES

A graph is acyclic, if it has no cycles.

A tree is a connected acyclic graph. i, e a tree is a simple graph having neither a self-loop nor parallel edges. Trees with three, four and five vertices are given in fig. 10.30(a),(b) and (c)

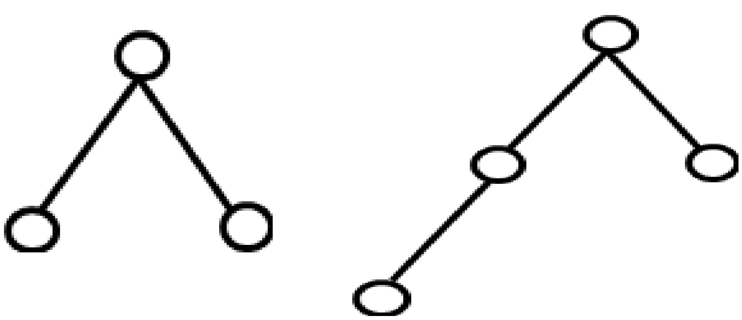


Fig. 10.30 (a), (b)

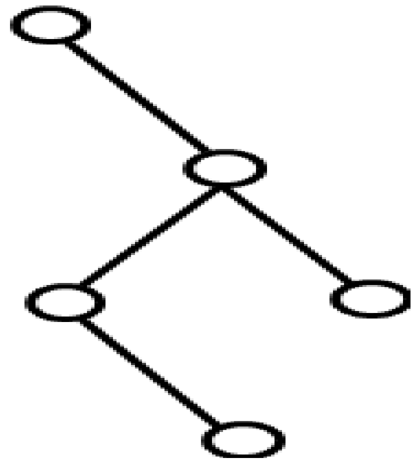


Fig. 10.30. (c)

Some properties of trees :

Theorem : Prove that a graph G is a tree iff every pair of vertices is connected by a unique path.

Proof : First suppose that the graph G is a tree. So, G is a connected graph without any circuits. Since G is connected then there must exist at least one path between every pair of vertices in G. Now suppose that between two vertices u and v in G, there are two distinct path. The union of these two paths will contain a circuit and G cannot be a tree, which is a contradiction. Hence in a tree every pair of vertices are connected by a unique path.

Conversely, suppose wehave a graph G, in which every pair of vertices are connected by a unique path, so G is connected. we need to show that G has no cycles. But if there is a cycle in G, then there are two paths between any two vertices on the cycle. which is contradiction that there must be a unique path between any two vetices of G. Hence G can not contain any cycle. So G is a tree.

Theorem : Prove that a tree with n-vertices has n–1 edges.

Proof : We prove that theorem by induction on n vertices.

Base case : Let n = 1, then this is the trival tree with o edges. so the theorem is true for n = 1.

Inductive case :

Let us assume that the theorem holds for all trees with fewer than n vertices.

Let us consider a tree T with n vertices. let e be an edge with end vertices u and v. Since T is a tree, so there is no other path between u and v except e then T-e is disconnected and has two components T_1 and T_2 has fewer than n vertices say n_1 and n_2 respectively and therefore by the induction bypthesis T_1 has $(n_1–1)$ edges and t_2 has $(n_2–1)$ edges.

$\therefore$ number of edges in T = number of edges in T_1+ number of edges in t_2 + 1

$$= (n_1–1) + (n_2–1) + 1$$

$$= n_1 + n_2–1$$

$$= n1$$

Hence a tree with n vertices has n–1 edges.

Theorem : Prove that, in any tree with two or more vertices there are at least two pendant vertices.

Proof : Let T be a tree with n vertices, then T has n–1 edges,

Again, we know that, $\sum_{i=1}^{n} d(v_i) = 2e$, where

e is the number of edges in T

$$\therefore \sum_{i=1}^{n} d(v_i) = 2e = 2(n-1) \quad \text{..........(i)}$$

Since no vertex of T can be of zero degree. So, from (1), we must have at least two vertices of degree one in T. It means taht in any tree with two or more vertices there are at least two pendant vertices.

Distance and centres in a tree : In a connected graph G, the distance d(u,v) between two of its vertices u and v is the length of the shortest path. i,e the number of edges in the shortest path between them. It is very easier to determine the distance between any two vertices of a tree because, there is exactly one path between any two vertices of the tree.

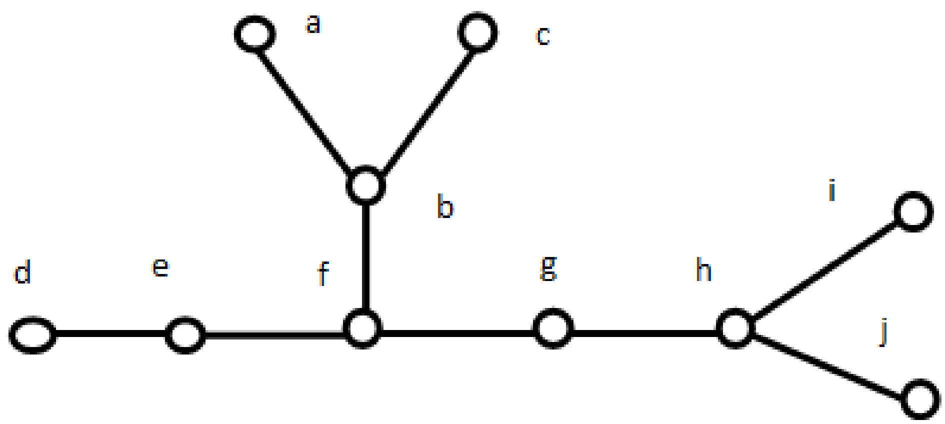


fig. 10.31

The graph in fig. 11.32, d (a, b) = 1, d (a, d) = 4, d(b, h) = 3, d (a, j) = 5 and so on.

The ecentricity E (v) of a vertex v in a, graph G is the distance from v to the vertex farthest from v in G, i.e

$$E(v) = \max \{d(u,v) : u \in v\}$$

The graph in fig. E(a) = 5, E(b) = 4, E(f) = 3, E(g) = 3, E(h) = 4 and so one.

A vertex with minimum eccentricity in a graph G is called the centre of G.

The diameter of a tree is the maximum distance between any two vertices of the tree.

Example : Find the eccentricities of all the vertices centers and diameter of the tree in the following fig. 11.32

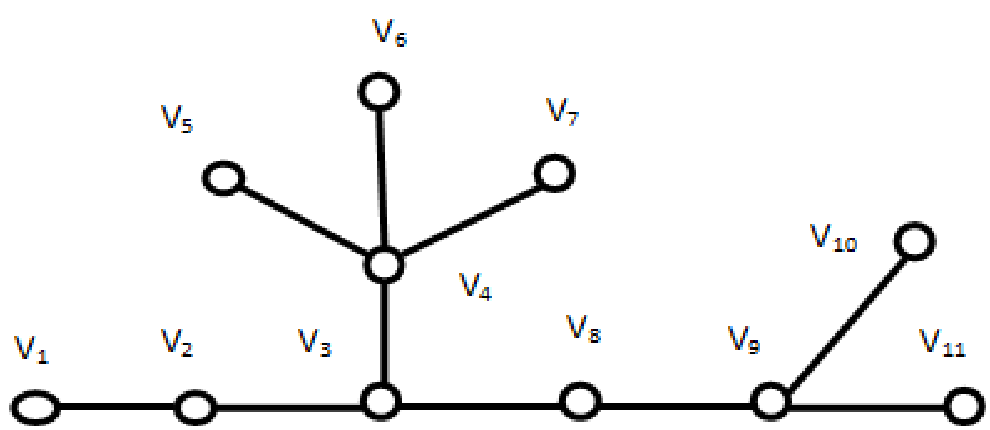


fig. 10.32

Solution :

$E(v_1) = 5$	$E(v_2) = 4$	$E(v_3) = 3$	$E(v_4) = 4$
$E(v_5) = 5$	$E(v_6) = 5$	$E(v_7) = 5$	$E(v_8) = 3$
$E(v_9) = 4$	$E(v_{10}) = 5$	$E(v_{11}) = 5$	

V_3 is the center, diameter = 5

Theorem : Prove that every tree has either one or two centres.

Proof : The maximum distance, max d(u,v) from a given vertex v to any other vertex u occurs only when u is a is a pendant vertex. Now consider a tree T having more thatn two vertices. We know that a tree must have two or more pendant vertices. Deleting all pendan vertices from T. The resulting graph T' is still a tree, decreases the eccentricities of the remaining vertices by one. Therefore, all vertices that T had as centres will still remain centers in T'. From T' we can again remove all pendant vertices and get another tree T''. We continue this process until there is left either a vertax which id the confer of T or an edge whose end vertices are the two centers of T.

Rooted trees : A Tree in which one vertex, called the root of the tree is distinguished from all the others is called a rooted tree. fig.11.34 is an example of a rooted tree where vertex v_1 is the root of the tree that appears on the top of the tree. A rooted tree grows downwords i.e to form a rooted tree, we first placethe root at the tree. Under the root and on the same level, we place the vestices that can be reached from the root on the same path of length one. Under each of these vertices and on the same lavel, we place the vertices that can be reached from the root a path of length two and so one.

Level of a vertex : The level of a vertex is the number of edges along the unique path between it and the root. The level of the root is defined as zero. The vertices immedicely under the root are said to be in level one and so on.

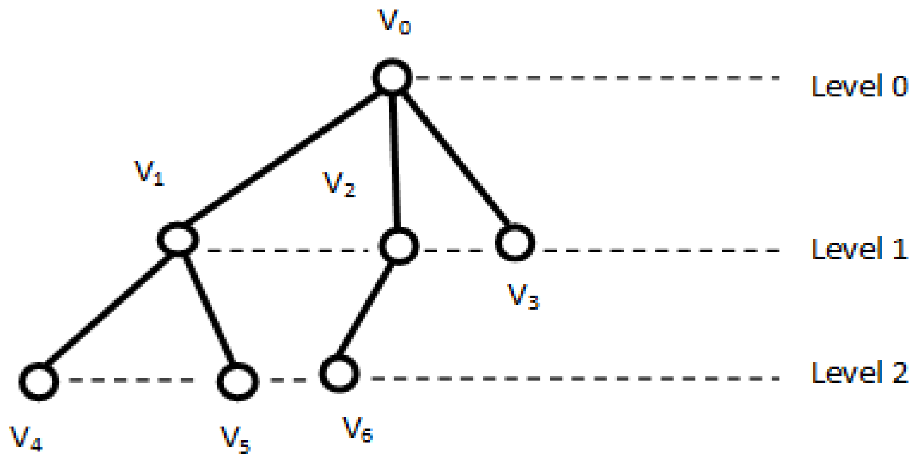


fig. 10.33

Height of the tree : The height of a tree is the maximum level of any vertex in the tree. This equals to the length of the longest path from the root of any pendent vertices. The depth of a vertex v in a tree is the length of the path from the root. The height of the tree in fig. 11.34 is 2 and depth of the vertex v_3 is one.

Children, parent and siblings : The edges in a rooted tree is defined as predecessor-successor or parent-child relationship. In fig. vertex v_0 is the predecessor of veitices v_1, v_2 and v_3. These vertices are called level 1 vertices, while v_0 is said to at level 0. Here, v_0 is called the parentof level 1 vertices. The vertices v_1, v_2 and v_3 are called children of the vertex v_0. Similarly v_4 vs are children of v_1 and $v_1$is the parent of the vertex v_4 and v_5. The vertices having the same parent are called sibliags of each other.

Descendants and Ancestor : The descendant of a vertex v_1 is the set consisting of all children of v_1 together with the descendants of those children. In fig.11.34 vertices v_4, v_5, v_1 are desendants of V_0.

A vertex n_1 is called an anestor of vertex n_2 if n_1 is either the parcent of n_2 or the parcent of some anestor of n_2. In fig 11.35 v_0 is ancestor or descendant of v_6.

Binary tree : A binary tree is a rooted tree in which each vertex has at most two children (vertices), Each child is designated either as left child or as a right child and am internal vertex has atmost one left and one right child. A binary tree on also defined as a tree in which there exsactly one vertex of degree two and each of the remaining vertices is of degree one or three.

Theorem : Prove that the number of vertices n in a binary tree is odd.

Proof : In a binary tree there is exactly one vertex of degree 2 i,e even and the remaining n–1 vertices are of odd degrees. Again, we know that, in a graph, the number of vertices of odd degree is even, So (n–1) is even, Hence n is odd.

Theorem : Prove that if T is a binary tree with n vetices and p be the number of pendant vertices then 2p = n + 1

Proof : Since P be the number of pendant vertices, of a binary tree with n vertices. Then n–p–1 is the number of degree three. (1 is corresponds to the root of the tree whose degree is two), Therefore, the total number of edges in T

equalls

$$\frac{1}{2}\ [p + 3\ (n–p–1) + 2] = n–1$$

$$\Rightarrow\ 3n–2p–1c\ 2\ (n–1)$$

$$\Rightarrow\ 2p = n + 1$$

Remark : i) The minimum possible height of an n-vertex binary tree is $[\log_2 (n +1)–1]$, where [n] denotes the smallest integer greater than or equal to n.

ii) the maximum height of a binary tree of n vertices is $\frac{n-1}{2}$

Example : Find the maximum and minimum height of a binary tree of 13 vertices.

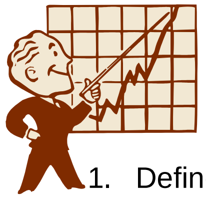
Solution : The maximum height of abinary tree of 13 vertices

$$= \frac{13-1}{2} = 6$$

Again, the minimum height of the binary tree of 13 vertices

$$= [\log_2 (13 +1) –1]$$

$$= [\log_2 14–1]$$



CHECK YOUR PROGRESS - 3

1. Define a tree
2. What do you mean by centers and eccentricity of a tree?
3. What is a Rooted tree?
4. What is weighted graph?

10.9 LET US SUM UP

- A graph $G = (v,E)$ is a pair of sets, where
  $V = \{v_1, v_2, \ldots \ldots \ldots\}$ is a set of vertices and
  $E = \{e, e_2, \ldots \ldots \ldots\}$ is a set of edges connecting pair of vertices.
- A graph is said to be undircted graph if its edges are unordered pairs of distinct vertices otherwise the graph is said to be directed.
- The degree of a vertex is the number of edges incident with that vertex.
- A loop is an edge from a vertex to itself. It there is more than one edge between a pair of vertices, them these edges are called paralled edges.
- A graph with no loops and paralled edges is called a simple graph.
- A simple graph in which there is an edge between every pair of vertices is called a complete graph.
- The number of vertices of odd degree in a graph is always even.
- In computers, a graph can be represented in two ways, viz, adjacency matrix and incidence matrix.
- The simple graph $G_1 = (v_1, E_1)$ and $G_2 = (v_2, E_2)$ are isomorphic if there is a one-to-one and onto function f from v_1 to v_2 with the property that vertices a and b are adjacent in G_1 iff f(a) and f(b) are adjacent in G_2, $\forall$ a,b $\in V_1$ Such a function f is called an isomorphism.

- A graph is connected if we can reach any vertex from any other vertex by traveling along the edges. Otherwise, the graph is disconnected.
- A graph is Hamiltonian if every vertex of the graph has even number of degrees.
- A tree with n vertices has n–1 edges.
- Every tree has either one or two centres.
- A tree T is said to be a spanning tree of a connected graph G if T is a subgraph of G and T contains all vertices of G.

10.10 ANSWER TO CHECK YOUR PROGRESS

CHECK YOUR PROGRESS-1

1. A graph with no loops and paralled edges is called a simple graph.
2. The degree of a vertex is the number of edges incident with that vertex.
3. A vertex of degree one is called a pendant vertex and a vertex of degree zero is called an isolated vertex
4. A vertex is said to be an even or odd vertices according as its degree is an even or odd number.
5. A simple graph is which there exists an edge between every pair of vertices is called a complete graph. Again a graph in which every vertex has the same degree is called a regular graph.

CHECK YOUR PROGRESS-2

1. Suppose that G be a simple undirected graph with n vertices. suppose that the vertices of G are listed arbitraily as v_1, v_2, ..., v_n. The adjacency matrix denoted by A(G) of G is an n×n matrix [aij] defined as :

$[aij] = 1$, if vertex v_i is adjacent to v_j
0, otherwise

2. Two simple graph $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a one-to-one and onto function f from V_1 to V_2 with the property that vertices a and b are adjacent in G_1 iff f(a) and f(b) are adjacent in G_2, $\forall$ a,b $\in V_1$
   Such a function f is called an isomorphism
3. Vertex v in a connected graph G is called a cutpoint if G–v is disconnected. Again an edge e of a connected. Again an edge e of a connected graph G is called G bridge if G–e is disconnected.
4. The vertex connectivity of a graph G is defined as the minimum number of vertices whose removal from G leives the graph disconnected.
5. A path that passes through each edge exactly once but vertices may be repeated is called on Euler path. Again a cuircuit that covers every edge exactly once is called an euler circuit.

CHECK YOUR PROGRESS-3

1. A connected acyclic graph is called a tree.
2. The eccentricty of a vertex v in a graph G is the distance from v to the vertex fartest from v in G. A vertex with minimum eccentricity in a graph G is called the centre of G.
3. A tree in which one vertex, called the root of the tree is distinguished from all the other vertices is called a rooted tree.
4. A connected graph G in which each of its edges are assigned a positive number is called a weighted graph.

10.11 FURTHER READING

Deo, Narsingh, 2009. Graph Theory with application to Enginnering and computer science, PHI Learning private limited, New Delhi.

Rosen, Kenneth H. 2003, Discrete Mathematics and its application, 3rd edition, New Delhi; Tata Mc. raw Hill Publishing Company limited.

Harary, Frank, 2001, Graph Theory. Tenth edition, New Delhi, Narosa publishing House.

Mott. Joe. L, Kandel, Abraham, Baker Te odore p. Discrete Mathematics for computer Scientists and Mathematicians, 2nd edition, New Delhi : Prentice Hall of India Pvt. Ltd.

Tyengar, N. Ch. Z. N., V. M. chandrasekaram, K.A. Venkatesh and P.S. Arunachalam, 2008. Discrete Mathematics. New Delhi : Vikas publishing House Pvt. Ltd.

10.12 PROBABLE QUESTIONS

Short Answer Questions

1.Define a graph

2. Draw a comple graph with 5 vertices
3. Draw two 3-regular graph
4. Find the number of edges of complete graph K_5
5. How many vertices and how many edges do graph $k_{m,n}$ have
6. For which values of m and n is $k_{m,n}$ regular?
7. What is incidence matrix?
8. When a connected graph is said to be Hamiltonian
9. What do you mean by level of a rooted tree
10. Waht do mean by the height of a tree

Long Answer Questions

1. Let G be a graph with n vertices and e edges, then prove that

$$\sum_{i=1}^{n} d(v_i) = 2e$$

2. How many edges does a graph have if it has vertices of degree 4, 3, 3, 2, 2? Draw such a graph.
3. Does thre exist a simple graph with six vertices of these degrees? If so, draw shcu a graph

   i) 0, 1, 2, 3, 4, 5

   ii) 2, 2, 2, 2, 2, 2
4. Are the simple graphs with the following adjacency matrices are isomorphic

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

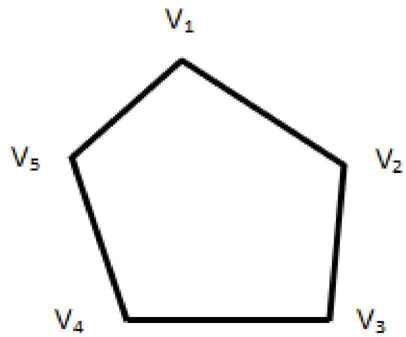
5. Let G be a graph with n vertices. P of which has degree k and the others have degree k+1. Prove that P = (k + 1) n–ze, where e is the nuimber of edges in G
6. The adjacency matrix of a graph is given below :

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

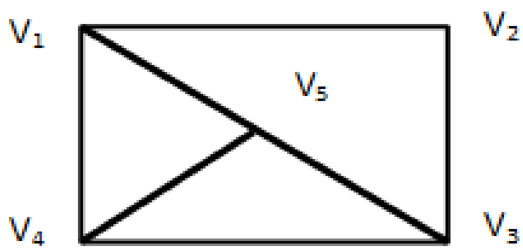
   Discuss whether the graph is connected or not?
7. Prove that the number of vertices of odd degree in a graph is always even.
8. Prove that a simple graph with n vertices must be connected if it has more than $\frac{(n-1)(n-2)}{2}$ edges.

9. Find the number of edges in the graphs K_{12} and K_{15}.
10. Determine whether the given pair of graphs is isomorphic or not?

i)



ii)



11. Prove that every tree has either one or two centers.
12. Prove that a connected graph with n vertices has at least n-1 edges
13. Prove that if T is a binary tree with n vertices and l pendant vertices, then $2\ell = n + 1$
14. It a graph G is not conected, prove that its complement $\overline{G}$ is connected. Is the converse true?
15. Find the maximum and minimum height of a binary tree with 13 vertices.