SPECTRUM

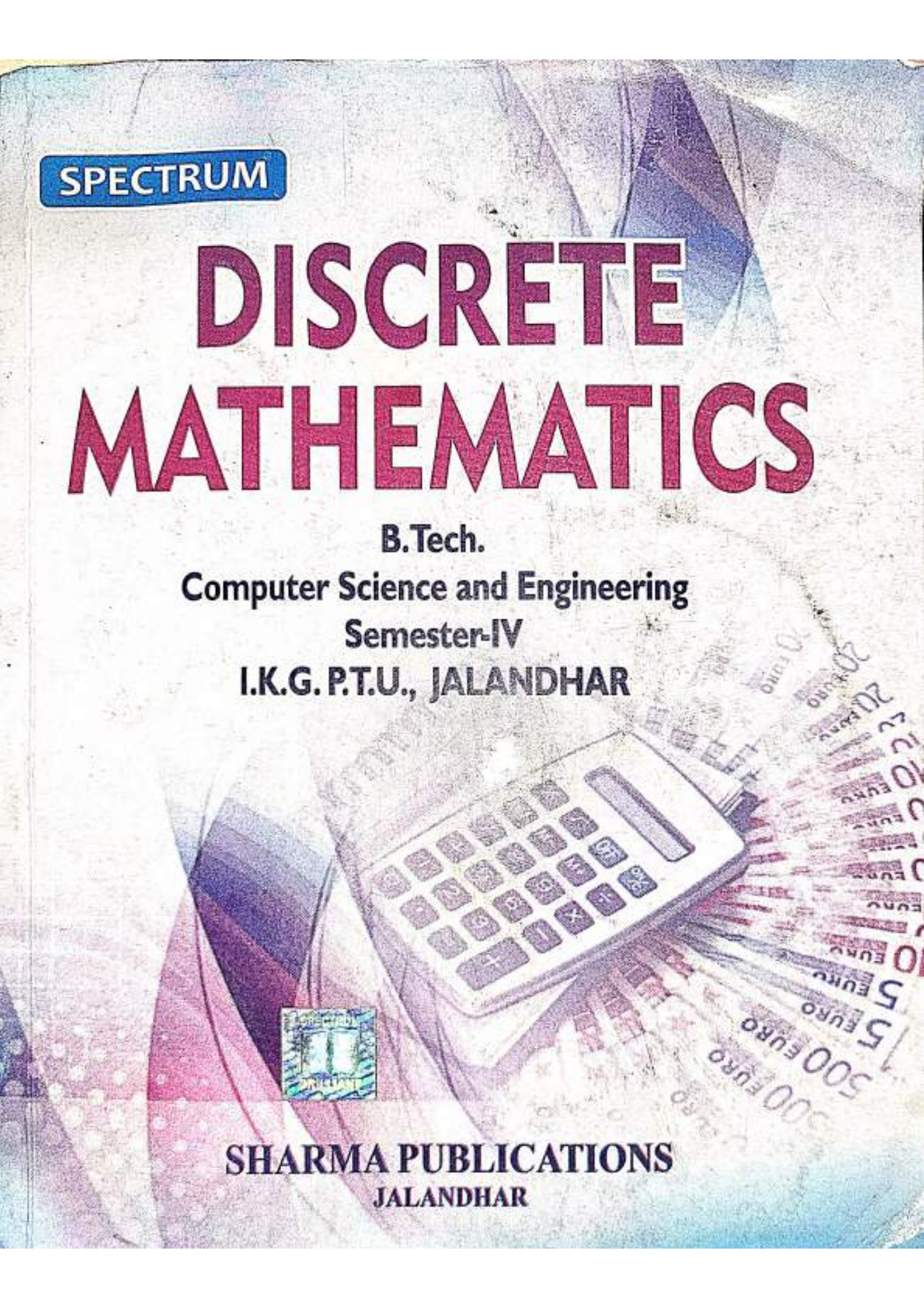
DISCRETE MATHEMATICS

B.Tech.

Computer Science and Engineering

Semester-IV

I.K.G. P.T.U., JALANDHAR



SHARMA PUBLICATIONS

JALANDHAR

SYLLABUS

BTCS401-18

DISCRETE MATHEMATICS

4 Credits

3 L : 1 T : 0 P

Detailed contents :

Module 1 :

Sets, Relation and Function : Operations and Law of Sets, Cartesian Products, Binary Relation, Partial Ordering Relation, Equivalence Relation, Image of a Set, Sum and Product of Functions, Bijective functions, Inverse and Composite Function, Size of a Set, Finite and infinite Sets, Countable and uncountable Sets, Cantor's diagonal argument and The Power Set theorem, Schroeder-Bernstein theorem.

Principles of Mathematical Induction : The Well-Ordering Principle, Recursive definition, The Division algorithm :Prime Numbers, The Greatest Common Divisor Euclidean Algorithm, The Fundamental Theorem of Arithmetic.

Module 2 :

Basic counting techniques-inclusion and exclusion, pigeon-hole principle permutation and combination.

Module 3 :

Prepositional Logic : Syntax, Semantics, Validity and Satisfiability, Basic Connectives and Truth Tables, Logical Equivalence : The Laws of Logic, Logical Implication, Rules of Inference, The use of Quantifiers. **Proof Techniques :** Some Terminology, Proof Methods and Strategies, Forward Proof, by Contradiction, Proof by Contraposition, Proof of Necessity and Sufficiency.

Module 4 :

Algebraic Structures and Morphism : Algebraic Structures with on Binary Operation, Semi Groups, Monoids, Groups, Congruence Relation and Quotient Structures, Free and Cyclic Monoids and Groups, Permutation Groups, Substructures, Normal Subgroups. Algebraic Structures with two Binary Operation, Rings, Integral Domain and fields. Boolean Algebra and Boolean Ring, Identities of Boolean Algebra, Duality, Representation of Boolean Function, Disjunction and Conjunction Normal Form.

Module 5 :

Graphs and Tree : Graphs and their properties, Degree, Connectivity, Path, Cycle, Sub Graph, Isomorphism, Eulerian and Hamiltonian Walks, Graph Colouring, Colouring maps and Planar Graphs, Colouring Vertices, Colouring Edges, List Colouring, Perfect Graph, definition properties and Example, rooted trees, tree and sorting, weighted trees and prefix codes, Bi-connected component and Articulation Points, Shortest distances.

CONTENTS

MODULE-1

1

SETS, RELATION AND FUNCTION

SECTION-I
SET THEORY

1.1. Introduction

Set is a basic and unifying idea of mathematics. In fact all mathematical ideas can be expressed in terms of sets. In almost whole of the business mathematics, the set theory is applied in one form or the other.

1.2. Def. of a set

A set is a collection of well defined and different objects.

By the words 'well defined' we mean that we are given a rule with the help of which we can say whether a particular object belongs to the set or not. The word 'different' implies that repetition of objects is not allowed.

The words 'family', 'class', 'collection' are also used as synonyms for the word set when the elements are themselves sets.

Element of a Set

Each object of the set is called an element of the set.

Examples of sets

(*i*) The set of days of a week.

(*ii*) The set of integers from 1 to 100000.

(*iii*) The set of even integers.

(*iv*) The set of all states of India.

(*v*) The set of all solutions of equation $x^2 = 1$.

Set Notations

Sets are generally denoted by capital letters A, B, C,.....

The elements of sets are denoted mostly by small letters *a, b, c*...

Some Standard Sets

N = Set of all natural numbers 1, 2, 3, 4,.....

W = Set of all whole numbers 0, 1, 2, 3, 4,.....

I or **Z** = Set of all integers

Q = Set of all rational numbers

R = Set of all real numbers

Methods of Designating a Set

A set can be specified in two ways :

(1) Tabular, Roster or Enumeration Method :

When we represent a set by listing all its elements within curly brackets { }, separated by commas is called the tabular, roaster or enumeration method.

(*i*) A set of vowels : A = {*a, e, i, o, u* },

(*ii*) A set of positive even integers upto 10 : B = {2, 4, 6, 8, 10}

(*iii*) A set of odd natural numbers : C = {1, 3, 5,.....}.

(2) Selector, Set-builder or Rule Method :

In this method, we do not list all the elements but the set is represented by specifying the defining property

For example,

A = { x : x is a vowel in English alphabets }

B = { x : x is a positive even integer up to 10 }

C = {x/x is an odd positive integer }

Here (:) or (/) means such that.

Note 1. The order of elements in a set is immaterial.

Thus {2, 5, 9, 11}, {2, 9, 5, 11}, {11, 5, 2, 9} represent the same set.

2. Repetition of elements is not allowed in a set.

Membership of a Set

If an object x is a member of the set A, we write $x \in A$, which can be read as 'x belongs to A' 'A contains x'. Similarly we write $x \notin A$ to show that x is not a member of the set A.

Example. Let A = {1, 2, 5, 7, 9, 10}.

Here $5 \in A$, but $6 \notin A$.

Type of Sets

Finite Set

A set is said to be finite if it has finite number of elements.

Examples :

A = {2, 4, 6, 8 }

B = { x : x is a student of Modi College, Patiala }

Set of months of the year

Set of even natural numbers less than 100.

Infinite Set

A set is said to be infinite if it has an infinite number of elements.

Examples :

$A = \{1, 2, 3.....\}$

$B = \{x : x \text{ is an odd integer }\}$

$C = \{x : x \text{ is a multiple of } 6\}$

Singleton Set

A set containing only single element is called a singleton or a unit set.

Example : $A = \{x : x \text{ is a perfect square and } 30 \le x \le 40\} = \{6\}$

$B = \{x : x \text{ is a positive integer satisfying } x^2 = 4\} = \{2\}$

$C = \{3\}$

Empty, Null or Void Set :

A set which contains no element, is called a null set and is denoted by ϕ (read as phi).

Examples : $A = \left\{x : x \text{ is a positive integer satisfying } x^2 = \frac{1}{4}\right\}$

$B = \{x : x \text{ is a fraction satisfying } x^2 = 9\}$

Sub-Set, Super-Set

If every element of a set A is a element of a set B, then A is called sub-set of B and B is called super-set of A.

Or if $x \in A \Rightarrow x \in B$, then A is a sub set of B and B is a super set of A.

We write these as $A \subset B$ and $B \supset A$.

Thus $A \subset B$ means A is contained in B or B contains A.

Note 1. Since every element of A belongs A

$\therefore$ $A \subset A$ $\Rightarrow$ *every set is sub set of itself.*

2. The empty set ϕ is considered to be a Subset of every set

3. If set A has n elements then number of subsets of A is 2^n.

Example. Let $A = \{1, 2, 3, 4, 5, 6, 8, 10\}$

and $B = \{2, 4, 6, 10\}$, $C = \{1, 2, 7, 8\}$, $D = \{2, 7, 8, 1\}$

Now every element of B is an element of A

$\therefore$ $B \subset A$

Again $7 \in C$, but $7 \notin A$

$\therefore$ $C \not\subset A$ *i.e.,* C is not a sub-set of A.

Now every member of D is a member of C and every member of C is a member of D.

$\therefore$ $C \subset D$ and $D \subset C$

In this case we can also write $C \subseteq D$ and $D \subseteq C$.

Equality of Sets

Two sets A and B are said to be equal if both have the same elements. In other words, two sets A a B are equal when every element of A is an element of B and every element of B is an element of A.

i.e., If $A \subset B$ and $B \subset A$, then $A = B$.

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

$B = \{x : x \text{ is a natural number and } 1 \leq x \leq 10\}$

Here $A = B$.

Proper Sub-set

A non-empty set A is said to be a proper subset of B if $A \subset B$ and $A \neq B$.

Note 1. ϕ and A are called improper subsets of A.

Power set

The power set of a finite set is the set of all sub-sets of the given set. Power set of A is denoted by P(A)

Example. Take $A = \{1, 2, 3\}$

$P(A) = \{\phi, \{1\}, (2)\ \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

Universal Set

If all the sets under consideration are sub-sets of a fixed set U, then U is called a universal set.

Example. In Plane geometry, the universal set consists of points in a plane.

Comparable and Non-comparable Sets

Two sets are said to be comparable if one of the two sets is a sub-set of the other.

Example . Let $A = \{2, 3, 5\}$, $B = \{2, 3, 5, 6\}$, $C = \{1, 5\}$

Here $A \subset B$

$\therefore$ A and B are comparable sets. On the other hand $A \not\subset C$, $C \not\subset A$

$\therefore$ A, C are Non-comparable.

Order of a Finite Set

The number of different element of a finite set A is called the order of A and is denoted by O(A).

Cardinality : Number of different elements in a set is known as its cardinality.

Example If $A = \{2, 3, 6, 8\}$, then $O(A) = 4$

Equivalent Sets

Two finite sets A and B are said to be equivalent sets if the total number of elements in A is equal the total number of elements in B.

Example. Let $A = \{1, 2, 3, 4, 6\}$, $B = \{1, 2, 7, 9, 12\}$

$\therefore$ $O(A) = 5 = O(B)$ $\Rightarrow$ A and B are equivalent sets.

We write the above fact as $A \sim B$

ILLUSTRATIVE EXAMPLES

Example 1. Write the following sets in Roster form :

(*i*) $A = \{x \in N : x^2 = 25\}$ (*ii*) $B = \{x \in N : |x| \le 4\}$ (*iii*) $C = \{x : x^2 - 3x + 2 = 0\}$

(*iv*) $D = \{x : x$ is a positive multiple of 3 and 7 but less than 28$\}$

Sol. (*i*) $x^2 = 25 \Rightarrow x = 5, -5$

But $x \in N$, $\therefore x = 5$

$\therefore$ $A = \{5\}$

(*ii*) $|x| = x$ as $x \in N$

$\therefore$ $|x| \le 4 \Rightarrow x \le 4 \Rightarrow x = 1, 2, 3, 4$

$\therefore$ $B = \{1, 2, 3, 4\}$

(*iii*) $x^2 - 3x + 2 = 0 \Rightarrow (x-1)(x-2) \Rightarrow x = 1, 2$

$\therefore$ $C = \{1, 2\}$

(*iv*) Since x is a positive multiple of 3 and 7

$\therefore$ x is a multiple of 21

$\therefore$ $D = \{21\}$

Example 2. Redefine each of the following sets, using set builder notation :

(*a*) $\{-2, -4, -6, \ldots\ldots\}$ (*b*) $\{0, 3, -3, 6, -6, 9\ldots\ldots\}$

(*c*) $\{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, \ldots\ldots\}$ (*d*) $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\ldots\right\}$

(*e*) $\{0, 1, 2, \ldots\ldots, 99, 100\}$

Sol. (*a*) Let $A = \{-2, -4, -6, \ldots\ldots\} = \{-2x : x \in I\}$

(*b*) Let $A = \{0, 3, -3, 6, -6, 9\ldots\ldots\} = \{3x : x \in I\}$

(*c*) Let $A = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, \ldots\ldots\}$

$= \{x : x = 2n$ or $x = 3n : n \in N\}$

(*d*) Let $A = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\ldots\right\} = \left\{x : x = \frac{1}{n} : n \in N\right\}$

(*e*) Let $A = \{0, 1, 2, \ldots\ldots, 99, 100\} = \{x : x \in I$ s.t. $0 \le x \le 100\}$

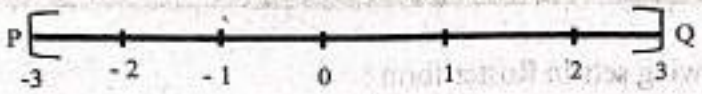
Example 3. Define geometrically, the following set :

(*a*) $\{x \in R : |x| \le 3\}$ (*b*) $\{x \in Z, : |x| \le 3\}$

(*c*) $\{x \in N, |x| \le 3\}$ (*d*) $\{(x, y), x, y \in R, x^2 + y^2 = 25\}$

Sol. (*a*) Let $A = \{x \in \mathbf{R} : |x| \leq 3\} = \{x \in \mathbf{R} : -3 \leq x \leq 3\}$

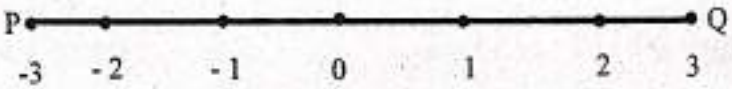
The set A is represented by



by the points on the line from P to Q including the points P and Q.

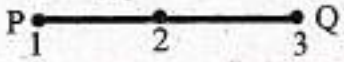
(*b*) Let $A = \{x \in \mathbf{Z}, : |x| \leq 3\} = \{-3, -2, -1, 0, 1, 2, 3\}$

The set A is represented by the points marked by dot on the line PQ.



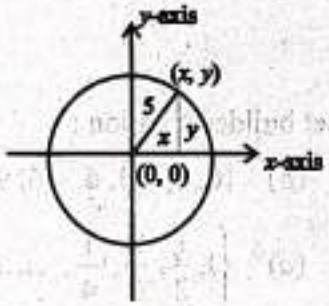
(*c*) Let $A = \{x \in \mathbf{N}, |x| \leq 3\} = \{1, 2, 3\}$

The set A is represented by the points marked by dot on the line PQ



(*d*) Let $A = \{(x, y) ; x, y \in \mathbf{R} ; x^2 + y^2 = 25\}$

The set A is represented by all the points which lie on the circle whose centre is at the point (0, 0) a radius as shown below :



Example 4. Determine which of the following pairs of sets are equal :

(*a*) S = {*x*: *x* is an integer divisible by both 3 and 2} and Q = {6, 12, 18, 24,.....}

(*b*) X = {*x*: *x* is real and $x^2 < x$} and T = {*x* : *x* is real and $0 < x < 1$}

(*c*) Let A = {1, 2, 3, 4}, B = {*x* : *x* is a positive integer and $x^2 < 18$}.

Sol. (*a*) S = {*x*: *x* is an integer divisible by both 3 and 2}

$= \{x : x = 3n$ or $x = 2n$ where $n \in I\}$

$= \{.....-9, -8, -6, -4, -3, -2, 0, 2, 3, 4, 6, 8, 9,.....\}$

Q = {6, 12, 18, 24,.....}

Since $-6 \in S$ and $-6 \notin Q$

$\therefore \quad S \neq Q$

(*b*) $X = \{x : x \text{ is real and } x^2 < x\}$

Since $x^2 < x \Rightarrow x^2 - x < 0$

$\Rightarrow x(x-1) < 0$

$\Rightarrow 0 < x < 1$

$\therefore$ $X = \{x: x \text{ is real and } 0 < x < 1\}$

$= T$

$\therefore$ $X = T$

(*c*) $A = \{1, 2, 3, 4\}$

$B = \{x : x \text{ is positive integer and } x^2 < 18\}$

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

yes, $A = B$

Example 5. Is the set $A = \{ x : x^2 - 5x + 6 = 0 \text{ and } x^2 - 3x + 2 = 0 \}$ empty ? Justify.

Sol. $A = \{x : x^2 - 5x + 6 = 0 \text{ and } x^2 - 3x + 2 = 0 \}$

Now $x^2 - 5x + 6 = 0 \Rightarrow (x-2)(x-3) = 0 \Rightarrow x = 2, 3$

Also $x^2 - 3x + 2 = 0 \Rightarrow (x-1)(x-2) = 0 \Rightarrow x = 1, 2$

$\therefore$ there is a value 2 of x which satisfies $x^2 - 5x + 6 = 0$ and $x^2 - 3x + 2 = 0$

$\therefore$ $A = \{ 2 \} \Rightarrow$ A is not an empty set.

Example 6. Enumerate elements in following sets :

(*a*) $\{x \in R \mid x^2 - 3x + 2 = 0\}$ (*b*) $\{x \in R \mid x^2 + 1 = 0\}$ (*c*) $\{x \in C \mid x^2 + 1 = 0\}$

Sol. (*a*) Let $A = \{ x \in R \mid x^2 - 3x + 2 = 0\}$

Solution Set : $x^2 - 3x + 2 = 0$

$x - 2x - 1x + 2 = 0$

$(x-2)(x-1) = 0$

$\therefore$ $x = 1, 2$

$\therefore$ $A = \{1, 2\}$.

(*b*) Let $B = \{x \in R \mid x^2 + 1 = 0\}$

$x^2 + 1 = 0 \Rightarrow x = \pm \sqrt{-1} \notin R$

$\therefore$ Set B has no Solution.

$\therefore$ $B = \phi$.

(*c*) Let $D = \{x \in C \mid x^2 + 1 = 0\}$

$x^2 + 1 = 0 \Rightarrow x = \pm \sqrt{-1} \Rightarrow x \pm i \in C$.

$\therefore$ $D = \{-i, i\}$

Example 7. Find the cardinal number of each set :

(*i*) $A = \{x : x^2 = 25, 3x = 6\}$ (*ii*) Power set P(B) of $B = \{1, 4, 5, 9\}$

(*iii*) $A = \{x : x \in N, x^2 = 5\}$ (*iv*) B {6, 7, 8, 9, ...}

Sol. (*i*) $A = \{x : x^2 = 25, 3x = 6\}$

Since $x^2 = 25 \Rightarrow x = \pm 5$ and $3x = 6 \Rightarrow x = 2$

$\therefore \quad A = \phi$

Card (A) = 0 *i.e.*, # (A) = 0

(*ii*) Here $B = \{1, 4, 5, 9\}$

$\therefore$ P (B) = {ϕ, {1}, {4}, {5}, {9}, {1, 4}, {1, 5}, {1, 9}, {4, 5}, {4, 9}, {5, 9}, {1, 4, 5}, {1, 4, 9},
{4, 5, 9}, {1, 5, 9}, {1, 4, 5, 9

$\therefore$ Cardinal number of (P (B)) = 16

(*iii*) As $x^2 = 5$

$\Rightarrow \quad x, \pm\sqrt{5} \subset N$

$\therefore$ Cardinal number is ϕ

(*iv*) Cardinal number is ∞

Example 8. List all the members of the power set of each of the following sets :

(*a*) $A = \{a, b, 2, 3\}$ (*b*) $C = \{\{a\}, \{b\}\}$ (*c*) $D = \{\phi, \{\phi\}\}$

Sol. Here $A = \{a, b, 2, 3\}$

$\therefore$ P (A) = {ϕ, {*a*}, {*b*}, {2}, {3}, {*a*, *b*}, {*a*, 2}, {*a*, 3}, {*b*, 2}, {*b*, 3}, {2, 3}, {*a*, *b*, 2}, {*a*, *b*, 3
{*b*, 2, 3}, {*a*, 2, 3}, {*a*, *b*, 2, 3

(*b*) $C = \{\{a\}, \{b\}\}$

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

(*c*) $D = \{\phi, \{\phi\}\}$

$\therefore$ P (D) = $\{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$

Example 9. Let A = {*r*, *s*, *t*, *u*, *v*, *w*}, B = {*u*, *v*, *w*, *x*, *y*, *z*}, C = {*s*, *u*, *y*, *z*}, D = {*u*, *v*}, E = {*s*, *u*} a
F = {*s*}. Let X be an unknown set.

Determine which sets A, B, C, D, E or F con equal X if we are given

(*i*) $X \subset A$ and $X \subset B$ (*ii*) $X \not\subset B$ and $X \subset C$

(*iii*) $X \not\subset A$ and $X \not\subset C$ (*iv*) $X \subset B$ and $X \not\subset C$.

Sol. (*i*) The only set which is a subset of both A and B is D. Notice that C, E, and F are not subsets of since $s \in C, E, F$ and $s \notin B$.

(*ii*) Set X can equal C, E or F since they are subsets of C and these are not subsets of B.

(*iii*) Only B is not a subset of either A or C. D and A are subsets of A ; C, E, F are subsets of C. Th
X = B.

(*iv*) Both B and D are subsets of B and are not subsets of C. Hence X = B or X = D.

Example 10. Two finite sets have m and n elements. The total number of subsets of the first set is 56 more than the total number of subsets of the second set. Find the values of m and n.

Sol. Let A and B be two sets having m and n elements respectively. Then,

Number of subsets of A $= 2^m$,

Number of subsets of B $= 2^n$.

It is given that $2^m - 2^n = 56$

$\Rightarrow \quad 2^n(2^{m-n}-1) = 2^3(2^3-1)$

$\Rightarrow \quad n = 3$ and $m - n = 3$

$\Rightarrow \quad n = 3$ and $m = 6$.

Example 11. Prove that a set containing n distinct elements has 2^n subsets.

Sol. Let $A = \{a_1, a_2, a_3, ..., a_n\}$

where a_i's are distinct.

A selection of r objects from the elements of the set A can be made in ${}^nC_r$ way. $0 \le r \le n$. Hence, there are ${}^nC_r$ subsets of a A which contains r elements.

$\therefore$ Number of subsets of A containing no elements is ${}^nC_0$.

Number of subsets of A containing 1 element is ${}^nC_1$.

Number of subsets of A containing 2 element is ${}^nC_2$.

.....

.....

.....

Number of subsets of A containing n elements is ${}^nC_n$.

Hence, the total number of elements of A

$= {}^nC_0 + {}^nC_1 + {}^nC_2 + ... + {}^nC_n$

$= 2^n$.

Example 12. What is the number of subsets of a set having n elements. Write down all the proper subsets of the set {1, 2, 3}.

Sol. The number of subsets of a set having n elements $= 2^n$.

No. of proper subsets of a set $= 2^n - 1$

Let $A = \{1, 2, 3\}$, $n = 3$

No. of proper subsets of $A = 2^3 - 1 = 7$

Proper subsets of A are ϕ, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}.

EXERCISE 1.1

1. List the elements in each of the following sets using braces and ellipses where necessary

   (*a*) $\{x : x$ is a natural number divisible by 5$\}$ (*b*) $\{x : x$ is a negative odd integer$\}$

   (*c*) $\{x : x$ is an even prime number$\}$ (*d*) $\{x : x - 1$ is an integer divisible by 4$\}$

   (*e*) $\{x : x$ is an integer divisible by 2 and by 5$\}$

2. Write the following sets in Roster form :

   (*i*) $\{x : x$ is a vowel before g in the English alphabet$\}$

   (*ii*) $\{x \in \mathbf{N} : x$ is a prime number between 6 and 30$\}$

   (*iii*) $\{x \in \mathbf{N} : 3x + 5 < 31\}$

   (*iv*) $\{x : x^2 + 5x + 6 = 0\}$

3. Enumerate the element , in the following sets :

   (*a*) $\{x \in \mathbf{R}/x^2 - 3x + 2 = 0\}$ (*b*) $\{x \in \mathbf{R}/x^2 + 1 = 0\}$ (*c*) $\{x \in \mathbf{C}/x^2 + 1 = 0\}$

4. Describe the following sets in set builder form :

   (*i*) A = {5, 6, 7, 8, 9, 10, 11} (*ii*) B = {2,4, 6, 8, 10}

   (*iii*) C = {18, 27, 36, 45, 54, 63, 72, 81,90}

5. Describe the following sets using set builder notation

   (*a*) {3, 5, 7, 9,..... 77, 79}

   (*b*) The rational numbers that are strictly between -1 and 1

   (*c*) The even integers

6. Which of the following sets are null sets ?

   (*i*) $A = \{x : x \in \mathbf{N}, x < 1\}$ (*ii*) $B = \{x : x + 4 = 4\}$ (*iii*) $C = \{x : x < 1$ and $x > 3\}$

7. What is the set $\{x : x \in \mathbf{R}, x^2 = 9, 2x = 4\}$?

8. What is the set $\{x : x \in \mathbf{R}, x^2 = 4, x^2 - 3x + 2 = 0\}$?

9. Is the set $A = \{x : x^3 = 8$ and $2x + 3 = 0\}$ empty ? Justify

10. Let $A = \{x : x$ is rational and $0 \le x \le 2\}$ and let

    $B = \{x : x$ is rational and $1 \le x \le 3\}$.

    Indicate whether each of the following is true or false.

    (*a*) $0{\cdot}5 \in A$, (*b*) $2^{1/2} \in B$

    (*c*) $2{\cdot}6 \in A$. or $2{\cdot}6 \in B$ (*d*) $\exists\ x / x \in A$ and $x \in B$

11. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$ and $C = \{1, 5, 9\}$. Determine which of the following statements ar true ? Give reason for your answer.

    (*a*) $3 \in A$ (*b*) $\{3\} \in A$ (*c*) $\{3\} \subseteq A$ (*d*) $B \subseteq A$ (*e*) $A \subseteq B$

    (*f*) $\phi \subseteq C$ (*g*) $\phi \in A$

12. Find the cardinal number of each set :

(*i*) $A = \{x : x \in N, x^2 = 5\}$ (*ii*) $B = \{6, 7, 8, 9, ...\}$

13. List some of the elements of the power set of the integer. Use set builder notation for at least two of these elements.

ANSWERS

1. (*a*) $\{5, 10, 15, 20, ...\}$ (*b*) $\{-1, -3, -5, -7, ...\}$ (*c*) $\{2\}$

(*d*) $\{...., -7, -3, 1, 5, 9, 13, ...\}$ (*e*) $\{.....-20, -10, 0, 10, 20, ...\}$

2. (*i*) $\{a, e\}$ (*ii*) $\{7, 11, 13, 17, 19, 23, 29\}$ (*iii*) $\{1, 2, 3, 4, 5, 6, 7, 8\}$

(*iv*) $\{-2, -3\}$

3. (*a*) $\{1, 2\}$ (*b*) ϕ (*c*) $\{i, -i\}$

4. (*i*) $\{x : x$ is positive integer from 5 to 11$\}$

(*ii*) $\{x : x = 2n,\ n = 1, 2, 3, 4, 5\}$

(*iii*) $\{x : x$ is a two digit number in which the sum of two digits is 9$\}$

5. (*a*) $\{2k + 1 : k \in I$ such that $1 \le k \le 39\}$

(*b*) $\{x \in Q : -1 < x < 1\}$ (*c*) $\{x : x = 2n : n \in I\}$

6. A, C **7.** ϕ **8.** $\{2\}$ **9.** Yes

10. (*a*) True (*b*) True (*c*) True (*d*) True

11. (*a*) True (*b*) False (*c*) True (*d*) True

(*e*) True (*f*) True (*g*) False

12. (*i*) 0 (*ii*) ∞

13. ϕ, $\{1, 2, 3, 4, 5\}$, **E**, **N**, **W** ; $E = \{x : x$ is a natural number$\}$,

$W = \{x : x$ is whole number$\}$

Operation on Sets

1.3. Venn Diagrams

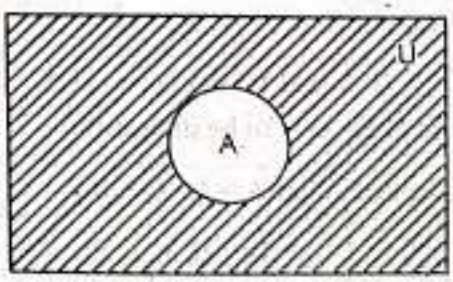
The relations between sets can be illustrated by certain diagrams called Venn diagrams. In a Venn diagram, universal set U is represented by a rectangle and any sub-set of U is represented by a circle within a rectangle U.

1.4. Complement of a Set

Let A be a subset of universal set U. Then the complement of A is the set of all those elements of U which do not belong to A and we denote complement of A by A^c or A'.

We can write

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



A^c is Shaded like

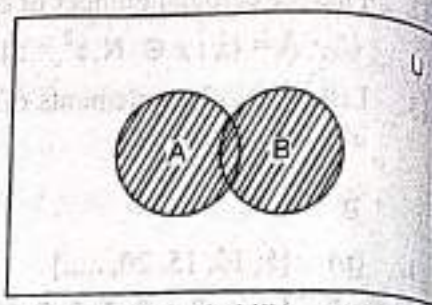
The complement of A is the shaded region

Example : If $U = \{2, 4, 6, 8, 10\}$ $A = \{4, 8\}$ then $A^c = \{2, 6, 10\}$

Note : $U^c = \phi$ and $\phi^c = U$, $(A^c)^c = A$

1.5. Union of Two Sets

If A and B be two given sets, then their union is the set consisting of all the elements of A together with all the elements in B. We should not repeat the elements. The union of two sets A and B is written as A ∪ B.



A ∪ B is Shaded like

The union of two sets A and B

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

Example : Let $A = \{1, 2, 3, 5, 8\}$,

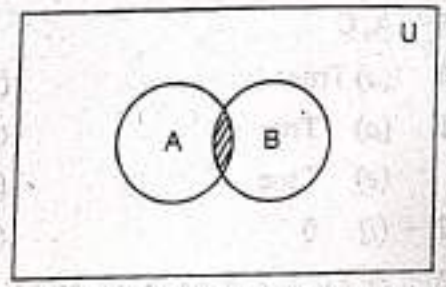
$B = \{2, 4, 6\}$

$\therefore \quad A \cup B = \{1, 2, 3, 4, 5, 6, 8\}$

Note : If $A_1, A_2, \ldots, A_n$ is a fermily of sets, then their union is denoted by $\bigcup_{i=1}^{n} A_i$ or $A_1 \cup A_2 \cup A_3 \ldots \ldots \cup A_n$.

1.6. Intersection of Two Sets

The intersection of two sets A and B, denoted by A ∩ B, is the set of all elements, which are common to A and B.



A ∩ B is Shaded like

The intersection of two sets A and B

In symbols,

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

Example. Let $A = \{2, 4, 6, 8, 10, 12\}$,

$B = \{2, 3, 5, 7, 11\}$

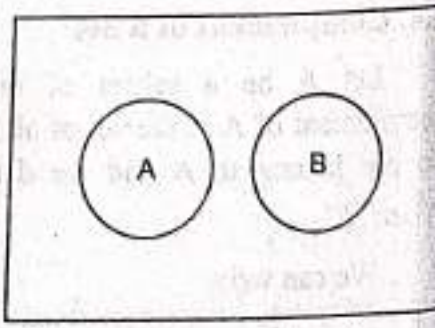
$A \cap B = \{2\}$

Note : If $A_1, A_2, \ldots\ldots, A_n$ is a finite family of sets, then their intersection is denoted by

$$\bigcap_{i=1}^{n} A_i \quad \text{or } A_1 \cap A_2 \cap A_3 \ldots\ldots \cap A_i$$

Disjoint Sets

If A and B two given sets such that $A \cap B = \phi$, then the sets A and B are said to be **disjoint.**



A and B are disjoint sets

Example. Let $A = \{a, b, c, d\}$,

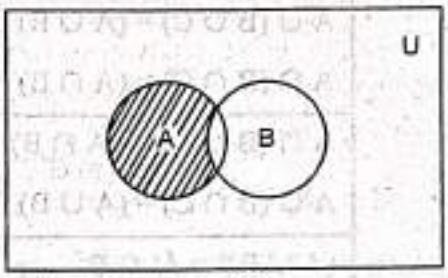
$B = \{l, m, n, p\}$,

$\therefore \quad A \cap B = \phi$

Thus A and B are disjoint sets.

1.7. Difference of Two Sets

The difference of two set A and B is the set of those elements of A which do not belong to B. We denote this by A – B.



A – B is Shaded like

In symbols, we write

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

A – B is also sometimes written as A\ B.

Example . Let $A = \{a, b, c, d, e\}$,

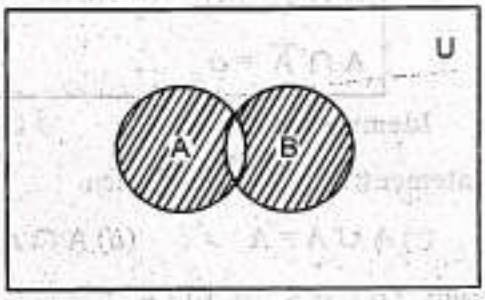
$B = \{c, d, e, f, g\}$

Then $A - B = \{a, b\}$

Note. $B - A \neq A - B$

Symmetric Difference of Two Sets

If A and B are any two sets, then the set $(A - B) \cup (B - A)$ is called symmetric difference of A and B and is denoted by $A \Delta B$.



$A \Delta B$ is Shaded like

In other words, the symmetric difference of A and B consists of all the elements that belong to exactly one of the sets A and B and not to both.

In symbols, we write

$$A \Delta B = \{x : (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A)\}$$

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

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

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

$= \{4\} \cup \{3, 5, 6\} = \{3, 4, 5, 6\}$

1.8. Some Fundamental Laws of Algebra of Sets

Table : Basic Laws of Set Theory

Identity	Name
$A \cup \phi = A$ $A \cap U = A$	Identity Laws
$A \cup U = U$ $A \cap \phi = \phi$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Law
$\overline{(\overline{A})} = A$	Complementation Law
$A \cup B = B \cup A$	Commutative Laws

$A \cap B = B \cap A$	
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^{c'}$	De Morgan's Laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption Laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \phi$	Complement Laws

I. Idempotent Laws

Statement. If A is any set, then

(*i*) $A \cup A = A$ (*ii*) $A \cap A = A$

Proof. (*i*) L.H.S. $= A \cup A$

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

$=$ R.H.S.

(*ii*) L.H.S. $= A \cap A$

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

$=$ R.H.S.

II. Identity Laws

Statement. If A is any set, then

(*i*) $A \cup \phi = A$ (*ii*) $A \cap U = A$

Proof. (*i*) L.H.S. $= A \cup \phi = \{x : x \in A \cup \phi\}$

$= \{x : x \in A \text{ or } x \in \phi\} = \{x : x \in A\}$

$= A$

$=$ R.H.S.

(*ii*) L.H.S. $= A \cap U = \{x : x \in A \cap U\}$

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

$= A =$ R.H.S.

III. Commutative Laws

Statement. If A and B are any two sets, then

(*i*) $A \cup B = B \cup A$ (*ii*) $A \cap B = B \cap A$

Proof. (*i*) L.H.S. $= A \cup B$

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

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

$=$ R.H.S.

(*ii*) L.H.S. $= A \cap B$

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

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

$=$ R.H.S.

IV. Associative Laws

Statement. If A, B and C are any three sets, than

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

Proof. (*i*) L.H.S. $= A \cup (B \cup C)$

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

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

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

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

$=$ R.H.S.

(*ii*) L.H.S. $= A \cap (B \cap C)$

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

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

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

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

$=$ R.H.S.

V. Distributive Laws

Statement. If A, B, C are any three sets, then

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

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

Proof. L.H.S. $= A \cup (B \cap C)$

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

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

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

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

= R.H.S.

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

Note. We can also prove above result by showing that

$A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$

(*ii*) L.H.S. $= A \cap (B \cup C)$

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

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

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

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

= R.H.S.

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

VI. De Morgan's Laws

Statement. If A and B are two sub-sets of U, then

(*i*) $(A \cup B)^c = A^c \cap B^c$

OR

Complement of union of two sets is equal to the intersection of complements of two sets.

(*ii*) $(A \cap B)^c = A^c \cup B^c$

OR

Complement of intersection of two sets is equal to the union of complements of two sets.

Proof. (*i*) L.H.S. $= (A \cup B)^c$

$= \{x : x \in (A \cup B)^c\} = \{x : x \notin (A \cup B)\} = \{x : x \notin A \text{ and } x \notin B\}$

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

$= A^c \cap B^c$

= R.H.S.

$\therefore \quad$ L.H.S. = R.H.S.

$\therefore \quad (A \cup B)^c = A^c \cap B^c$

(*ii*) L.H.S. $= (A \cap B)^c$

$= \{x : x \in (A \cap B)^c\} = \{x : x \notin (A \cap B)\} = \{x : x \notin A \text{ or } x \notin B\}$

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

$= A^c \cup B^c$

= R.H.S.

$\therefore \quad$ L.H.S. = R.H.S.

$\therefore \quad (A \cap B)^c = A^c \cup B^c$

1.9. If A, B are two sets, then prove that $B - A = B \cap A^c$

Proof. L.H.S. $= B - A$

$= \{x : x \in B - A)\} = \{x : x \in B \text{ and } x \notin A\} = \{x : x \in B \text{ and } x \in A^c\}$

$= \{x : x \in (B \cap A^c)\}$

$= B \cap A^c$

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

$\therefore\ B - A = B \cap A^c$

1.10. If A, B, C are any sets, prove that

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

Proof. (*i*) L.H.S. $= A - (B \cup C)$

$= A \cap (B \cup C)^c$ $[\because\ B - A = B \cap A^c]$

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

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

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

$\therefore$ L.H.S. = R.H.S.

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

(*ii*) L.H.S. $= A - (B \cap C) = A \cap (B \cap C)^c$

$= A \cap (B^c \cup C^c) = (A \cap B^c) \cup (A \cap C^c) = (A - B) \cup (A - C)$

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

$\therefore$ L.H.S. = R.H.S.

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

ILLUSTRATIVE EXAMPLES

Example 1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$ and $C = \{1, 5, 9\}$ and let the universal set $U = \{0, 1, 2, \ldots\ldots, 9\}$. Determine

(*a*) $A \cap B$ (*b*) $A \cup B$ (*c*) $B \cup A$ (*d*) $A \cup C$ (*e*) $A \cap C$

(*f*) $A - B$ (*g*) $B - A$ (*h*) A^c (*i*) C^c

Sol. (*a*) $A \cap B = \{x : x \in A \text{ and } x \in B\} = \{2, 3\}$

(*b*) $A \cup B = \{x : x \in A \text{ or } x \in B\} = \{0, 2, 3\}$

(*c*) $B \cup A = \{x : x \in B \text{ or } x \in A\} = \{0, 2, 3\}$

(*d*) $A \cup C = \{x : x \in A \text{ or } x \in C\} = \{0, 2, 3, 5, 9\}$

(*e*) $A \cap C = \{x : x \in A \text{ and } x \in C\} = \{\}$ or ϕ

(*f*) $A - B = \{x: x \in A \text{ and } x \notin B\} = \{0\}$

(*g*) $B - A = \{x : x \in B \text{ and } x \notin A\} = \{\}$ or ϕ

(*h*) $A^c = \{x : x \in U \text{ and } x \notin A\} = \{1, 4, 5, 6, 7, 8, 9\}$

(*i*) $C^c = \{x: x \in U \text{ and } x \notin A\} = \{0, 2, 3, 4, 6, 7, 8\}$

Example 2. Let $A = \{x : x \text{ is an even integer}\}$ and let $B = \{x : x \text{ is an integer divisible by 6 }\}$. Let $C = \{x: x \text{ is an integer divisible by 2 or 3}\}$, and let $D = \{x$ an integer divisible by 2 and 3$\}$. Determine which of the following relations hold. If containment determine whether it is proper

(*a*) $A \subset B$ (*b*) $B \subset C$ (*c*) $C \subset B$ (*d*) $D \subset B$ (*e*) $A \subset D$ (*f*) $D \subset C$ (*g*) $C \subset D$.

Sol. Here $A = \{x : x \text{ is an integer}\} = \{\ldots\ldots -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$

$B = \{x: x \text{ is an integer divisible by } 6\} = \{\ldots\ldots -12, -6, 0, 6, 12, \ldots\}$

$C = \{x: x \text{ is an integer divisible by 2 or 3}\}$

$= \{\ldots\ldots -6, -4, -3, -2, 0, 2, 3, 4, 6, \ldots\ldots\}$

$D = \{x: x \text{ is an integer divisible by 2 and 3}\}$

$= \{\ldots\ldots -12, -6, 0, 6, 12, \ldots\ldots\}$

(*a*) $A \subset B$ does not hold as $-3 \in A$ but $-3 \notin B$

(*b*) $B \subset C$ holds as any integer which is divisible by 6 is also divisible by 2 or 3.

(*c*) $C \subset B$ does not hold as $2 \in C$ but $2 \notin B$.

(*d*) $D \subset B$ holds since $D = B$

(*e*) $A \subset D$ does not hold as $1 \in A$ but $1 \notin D$

(*f*) $D \subset C$ holds as any integer which is divisible by 2 and 3 is also divisible by 2 or 3.

(*g*) $C \subset D$ does not hold as $2 \in C$ but $2 \notin D$.

Example 3. Prove that $A \cup A^c = U$ and $A \cap A^c = \phi$

Sol. Let x be any element $A \cup A^c$

$\Rightarrow \quad x \in A$ or $x \in A^c \quad \Rightarrow \quad x \in A$ or $x \notin A \quad \Rightarrow x \in U$

$\therefore \quad x \in A \cup A^c \Rightarrow x \in U$

$\Rightarrow \quad A \cup A^c \subseteq U$

Conversely, let x be any element of U

$\Rightarrow$ either $x \in A$ or $x \notin A \quad \Rightarrow$ either $x \in A$ or $x \in A^c$

$\Rightarrow \quad x \in A \cup A^c$

$\therefore \quad x \in U \quad \Rightarrow \quad x \in A \cup A^c$

$\therefore \quad U \subseteq A \cup A^c$

From (1) and (2) we get

$A \cup A^c = U$

Further let x be any element of $A \cap A^c$

$\Rightarrow x \in A$ and $x \in A^c \Rightarrow x \in A$ and $x \notin A$. $\Rightarrow x \in \phi$

$\therefore A \cap A^c \subset \phi$

But $\phi \subset A \cap A^c$ always

$\therefore A \cap A^c = \phi$.

Example 4. For sets A and B, prove that $A \cup B = (A \backslash B) \cup (B \backslash A) \cup (A \cap B)$.

Sol. R.H.S. $= (A \backslash B) \cup (B \backslash A) \cup (A \cap B)$

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

$= (A \cap B^c) \cup [(B \cap A^c)] \cup (A \cap B)]$ $[A - B = A \cap B^c]$

$= (A \cap B^c) \cup [(B \cap A^c) \cup (B \cap A)]$ [Commutative Law]

$= (A \cap B^c) \cup [B \cap (A^c \cup A)]$ [Distributive Law]

$= (A \cap B^c) \cup (B \cap X)$ $[A \cup A^c = X]$

$= (A \cap B^c) \cup B$

$= (A \cup B) \cap (B^c \cup B)$ [Distributive Law]

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

$= A \cup B$

$=$ L.H.S.

Example 5. Let A and B be two sets. Prove that

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

Sol. $A \Delta B$ is symmetric difference of sets A and B. It is defined as the set of elements that belong to set A or set B but not to both.

$$A \Delta B = \{x : (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A)\}$$
$$= \{x : (x \in A - B) \text{ or } (x \in B - A)\}$$
$$= \{x : (x \in A - B) \cup (x \in B - A)\}$$
$$= (A - B) \cup (B - A)$$

Hence proved.

Example 6. For sets A, B and C using properties of sets, prove that

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

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

(v) $A \cup B = (A - B) \cup B$.

Sol. (i) $A - (B \cup C) = A \cap (B \cup C)'$ $[\because X - Y = X \cap Y']$

$= A \cap (B' \cap C')$ $[\because (B \cup C)' = B' \cap C]$

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

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

(*ii*) $A - (B \cap C) = A \cap (B \cap C)'$ [$\because X - Y = X \cap Y'$

$= A \cap (B' \cup C')$ [$\because (B \cap C)' = B' \cup C'$

$= (A \cap B') \cup (A \cap C')$ [$\because \cap$ is distribution over

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

(*iii*) $(A \cup B) - C = (A \cup B) \cap C'$ [$\because X - Y = X \cap Y'$

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

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

(*iv*) $A - B = A - (A \cap B)$

Let $x \in A - B$

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

iff $x \in A$ and $x \notin A \cap B$

iff $x \in A - (A \cap B)$

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

(*v*) $A \cup B = (A - B) \cup B$

Let $x \in A \cup B$

iff $x \in A$ or $x \in B$

iff $x \in A$ and $x \notin B$ or $x \in B$

iff $x \in A - B$ or $x \in B$

iff $x \in (A - B) \cup B$

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

Example 7. Prove that : $A \cup B = A \cap B$ iff $A = B$

Sol. (*i*) Assume that $A \cup B = A \cap B$

Let x be any element of A

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

$\Rightarrow x \in A \cap B$ [$\because$ of

$\Rightarrow x \in B$

$\therefore x \in A \Rightarrow x \in B$

$\therefore A \subset B$

Similarly $B \subset A$

From (2) and (3), $A = B$.

$\therefore A \cup B = A \cap B \Rightarrow A = B$

(ii) Assume that $A = B$

$\therefore A \cup B = A \cup A = A$

$A \cap B = A \cap A = A$

$\therefore A \cup B = A \cap B$

$\therefore A = B \Rightarrow A \cup B = A \cap B$

Example 8. Let A and B are any two sets. Prove that $(A - B) \cup B = A \cup B$

Sol. L.H.S. $= (A - B) \cup B = (A \cap B') \cup B$

$= (A \cup B) \cap (B' \cup B)$ (By Distributive Law)

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

Example 9. Let A, B and C be subsets of Set U. Show that $(A \cup B) - (C - A) = (A \cup B) \cap (C' \cup A)$.

Sol. L.H.S. $= (A \cup B) - (C - A) = (A \cup B) - (C \cap A')$

$= (A \cup B) \cap (C \cap A')' = (A \cup B) \cap (C' \cup (A')')$ (By De Morgan's Law)

$= (A \cup B) \cap (C' \cup A)$ $[\because (A')' = A]$

Example 10. For set A, B and C, show that $(A \cup B) - (C - A) = A \cup (B - C)$.

Sol. L.H.S. $= (A \cup B) - (C - A) = (A \cup B) - (C \cap A') = (A \cup B) \cap (C \cap A')'$

$= (A \cup B) \cap (C' \cup (A')')$ (By De Morgan's Law

$= (A \cup B) \cap (C' \cup A)$ $[\because A' = A]$

$= (A \cup B) \cap (A \cup C')$ (Commutative Law)

$= A \cup (B \cap C')$ (Distributive Law)

$= A \cup (B - C)$

$=$ R.H.S.

Example 11. Let A and B be the following subsets of the real numbers :

$A = \{x : 0 < x < 5\}$ and $B = \{x : 2 < x \leq 8\}$. Express $A \cup B$ as the union of three disjoint sets.

Sol. $A = \{x : 0 < x < 5\}$, $B = \{x : 2 < x < 8\}$

We know that

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

Here $(A \backslash B) = \{x : 0 < x \leq 2\}$

$(B \backslash A) = \{x : 5 \leq x < 8\}$

and $A \cap B = \{x : 0 < x < 2\}$

$\therefore A \cup B = \{x : 0 < x \leq 2\} \cup \{x : 5 \leq x < 8\} \cup \{x : 0 < x < 2\}$.

Example 12. Let $X = \{1, 2, 3, 4\}$

If $R = \{\langle x, y\rangle / x \in X \wedge y \in X \wedge (x - y)$ is an integral non-zero multiple of $2\}$

$S = \{\langle x, y\rangle | x \in X \wedge y \in X \wedge (x - y)$ is an integral non-zero multiple of $3\}$

Find $R \cup S$ and $R \cap S$.

Sol. $X = \{1, 2, 3, 4\}$

$R = \{\langle x, y\rangle / x \in X \wedge y \in X \wedge (x - y)$ is an integral non-zero multiple of $2\}$

$= \{\langle 1, 3\rangle, \langle 2, 4\rangle\}$

$S = \{\langle x, y\rangle | x \in X \wedge y \in X \wedge (x - y)$ is an integral non-zero multiple of $3\}$

$= \{\langle 1, 4\rangle\}$

$\therefore \quad R \cup S = \{\langle 1, 3\rangle, \langle 2, 4\rangle, \langle 1, 4\rangle\}$

and $R \cap S = \{\ \}$ or ϕ.

Example 13. For $A = \{1, 2, \{1, 3\}, \phi\}$, determine the following sets :

(*i*) $A - \{1\}$ (*ii*) $A - \phi$ (*iii*) $A - \{\phi\}$ (*iv*) $A - \{1, 2\}$

Sol. We know $A - B = \{x : x \in A$ and $x \notin B\}$

(*i*) $A - \{1\} = \{2, \{1, 3\}, \phi\}$ (*ii*) $A - \phi = A$

(*iii*) $A - \{\phi\} = \{1, 2, \{1, 3\}\}$ (*iv*) $A - \{1, 2\} = \{\{1, 3\}, \phi\}$

Example 14. $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$, $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Find $A \cup B$, $A \cap B$, $A - B$, $\overline{A}$.

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

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

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

$\overline{A} = U - A$

$= \{1, 2, 3, 4, 5, 6, 7, 8, 9\} - \{1, 2, 3\}$

$= \{4, 5, 6, 7, 8, 9\}$

Example 15. Find $A \cup (B \backslash A) = A \cup B$.

Sol. L.H.S. $= A \cup (B \backslash A) = A \cup (B - A)$

$= A \cup (B \cap A^c)$ [$A - B = A$

$= (A \cup B) \cap (A \cup A^c)$ [Distributive

$= (A \cup B) \cap X$ [$A \cup A$

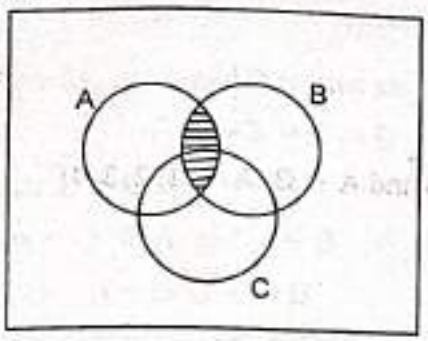
$= A \cup B$ [$A \cap X$

$=$ R.H.S.

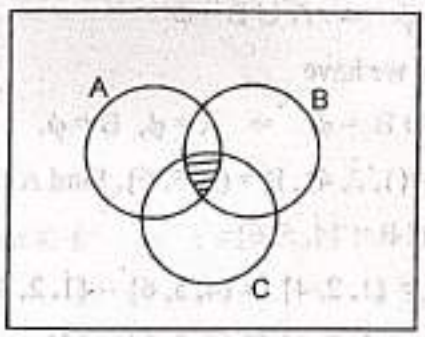
Example 16. Draw venn diagram of $(A \cap B) \cap C$ and $A \cap (B \cap C)$.

Sol.

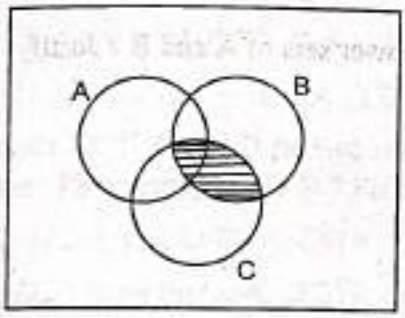
$A \cap B$



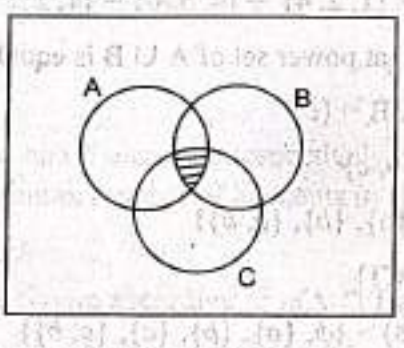
$(A \cap B) \cap C$



$B \cap C$



$A \cap (B \cap C)$



Example 17. If A, B are two sets, then show that $A \cup B = \phi \Leftrightarrow A = \phi, B = \phi$.

Sol. Let $A \cup B = \phi$

We know $A = \phi$, $B = \phi$

Let $x \in A$

$\Rightarrow$ $x \in A \cup B$ $[\because A \subset A \cup B]$

$\Rightarrow$ $x \in \phi$ $[A \cup B = \phi]$

$\therefore$ $A \subseteq \phi$

Also $\phi \subseteq A$

$\therefore$ $A = \phi$

Similarly, we can show $B = \phi$

$\therefore$ $A \cup B = \phi \Rightarrow A = \phi, B = \phi$ ...(1)

Again, let $A = \phi$, $B = \phi$

We show $A \cup B = \phi$

Let $x \in A \cup B$

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

$\therefore$ $A \cup B \subseteq \phi$

Also $\phi = A \cup B$

$\therefore$ $A \cup B = \phi$

$\therefore$ $A = \phi,\ B = \phi \Rightarrow A \cup B = \phi$

From (1) and (2), we have

$A \cup B = \phi \Rightarrow A = \phi,\ B = \phi.$

Example 18. Let $A = \{1, 2, 4\}$, $B = (4, 5, 6)$, Find $A \cup B$, $A \cap B$ and $A - B$. $A = \{1, 2, 3, 4\}$

Sol. $A = \{1, 2, 4\}$ and $B = \{4, 5, 6\}$

(*i*) $A \cup B = \{1, 2, 4\} \cup \{4, 5, 6\} = \{1, 2, 4, 5, 6\}$

(*ii*) $A \cap B = \{1, 2, 4\} \cap \{4, 5, 6\} = \{4\}$

(*iii*) $A - B = \{1, 2, 4\} - (4, 5, 6\} = \{1, 2\}.$

Example 19. Is it true that power set of $A \cup B$ is equal to union of power sets of A and B ? Justify.

Sol. Let $A = \{a, b\}$, $B = \{c\}$

then $A \cup B = \{a, b, c\}$

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

$P(B) = \{\phi, \{C\}\}$

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

where as

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

showing that $P(A \cup B) \neq P(A) \cup P(B)$

Example 20. Prove that $P(A \cap B) = P(A) \cap P(B)$

Sol. Let $X \in P(A \cap B)$

then $X \subseteq (A \cap B)$

$\Rightarrow$ $X \subseteq A$ and also $X \subset B$ ($\because A \cap B \subseteq A$ and also $A \cap$

$\Rightarrow$ $X \in P(A)$ and also $X \in P(B) \Rightarrow X \in P(A) \cap P(B)$

Hence $P(A \cap B) \subseteq P(A) \cap P(B)$

Conversely, let $Y \in P(A) \cap P(B)$

$\Rightarrow$ $Y \in P(A)$ and $Y \in P(B) \Rightarrow Y \subseteq A$ and $Y \subseteq B$

$\Rightarrow$ each element of Y is contained in both A & B $\Rightarrow$ each element of Y is contained in $A \cap$

$\Rightarrow$ $Y \subseteq A \cap B \Rightarrow Y \in P(A \cap B)$

Hence $P(A) \cap P(B) \subseteq P(A \cap B)$

From (1) and (2); we get

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

Example 21. Find power set P(A) of A = {1, 2, 3, 4}.

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

Example 22. Let A and B be two sets. Prove that

$$A - B = A \cap B^c$$

Sol. Let $x \in A - B$

$\Rightarrow$ $x \in A$ and $x \notin B$ $\Rightarrow$ $x \in A$ and $x \in B^c$ $\Rightarrow$ $x \in A \cap B^c$

$\therefore$ $A - B \subseteq A \cap B^c$ ...(*i*)

Conversely let $x \in A \cap B^c$, then

$\Rightarrow$ $x \in A$ and $x \in B^c$ $\Rightarrow$ $x \in A$ and $x \notin B$ $\Rightarrow$ $x \in A - B$

$\therefore$ $A \cap B^c \subseteq A - B$

$\therefore$ $A - B = A \cap B^c$. ...(*ii*)

Example 23. If A and B be two sets containing 3 and 6 elements respectively, what can be the minimum number of elements in A $\cup$ B ? Find also, the maximum number of elements in A $\cup$ B.

Sol. We have $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

This shows that $n(A \cup B)$ is minimum or maximum according as $n(A \cap B)$ is maximum or minimum respectively.

Case I : When $n(A \cap B)$ is minimum, *i.e.* $n(A \cap B) = 0$. This is possible only when $A \cap B = \phi$. In this case, $n(A \cup B) = n(A) + n(B) - 0 = n(A) + n(B) = 3 + 6 = 9$. So, maximum number of elements in A $\cup$ B is 9.

Case II : When $n(A \cap B)$ is maximum.

This is possible only when $A \subseteq B$. In this case, $n(A \cap B) = 3$.

$\therefore$ $n(A \cup B) = n(A) + n(B) - n(A \cap B) = 3 + 6 - 3 = 6$

so, minimum number of elements in A $\cup$ B is 6.

EXERCISE 1.2

1. Let A = {0, 2, 3}, B = {2, 3} and C = {1, 5, 9}. Let D = {3, 2} and let E = {2, 3, 2}. Determine which of the following are true. Give reason for your decisions.
   (*a*) A = B (*b*) B = C (*c*) B = D (*d*) B = E (*e*) $A \cap B = B \cap A$
   (*f*) $A \cup B = B \cup A$ (*g*) $A - B = B - A$
2. Determine whether each of the following inclusions is proper :
   (*a*) $A \subset B$ where A = {*x* : *x* is an odd prime} and B = {*x* : *x* is an integer not divisible by 2}
   (*b*) $S \subset T$, where S = {*x* : *x* is a real number with *a* finite decimal expansion}, and T = {*x* : *x* is a rational number}
   (*c*) $X \subset Y$, where X = {*x* : x^2 is integer divisible by 9} and Y = {*x* : *x* is an integer divisible by 3}

3. Prove that each of the following relations holds

(*a*) $A \subset B$ where $A = \{x : x \text{ is an integer multiple of } 10\}$ and $B = \{x : x \text{ is an integer multiple of } 5\}$

(*b*) $A = B$, where $A = \{x : x \text{ is even integer}\}$ and $B = \{x : x^2 \text{ is an even integer}\}$

4. Let $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $A = \{x \in U : x \text{ multiple of } 3\}$,

$B = \{x \in U : x^2 - 5 \geq 0\}$.

Determine (*a*) $A \cup B$ (*b*) $A \cap B$ (*c*) B^c

5. Let A and B be subsets of natural numbers defined as follows :

$A = \{x$: if p is prime and if x is divisible by p, then x is divisible by $p^2\}$

and $B = \{x$: there is an integer y such that $x = y^2\}$.

Prove that $B \subset A$. Show that the containment is proper.

6. Let U be the set of letters of the alphabet. Let $A = \{a, b, c, \ldots\ldots, l\}$, $B = \{h, i, j \ldots\ldots, q\}$ and $C = \{o, p, q, \ldots\ldots z\}$. Find the elements in each of the following set :

(*a*) $A \cap B$ (*b*) $A \cup C$ (*c*) $A \cap (B \cup C)$ (*d*) $(A \cap B) \cup C$ (*e*) $A^c \cap B^c$

(*f*) $(A \cap B)^c$ (*g*) $A \backslash B$ (*h*) $B \backslash A$ (*i*) $A \backslash (B \backslash C)$ (*j*) $A \backslash (C \backslash B)$

7. Let U be the set of integers and let $A = \{x : x \text{ is divisible by } 3\}$, let $B = \{x : x \text{ is divisible by } 2\}$. Let $C = \{x : x \text{ is divisible by } 5\}$ Find the elements in each of following set :

(*a*) $A \cap B$ (*b*) $A \cup C$ (*c*) $A \cap (B \cup C)$ (*d*) $(A \cap B) \cup C$ (*e*) $A^c \cap B^c$

(*f*) $(A \cap B)^c$ (*g*) $A \backslash B$ (*h*) $B \backslash A$ (*i*) $A \backslash (B \backslash C)$ (*j*) $A \backslash (C \backslash B)$

8. Answer true or false

(*a*) $A^c \cup B^c = (A \cup B)^c$ (*b*) $A^c = U \backslash A$ (*c*) $A \cup (B \cup C) = (A \cup B) \cup C$

(*d*) $A \cup (B \cap C) = (A \cup B) \cap C$ (*e*) $A \backslash (B \backslash C) = (A \backslash B) \backslash C$

9. Let $A = \{a, b, c, d, e\}$, $B = \{a, b\}$, $C = \{B, \phi\}$, $D = \{a, b, \{a, b\}\}$. Find $A \cap B$, $C \cap D$, $A \cap D$, $C \cap$ and $D \cap P(A)$. Indicate whether, each of the following is true or false :

(*a*) $A \in P(A)$ (*b*) $C \subset P(A)$ (*c*) $D \subset P(A)$ (*d*) $B \subset D$

(*e*) $B \in D$ (*f*) $\{a, b\} \in C$

10. Prove that if $A \subset B$ and $B \subset C$, then $A \subset C$.

11. Prove that $A \backslash B$ and $B \backslash A$ are disjoints.

12. Prove that if $A \subset B$, then $P(A) \subset P(B)$.

13. Let A and B sets, then $(A \cap B) \cup (A \cap B^c) = A$.

14. Let A, B, C be sets. If $A \subseteq B$ and $B \cap C = \phi$, then $A \cap C = \phi$.

15. Prove that $A' - B' = B - A$.

ANSWERS

1. (a) False (b) False (c) True (d) True (e) True (f) True (g) False
2. (a) Proper (b) Not proper (c) Not proper
4. (a) {0, 3, 4, 5, 6, 7, 8, 9} (b) {3, 6, 9} (c) {0, 1, 2}
6. (a) {h, i, j, k, l} (b) {a, b, c, ..., j, k l, o, p, q.....X}
   (c) { n, i, j, k, l} (d) {h, i, j, k, l, o, p, q, ..., z}
   (e) {r, s, t,....., z} (f) {a, b, c, d, e, f, g, m, n, o, p, ..., z}
   (g) {a, b, c, d, e, f, g} (h) {m, n, o, p, q}
   (i) {a, b, c, d, e, f, g} (j) {a, b, c,....., l}
7. (a) {.....– 12, – 6, 0, 6, 12,.....}
   (b) {.....– 9, – 6, – 5, – 3, 0, 3, 5, 6,.....}
   (c) {.....– 15, – 12, – 6, 0, 6, 12, 15,.....}
   (d) {.....– 12, – 10, 6, – 5, 0, 5, 6, 10, 12,.....}
   (e) {.....– 11, – 7, – 5, – 1, 1, 5, 7, 11,.....}
   (f) {–7, – 5, – 3, – 2, – 1, 1, 2, 3, 4, 5,.....}
   (g) {.....– 15, – 9, – 3, 3, 9, 15,.....}
   (h) {.....– 10, – 8, – 4, – 2, 2, 4, 8, 10.....}
   (i) {.....– 15, – 9, – 3, 3, 9, 15,.....}
   (j) {....., – 18, – 12, – 9, – 6, – 3, 0, 3, 9, 12, 18.....}
8. (a) False (b) True (c) True (d) False (e) False
9. (a) True (b) True (c) False (d) False (e) True (f) True

1.11. Some Important Problems

We give below some other important problems on union and intersection.

ILLUSTRATIVE EXAMPLES

Example 1. Give examples of three sets A, B, C for which $A - (B - C) = (A - B) - C$

Sol. Take $A = \{1, 2, 3\}, B = \{3, 4, 5\}, C = \{6, 7\}$

$\therefore \quad B - C = \{3, 4, 5\} - \{6, 7\} = \{3, 4, 5\}$

$A - (B - C) = \{1, 2, 3\} - \{3, 4, 5\} = \{1, 2\}$ ...(1)

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

$(A - B) - C = \{1, 2\} - \{6, 7\} = \{1, 2\}$ ...(2)

From (1) and (2), we get,

$A - (B - C) = (A - B) - C$

Example 2. Give an example of three sets A, B and C such that

$A \cap B \neq \phi, B \cap C \neq \phi, A \cap C \neq \phi$ but $A \cap B \cap C = \phi$

Sol. Let $A = \{1, 2, 3\}, B = \{3,4, 5\}, C = \{4, 5, 2\}$

$\therefore \quad A \cap B = \{3\} \neq \phi, B \cap C = \{4, 5\} \neq \phi, C \cap A = \{2\} \neq \phi$

But $A \cap B \cap C = \phi$

Example 3. Prove that $A \subset B \Leftrightarrow B^c \subset A^c$ for all sets A, B.

Sol. (*i*) Assume that $A \subset B$

We are to prove that $B^c \subset A^c$

Let x be an element of B^c

$\therefore \quad x \in B^c$

$\therefore x \notin B$

$\Rightarrow \quad x \notin A$ [∵ o

$\Rightarrow \quad x \in A^c$

$\therefore \quad B^c \subset A^c$

$\therefore \quad A \subset B \quad \Rightarrow \quad B^c \subset A^c$

(*ii*) Assume that $B^c \subset A^c$

We are to prove that $A \subset B$.

Let y by any element of A.

$\therefore \quad y \in A \Rightarrow y \notin A^c$

$\Rightarrow \quad y \notin B^c$ [∵ o

$\Rightarrow \quad y \in B$

$\therefore \quad A \subset B$

$\therefore \quad B^c \subset A^c \Rightarrow A \subset B$

Combining the results proved in (*i*) and (*ii*), we get,

$A \subset B \Leftrightarrow B^c \subset A^c$

Example 4. If A, B and C are any sets, prove that

$A \cup B = A \cup C$ and $A \cap B = A \cap C \quad \Rightarrow \quad B = C$

Sol. Let x be any element of B

$\therefore \quad x \in A \quad$ or $\quad x \notin A.$

Case I. $x \in A$

$\therefore \quad x \in A \cap B$

$\Rightarrow \quad x \in A \cap C \qquad [\because \ A \cap B = A \cap C]$

$\Rightarrow \quad x \in C \qquad [\because \ x \in B]$

But x is any element of B

$\therefore \quad B \subset C$

Case II. $x \notin A$

$\therefore \quad x \in A \cup B$

$\Rightarrow \quad x \in A \cup C \qquad [\because \ A \cup B = A \cup C]$

$\Rightarrow \quad x \in C \qquad [\because \ x \notin A]$

But x is any element of B

$\therefore \quad B \subset C$

$\therefore$ from both the cases, it is clear that

$$B \subset C \qquad \ldots (1)$$

Similarly $\quad C \subset B \qquad \ldots (2)$

From (1) and (2), $B = C$

$\therefore \quad A \cup B = A \cup C$ and $A \cap B = A \cap C \Rightarrow B = C.$

Example 5. For any sets A and B, prove that

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

Sol. R.H.S. $= (A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)' \qquad [\because \ A - B = A \cap B']$

$= (A \cup B) \cap (A' \cup B') = [(A \cup B) \cap A'] \cup [(A \cup B) \cap B']$

$= [(A \cap A') \cup (B \cap A')] \cup [(A \cap B') \cup (B \cap B')]$

$= [\phi \cup (B \cap A')] \cup [(A \cap B') \cup \phi]$

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

$=$ L.H.S.

Example 6. Show that $A \cap (B - C) = (A \cap B) - (A \cap C)$

Sol. R.H.S. $= (A \cap B) - (A \cap C) = (A \cap B) \cap (A \cap C)^c = (A \cap B) \cap (A^c \cup C^c)$

$= [(A \cap B) \cap A^c] \cup [(A \cap B) \cap C^c] = [(A \cap A^c) \cap B] \cup [A \cap (B \cap C^c)]$

$= (\phi \cap B) \cup [A \cap (B - C)] = \phi \cup [A \cap (B - C)]$

$= A \cap (B - C)$

$=$ L.H.S.

EXERCISE 1.3

1. Verify the following identities :

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

   where, A, B, C are three sets defined by

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

2. If X and Y are two sets, then find $X \cap (X \cup Y)^c$.

3. Show that (*i*) $A \subset A \cup B$ (*ii*) $A \cap B \subset A$.

4. Prove the following :

   (*i*) $B \subset A \cup B$ (*ii*) $A \cap B \subset B$ (*iii*) $B \subset A \Leftrightarrow A \cap B = B$

   (*iv*) $A \subset C$ and $B \subset D \Rightarrow A \cup B \subset C \cup D$ (*v*) $B \subset C \Rightarrow A \cap B \subset A \cap C$

   (*vi*) $A = B \Leftrightarrow A \subset B$ and $B \subset A$.

5. For any two sets A and B, prove that $A \cap B = \phi \Rightarrow A \subset B^c$.

6. Prove that

   (*i*) $A \cap (A' \cup B) = A \cap B$ (*ii*) $A - (A - B) = A \cap B$

7. Prove that $A^c \setminus B^c = B \setminus A$.

8. Prove the following :

   (*i*) $(A - B) \cap B = \phi$ (*ii*) $A \cap (B - A) = \phi$ (*iii*) $A \cup (B - A) = A \cup B$

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

   (*vi*) $(A - B) - C = A - (B \cup C) = (A - B) \cap (A - C)$ (*vii*) If $A \subset B$, then $B - (B - A) =$

9. Prove that $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

ANSWERS

2. ϕ

SECTION-II
RELATIONS

1.12. Ordered Pair

Let A and B be two given non-empty sets. If $a \in A$ and $b \in B$, then (a, b) denotes an ordered pair whose first component is a and the second component is b.

The ordered pair (a, b) and (b, a) are different unless $a = b$. Also two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.

Note 1. Ordered pairs (2, 5) and (5, 2) are not equal whereas the sets {5, 2} and {2, 5} are equal.

Note 2. In the definition of an ordered pair, a and b may not be distinct *i.e.*, (a, a) and (b, b) are also ordered pairs.

1.13. Cartesian Product of Sets

Cartesian Product of Two Sets. If A and B are two non-empty sets, then the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$ is called the cartesian product of sets A and B and is denoted by $A \times B$..

In symbols, $A \times B = \{ (a, b) : a \in A, b \in B\}$

Note 1. $A \times B$ and $B \times A$ are different sets if $A \neq B$.

2. $A \times B = \phi$ when one or both of A, B are empty.

Cartesian Product of Three Sets. The set of all ordered triplets (a, b, c), of elements

$a \in A$, $b \in B$, $c \in C$ is called the Cartesian product of the three sets A, B, C and is denoted by $A \times B \times C$.

We know that

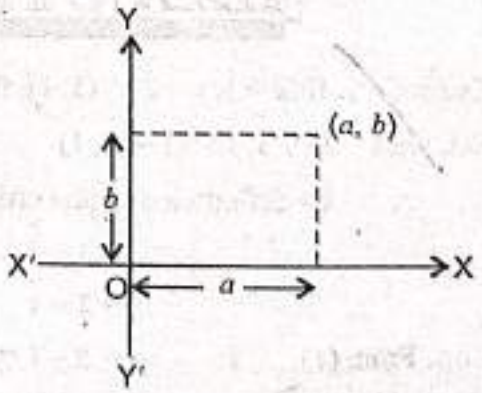
$$A^2 = A \times A = \{(x, y) : x, y \in A\}$$

$$\therefore \quad A^3 = A \times A \times A = \{x, y, z) : x, y, z \in A\}$$

1.14. Graphical Representation of A × B

Draw two perpendicular lines X'OX and Y'OY intersecting at O, where X'OX is horizontal and Y'OY is vertical. Now on horizontal line X'OX represent the elements of A and on vertical line Y'OY, represent the elements of B.

Now if $a \in A$, $b \in B$, draw a vertical line through a and a horizontal line through b. The point where they meet represents the ordered pair (a, b), The set of all such points obtained graphically represents $A \times B$.



Note 1. If A is the set of all numbers, then A consists of all points in a line. A × A will consist of all points in the plane.

Note 2. The ordered pair (a, b) represents a point whose co-ordinates are (a, b).

Note 3. Let n (A) denote the number of elements of A.

Then n (A × B) = n (A) × n (B).

1.15. Prove that

(*i*) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ (*ii*) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Proof. (*i*) L.H.S. $= A \times (B \cup C)$

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

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

$= \{(x, y) : (x, y) \in (A \times B) \text{ or } (x, y) \in (A \times C)\}$

$= \{(x, y) : (x, y) \in (A \times B) \cup (A \times C)\} = (A \times B) \cup (A \times C)$

= R.H.S.

$\therefore A \times (B \cup C) = (A \times B) \cup (A \times C)$

(*ii*) L.H.S. $= A \times (B \cap C)$

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

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

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

$= \{(x, y) : (x, y) \in (A \times B) \cap (A \times C)\} = (A \times B) \cap (A \times C)$

= R.H.S.

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

ILLUSTRATIVE EXAMPLES

Example 1. If $(x + 1, y - 2) = (3, 1)$, find the values of x and y.

Sol. Here $(x + 1, y - 2) = (3, 1)$

$\therefore$ by definition of equal ordered pairs,

$x + 1 = 3$ ...(1)

$y - 2 = 1$ ...(2)

From (1), $x = 3 - 1 = 2$

From (2), $y = 1 + 2 = 3$

$\therefore$ $x = 2, y = 3$.

Example 2. If G = {7, 8} and H = {5, 4, 2}, find G × H and H × G.

Sol. G = {7, 8}, H = {5, 4, 2}

∴ G × H = {7, 8} × {5, 4, 2} = {(7, 5), (7, 4), (7, 2), (8, 5), (8, 4), (8, 2)}

H × G = {5, 4, 2} × {7, 8} = {(5, 7), (5, 8), (4, 7), (4, 8), (2, 7), (2, 8)}

Example 3. If A × B = {(*a*, *x*), (*a*, *y*), (*b*, *x*), (*b*, *y*)}, find A and B.

Sol. A × B = {(*a*, *x*), (*a*, *y*), (*b*, *x*), (*b*, *y*)}

∴ A = set of first elements = {*a*, *b*}

and B = set of second elements = {*x*, *y*}

Example 4. The cartesian product A × A has a elements among which are found (–1, 0) and (0, 1). Find the set A and the remaining elements of A × A.

Sol. Since (–1, 0) ∈ A × A and (0, 1) ∈ A × A

∴ –1, 0 ∈ A and 0, 1, ∈ A ⇒ –1, 0, 1 ∈ A.

Now A × A has 9 elements ⇒ A has 3 elements

∴ A = {–1, 0, 1}

Remaining elements of A × A and (–1, –1), (–1, 1), (0, –1), (0, 0), (1, –1), (1, 0), (1, 1)

Example 5. Let A = {1, 2, 3}, B = {3, 4} and C = {4, 5, 6}. Find

(*i*) A × (B ∩ C) (*ii*) (A × B) ∩ (A × C) (*iii*) A × (B ∪ C) (*iv*) (A × B) ∪ (A × C).

Sol. Here A = {1, 2, 3}, B = {3, 4}, C = {4, 5, 6}

∴ B ∪ C = {3, 4} ∪ {4, 5, 6} = {3, 4, 5, 6}

B ∩ C = {3, 4} ∩ {4, 5, 6} = {4}

A × B = {1, 2, 3} × {3, 4} = {(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)}

A × C = {1, 2, 3} × {4, 5, 6} = {(1, 4, (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)}

(*i*) A× (B ∩ C) = {1, 2, 3} × {4} = {(1, 4), (2, 4), (3, 4)}

(*ii*) (A × B) ∩ (A × C) = {(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)}

∩ {(1, 4), (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)}

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

(*iii*) A × (B ∪ C) = {1, 2, 3} × {3, 4, 5, 6}

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

(*iv*) (A×B) ∪ (A × C) = {(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4)}

∪ {(1, 4), (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)}

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

Example 6. Let $A = \left\{\frac{1}{2}, 2\right\}$, $B = \{2, 3, 5\}$, $C = \{-1, -2\}$, then verify that

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

Sol. Here $A = \left\{\frac{1}{2}, 2\right\}$, $B = \{2, 3, 5\}$, $C = \{-1, -2\}$

$\therefore \quad B \cup C = \{2, 3, 5\} \cup \{-1, -2\} = \{2, 3, 5, -1, -2\}$

$$A \times B = \left\{\frac{1}{2}, 2\right\} \times \{2, 3, 5\} = \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3), (2, 5)\right\}$$

$$A \times C = \left\{\frac{1}{2}, 2\right\} \times \{-1, -2\} = \left\{\left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, -1)\ (2, -2)\right\}$$

$$\text{L.H.S.} = A \times (B \cup C) = \left(\frac{1}{2}, 2\right) \cup \{2, 3, 5, -1, -2\}$$

$$= \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), \left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, 2), (2, 3), (2, 5)\ (2, -1), (2, -2)\right\}$$

$$\text{R.H.S.} = (A \times B) \cup (A \times C)$$

$$= \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3)\ (2, 5)\right\} \cup \left\{\left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, -1), (2, -2)\right\}$$

$$= \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), \left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, 2), (2, 3), (2, 5), (2, -1), (2, -2)\right\}$$

$\therefore$ L.H.S. = R.H.S.

Example 7. Let $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ and $C = \{4, 5\}$. Verify that $A \times (B \cap C) = (A \times B) \cap (A \times$

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

$B \cap C = \{2, 3, 4\} \cap \{4, 5\} = \{4\}$

$L.H.S. = A \times (B \cap C) = \{1, 2, 3\} \times \{4\} = \{(1, 4), (2, 4), (3, 4)\}$

Now $A \times B = \{1, 2, 3\} \times \{2, 3, 4\} = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$

$A \times C = \{1, 2, 3\} \times \{4, 5\} = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$

$R.H.S. = (A \times B) \cap (A \times C)$

$= \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$

$\cap \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3,$

$= \{(1, 4), (2, 4), (3, 4)\}$

$\therefore \quad L.H.S. = R.H.S.$

Example 8. Let A be a non-empty set such that $A \times B = A \times C$. Show that $B = C$.

Sol. Here $A \times B = A \times C$

Let b be any element of B. ...(1)

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

$\Rightarrow$ $(a, b) \in A \times C$

$\Rightarrow$ $b \in C$ [$\because$ of (1)]

$\therefore$ $b \in B \Rightarrow b \in C$

$\therefore$ $B \subset C$

Let c be any element of C ...(2)

$\therefore$ $(a, c) \in A \times C \ \forall \ a \in A$

$\Rightarrow$ $(a, c) \in A \times B$

$\therefore$ $c \in B$ [$\because$ of (1)]

$\therefore$ $c \in C \Rightarrow c \in B$

$\therefore$ $C \subset B$

From (2) and (3), we get ...(3)

$B = C$.

Example 9. For any three sets A, B, C prove that $(A - B) \times C = (A \times C) - (B \times C)$

Sol. L.H.S. $= (A - B) \times C$

$= \{(x, y) : x \in (A - B) \text{ and } y \in C\} = \{(x, y) : (x \in A \text{ and } x \notin B) \text{ and } y \in C\}$

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

$= \{(x, y) : (x, y) \in (A \times C) \text{ and } (x, y) \notin (B \times C)\}$

$= \{(x, y) : (x, y) \in (A \times C) \setminus (B \times C)\} = (A \times C) \setminus (B \times C) = (A \times C) - (B \times C)$

$=$ R.H.S.

Example 10. Let $A = \left\{\frac{1}{2}, 2\right\}$, $B = \{2, 3, 5\}$, $C = \{-1, -2\}$, then verify that $A \times (B - C) = (A \times B) - (A \times C)$.

Sol. Here $A = \left\{\frac{1}{2}, 2\right\}$, $B = \{2, 3, 5\}$, $C = \{-1, -2\}$

$\therefore$ $B - C = \{2, 3, 5\} - \{-1, -2\} = \{2, 3, 5\}$

$$A \times B = \left\{\frac{1}{2}, 2\right\} \times \{2, 3, 5\} = \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3), (2, 5)\right\}$$

$$A \times C = \left\{\frac{1}{2}, 2\right\} \times \{-1, -2\} = \left\{\left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, -1), (2, -2)\right\}$$

$$\text{L.H.S.} = A \times (B - C) = \left\{\frac{1}{2}, 2\right\} \times \{2, 3, 5\} = \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3), (2, 5)\right\}$$

$$\text{R.H.S.} = (A \times B) - (A \times C)$$

$$= \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3), (2, 5)\right\} - \left\{\left(\frac{1}{2}, -1\right), \left(\frac{1}{2}, -2\right), (2, -1), (2, -2)\right\}$$

$$= \left\{\left(\frac{1}{2}, 2\right), \left(\frac{1}{2}, 3\right), \left(\frac{1}{2}, 5\right), (2, 2), (2, 3), (2, 5)\right\}$$

$\therefore$ L.H.S. = R.H.S.

Example 11. If A and B be non-empty subsets, then show that $A \times B = B \times A$ iff $A = B$

Sol. (*i*) Assume that $A \times B = B \times A$ ...(

Let x be any element of A.

Now $x \in A \Rightarrow (x, y) \in A \times B \; \forall y \in B$

$\Rightarrow (x, y) \in B \times A$ [$\because$ of (

$\Rightarrow x \in B$

$\therefore x \in A \Rightarrow x \in B$

$\therefore A \subset B$ ...(I)

Let z be any element of B

Now $z \in B \Rightarrow (t, z) \in A \times B \; \forall t \in A$

$\Rightarrow (t, z) \in B \times A$ [$\because$ of (

$\Rightarrow z \in A$

$\therefore z \in B \Rightarrow z \in A$

$\therefore B \subset A$ ...(II)

From (I) and (II), we get,

$A = B$

(*ii*) Assume that $A = B$ ...

$\therefore A \times B = A \times A$ [$\because$ of (

and $B \times A = A \times A$ [$\because$ of (

$\therefore$ we have, $A \times B = B \times A$

Hence $A \times B = B \times A$ iff $A = B$

EXERCISE 1.4

1. If $\left(\frac{x}{3} + 1, y - \frac{2}{3}\right) = \left(\frac{5}{3}, \frac{1}{3}\right)$, find the values of x and y.

2. If the set A has 3 elements and the set $B = \{3, 4, 5\}$, then find the number of elements in $(A \times B$

3. If $P = \{a, b, c\}$ and $Q = \{r\}$, form the sets $P \times Q$ and $Q \times P$. Are these two products equal ?

4. If $P = \{1, 2\}$, form the set $P \times P \times P$.
5. If $\mathbf{R}$ is the set of all real numbers, what do the cartesian products $\mathbf{R} \times \mathbf{R}$ and $\mathbf{R} \times \mathbf{R} \times \mathbf{R}$ represent ?
6. If $A \times B = \{(p, q), (p, r), (m, q), (m, r)\}$, find A and B.
7. Let $A = \{1, 2\}$ and $B = \{3, 4\}$. Write $A \times B$. How many subsets will $A \times B$ have ? List them.
8. State whether each of the following statements are true or false. If the statement is false, rewrite the given statement correctly.
   (*i*) If $P = \{m, n\}$ and $Q = \{n, m\}$, then $P \times Q = \{(m, n), (n, m)\}$.
   (*ii*) If A and B are non-empty sets, then $A \times B$ is a non-empty set of ordered pairs (x, y) such that $x \in A$ and $y \in B$.
   (*iii*) If $A = \{1, 2\}$, $B = \{3, 4\}$, then $A \times (B \cap \phi) = \phi$.
9. Let A and B be two sets such that $n(A) = 5$ and $n(B) = 2$.
   If $(a_1, 2), (a_2, 3), (a_3, 2), (a_4, 3), (a_5, 2)$ are in $A \times B$ and a_1, a_2, a_3, a_4 and a_5 are distinct. Find A and B.
10. Let A and B be two sets such that $n(A) = 3$ and $n(B) = 2$. If $(x, 1), (y, 2), (z, 1)$ are in $A \times B$, find A and B, where x, y, z are distinct elements.
11. Let $A = \{1, 2\}$, $B = \{1, 2, 3, 4\}$, $C = \{5, 6\}$ and $D = \{5, 6, 7, 8\}$. Verify that
   (*i*) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
   (*ii*) $A \times C$ is a subset of $B \times D$.
12. Let $A = \{1, 2, 3\}$, $B = \{4\}$ and $C = \{5\}$. Verify that
   (*i*) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
   (*ii*) $A \times (B - C) = (A \times B) - (A \times C)$.
13. Let $A = \{1, 2, 3, 4\}$ and $S = \{(a, b) : a \in A, b \in A, a \text{ divides } b\}$. Write S explicitly.
14. A, B, C are any three sets, then prove that $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
15. If A, B, C are any three sets, then prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$
16. For any three sets A, B, C, prove that $A \times (B - C) = (A \times B) - (A \times C)$.
17. Prove that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
18. Let A and B be two non-empty sets having n elements in common. Prove that $A \times B$ and $B \times A$ have n^2 elements in common.

ANSWERS

1. $x = 2, y = 1$ 2. 9 3. No
4. $\{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$
5. Coordinates of all the points in two dimensional space
   Coordinates of all the points in three dimensional space
6. $A = \{p, m\}$, $B = \{q, r\}$

7. Subsets of A × B are

ϕ, {(1, 3)}, {(1, 4)}, {(2, 3)}, {(2, 4)}, {(1, 3), (1, 4)},
{(1, 3), (2, 3)}, {(1, 3), (2, 4)}, {(1, 4), (2, 3)}, {(1, 4), (2, 4)},
{(2, 3), (2, 4)} ; {(1, 3), (1, 4), (2, 3)}, {(1, 3), (1, 4), (2, 4)},
{(1, 4), (2, 3), (2, 4)}, {(1, 3), (2, 3), (2, 4)}, A × B

A × B has 16 subsets.

8. (*i*) False

Here P = {*m*, *n*}, Q = {*n*, *m*}

∴ P × Q = {(*m*, *n*), (*m*, *m*), (*n*, *n*), (*n*, *m*)}

is the correct statement.

(*ii*) True (*iii*) True

9. A = { a_1, a_2, a_3, a_4, a_5 }, B = {2, 3}

10. A = {*x*, *y*, *z*}, B = {1, 2}

13. {(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)}

1.16. Relation

A relation R from a non-empty set A to a non-empty set B is a subset of the cartesian product A × The subset is derived by describing a relationship between the first element and the second element of ordered pairs in A × B. The second element is called the **image** of the first element.

Let R be a relation from A into B. If $(a, b) \in R$, then we write it as a R b and read it, a is in rela to b.

If $(a, b) \notin R$, then we write it an a R b and read it, a is not related to b by the relation R.

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

∴ A × B = {1, 2, 3} × {4, 5} = {(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)}

Now any subset of A × B is a relation from A into B.

Consider

R_1 = {(1, 4), (2, 5), (3, 4)}

R_2 = {(1, 2), (3, 5)}

Clearly R_1 is a relation from A into B as R_1 is a subset of A × B.

Now 1 R 4, 2 R 5, 3 R 4

Again R_2 is not a relation from A into B as R_2 is not a subset of A × B. Here 1 $\not R$ 2.

1.17. Domain and Range of a Relation

If R is a relation from a set A to a set B. Then the set of the first components of the elements of called the domain of R and the set of the second components of the elements of R is called the range of

Thus, domain of R = { a : $(a, b) \in R$}, and range of R = { b : $(a, b) \in R$}.

The whole set B is called the codomain of the relation R.

If R is a relation from a set A to the set A, then R is called **a relation on A**. Thus a relation on a set A is defined as any subset of $A \times A$.

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

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

Let $R = \{(1, 2), (2, 2), (3, 2), (3, 3)\}$.

Then $R \subseteq A \times A$. Therefore R is a relation on the set A.

Since $(1, 2) \in R$, therefore 1 R 2 *i.e.*, 1 is R related to 2.

Again, since $(1,1) \notin R$ so 1 R 1 *i.e.*, 1 is not R related to 1.

Domain of $R = \{1, 2, 3\}$.

Range of $R = \{2, 3\}$.

Example : For any $a, b \in \mathbf{N}$, the set of natural numbers, define a relation R by a R b if a divides b.

Then $R = \{(1, 1), (1, 2), (1, 3), \ldots, (2, 2), (2, 4), \ldots (3, 3), (3, 6), \ldots\}$

Then R is clearly a subset of $\mathbf{N} \times \mathbf{N}$ and hence a relation on **N**.

$(1, 2) \in R$ since 1 divides 2

$(2, 1) \notin R$ since 2 does not divide 1.

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

Then $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$

Let $R = \{(1, 3), (2, 4)\}$

Then $R \subseteq A \times B$ and hence R is a relation from A to B.

1 R 3 since $(1,3) \in R$.

1 R 4 since $(1,4) \notin R$.

Domain of $R = \{1, 2\}$.

Range of $R = \{3, 4\}$.

1.18. Representation of Relations

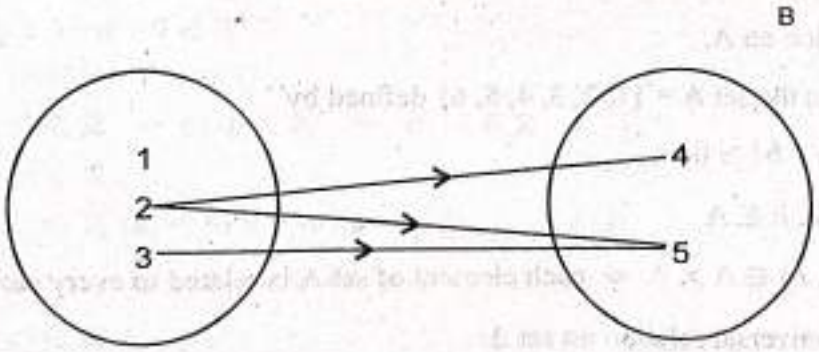
A relation may be represented algebraically either by the **Roster method** or by the **Set-builder method.**

Graphical and Tabular Methods.

Another method is that of an arrow diagram which is a visual representation of a relation.

Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Then relation

$R = \{(2, 4), (2, 5), (3, 5)\}$ from A into B is represented by arrow diagram as shown in the figure given below :



Above relation R can be represented in **tabular form** as follows :

R	4	5
1	0	0
2	1	1
3	0	1

In tabular form, if $(a, b) \in R$, then we write 1 and if $(a, b) \notin R$, we write 0. Since $(1, 4) \notin$ write 0 in the row containing 1 and the column containing 4. Also $(2, 4) \in R$, so we write 1 in th containing 2 and the column containing 4.

Note : Total Number of Relations

Let A and B be two non-empty finite sets having m and n elements respectively. Then $A \times B$ h elements. Therefore number of subsets of $A \times B$ is 2^{mn}.

1.19. Particular Types of Relations

As we know that every subset of $A \times B$ is a relation from A into B, so there are 2^{mn} relation A into B. These relations also include ϕ and $A \times B$.

1. **Empty Relation**

   If $R = \phi$, then R is called the **empty** relation.

2. **Universal Relation**

   If $R = A \times B$, then R is called the **universal** relation.

Note : Both the empty relation and the universal relation are called **trivial** relations.

Consider the relation R on the set $A = \{1, 2, 3, 4, 5\}$ defined by

$$R = \{(a, b) : a - b = 16\}$$

Now $a - b \neq 16$ for any two elements of A.

$\therefore$ $(a, b) \notin R$ for any $a, b \in A$.

$\Rightarrow$ R does not contain any element of $A \times A$ $\Rightarrow$ R is empty set

$\Rightarrow$ R is the empty relation on A.

Consider the relation R on the set $A = \{1, 2, 3, 4, 5, 6\}$ defined by

$$R = \{(a, b) \in R : |a - b| \geq 0\}$$

Now $|a - b| \geq 0$ for all $a, b \in A$

$\Rightarrow$ $(a, b) \in R$ for all $(a, b) \in A \times A$ $\Rightarrow$ each element of set A is related to every element of s

$\Rightarrow$ $R = A \times A \Rightarrow$ R is universal relation on set A.

3. Inverse of a Relation

Let A, B be two sets and let R be a relation from a set A to a set B. Then, the inverse of R, denoted by R^{-1}, is a relation from B to A and is defined by

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

$\therefore \quad (a, b) \in R \Leftrightarrow (b, a) \in R^{-1}$

and Domain of R = Range of R^{-1} and Range of R = Domain of R^{-1}

4. Identity Relation

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

ILLUSTRATIVE EXAMPLES

Example 1. Let A = {1, 2, 3, 4, 5} and B = {2, 4, 6, 8, 10}.
Let R = {(a, b) : $a \in A$, $b \in B$, a divides b} be a relation from A into B. Find R. Show that domain of R is A and range of R is B.

Sol. Here A = {1, 2, 3, 4, 5}, B = {2, 4, 6, 8, 10}

A × B = {1, 2, 3, 4, 5} × {2, 4, 6, 8, 10} = {(1, 2), (1, 4), (1, 6), (1, 8), (1, 10), (2, 2), (2, 4), (2, 6), (2, 8) (2, 10), (3, 2), (3, 4), (3, 6), (3, 8), (3, 10), (4, 2), (4, 4), (4, 6), (4, 8), (4, 10), (5, 2), (5, 4), (5, 6), (5, 8), (5, 10)}

Now R = {(a, b) : $a \in A$, $b \in B$, a divides b}

$\therefore$ R = {(1, 2), (1, 4), (1, 6), (1, 8), (1, 10), (2, 2), (2, 4), (2, 6), (2, 8), (2, 10), (3, 6), (4, 4), (4, 8), (5, 10)}

Domain of R = {1, 2, 3, 4, 5} = A

Range of R = {2, 4, 6, 8, 10} = B

Example 2. Let R be a relation from **Q** into **Q** defined by

R = {(a, b) : $a, b \in \mathbf{Q}$ and $a - b \in \mathbf{Z}$}. Show that

(*i*) $(a, a) \in R$ for all $\in \mathbf{Q}$, (*ii*) $(a, b) \in R$ implies $(b, a) \in \mathbf{R}$,

(*iii*) $(a, b) \in R$, $(b, c) \in R$ implies $(a, c) \in \mathbf{R}$.

Sol. Here R is a relation from **Q** into **Q** defined by

$\mathbf{R} = \{(a, b) : a, b \in \mathbf{Q}$ and $a - b \in \mathbf{Z}\}$

(*i*) Since $a - a = 0 \in \mathbf{Z}$

$\therefore \quad (a, a) \in \mathbf{R} \quad \forall \; a \in \mathbf{Q}$

(*ii*) $(a, b) \in \mathbf{R} \Rightarrow a - b \in \mathbf{Z} \Rightarrow b - a \in \mathbf{Z}$

$\therefore \quad (b, a) \in \mathbf{R}$

(*iii*) $(a, b) \in \mathbf{R}, (b, c) \in \mathbf{R} \Rightarrow a - b \in \mathbf{Z}, \; b - c \in \mathbf{Z}$

$\therefore \quad a - c = (a - b) + (b - c) \in \mathbf{Z}$

$\therefore \quad (a, c) \in \mathbf{R}$

Example 3. Let A = {3, 5} and B = {7, 11}.

Let R = {$(a, b) : a \in A, b \in B, a - b$ is odd}. Show that R is an empty relation from A into B.

Sol. Here A = {3, 5}, B = {7, 11}

R = {$(a, b) : a \in A, b \in B, a - b$ is odd }

Now 3 – 7 = –4, 3 – 11 = –8, 5 – 7 = –2, 5 – 11 = –6 are not odd numbers.

$\therefore$ R is an empty relation.

Example 4. Let A = {1, 2, 3, 4, 6}. Let R be the relation on A defined by

{$(a, b) : a, b \in A, b$ is exactly divisible by a}

(*i*) Write R in roster form

(*ii*) Find the domain of R

(*iii*) Find range of R.

Sol. Here A = {1, 2, 3, 4, 6}

R = {$(a, b) : a, b \in A, b$ is exactly divisible by a}

(*i*) In roaster form,

R = {(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)}

(*ii*) Domain of R = {1, 2, 3, 4, 6}

(*iii*) Range of R = {1, 2, 3, 4, 6}

Example 5. Let A = {1, 2, 3, 4} and B = {x, y, z}. Let R be *a* relation from A into B defined by R = {$(1, x)$, $(1, z)$, $(3, x)$, $(4, y)$}. Represent R in the tabular form.

Sol. Here A = {1, 2, 3, 4}, B = {x, y, z}

R is a relation from A into B defined by

R = {$(1, x), (1, z), (3, x), (4, y)$}

$\therefore$ domain of R = {1, 3, 4} and range of R = {x, y, z}.

Tabular form of relation R is

R	x	y	z
1	1	0	1
2	0	0	0
3	1	0	0
4	0	1	0

Example 6. If R is the relation "less than" from A = {1, 2, 3, 4, 5} to B = {1, 4, 5}, write down the set of ordered pairs corresponding to R. Also find the inverse relation to R.

Sol. A {1, 2, 3, 4, 5}, B = {1, 4, 5}

R is the relation "less than" from A to B

$\therefore$ R = {(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)}

$\therefore$ R^{-1} = {(4, 1), (5, 1), (4, 2), (5, 2), (4, 3), (5, 3), (5, 4)}

Example 7. Determine the domain and range of the relation R defined by :

(*i*) $R = \{(x, y) : x \in \mathbf{N}, y \in \mathbf{N} \text{ and } x + y = 10\}$

(*ii*) $R = \{(x, y) : x \in \mathbf{N}, x < 5, y = 3\}$.

Sol. (*i*) $x + y = 10 \Rightarrow y = 10 - x$

$x = 1 \Rightarrow y = 10 - 1 = 9$

$x = 2 \Rightarrow y = 10 - 2 = 8$

$x = 3 \Rightarrow y = 10 - 3 = 7$

$x = 4 \Rightarrow y = 10 - 4 = 6$

$x = 5 \Rightarrow y = 10 - 5 = 5$

$x = 6 \Rightarrow y = 10 - 6 = 4$

$x = 7 \Rightarrow y = 10 - 7 = 3$

$x = 8 \Rightarrow y = 10 - 8 = 2$

$x = 9 \Rightarrow y = 10 - 9 = 1$

$x = 10 \Rightarrow y = 10 - 10 = 0 \notin N$

$\therefore$ domain of R = {1, 2, 3, ..., 8, 9}

and range of R = {1, 2, 3, ..., 8, 9}

(*ii*) $x + y = 10$

When $y = 3$, then $x + 3 = 10 \Rightarrow x = 7$

$\therefore$ there is no $x \in \mathbf{N}$, $x < 5$, $y = 3$ which satisfies $x + y = 10$

$\therefore$ domain of R = ϕ, range of R = ϕ.

Example 8. Let A = {1, 2, 3, 4, 5, 6}.

Define a relation R on set A by $R = \{(x, y) : y = x + 1\}$

(*i*) Depict this relation using an arrow diagram.

(*ii*) Write down the domain, co-domain and range of R.

Sol. $y = x + 1$

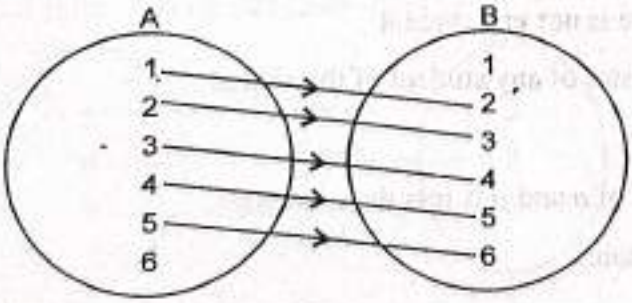
(*i*) Putting $x = 1, 2, 3, 4, 5, 6$, we get,

$y = 2, 3, 4, 5, 6, 7$.

For $x = 6$, we get $y = 7$ which does not belong to set A.

$\therefore$ R = {(1, 2), (2, 3), (3, 4), (4, 5), (5, 6)}

The arrow diagram representing R is as follows :

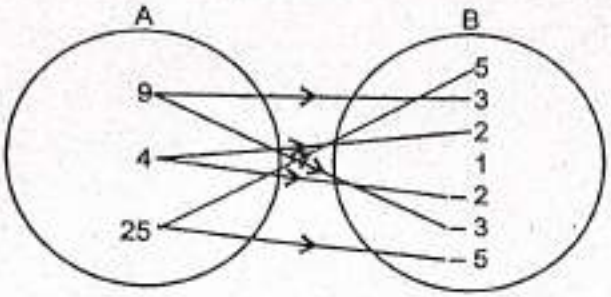


(*ii*) ∴ Domain of R = {1, 2, 3, 4, 5},

and Range of R = {2, 3, 4, 5, 6}.

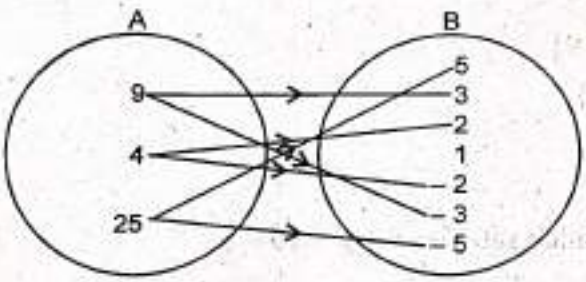
Example 9. The figure given below shows a relation R between the sets A and B. Write this relation R in

(*i*) Set builder form (*ii*) Roster form.



What is its domain and range ?

Sol. Given figure is



(*i*) Relation R consists of elements (x, y), where x is the square of y *i.e.* $x = y^2$. Therefore, relation R in Roster from is

$$R = \{(x, y) : x = y^2,\ x \in A,\ y \in B\}$$

(*ii*) $R = \{(9, 3), (9, -3), (4, 2), (4, -2), (25, 5), (25, -5)\}$

The domain of R is {9, 4, 25}

The range of R is {–5, –3, –2, 2, 3, 5}.

Example 10. Let A be the set of all students of a boys school. Show that the relation R in A given by $R = \{(a, b) : a$ is sister of $b\}$ is the empty relation and $R' = \{(a, b) :$ the difference between heights of a and b is less than 3 meters$\}$ is the universal relation.

Sol. Since the school is boys school *i.e.* there is not girl student

∴ no student of the school can be sister of any student of the school.

∴ $R = \phi \Rightarrow$ R is the empty relation.

Clearly the difference between heights of a and b is less than 3 metres.

∴ $R' = A \times A$ is the universal relation.

EXERCISE 1.5

1. Let A = {1, 2, 3, 4} and B = {x, y, z}. Let R be *a* relation from A into B defined by R = {(1, x), (1, z), (3, x), (4, y)}. Find the domain and range of R.
2. Let R be the relation on **Z** defined by R = {$(a, b) : a, b \in \mathbf{Z}$, $a - b$ is an integer}. Find the domain and range of R.
3. Let R be a relation from **N** into **N** defined by R = {$(a, b) : a, b \in \mathbf{N}$ and $a = b^2$}. Are the following true ?

   (*i*) $(a, a) \in \mathbf{R}$, for all $a \in \mathbf{N}$.

   (*ii*) $(a, b) \in \mathbf{R}$ implies $(b, a) \in \mathbf{R}$

   (*iii*) $(a, b) \in \mathbf{R}$, $(b, c) \in \mathbf{R}$ implies $(a, c) \in \mathbf{R}$

   Justify your answer in each case.
4. Let R be the relation on **Z** defined by R = {$(a, b) : a \in \mathbf{Z}, b \in \mathbf{Z}, a^2 = b^2$}. Find

   (*i*) R (*ii*) domain of R (*iii*) Range of R.
5. Let R be the relation on the set **N** of naturals defined by $a + 3b = 12$. Find

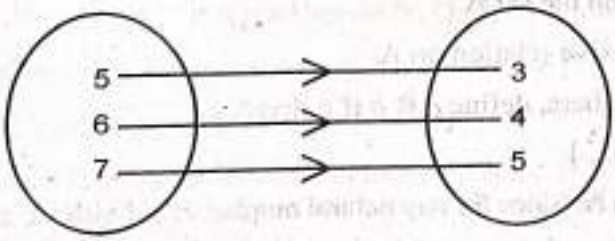
   (*i*) R (*ii*) domain of R (*iii*) Range of R
6. Let A = {1, 2, 3, ..., 14}. Define a relation R from A to A by R = {$(x, y) : 3x - y = 0$, where $x, y \in$ A}. Write down its domain, codomain and range.
7. Define a relation R on the set **N** of natural numbers by

   R = {$(x, y) : y = x + 5$, x is a natural number less than 4 ; $x, y \in \mathbf{N}$}

   Depict this relationship using roster form. Write down the domain and range.
8. A = {1, 2, 3, 5} and B = {4, 6, 9}. Define a relation R from A to B by

   R = {(x, y) : the difference between x and y is odd ; $x \in$ A, $y \in$ B}.

   Write R in roster form.
9. Let A = {1, 2} and B = {3, 4}. Find the number of relations from A into B.
10. Let A = {1, 2). List all the relation on A.
11. Let A {x, y, z} and B = {1, 2}. Find the number of relations from A into B.
12. The figure given below shows a relationship between the sets P and Q. Write this relation in (*i*) set-builder form (*ii*) roaster form.



What is its domain and range ?

ANSWERS

1. Domain = {1, 3, 4}, Range = { x, y, z}
2. Domain = **Z** , Range = **Z**
3. (*i*) No ; $(a, a) \in \mathbf{R}$ is true for $a = 1$
   (*ii*) No ; $(4, 2) \in \mathbf{R}$ but $(2, 4) \notin \mathbf{R}$
   (*iii*) No ; $(16, 4) \in \mathbf{R}$, $(4, 2) \in \mathbf{R}$ but $(16, 2) \notin \mathbf{R}$
4. (*i*) $R = \{(a, a) : a \in \mathbf{Z}\} \cup \{(a, -a) : a \in \mathbf{Z}\}$
   (*ii*) Domain = **Z** (*iii*) Range = **Z**
5. (*i*) R = {(9, 1), (6, 2), (3, 3)} (*ii*) Domain = {9, 6, 3}
   (*iii*) Range = {1, 2, 3}
6. Domain = {1, 2, 3, 4}, Codomain = {1, 2, 3, ..., 14}, Range = {3, 6, 9, 12}
7. R = {(1, 6), (2, 7), (3, 8)}, Domain = {1, 2, 3}, Range = {6, 7, 8}
8. R = {(1, 4), (1, 6), (2, 9), (3, 4), (3, 6), (5, 4), (5, 6)} 9. 16
10. ϕ, {(1,1)},{(2,2)},{(1,2)}, {(2,1)}, {(1,1)}, {(2,2)}, {(1,1), (1, 2)},
    {(1,1), (2, 1)}, {(2, 2), (1, 2)}, {(2, 2), (2, 1)}, {(1, 2), (2, 1)},
    {(1, 1), (2, 2), (1, 2)}, {(1,1), (2, 2), (2, 1)}, {(1,1), (1,2), (2, 1)},
    {(2,2), (1, 2), (2, 1)}, A × A
11. 64
12. (*i*) $R = \{(x, y) : y = x - 2, x \in A, y \in B\}$
    (*ii*) R = {(5, 3), (6, 4), (7, 5)}, Domain = {5, 6, 7}, Range = {3, 4, 5}

1.20. Properties of Relations

Reflexive Relation

A relation R on a set A is called a reflexive relation if $(x, x) \in R$ for all $x \in A$ *i.e.*, if x R x for every $x \in R$.

Example. Let A = { 1, 2}.

Then A × A = {(1, 1), (1, 2), (2, 1), (2, 2)}.

Let R = { (1, 1), (2, 2), (1, 2) }.

Then $R \subseteq A \times A$ and so R is a relation on the set A.

Since $(x, x) \in R \; \forall \; x \in A$, so R is a reflexive relation on A.

Example. For $a, b \in \mathbf{N}$, the set of natural numbers, define a R b if a divides b

Then R = {(1, 1), (1, 2),....,(2, 2), (2, 4)....}

Then $R \subseteq \mathbf{N} \times \mathbf{N}$ and so R is a relation on **N**. Since for any natural number x, x divides x, so x R $x \; \forall \; x \in$ Therefore R is a reflexive relation.

Example. We define a relation S on the set of real numbers **R** by a S b if a is less than b where $a, b \in \mathbf{R}$. It is not a reflexive relation since for any $a \in \mathbf{R}$, a is not less then a and hence $(a, a) \notin$ S.

Example : The relation R defined on set of lines by l_1 R l_2 if l_2 is parallel to l_2 is reflexive, since every line is parallel to itself.

Example : The relation R defined on set of natural numbers a R b if $a > b$ is not reflexive

$\because$ $a > a$ is not true.

Irreflexive Relation

A relation R on a set A is irreflexive if a R a, *i.e.* $(a, a) \notin$ R for every $a \in$ A.

$\therefore$ R is irreflexive if no element is related to itself.

Example. Let A = {1, 2} and let R = {(1, 2), (2, 1)}

$\therefore$ R is irreflexive as (1, 1) (2, 2) $\notin$ R.

Example. Let A = {1, 2} and let R = {(1, 2), (2, 2)}

$\therefore$ R is not irreflexive as (2, 2) $\in$ R.

Note : Here R is not reflexive as (1, 1) $\notin$ R.

Symmetric Relation

A relation R on a set A is called a symmetric relation if a R $b \Rightarrow b$ R a where $a, b \in$ A, *i.e.*, if $(a, b) \in$ R $\Rightarrow (b, a) \in$ R where $a, b \in$ A.

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

Then A×A = { (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)}

Let R = {(1, 1), (1, 3), (3, 1)} and R_1 = { (1, 2), (1, 3), (3, 1) }

Then R, $R_1 \subseteq A \times A$

Therefore R and R_1 are both relations on A

Since $(x, y) \in R \Rightarrow (y, x) \in R$, therefore R is a symmetric relation on A.

Since (1,2) $\in R_1$ but (2,1) $\notin R_1$, therefore $(x, y) \in R_1 \Rightarrow (y, x) \in R_1$ does not hold in R_1 always.

$\therefore$ R_1 is not a symmetric relation.

Example. For $a, b \in$ **N**, the set of natural numbers define a relation R by a R b if $a < b$. Then R = {(1, 2), (1, 3),.....,(2, 3), (2, 4).....}.

Since R $\subseteq$ **N** × **N**, so R is a relation on **N**. (1, 2) $\in$ R since 1 is less than 2.

But (2, 1) $\notin$ R since 2 is not less than 1.

Therefore R is not a symmetric relation on **N**.

Example : Relation R defined on set of lines by l_1 R l_2 if l_1 is perpendicular to l_2 is symmetric

$\because$ if $l_1 \perp l_2$ then $l_2 \perp l_1$.

Asymmetric Relations :

A relation R on a set A is asymmetric if whenever a R b, then b R a.

Example. Let A = **R**, the set of real numbers and let R be the relation '<'.

If $a < b$, then $b \not< a$ (b is not less than a), so '<' is asymmetric.

Example. Let A = {1, 2, 3} and let R = {(1, 2), (2, 1), (2, 3)}. Is R symmetric, asymmetric or antisymmetric ?

Sol. Here A = {1, 2, 3}, R = {(1, 2), (2, 1), (2, 3)}.

Symmetry : R is not symmetric either since (2, 3) ∈ R but (3, 2) ∉ R

Asymmetry : R is not asymmetric since both (1, 2) and (2, 1) ∈ R

Antisymmetry : R is not antisymeetric since (1, 2) and (2, 1) ∈ R.

Anti-Symmetric Relation

A relation R on a set A is called an anti-symmetric relation if a R b and b R a implies that $a = b$.

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

OR

A relation R on a set A is called anti-symmetric if $a, b \in A$ $(a \neq b)$

and $(a, b) \in R \Rightarrow (b, a) \notin R$.

Example. Let A be the set of all lines in a plane. Let $L_1, L_2 \in A$. We define a relation R on A by L_1 R L_2 $L_1 \parallel L_2$ *i.e.*, if L_1 is parallel to L_2. Since in any plane there exist different lines L_1 and L_2 such that $L_1 \parallel$ and $L_2 \parallel L_1$ but $L_1 \neq L_2$ *i.e.*, L_1 R L_2 and L_2 R L_1 but $L_1 \neq L_2$, therefore R is not an anti-symmetric relati

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

Then R = {(1,1), (1,2), (2,1)} is a relation on the set A.

Since (1,2) ∈ R and (2,1) ∈ R but 1 ≠ 2, therefore R is not anti-symmetric relation.

But $R_1 = \{(3, 3)\}$ is an anti-symmetric relation on A.

Example. For $a, b \in N$ the set of natural numbers define a R b if $a \leq b$.

Let $a, b \in N$ such that a R b and b R a.

$\therefore$ $a \leq b$ and $b \leq a \Rightarrow a = b$.

$\therefore$ R is an anti-symmetric relation.

Note : Compatible Relation : A relation R in A is said to be compatible relation if it is reflexive a symmetric.

Transitive Relation

A relation R on a set A is called a transitive relation if

a R b, b R $c \Rightarrow a$ R $c \; \forall \; a, b, c \in A$

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

and $(b, c) \in R \Rightarrow (a, c) \in R$ where $a, b, c \in A$.

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

Then $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

Let $R = \{(1, 1), (2, 2), (1, 3), (2, 3), (2, 1)\}$

Let $R_1 = \{(1, 2), (2, 3), (2, 1)\}$

Then R and R_1 are both subsets of $A \times A$.

Therefore, R and R_1 are both relations on A.

Also $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$. Thus R is a transitive relation.

Further, $(1, 2)$ and $(2, 3) \in R_1$, but $(1, 3) \notin R_1$.

Thus R_1 is not a transitive relation

Example. For $a, b \in \mathbf{N}$, the set of natural numbers, define $a \, R \, b$ if $2a + b = 10$.

The natural numbers a and b satisfying the relation $2a + b = 10$ are given by :

$a = 1, b = 8$, $a = 2, b = 6$, $a = 3, b = 4$, $a = 4, b = 2$

$\therefore$ $R = \{(1, 8), (2, 6), (3, 4), (4, 2)\}$

Since $(3, 4) \in R$ and $(4, 2) \in R$ but $(3, 2) \notin R$. Therefore R is not a transitive relation.

Circular Relation

A relation R is called circular if $(a, b) \in R, (b, c) \in R \Rightarrow (c, a) \in R$.

Example. Show that a relation is reflexive and circular iff it is equivalence relation.

Sol. Let R be reflexive and circular

$\therefore$ $(a, a) \in R$ and $(a, b) \in R, (b, c) \in R \Rightarrow (c, a) \in R$.

Since $(c, a) \in R$ and $(a, a) \in R$ and R is circular, we have $(a, c) \in R$

$\therefore$ $(c, a) \in R \Rightarrow (a, c) \in R$, which shows that R is symmetric.

Again $(a, b) \in R, (b, c) \in R \Rightarrow (c, a) \in R$, since R is circular

$\Rightarrow$ $(a, c) \in R$ as R is proved to be symmetric

$\therefore$ R is transitive.

$\therefore$ R is reflexive, symmetric and transitive and so is an equivalence relation.

Conversely, let R be reflexive, symmetric and transitive

$\therefore$ $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ ($\because$ of transitivity)

$\Rightarrow (c, a) \in R$ ($\because$ of symmetry)

$\therefore$ R is circular and so R is reflexive and circular.

Equivalence Relation

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

Example. Let X be the set of all triangles in a plane.

For any two triangles Δ_1 and Δ_2 in X define $\Delta_1 \, R \, \Delta_2$, if Δ_1 and Δ_2 are congruent triangles. Then

(*i*) **R is Reflexive.** Since each triangle is congruent to itself, so $\Delta \, R \, \Delta$ for each Δ in X.

(ii) R is Symmetric. Let Δ_1 and $\Delta_2 \in X$ such that $\Delta_1 \, R \, \Delta_2$. Then Δ_2 and Δ_1 are congruent triang Hence $\Delta_2 \, R \, \Delta_1$.

(iii) R is Transitive. Let Δ_1 , Δ_2 , $\Delta_3 \in X$ such that $\Delta_1 \, R \, \Delta_2$ and $\Delta_2 \, R \, \Delta_3$. Then Δ_1 , Δ_2 congruent triangles and so are Δ_2 and Δ_3. This implies that the Δ_1 and Δ_3 are also congruent triang Hence $\Delta_1 \, R \, \Delta_3$.

So, R is reflexive, symmetric and transitive.

Therefore, R is an equivalence relation on X.

Partial Order Relation

A relation R on a set X is said to be a partial order relation if it satisfies the following three conditions :

(i) $x \, R \, x$, for every $x \in X$ (reflexivity)

(ii) $x \, R \, y$ and $y \, R \, x \Rightarrow x = y$ (anti-symmetry)

(iii) $x \, R \, y$ and $y \, R \, z \Rightarrow x \, R \, z$ (transitivity), $x, y, z \in X$

Remark : The only equivalence relation on a set X which is also a partial order relation on X is the ide relation I_X, that is, the relation defined by $x \, R \, Y$ iff $x = y$.

1.21. Composition of Relations

Let R be an relation from a set A to a set B and S be a relation from set B to a set C. Then composition relation denoted by SoR is a relation from a set A to a set C defined as

$$SoR = \{(a, c) : \exists \, b \in B \text{ for which } (a, b) \in R, (b, c) \in S\}$$

Also if A be any non-empty set and R, S be any two relations on A. Then composition of R a denoted by SoR is defined as

$$SoR = \{(a, c) : \exists \, b \in A \text{ for which } (a, b) \in R, (b, c) \in S\}$$

Example. Let $A = \{1, 2, 3, 4, 5, 6, 7\}$

and $R = \{(1, 2), (2, 5), (3, 6), (7, 4)\}$

$S = \{(1, 4), (7, 5), (3, 7), (4, 3)\}$

be two relations on a set A

Then $SoR = \{(7, 3)\}$

$RoS = \{(3, 4), (4, 6)\}$

$R^{-1} = \{(2, 1), (5, 2), (6, 3), (4, 7)\}$

$S^{-1} = \{(4, 1), (5, 7), (7, 3), (3, 4)\}$

From above example it is clear that

$$RoS \neq SoR.$$

Now we discuss some theorems on composition of relations.

1.22. Let A, B and C be sets, R is relation from A to B, and S is a relation from B to C. Then prov $(SoR)^{-1} = R^{-1}oS^{-1}$.

Proof : Let $c \in C$ and $a \in A$

then $(c, a) \in (SoR)^{-1}$ iff $(a, c) \in SoR$

Now $(a, c) \in SoR$ which means there exist $b \in B$

such that $(a, b) \in R$ and $(b, c) \in S$

$\Rightarrow$ $(b, a) \in R^{-1}$ and $(c, b) \in S^{-1}$ or $(c, b) \in S^{-1}$ and $(b, a) \in R^{-1} \Rightarrow (c, a) \in R^{-1} o S^{-1}$

So $(SoR)^{-1} = R^{-1} o S^{-1}$

1.23. Let A, B, C, D be sets. Suppose R is a relation from A to B, S is relation from B to C and T is a relation from C to D. Then show that

$$(RoS)oT = Ro(SoT).$$

Proof : Let $(a, d) \in (RoS)oT$

Then there exists some $c \in C$ such that

$$(a, c) \in RoS \text{ and } (c, d) \in T$$

Since $(a, c) \in RoS$, so there exist b in B such that

$$(a, b) \in R \text{ and } (b, c) \in S$$

Now $(b, c) \in S$ and $(c, d) \in T$

$\Rightarrow$ $(b, d) \in SoT$

Again $(a, b) \in R$ and $(b, d) \in SoT$

$\Rightarrow$ $(a, d) \in Ro(SoT)$

$\therefore$ $(RoS)oT \subset Ro(SoT)$ ...(1)

Similarly, $Ro(SoT) \subset (RoS)oT$ ...(2)

From equations (1) and (2)

$$Ro(SoT) = (RoS)oT.$$

1.24. Let R be a relation from X to Y and X_1, X_2 be two subsets of X then

(*i*) $X_1 \subseteq X_2 \Rightarrow R(X_1) \subseteq R(X_2)$

(*ii*) $R(X_1 \cup X_2) = R(X_1) \cup R(X_2)$

(*iii*) $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$

Proof : (*i*) Let $b \in R(X_1)$

Since $b \in R(X_1)$ $\therefore$ there exist $a \in X_1$

such that $(a, b) \in R(X_1)$

But $X_1 \subseteq X_2$, $\therefore$ $a \in X_2$

as $a \in X_2 \Rightarrow b \in R(X_2)$

$\therefore$ $R(X_1) \subseteq R(X_2)$

(*ii*) Let $b \in R(X_1 \cup X_2)$

$\therefore$ there exist some $a \in X_1 \cup X_2$

s.t. $(a, b) \in R(X_1 \cup X_2)$

Now $a \in X_1 \cup X_2 \Rightarrow a \in X_1$ or $a \in X_2$

If $a \in X_1 \Rightarrow b \in R(X_1)$

Similarly if $a \in X_2 \Rightarrow b \in R(X_2)$

so $b \in R(X_1) \cup R(X_2)$

$\therefore$ $R(X_1 \cup X_2) \subseteq R(X_1) \cup R(X_2)$

Also we know $X_1 \subseteq X_1 \cup X_2$ and $X_2 \subseteq X_1 \cup X_2$

By part (*i*) $R(X_1) \subseteq R(X_1 \cup X_2)$

$R(X_2) \subseteq R(X_1 \cup X_2)$

$\Rightarrow$ $R(X_1) \cup R(X_2) \subseteq R(X_1 \cup X_2)$

From (1) and (2)

$R(X_1 \cup X_2) = R(X_1) \cup R(X_2)$.

(*iii*) Let $b \in R(X_1 \cap X_2)$

$\therefore$ there exist some $a \in X_1 \cap X_2$

s.t. $(a, b) \in R(X_1 \cap X_2)$

Now $a \in X_1 \cap X_2 \Rightarrow a \in X_1$ and $a \in X_2$

$\Rightarrow$ $b \in R(X_1)$ and $b \in R(X_2) \Rightarrow b \in R(X_1) \cap R(X_2)$

$\therefore$ $R(X_1 \cap X_2) \subseteq R(X_1) \cap R(X_2)$

1.25. Equivalence Class

Let R be an equivalence relation on a non-empty set X. let $a \in X$. Then the equivalence class denoted by $[a]$, is defined as follows :

$$[a] = \{ b \in X : b \, R \, a \}.$$

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

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

$[1] = \{ 1, 2 \}$ since only 1 and 2 are related to 1

Similarly, $[2] = \{ 2, 1 \}$ and $[3] = \{ 3 \}$

We observe that any two equivalence classes are either disjoint or identical. The distinct equiva classes are [1] and [3].

Also $A = [1] \cup [3]$ and $[1] \cap [3] = \phi$

Then $R = \{ (1,1), (2,2), (3,3), (1,2), (2,1)\}$

is an equivalence relation on A.

1.26. Suppose that R is an equivalence relation on a set X. Then

(*i*) $a \in [a] \; \forall \; a \in X$.

(*ii*) $a \in [b]$ if and only if $[a] = [b] \; \forall \; a, b \in X$.

(*iii*) $[a] = [b]$ or $[a] \cap [b] = \phi \; \forall \; a, b \in X$ *i.e.*, any two equivalence classes are disjoint or identical.

Proof : (*i*) Since R is an equivalence relation on X.

$\therefore$ R is reflexive.

$\therefore$ $a \, R \, a \; \forall \; a \in X. \Rightarrow a \in [a] \; \forall \; a \in X.$

(*ii*) Let $a, b \in X$ such that $a \in [b]$ ...(1)

$\therefore$ $a \, R \, b$

$\Rightarrow$ $b \, R \, a$, since R is equivalence relation ...(2)

Now we show that $[a] = [b]$.

Let $p \in [a]$.

$\therefore$ $p \, R \, a$ ...(3)

From, (1) and (3), $p \, R \, b$, since R is an equivalence relation

$\therefore$ $p \in [b]$.

So $p \in [a] \Rightarrow p \in [b]$. Therefore $[a] \subseteq [b]$.

Now let $q \in [b]$.

$\therefore$ $q \, R \, b$. Also $b \, R \, a$ (From (2)).

$\therefore$ $q \, R \, a$ and hence $q \in [a]$.

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

Hence $[a] = [b]$

Conversely let $[a] = [b]$ for some $a, b \in X$.

From (*i*), $a \in [a]$.

$\therefore$ $a \in [b]$, since $[a] = [b]$.

(*iii*) Let $a, b \in X$.

If $[a] \cap [b] = \phi$, then we have nothing to prove.

If $[a] \cap [b] \neq \phi$, then there exists $p \in X$ such that $p \in [a] \cap [b]$.

$\therefore$ $p \in [a]$ and $p \in [b]$

$\Rightarrow$ $[p] = [a]$ and $[p] = [b]$, [From (*ii*)]

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

1.27. The distinct equivalence classes of an equivalence relation on a set form a partition of that set.

Proof : Let R be an equivalence relation on a set X. Therefore R is also a reflexive relation.

$\therefore$ $a \, R \, a \; \forall \; a \in X$.

$\therefore$ $a \in [a] \; \forall \; a \in X$. ...(1)

where $[a]$ denotes the equivalence class of a.

We prove that $X = \bigcup_{a \in X} [a]$.

Let $a \in X$.

Then $a \in [a]$ [From

$\therefore$ $a \in \bigcup_{a \in X} [a]$

$\therefore$ $X \subset \bigcup_{a \in X} [a]$

Since $[a] = \{ b \in X : b \, R \, a \}$, therefore

$[a] \subseteq X \; \forall \, a \in X$

$\therefore$ $\bigcup_{a \in X} [a] \subseteq X$

From (2) and (3), we get $X = \bigcup_{a \in X} [a]$. If we delete the repetitions from this union, we get

union of distinct equivalence of X under R.

Now we prove that any two distinct equivalence classes are disjoint.

Let $[a]$ and $[b]$ be any two distinct equivalence classes where $a, b \in X$

We want to prove that $[a] \cap [b] = \phi$.

If possible, let $[a] \cap [b] \neq \phi$.

$\therefore$ $\exists \, x \in X$ such that $x \in [a] \cap [b]$.

$\therefore$ $x \in [a]$ and $x \in [b]$.

$\therefore$ $x \, R \, a$ and $x \, R \, b$.

$\Rightarrow$ $a \, R \, x$ and $b \, R \, x$.

Now we prove that $[a] = [b]$.

Let $p \in [a]$.

$\therefore$ $p \, R \, a$. Also $a \, R \, x$ (From

$\therefore$ $p \, R \, x$. Also $x \, R \, b$ (From

$\therefore$ $p \, R \, b$ (Since R is an equivalence rela

$\Rightarrow$ $p \in [b]$

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

Now let $q \in [b]$

$\therefore$ $q \, R \, b$. Also $b \, R \, x$ (From

$\therefore$ $q \, R \, x$. (Since R is equivalence relation)

Also $x \, R \, a$ (From

$\therefore$ $q \, R \, a \Rightarrow q \in [a]$

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

Hence $[a] = [b]$.

But this is against our supposition that $[a]$ and $[b]$ are distinct equivalence classes. So, our supposition that $[a] \cap [b] \neq \phi$ is wrong.

Thus $[a] \cap [b] = \phi$.

Therefore, X is union of distinct equivalence classes and any two distinct equivalence classes are disjoint.

Hence the set of distinct equivalence classes of R forms a partition of X.

1.28. For any partition of X, there is an equivalence relation on X whose equivalence classes are the sets in the partition.

Proof : Let $\{A_\lambda\}_{\lambda \in \Lambda}$ be a partition of X. Therefore we have

(*i*) $X = \bigcup_{\lambda \in \Lambda} A_\lambda$,

(*ii*) $A_\lambda \cap A_\mu = \phi$ if $\lambda \neq \mu$ where λ and $\mu \in \Lambda$.

For $a, b \in X$, define $a \, R \, b$ if and only if a, b are in the same A_λ.

Then for any $a, b, c, \in \Lambda$, we have :

(*i*) R is reflexive

Let $a \in X$.

$\therefore$ by (*i*) $a \in \bigcup_{\lambda \in \Lambda} A_\lambda$ so that $a \in A_\lambda$ for some $\lambda \in \Lambda$.

Therefore $a \, R \, a$.

(*ii*) R is symmetric

Let $a \, R \, b$.

$\therefore$ a and b belong to A_α for some $\alpha \in \Lambda$.

$\Rightarrow$ b and a belong to some A_α. $\Rightarrow$ $b \, R \, a$.

(*iii*) Let $a \, R \, b$ and $b \, R \, c$.

$\therefore$ a and b belong to same A_α for some $\alpha \in \Lambda$ and b, c belong to same A_β for some $\beta \in \Lambda$.

$\therefore$ $b \in A_\alpha$ and A_β both *i.e.*, $b \in A_\alpha \cap A_\beta$.

$\Rightarrow$ $\alpha = \beta$, For if $\alpha \neq \beta$, then by (*ii*) $A_\alpha \cap A_\beta = \phi$.

$\therefore$ a and c belong to same A_α.

$\therefore$ $a \, R \, c$.

Therefore R is reflexive, symmetric as well as transitive relation on X. Hence R is an equivalence relation on X.

Now we prove that each equivalence class of X is equal to A_λ.

Let $[a]$ denote the equivalence of a for any $a \in X$.

Then $[a] = \{ b \in X : b \, R \, a \}$.

$= [b \in X : b$ and a are in the same A_λ for some $\lambda \in \Lambda \} = A_\lambda$.

$\therefore$ Equivalence class of X is equal to A_λ.

Conversely we prove that each A_λ is equal to some equivalence of X.

Consider any A_λ

Take any $a \in A_\lambda$

Such an a exist, since A_λ is non-empty.

We prove that $A_\lambda = [a]$

Let $b \in A_\lambda$. Then a and b belong to same A_λ

$\therefore$ $b \, R \, a$ and hence $b \in [a]$

$\therefore$ $b \in A_\lambda \Rightarrow x \in A_\lambda \Rightarrow A_\lambda \subseteq [a]$

Now, let $x \in [a]$

$\therefore$ $x \, R \, a$ and hence x, a belong to same A_α

But $a \in A_\lambda \quad \therefore x \in A_\lambda$

$\therefore$ $x \in [a] \Rightarrow x \in A_\lambda \Rightarrow [a] \subseteq A_\lambda$

Hence $A_\lambda = [a]$

$\therefore$ $\{A_\lambda\}_{\lambda \in \Lambda}$ is the set of all equivalence classes under the relation R.

1.29. Quotient of A by R

Let R be an equivalence relation on A. Then the collection of equivalence classes of the elements is called Quotient of A by R and is denoted by A | R.

$\therefore$ $A \mid R = \{ [a] : a \in A \}$.

1.30. Fundamental Theorem on Relations

If R is an equivalence relation on A, then prove that A | R is the partition of A.

Proof : We know that $A \mid R = \{ [a] : a \in A \}$. Therefore it is sufficient to show that A is the union o *disjoint* equivalence classes.

Let $P = \cup [a], a \in A$

$\therefore$ $P \subseteq A$

Also for each $a \in A$, there exists an equivalence class $[a]$ containing a.

$\therefore$ $a \in A \Rightarrow a \in [a] \Rightarrow a \in P$

$\Rightarrow A \subseteq P$

From (1) and (2), we get

$A = P$.

1.31. Relation Induced by the Partition

Let $A = A_1 \cup A_2 \cup \ldots \cup A_n$ be a partition of a set A. A relation R on A is said to be rel induced by the partition if for all $a, b \in A$,

$a \, R \, b \Leftrightarrow$ there is a subset A_i of the partition such that both a and b are in A_i

1.32. Let A be a set with partition $\{A_1, A_2, ..., A_n\}$ and let R be the relation induced by the partition. Then R is an equivalence relation.

Proof : (*i*) Suppose that $a \in A$.

Since $\{A_1, A_2, ..., A_n\}$ is a partition of A, So $a \in A_i$ for some *i*.

$\therefore$ there is a set A_i of the partition such that $a \in A_i$ and $a \in A_i \Rightarrow a R a$

$\therefore$ R is reflexive.

(*ii*) Let $a, b \in A$ such that $a R b$.

$\therefore$ there is a subset A_i of the partition such that both *a* and *b* are in A_i

i.e. both *b* and *a* belong to some $A_i \Rightarrow b R a$,

$\therefore$ R is symmetric.

(*iii*) Let $a, b, c \in A$ such that $a R b$ and $b R c$.

$\therefore$ there are subsets A_i and A_j of the partition such that $a, b, \in A_i$ and $b, c \in A_j$

We claim that $A_i = A_j$.

If possible, suppose that $A_i \neq A_j$. Then $A_i \cap A_j = \phi$ as all sets of the partition are disjoint.

But *b* is in both A_i and A_j. Hence $A_i \cap A_j \neq \phi$.

$\therefore$ we arrive at a contradiction. Therefore our supposition is wrong.

$\therefore$ $A_i = A_j$ showing that *a*, *b* and *c* are all in A_i. In particular *a* and *c* are both in A_i showing that $a R c$ and so R is transitive.

ILLUSTRATIVE EXAMPLES

Example 1. (*i*) Give an example of a relation which is reflexive but neither symmetric nor transitive.

(*ii*) Give an example of a relation which is symmetric but neither reflexive nor transitive.

(*iii*) Given an example of a relation which is reflexive and symmetric but not transitive.

(*iv*) Give an example of a relation which is reflexive and transitive but not symmetric.

(*v*) Give an example of a relation which is reflexive and anti-symmetric but not transitive.

(*vi*) Give an example of a relation which is symmetric and transitive but not reflexive.

(*vii*) Give an example of a relation which is reflexive and anti-symmetric but neither symmetric nor transitive .

(*viii*) Give an example of a relation which is neither reflexive, nor symmetric, nor transitive nor anti-symmetric.

(*ix*) Give an example of a relation which is reflexive, symmetric, transitive and anti-symmetric.

Sol. (*i*) Let $A = \{2, 3, 4\}$.

Then $A \times A = \{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4), (4, 2), (4, 3), (4, 4)\}$

Let $R = \{(2, 2), (3, 3), (4, 4), (2, 3), (4, 3), (3, 4)\}$

Since $R \subseteq A \times A$, therefore R is a relation on A.

R is reflexive since $(a, a) \in R \ \forall\, a \in A$.

R is not symmetric since $(2, 3) \in R$ but $(3, 2) \notin R$.

R is not transitive since $(2, 3)$ and $(3, 4) \in R$ but $(2, 4) \notin R$.

Further R is not anti-symmetric since $(3,4)$ and $(4, 3) \in R$ but $3 \neq 4$.

(*ii*) Let $A = \{1, 2\}$.

Then $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

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

Then $R \subseteq A \times A$ and hence R is a relation on the set A.

R is symmetric since $(a, b) \in R \Rightarrow (b, a) \in R$.

R is not reflexive since $1 \in A$ but $(1, 1) \notin R$.

R is not transitive since $(1, 2) \in R$, $(2, 1) \in R$ but $(1, 1) \notin R$ is not anti-symmetric since $(1, 2)$ and $(2, 1) \in R$ but $1 \neq 2$.

(*iii*) Let $A = \{1, 2, 3\}$

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

Let $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$.

R is a relation on A as $R \subseteq A \times A$.

R is reflexive as $(a, a) \in R \ \forall\, a \in A$.

Also, R is symmetric since $(a, b) \in R$ implies that $(b, a) \in R$.

But R is not transitive since $(1, 2) \in R$ and $(2, 3) \in R$ but $(1, 3) \notin R$.

Moreover, R is not anti-symmetric as $(1, 2) \in R$ and $(2, 1) \in R$ but $1 \neq 2$.

(*iv*) Let $A = \{1, 2, 3\}$.

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

Let $R = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$.

Then R is a relation on A as $R \subseteq A \times A$.

R is reflexive since $(a, a) \in R \ \forall\, a \in A$.

R is not symmetric as $(1, 3) \in R$ and $(3, 1) \notin R$.

R is transitive since $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

(v) Let $A = \{1, 2, 3\}$.

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

Let $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\}$.

R is a relation on A as $R \subseteq A \times A$.

R is a reflexive relation on A since $(a, a) \in R \; \forall \; a \in A$.

R is also a anti-symmetric relation on A since $(a, b) \in R$ and $(b, a) \in R$.

$\Rightarrow \quad a = b$.

R is not transitive since (1, 2) and (2, 3) $\in$R but (1, 3) $\notin$ R.

(vi) Let $A = \{1, 2, 3\}$

Then $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3,1), (3, 2), (3, 3)\}$

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

R is not reflexive as $3 \in A$ and $(3,3) \notin R$.

R is symmetric as $(a, b) \in R \Rightarrow (b, a) \in R$.

R is transitive since $(a, b) \in R$ and $(b, c) \in R$ implies that $(a, c) \in R$.

R is not anti-symmetric since (1,2) and (2,1) both belong to r and $1 \neq 2$.

(vii) Let $A = \{1, 2, 3\}$

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

Let $R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 3)\}$.

R is reflexive since as $(a, a) \in R \quad \forall \quad a \in A$.

R is not symmetric since $(1, 2) \in R$ and $(2, 1) \notin R$.

R is anti-symmetric as $(a, b) \in R \; (b, a) \in R \Rightarrow a = b$ holds in R.

R is not transitive since (1, 2) and (2, 3) $\in$R but (1, 3) $\notin$R.

(viii) Let $A = \{1, 2, 3\}$.

Then $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

Let $R = \{(1, 2), (2, 1), (2, 3)\}$.

Since $R \subseteq A \times A$, therefore R is a relation on the set A.

R is not reflexive since $1 \in A$ and $(1, 1) \notin R$.

R is not symmetric since $(2, 3) \in R$ and $(3, 2) \notin R$.

R is not transitive since $(1, 2)$ and $(2, 1) \in R$ and $(1, 1) \notin R$

R is not anti-symmetric since $(1, 2)$ and $(2,1) \in R$ but $1 \neq 2$

(*ix*) Let $A = \{1, 2\}$.

Then $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.

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

$\because$ $R \subseteq A \times A$. So R is a relation on the set A.

R is reflexive since $(a, a) \in R \ \forall \ a \in A$.

R is symmetric since $(a, b) \in R \Rightarrow (b, a) \in R$

R is transitive and anti-symmetric clearly.

Example 2. Check whether the relation R defined in the set $\{1, 2, 3, 4, 5, 6\}$ as $R = \{(a, b) : b = a + 1\}$ reflexive, symmetric or transitive.

Sol. Let $A = \{1, 2, 3, 4, 5, 6\}$

$R = \{(a, b) : b = a + 1\} = \{(a, a + 1)\} = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6)\}$

(*i*) R is not reflexive as $(a, a) \notin R \ \forall \ a \in A$

(*ii*) $(a, b) \in R \Rightarrow (b, a) \in R$ $[\because (a, b) \in R \Rightarrow b = a + 1 \Rightarrow a = b$

$\therefore$ R is not symmetric.

(*iii*) $(a, b) \in R, \ (b, c) \in R \Rightarrow (a, c) \in R$

$[\because (a, b), (b, c) \in R \Rightarrow b = a + 1, \ c = b + 1 \Rightarrow c = a$

$\therefore$ R is not transitive.

Example 3. Let R be the relation defined on the set of natural numbers **N** as

$R = \{(x, y) : x \in \mathbf{N}, \ y \in \mathbf{N}, \ 2x + y = 41\}$

Find the domain and range of this relation R. Also verify whether R is

(*i*) reflexive (*ii*) symmetric (*iii*) transitive

Sol. $2x + y = 41 \Rightarrow y = 41 - 2x$

$x = 1 \Rightarrow y = 41 - 2(1) = 41 - 2 = 39$

$x = 2 \Rightarrow y = 41 - 2(2) = 41 - 4 = 37$

$x = 3 \Rightarrow y = 41 - 2(3) = 41 - 6 = 35$

$x = 4 \Rightarrow y = 41 - 2(4) = 41 - 8 = 33$

.....

$x = 19 \Rightarrow y = 41 - 2(19) = 41 - 38 = 3$

$x = 20 \Rightarrow y = 41 - 2(20) = 41 - 40 = 1$

$x = 21 \Rightarrow y = 41 - 2(21) = 41 - 42 = -1 \notin \mathbf{N}$

$\therefore$ $R = \{(1, 39), (2, 37), (3, 35), (4, 33), \ldots\ldots, (20, 1)\}$

$\therefore$ domain of $R = \{1, 2, 3, 4, \ldots\ldots, 20\}$

and range of $R = \{1, 3, 5, 7, \ldots\ldots, 39\}$

(*i*) Now $1 \in N$ but $(1, 1) \notin R$

$\therefore$ R is not reflexive

(*ii*) $(1, 39) \in R$ but $(39, 1) \notin R$

$\therefore$ R is not symmetric

(*iii*) $(20, 1), (1, 39) \in R$ but $(20, 39) \notin R$

$\therefore$ R is not transitive.

Example 4. If R and R′ are reflexive relations on a set then so are $R \cup R'$ and $R \cap R'$.

Sol. Since R and R′ are relations on a set A.

$\therefore$ $R \subseteq A \times A$ and $R' \subseteq A \times A$.

$\Rightarrow$ $R \cup R' \subseteq A \times A$ and $R \cap R' \subseteq A \times A$.

$\therefore$ $R \cup R'$ and $R \cap R'$ are also relations on the set A.

We now show that $R \cup R'$ is reflexive relation on A.

Let $a \in A$.

$\therefore$ $(a, a) \in R$ and $(a, a) \in R'$. ($\because$ R and R′ are reflexive on A)

$\Rightarrow$ $(a, a) \in R \cup R'$ and $R \cap R' \; \forall \; a \in A$.

$\therefore$ $R \cup R'$ and $R \cap R'$ are reflexive relations on A.

Example 5. For any relation R in a set A, we can define the inverse relation R^{-1} by $a \; R^{-1} \; b$ if and only if $b \; R \; a$. Prove that

(*i*) As a subset of $A \times A$, $R^{-1} = \{(b, a) : (a, b) \in R\}$

(*ii*) R is symmetric if and only if $R = R^{-1}$.

Sol. (*i*) R^{-1} is defined by $a \; R^{-1} \; b$ iff $b \; R \; a$

$\therefore$ R^{-1} is defined by $(a, b) \in R^{-1}$ iff $(b, a) \in R$

$\Rightarrow$ R^{-1} is defined by $(b, a) \in R^{-1}$ iff $(a, b) \in R$

$\therefore$ as a subset of $A \times A$, $R^{-1} = \{(b, a) : (a, b) \in R\}$

(*ii*) R is symmetric if and only if $b \; R \; a = a \; R \; b$

But $b \; R \; a = a \; R^{-1} \; b$

$\therefore$ $a \; R^{-1} \; b = a \; R \; b$

Hence R is symmetric iff $R = R^{-1}$.

Example 6. Let Z be the set of all integers and R be the relation on Z defined as

$R = \{(a, b) : a, b \in Z \text{ and } (a - b) \text{ is divisible by } 5\}$.

Prove that R is an equivalence relation.

Sol. $R = \{(a, b) : 5 \text{ divides } a - b\}$, where R is in the set **Z** of integers.

(*i*) $a - a = 0 = 5 \cdot 0$

$\therefore$ 5 divides $a - a \Rightarrow (a, a) \in R \Rightarrow$ R is reflexive.

(*ii*) Let $(a, b) \in R$

$\therefore$ 5 divides $a - b$

$\Rightarrow$ $a - b = 5n$ for some $n \in \mathbf{Z} \Rightarrow b - a = 5(-n) \Rightarrow$ 5 divides $b - a \Rightarrow (b, a) \in R$

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

$\therefore$ R is symmetric.

(*iii*) Let (a, b) and $(b, c) \in R$

$\therefore$ 5 divides $a - b$ and $b - c$ both

$\therefore$ $a - b = 5n_1$ and $b - c = 5n_2$ for some $n_1, n_2 \in \mathbf{Z}$

$\therefore$ $(a - b) + (b - c) = 5n_1 + 5n_2$

$\Rightarrow$ $a - c = 5(n_1 + n_2) \Rightarrow$ 5 divides $a - c \Rightarrow (a, c) \in R$

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

$\therefore$ R is transitive

From (*i*), (*ii*), (*iii*) it follows that R is an equivalence relation.

Example 7. Show that each of the relation R in the set $A = \{x \in \mathbf{Z} : 0 \le x \le 12\}$, given by

(*i*) $R = \{(a, b) : |a - b| \text{ is a multiple of } 4\}$

(*ii*) $R = \{(a, b) : a = b\}$

is an equivalence relation. Find the set of all elements related to 1 in each case.

Sol. $A = \{x \in \mathbf{Z} : 0 \le x \le 12\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

(*i*) $R = \{(a, b) : |a - b| \text{ is a multiple of } 4\}$

As $|a - a| = 0$ is divisible by 4

$\therefore$ $(a, a) \in R \ \forall \ a \in A$.

$\therefore$ R is reflexive.

Next, let $(a, b) \in R$

$\Rightarrow$ $|a - b|$ is divisible by 4 $\Rightarrow$ $|-(b - a)|$ is divisible by 4 $\Rightarrow$ $|b - a|$ is divisible by 4

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

$\therefore$ R is symmetric.

Again, $(a, b) \in R$ and $(b, c) \in R$

$\Rightarrow$ $|a - b|$ is a multiple of 4 and $|b - c|$ is a multiple of 4

$\Rightarrow$ $a - b$ is a multiple of 4 and $b - c$ is a multiple of 4

$\Rightarrow$ $(a-b)+(b-c)$ is a multiple of 4 $\Rightarrow$ $a-c$ is a multiple of 4

$\Rightarrow$ $|a-c|$ is a multiple of 4 $\Rightarrow$ $(a, c) \in R$

$\therefore$ R is transitive.

$\therefore$ R is an equivalence relation.

Set of elements which are related to 1

$= \{a \in A : (a, 1) \in R\} = \{a \in A : |a-1| \text{ is a multiple of } 4\}$

$= \{1, 5, 9\}$ [$\because |1-1| = 0$, $|5-1| = 4$ and $|9-1| = 8$ are multiples of 4]

(*ii*) $R = \{(a, b) : a = b\}$

$\therefore$ $a = a \; \forall \; a \in A$,

$\therefore$ R is reflexive.

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

$\therefore$ R is symmetric.

Next, $(a, b) \in R$ and $(b, c) \in R$

$\Rightarrow$ $a = b$ and $b = c \Rightarrow a = c \Rightarrow (a, c) \in R$

$\therefore$ R is transitive.

$\therefore$ R is an equivalence relation.

Set of elements of A which are related to $1 = \{a \in A : (a, 1) \in R\} = \{a \in A : a = 1\} = \{1\}$.

Example 8. Prove that the following defines an equivalence relation on the x y-plane :

(x, y) R (s, t) if $x - s$ and $y - t$ are both integers.

Sol. (*i*) Since $x - x$ and $y - y$ are integers

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

$\therefore$ relation is reflexive.

(*ii*) Let (x, y) R (s, t)

$\therefore$ $x - s$ and $y - t$ are integers

$\therefore$ $s - x$ and $t - y$ are integers

$\therefore$ (s, t) R (x, y)

$\therefore$ relation is symmetric.

(*iii*) Let (x, y) R (s, t) and (s, t) R (u, v)

$\therefore$ $x - s, y - t, s - u, t - v$ are integers

Now $x - u = (x - s) + (s - u) =$ integer

and $y - v = (y - t) + (t - v) =$ integer

$\therefore$ $x - u$ and $y - v$ are integers

$\therefore$ (x, y) R (u, v)

$\therefore$ if (x, y) R (s, t) and (s, t) R (u, v), then (x, y) R (u, v)

$\therefore$ relation is symmetric.

Hence the result.

Example 9. If R is the relation in $\mathbf{N} \times \mathbf{N}$ defined by (a, b) R (c, d) if and only if $a + d = b + c$, show tha is equivalence relation.

Sol. Here (a, b) R $(c, d) \Leftrightarrow a + d = b + c$.

(i) Now (a, b) R (a, b) if $a + b = b + a$, which is true.

$\therefore$ relation R is reflexive.

(ii) Now (a, b) R (c, d)

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

$\therefore$ relation R is symmetric.

(iii) Now (a, b) R (c, d) and (c, d) R (e, f)

$\Rightarrow$ $a + d = b + c$ and $c + f = d + e \Rightarrow (a + d) + (c + f) = (b + c) + (d + e) \Rightarrow a + f = b + e$

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

$\therefore$ relation R is transitive.

Now R is reflexive, symmetric and transitive

$\therefore$ relation R is an equivalence relation.

Example 10. In $\mathbf{N} \times \mathbf{N}$, show that the relation defined by (a, b) R (c, d) if $a\,d = b\,c$ is an equiva relation.

Sol. Here (a, b) R $(c, d) \Leftrightarrow a\,d = b\,c$ (i) Now (a, b) R (a, b) if $a\,b = b\,a$, which is true

$\therefore$ relation R is reflexive.

(ii) Now (a, b) R (c, d)

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

$\therefore$ relation R is symmetric.

(iii) Now (a, b) R (c, d) and (c, d) R (e, f)

$\Rightarrow$ $a\,d = b\,c$ and $c\,f = d\,e \Rightarrow (a\,d)\,(c\,f) = (b\,c)\,(d\,e) \Rightarrow a\,d\,c\,f = b\,c\,d\,e$

$\Rightarrow (a\,f)\,(d\,c) = (b\,e)\,(d\,c) \Rightarrow a\,f = b\,e \Rightarrow (a, b)$ R (e, f)

$\therefore$ relation R is transitive

Now R is reflexive, symmetric and transitive

$\therefore$ relation R is an equivalence relation.

Example 11. Prove that mod m relation is an equivalence relation.

Sol. (i) Since $a \equiv a \pmod m$

$\therefore$ relation is reflexive

(ii) Let $a \equiv b \pmod m$

$\therefore$ $a = b + k\,m$

$\Rightarrow$ $b - a = (-k)\,m \Rightarrow b \equiv a \pmod m$

$\therefore$ relation is symmetric

(*iii*) Let $a \equiv b \pmod m$ and $b \equiv c \pmod m$

$\therefore \quad a = b + k_1 m$ and $b = c + k_2 m$

$\therefore \quad a = c + k_2 m + k_1 m$

$\therefore \quad a = c + (k_2 + k_1) m$

$\therefore \quad a = c + k m \Rightarrow a \equiv c \pmod m$

$\therefore$ relation is transitive

Hence the result

Example 12. Let R be a relation defined on the set of real numbers by a R b if $a \leq b$ where a, b are real number. Then R is a partial order relation.

Sol. (*i*) **R is reflexive** since $a \leq a$ for any real number a and hence a R a.

(*ii*) **R is anti-symmetric.** Let a and b be two real numbers such that a R b and b R a.

$\therefore \quad a \leq b$ and $b \leq a. \Rightarrow a = b \Rightarrow$ R is anti-symmetric

(*iii*) **R is transitive.** Let a, b, c be any real numbers such that a R b and b R c.

$\therefore \quad a \leq b$ and $b \leq c. \Rightarrow a \leq c$ *i.e.*, a R $c. \Rightarrow$ R is transitive.

$\therefore$ R is reflexive, anti-symmetric and transitive.

$\therefore$ R is a partial order relation on the set of real numbers.

Example 13. Show that intersection of two partial order relations is a partial order relation. But union of two partial order relations need not be partial order relation. Give suitable example.

Sol. Suppose that R_1 and R_2 be two partial order relation on a non-empty set X

We show that $R_1 \cap R_2$ is partial order relation on X

(*i*) **$R_1 \cap R_2$ is reflexive :** Let $a \in X$ be arbitrary

Then $(a, a) \in R_1$ and $(a, a) \in R_2$, since R_1, R_2 both being partial order relations are reflexive

So $(a, a) \in R_1 \cap R_2$

$\Rightarrow$ $R_1 \cap R_1$ is reflexive

(*ii*) **$R_1 \cap R_2$ is Anti-symmetric :** Let $a, b \in X$ such that $(a, b) \in R_1 \cap R_2$ and $(b, a) \in R_1 \cap R_2$

$\Rightarrow \{(a, b) \in R_1$ and $(a, b) \in R_2\}$ and $\{(b, a) \in R_1$ and $(b, a) \in R_2\}$

$\Rightarrow \{(a, b) \in R_1$ and $(b, a) \in R_1\}$ and $\{(a, b \in R_2$ and $(b, a) \in R_2\}$

$\Rightarrow \quad a = b$ and $a = b$ [$\because$ both R_1 & R_2 are anti-symmetric]

$\Rightarrow \quad a = b$

Thus $R_1 \cap R_2$ is anti-symmetric

(*iii*) **$R_1 \cap R_2$ is transitive :** Let $a, b, c \in X$ such that

$(a, b) \in R_1 \cap R_2$ and $(b, c) \in R_1 \cap R_2$

$\Rightarrow \{(a, b) \in R_1$ and $(a, b) \in R_2\}$ and $\{(b, c) \in R_1$ and $(b, c) \in R_2\}$

$\Rightarrow$ $\{(a, b) \in R_1$ and $(b, c) \in R_1\}$ and $\{(a, b) \in R_2$ and $(b, c) \in R_2\}$

$\Rightarrow$ $(a, c) \in R_1$ and $(a, c) \in R_2$ [$\because$ both R_1 and R_2 are transitive]

$\Rightarrow$ $(a, c) \in R_1 \cap R_2$

Thus $R_1 \cap R_2$ is transitive.

Hence $R_1 \cap R_2$ is partial order relation.

But $R_1 \cup R_2$ need not be partial order relation

For example : Let $X = \{1, 2, 3\}$ then

$X \times X = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$

Let $R_1 = \{(1, 1), (2, 2), (3, 3), (1, 2), (3, 1)\}$

$R_2 = \{(1, 1), (2, 2), (3, 3), (1, 3), (2, 1)\}$

Then R_1 and R_2 are subsets of $X \times X$, Therefore R_1 and R_2 are both relations on X.

R_1 is reflexive since $(a, a) \in R_1 \; \forall \; a \in X$

R_1 is anti-symmetric since for no $(a, b) \in R_1$ with $a \neq b$,

we have $(b, a) \in R_1$

R_1 is transitive since $(a, b) \in R_1$ and $(b, c) \in R_1 \Rightarrow (a, c) \in R_1$

$\therefore$ R_1 is partial order relations on X

Similarly, R_2 is also partial order relation on X

But $R_1 \cup R_2 = \{(1, 1), (2, 2), (3, 3), (1, 2), (3, 1), (1, 3), (2, 1)\}$

with $(1, 2) \in R_1 \cup R_2$ and $(2, 1) \in R_1 \cup R_2$ but $1 \neq 2$

$\therefore$ $R_1 \cup R_2$ is not anti-symmetric

Hence $R_1 \cup R_2$ is not a partial order relation.

EXERCISE 1.6

1. Give an example of relation which is transitive but neither reflexive nor symmetric nor anti-symmetric.
2. Give an example of a relation which is anti-symmetric and transitive but neither reflexive nor symmetric.
3. Give example of relation R on $A = \{1, 2, 3\}$ which is both symmetric and anti-symmetric and is neither symmetric nor anti-symmetric.
4. Show that the relation R in **R** defined as $R = \{(a, b) : a \leq b\}$, is reflexive and transitive but not symmetric.
5. Show that the relation R in the set **R** of real numbers, defined as
   $R = \{(a, b) : a \leq b^2\}$ is neither reflexive nor symmetric nor transitive.
6. Check whether the relation R in **R** defined by
   $R = \{(a, b) : a \leq b^3\}$ is reflexive, symmetric or transitive.

7. Consider the following five relation on set A = {1, 2, 3}

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

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

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

   ϕ = Empty relation

   A × A = Universal relation

   Determine whether or not each of above relations on A is

   (*i*) Reflexive (*ii*) Symmetric (*iii*) Transitive (*iv*) Anti-symmetric

8. The following three relations are defined on the set of natural numbers :

   $R = \{ (x, y) : x < y, \ x \in \mathbf{N}, \ y \in \mathbf{N} \}$

   $S = \{ (x, y) : x + y = 10, \ x \in \mathbf{N}, \ y \in \mathbf{N} \}$

   $T = \{(x, y) : x = y \text{ or } x - y = 1, \ x \in \mathbf{N}, \ y \in \mathbf{N} \}$

   Explain clearly which of the above relations are

   (*i*) Reflexive (*ii*) Symmetric (*iii*) Transitive.

9. Let R be the relation on N defined by R_y if x and y share a common factor other than 1. Determine the reflexivity and transitivity of R.

10. Show that the relation '~' in the set of 2 × 2 invertible matrices with real entries given by A ~ B iff $B = A^{-1}$ is symmetric but not reflexive. Is it transitive ?

11. Suppose R and S are symmetric relations on a set A. Show that R ∩ S is also symmetric.

12. If R and R′ are symmetric relations on a set A, then R ∩R′ is also a symmetric relation on A.

13. Show that the union of two symmetric relations on a set is again a symmetric relation on that set.

14. For any relation R in a set A, we can define the inverse relation R^{-1} by $a \ R^{-1} \ b$ iff $b \ R \ a$. Prove that R is symmetric iff $R^{-1} = R$.

15. Give an example of relation R on A = {1, 2, 3} having the stated property :

    R is neither symmetric nor antisymmetric, and R is transitive but R ∪ R^{-1} is not transitive.

16. R is a relation on set of positive integers s.t. R = {(*a*, *b*) : *a* – *b* is odd integer} Is R an equivalence relation ?

17. For two lines ℓ_1, ℓ_2 in a plane σ, the relation R defined by $\ell_1 \ R \ \ell_2$ if and only if ℓ_1 is perpendicular to ℓ_2 is neither reflexive nor transitive but symmetric. Hence R is not an equivalence relation.

18. Let R be symmetric and transitive relation on a set A. If for each $x \in A$, $\exists \ y \in A$ such that $(x, y) \in R$. Then R is an equivalence relation.

19. Prove that the intersection of two equivalence relations on a non-empty set is again an equivalence relation on that set.

20. Show that $R_1 \cup R_2$ may not be an equivalence relation on a set X if R_1, R_2 are equivalence relations on X.

21. Is inclusion of a subset in another, in the context of a universal set, an equivalence relation in the class of subsets of the sets ? Justify your answer.

22. Show that the relation R in the set **Z** of integers given by $R = \{(a, b) : 2 \text{ divides } a - b\}$ is an equivalence relation.

23. The relation $R \subseteq \mathbf{N} \times \mathbf{N}$ is defined by $(a, b) \in R$ if and only if 5 divides $b - a$. Show that R is an equivalence relation.

24. In the set **N** of all natural numbers. Let relation R be defined by

$R = \{(x, y)/x \in \mathbf{N}, y \in \mathbf{N} : x - y \text{ is divisible by } m\}$

Show that R is an equivalence relation.

25. For $a, b \in \mathbf{R}$ the set of real numbers, defined a S b if $|a| = |b|$ then S is an equivalence relation on **R**.

26. Let R be a relation on the set of A of ordered pairs of positive integers defined by (x, y) R(u, v) and only if $xv = yu$. Show that R is an equivalence relation.

27. For $\frac{a}{b}, \frac{c}{d} \in Q$ – the set of relational numbers, define $\frac{a}{b}$ R $\frac{c}{d}$ if and only if $ad = bc$. Show that R is an equivalence relation on Q.

28. Let **N** denote the set of all natural numbers and R be the relation on $\mathbf{N} \times \mathbf{N}$ defined by (a, b) R $(c, d) \Leftrightarrow ad(b + c) = bc(a + d)$. Check whether R is an equivalence relation on $\mathbf{N} \times \mathbf{N}$.

29. If R is an equivalence relation on a set A, then so is R^{-1}

30. For any $a, b \in \mathbf{N}$, the set of natural numbers, define a R b if and only if a divides b. Then R is a partial order relation.

31. In power set P (X) of X, show that the relation '$\subseteq$' is a partial order. Is it an equivalence relation?

ANSWERS

6. Not reflexive, not symmetric, not transitive.

7. R is not reflexive, not symmetric, anti-symmetric, transitive.

S is reflexive, symmetric, not anti-symmetric, transitive

T is not reflexive, not symmetric, anti-symmetric not transitive,

ϕ is not reflexive, symmetric, anti-symmetric, transitive

A × A is reflexive, symmetric, not anti-symmetric, transit

8. (*i*) R, S, T are not reflexive.

(*ii*) R, T are not symmetric and S is symmetric

(*iii*) R is transitive but S, T are not transitive.

9. R is neither reflexive nor transitive.

10. No. **16.** No **21.** No. **28.** Yes **31.** Yes

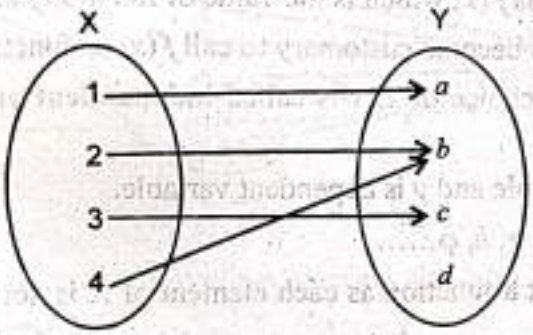
SECTION-III
FUNCTIONS

1.33. Definition of Function

Let X and Y be two non-empty sets. A subset f of $X \times Y$ is called a function from X to Y if for **every** $x \in X$, there exists a **unique** $y \in Y$ such that $(x, y) \in f$ or we say $y = f(x)$.

For example : $X = \{1, 2, 3, 4\}$, $Y = \{a, b, c, d\}$ then subset $f = \{(1, a), (2, b), (3, c), (4, b)\}$ is a function from X to Y $\because$ for each $x \in X$, we have $y \in Y$ such that $y = f(x)$.

Above function is also represented by following figure



Another Definition of Function

Let X and Y be two non-empty sets. Then a rule f which associates each element of X with a **unique** element of Y is called a function from X to Y.

The other terms used for functions are *mappings* or *transformations*. We denote this mapping by $f: X \to Y$ or $X \xrightarrow{f} Y$.

The set X is called the **domain** of f and is written as $D_f = X$. The set Y is called **co-domain** of f.

If an element $y \in Y$ is associated with an element x of X under the rule f, then y is called the **image** of x under the rule f, denoted by $f(x)$.

The set consisting of images of all the elements of X under f is called **Image** set or Range of f and is written as R_f or ran f.

$\therefore$ $R_f = \{f(x) ; x \in X\} = f(X)$ or $R_f = \{y : y = f(x) \text{ where } x \in X\} = f(X)$

Clearly $f(X) \subset Y$

In above example $D_f = \{1, 2, 3, 4\}$

$R_f = \{a, b, c\}$ and co-domain is $\{a, b, c, d\}$.

Note. Difference between Relation and Function

Function is a special case of that of a relation. A relation may relate each element of the domain to more than one element of the range, but a function relates each element of the domain to one and only one element of the co-domain.

It should be noted that every function is a relation but every relation is not a function.

Consider $X = \{1, 2, 3, 4,\}$, $Y = \{5, 6, 7\}$

$X \times Y = \{(1, 5), (1, 6), (1, 7), (2, 5), (2, 6), (2, 7), (3, 5), (3, 6), (3, 7), (4, 5), (4, 6), (4, 7)\}$

Let R be a subset of $X \times Y$ where $R = \{(1, 5), (2, 6), (2, 7), (3, 6), (4, 5)\}$

Here R is not a function from X to Y as $2 \in X$ is associated to two different elements 6, 7 of Y and for a function no two distinct ordered pairs have the same first element. But R is a relation as $R \subset X \times Y$.

Again take $R = \{(1, 5), (2, 7), (3, 6), (4, 5)\}$. In this case R is a function from X to Y as each element of X appears in the first element in one and only one ordered pair in R. R is also a relation from X to Y.

Remark : (*i*) To every $x \in X$, $\exists$ *a* unique $y \in Y$ such that $y = f(x)$. The unique element $y \in Y$ is also called the value of f at x and is denoted by $f(x)$.

(*ii*) Different element of X may be associated with the same element of Y.

(*iii*) There may be elements of Y which are not associated with any element of X.

(*iv*) We refer to a function as f and not as $f(x)$ which is the value of function f at x.

However, by *an abuse of language* it has become customary to call $f(x)$ as function instead of f.

(*v*) Since $f(x)$ or y depends upon the choice of x, x is called **independent** variable and y is called **dependent** variable.

e.g., $y = f(x) = x^2$, x is independent variable and y is dependent variable.

(*vi*) Functions are generally denoted by $f, g, h, \phi, \ldots\ldots$

Examples. The rule shown in the figure is not a function as each element of X is not associated. Here $5 \in X$ has no image in Y.

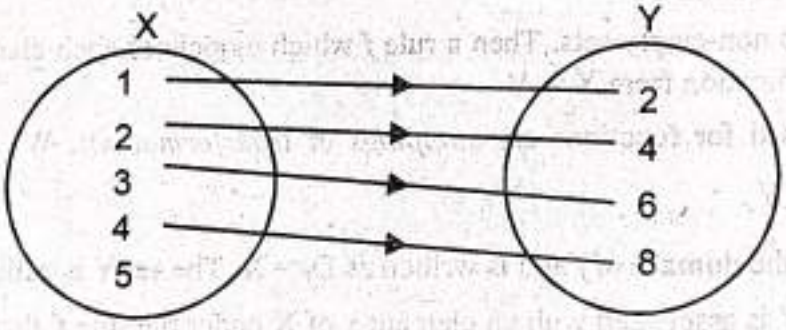


Fig. 1

(*ii*) The rule shown in the figure is not a function as $1 \in X$ is associated with more than one element namely a and b of Y.

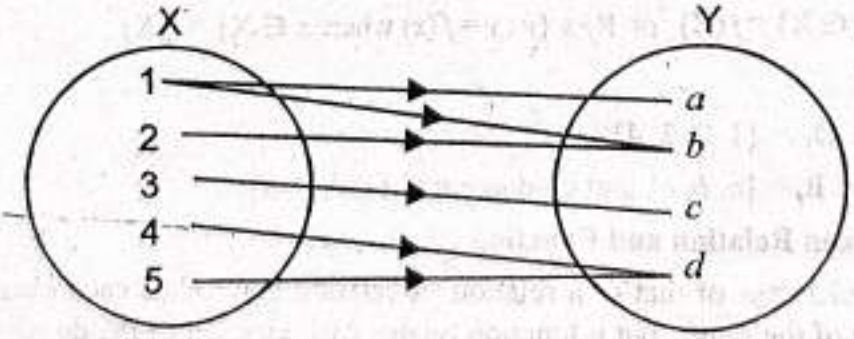


Fig. 2

(*iii*) The rule shown in the figure is a function as each element of X is associated with a unique element of Y.

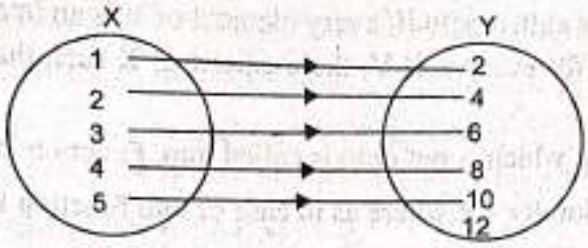


Fig. 3

(*iv*) The rule shown in the figure is a function as each element of X vbis associated with unique element of Y.

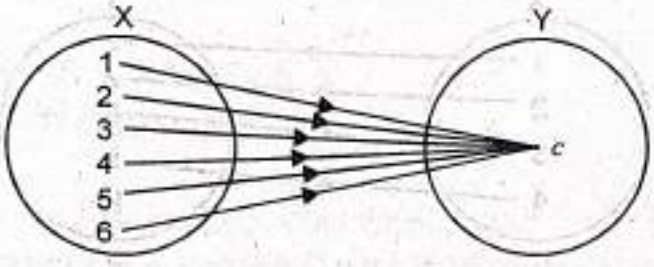


Fig. 4

(*v*) The rule shown in the figure is a function as each element of X is associated with unique element of Y.

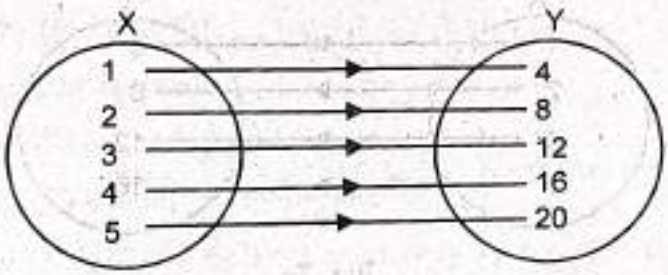


Fig. 5

Types of Functions :

One-one function or Injective function

A function f from X to Y is said to be **one-one** (abbreviated 1-1) iff

$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2) \; \forall \; x_1, x_2 \in X$, or equivalently

$f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \; \forall \; x_1, x_2 \in X$.

In other words if different elements of X under the rule f have different images in Y, then f is called one-one function.

Function shown in fig. 3 is one-one function.

Many-one Function

A function which is not 1-1 is called **many-one** function. Function in fig. 4 is many-one function.

Onto function or Surjective function

A function f from X to Y is called onto iff every element of Y is an image of at least one element of X. In other words we can say that for every $y \in Y$, there exist $x \in X$ such that $y = f(x)$. Function in fig. 5 is onto.

Into Function : A function which is not onto is called into. Function in fig. 3 is into function.

Remark : In case of onto function $R_f = Y$ where as in case of into function R_f is proper subset of Y.

Examples. (*i*) Let X = {1, 2, 3, 4}, Y = {2, 4, 6, 8, 10}

Then the function f depicted by the diagram is 1-1 into

$\because$ $10 \in Y$ has no pre-image in X.

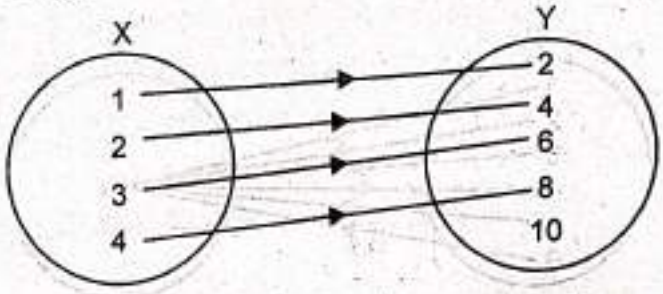


Fig. 6

(*ii*) Let X = {1, 2, 3, 4}, Y = {4, 8, 12, 16}

Then the function f depicted by the diagram is one-one onto.

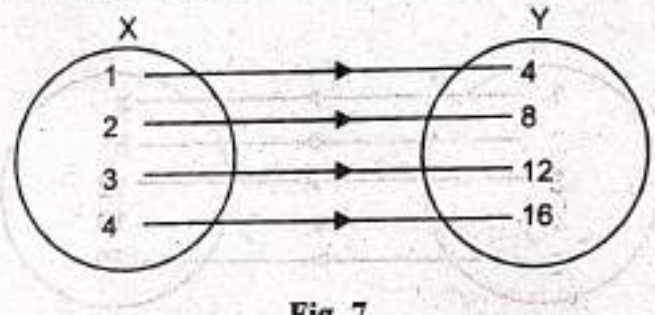


Fig. 7

(*iii*) Let X = {1, 2, 3, 4, 5, 6}, Y = {2}

Then the function f depicted by the diagram is many-one onto.

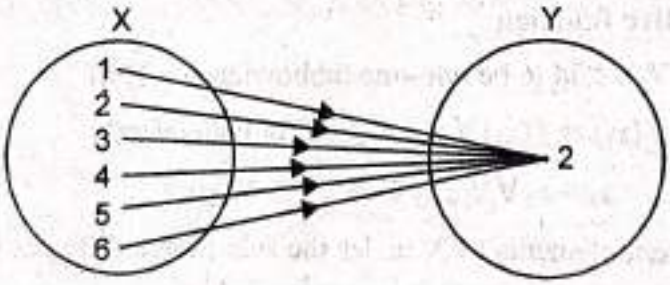


Fig. 8

Bijective function or one-one onto function :

A function which is one-one and onto is called bijective function. It is also called **one-one correspondence.**

Function shown in figure 5 is one-one onto.

Real Valued Function on real variables.

Let X, Y be two non-empty subsets of real numbers. The every function f from X to Y is called a real valued function on real variables.

Equal functions

Two real valued functions f and g are said to be equal iff $D_f = D_g$ and

$f(x) = g(x) \; \forall \; x \in D_f$. We write it as $f = g$.

Constant Function

A function $f: X \to Y$ is called a constant function if $f(x) = y$ for every $x \in X$ and for fixed $y \in Y$.

Function shown in figure 4 is a constant function.

Identity Mapping

Let $I_X : X \to X$ be defined by, $I_X(x) = x \; \forall \; x \in X$.

Then I_X is called the identity mapping on X.

Inverse Mapping

Let $f: X \to Y$ be a one-one onto mapping. Then the mapping $f^{-1} : Y \to X$ which associates to each element $y \in Y$ the unique element $x \in X$ such that $f(x) = y$ is called the inverse map of f.

Let $X = \{1, 2, 3\}$ $Y = \{a, b, c\}$ then $f: \{(1, a), (2, b), (3, c)\}$ is one-one as well as onto. So f^{-1} exist and is defined by $f^{-1} : Y \to X$

$$f^{-1} = \{(a, 1), (b, 2), (c, 3)\}.$$

Method to check one-one (injective) :

Let $f: X \to Y$ be any function.

(*i*) Take two arbitrary elements x_1, x_2 in domain of f.

(*ii*) Solve $f(x_1) = f(x_2)$. If $f(x_1) = f(x_2)$ gives only $x_1 = x_2$ (*i.e.* only one solution) then we say function is one-one. Otherwise function is not one-one. Then it is called many one.

Note : Many one function (not 1-1) can also be proved by taking example. Take two numbers x_1 and x_2 from X such that $x_1 \neq x_2$. Show that $f(x_1) = f(x_2)$.

Example 1. Let $f: N \to N$ defined by $f(x) = 2x + 5$. Prove that f is one-one.

Sol. Let $x_1, x_2 \in N$

such that $f(x_1) = f(x_2)$

$\Rightarrow \quad 2x_1 + 5 = 2x_2 + 5 \Rightarrow 2x_1 + 5 - 2x_2 - 5 = 0$

$\Rightarrow \quad 2(x_1 - x_2) = 0$

$\Rightarrow \quad x_1 - x_2 = 0 \qquad (\text{as } 2 \neq 0)$

$\Rightarrow \quad x_1 = x_2.$

So f is one-one.

Example 2. Let $f: Z \to Z$ defined by $f(x) = x^2$. Prove that f is not one-one.

Sol. To show f is not one-one, we take one example.

Let us take two integers 2 and -2

then $f(2) = (2)^2 = 4$

$f(-2) = (-2)^2 = 4$

Since $2 \neq -2$ but $f(2) = f(-2)$

So f is not one-one.

Method to check onto (Surjective) :

Let $f: X \to Y$ be any function.

(*i*) Take one arbitrary elements y in Y.

(*ii*) Take $y = f(x)$

(*iii*) Solve this equation and find x in terms of y.

(*iv*) If corresponding to every $y \in Y$, there exist $x \in X$ then f is called onto.

If for at least one $y \in Y$, there is no $x \in X$ then f is not onto (or into).

Example : Check wheater $f: N \to N$ defined by $f(x) = 2x + 5$ is onto or not ?

Sol. We take one element from co-domain of f

Let $y \in N$

if possible, let $y = f(x)$

$\Rightarrow$ $y = 2x + 5 \Rightarrow 2x = y - 5$ or $x = \dfrac{y-5}{2}$

We have to check wheater for every $y \in N$, we can find or not $x \in N$ (domain)

if $y = 6$, $x = \dfrac{6-5}{2} = \dfrac{1}{2} \notin N$

So $y = 6$ has no pre-image

$\therefore$ f is not onto.

ILLUSTRATIVE EXAMPLES

Example 1. A function f is defined on the set of integers as follows

$$f(x) = \begin{cases} 1+x & 1 \le x < 2 \\ 2x-1 & 2 \le x < 4 \\ 3x-10 & 4 \le x < 6 \end{cases}$$

(*i*) Find the domain of the function

(*ii*) Find the range of the function

(*iii*) Find the value of $f(4)$

(*iv*) State whether f is one-one or many one function.

Sol. $f(x) = \begin{cases} 1+x & 1 \le x < 2 \\ 2x-1 & 2 \le x < 4 \\ 3x-10 & 4 \le x < 6 \end{cases}$

(*i*) Domain of the function = $D_f = \{x : x \in I \text{ s.t. } f(x) \in I\}$, I = set of integers.

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

(*ii*) Range of the function = $R_f = \{(f(x) : \text{for all } x \in D_f\}$

x	1	2	3	4	5
$f(x)$	2	3	5	2	5

Clearly $R_f = \{2, 3, 5\}$

(*iii*) Since $f(x) = 3x - 10$ for $4 \le x < 6$

$\therefore \quad f(4) = 3(4) - 10 = 12 - 10 = 2$

(*iv*) From (*ii*) we observe that

$f(1) = 2$ and $f(4) = 2$ and $1 \ne 4$.

$\therefore$ f is many-one function.

Example 2. (*a*) Give an example of a map (*i*) which is one to one but not onto, (*ii*) which is not one to one but onto. (*iii*) which is neither one to one nor onto.

(*b*) Define the following functions on integers by

$$f(k) = k + 1, \; g(k) = 2k \text{ and } h(k) = \left[\frac{k}{2}\right].$$

(*i*) Which of these are one to one ?

(*ii*) Which of these are onto ?

Sol. (*i*) Consider the function $f: \mathbf{N} \to \mathbf{N}$ defined by $f(x) = x^2$

then f is one-one but not onto function.

For one-one

Let $n_1, n_2 \in \mathbf{N}$ be such that

$$f(n_1) = f(n_2) \Rightarrow n_1^2 = n_2^2$$

$\Rightarrow \quad n_1 = n_2$ $\quad [n_1 = \pm n_2$ but as $n_1 \in \mathbf{N}$ so reject negative]

$\therefore$ f is one-one

For onto Since $2 \in \mathbf{N}$ but $\nexists\ n \in \mathbf{N}$ such that

$$f(n) = 2$$

i.e., $\quad n^2 = 2$ $\quad$ [There is no natural number whose square is 2]

$\therefore$ f is not onto

(*ii*) Consider the function $f: \mathbf{Z} \to \mathbf{N} \cup \{0\}$ defined by

$$f(n) = |n|$$

Then f is not one-one function but onto.

For one-one

Let $n_1, n_2 \in \mathbf{Z}$ be such that

$$f(n_1) = f(n_2)$$

$\Rightarrow$ $|n_1| = |n_2| \Rightarrow n_1 = \pm n_2$

$\therefore$ f is not one-one function

For example $5, -5 \in \mathbf{Z}$

$$f(5) = 5,\ f(-5) = 5$$

So f is not one-one.

For onto Since $\mathbf{N} \cup \{0\} \subseteq \mathbf{Z}$

$\therefore$ for any $n \in \mathbf{N} \cup \{0\}$, $\exists\ n \in \mathbf{Z}$ such that

$$f(n) = |n| = n$$

$\therefore$ f is onto

(*iii*) Consider the function $f: \mathbf{Z} \to \mathbf{N} \cup \{0\}$ defined by

$$f(x) = |n^2|$$

For one-one : Let $n_1, n_2 \in \mathbf{Z}$ be such that

$\therefore$ $f(n_1) = f(n_2) \Rightarrow |n_1^2| = |n_2^2| \Rightarrow n_1 = \pm n_2$

$\therefore$ f is not one-one function

For onto : Since $2 \in \mathbf{N} \cup \{0\}$ but $\nexists\ n \in \mathbf{Z}$ such that $f(n) = 2$

$\therefore$ f is not onto.

(*b*) Given $f(k) = k + 1$, $g(k) = 2k$ and $h(k) = \left[\frac{k}{2}\right]$

Let $k_1, k_2 \in \mathbf{I}$ such that

$$f(k_1) = f(k_2) \Rightarrow k_1 + 1 = k_2 + 1 \Rightarrow k_1 = k_2$$

$\therefore$ f is one-one function

Again, let $g(k_1) = g(k_2) \Rightarrow 2k_1 = 2k_2 \Rightarrow k_1 = k_2$

$\therefore$ h is one-one function

Again, let $h(k_1) = h(k_2)$

$\Rightarrow$ $\left[\frac{k_1}{2}\right] = \left[\frac{k_2}{2}\right] \Rightarrow \frac{k_1}{2} = \frac{k_2}{2}$ not necessary

i.e. $k_1 = k_2$ not necessary

For example if $k_1 = 4, k_2 = 5$

$$h(k_1) = \left[\frac{4}{2}\right] = 2, \quad h(k_2) = \left[\frac{5}{2}\right] = 2$$

But $k_1 \neq k_2$

So h is not one-one.

(*ii*) **onto** (*a*) Let $y \in Z$ (Integer)

such that $y = f(k) \Rightarrow y = k + 1 \Rightarrow k = y - 1$

For all $y \in Z$, there exist $k \in Z$ such that $y = f(k)$ so f is onto.

(*b*) Again let $y \in Z$

such that $y = g(k) \Rightarrow y = 2k \Rightarrow k = \frac{y}{2}$

now for $y = 5$ $k = \frac{5}{2} \notin Z$ so g is not onto.

(*c*) Let $y \in Z$ such that $y = y(k)$

$$\Rightarrow \quad y = \left[\frac{k}{2}\right] \Rightarrow y < \frac{k}{2} < y + 1 \Rightarrow 2y \leq k < 2y + 2$$

So for every $y \in Z$ we have at two values of k, $2y$ and $2y + 1$ such that $y = h(k)$

So h is onto.

Example 3. If $f(x) = \frac{1}{1-x}$, then what is $f[f\{f(x)\}]$?

Sol. Here $f(x) = \frac{1}{1-x}$ ...(1)

$$\therefore \quad f\{f(x)\} = \frac{1}{1 - f(x)} = \frac{1}{1 - \frac{1}{1-x}} \qquad [\because \text{ of (1)}]$$

$$= \frac{1-x}{1-x-1}$$

$$\therefore \quad f\{f(x)\} = \frac{1-x}{-x}$$

$$\therefore \quad f[f\{f(x)\}] = \frac{1-f(x)}{-f(x)} = \frac{1-\frac{1}{1-x}}{-\frac{1}{1-x}} \qquad [\because \text{ of (1)}$$

$$= \frac{1-x-1}{-1} = \frac{-x}{-1}$$

$$\therefore \quad f[f\{f(x)\}] = x.$$

Example 4. Specify the types (one-to-one or onto or both or neither) of the following function :

(*i*) $f: N \to N$ and $f(j) = J(\text{mod } 4)$

(*ii*) $g: N \times N \to N$ such that $g(x, y) = x + y$

(*iii*) $X = R$, $Y = \{x : x \in R \text{ and } x > 0\}$ and $f(x) = |x|$.

Sol. (*i*) $f: N \to N$

One-one : $f(j) = J \text{ (mod 4)}$ [$f(j) = J(\text{mod } 4)$ means J is remainder when j is divided by 4

f is not one-one

$\because$ $f(3) = 3 \text{ (mod 4)} = 3$, $f(7) = 7 \text{ (mod 4)} = 3$

Now $f(3) = f(7)$

But $3 \neq 7$

So, f is not one-one.

Onto : Again f is not onto

$\because$ $f(j)$ can be 0, 1, 2, 3 only

for $5 \in N$ there is no j such that $f(j) = 5$.

(*ii*) $g: N \times N \to N$ such that $g(x, y) = x + y$

One-one : Let $(x_1, y_1), (x_2, y_2) \in N \times N$ such that $g(x_1, y_1) = g(x_2, y_2)$

$\Rightarrow$ $x_1 + y_1 = x_2 + y_2$

which does not implies $x_1 = x_2$, $y_1 = y_2$

e.g. $g(3, 7) = 10$, $g(7, 3) = 10$

But $(3, 7) \neq (7, 3)$

So, g is not one-one.

Onto : Now for $1 \in N$

there does not exist $(x, y) \in N \times N$ such that $g(x, y) = 1$ so, g is not onto.

(*iii*) $f(x) = |x|$

One-one : Let $x_1, x_2 \in R$ such that $f(x_1) = f(x_2)$

$\therefore$ $|x_1| = |x_2| \Rightarrow x_1 = x_2$ or $x_1 = -x_2$

so, f is not one-one. For example $f(3) = 3$ and $f(-3) = 3$. But $3 \neq -3$

Onto : Let $y \in \{x : x \in R \text{ and } x > 0\}$

i.e. $y > 0, y \in R$ then $\forall\ y \in R$

$\exists$ $x \in R$ such that $f(x) = y$

so, f is onto.

Example 5. Let A = B = {1, 2, 3, 4, 5}. Define functions f : A → B (if possible) such that:

(*i*) f is one-to-one and onto

(*ii*) f is neither one-to-one nor onto

(*iii*) f is one-one but not onto.

(*iv*) f is onto but not one-to-one.

Sol. (*i*) Let f : A → B defined by $f(x) = x, \forall\ x \in A$.

i.e. $f = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$ f is one-to-one and onto.

(*ii*) Let f : A → B defined by $f(x) = 1, \forall\ x \in A$.

i.e. $f = \{(1, 1), (2, 1), (3, 1), (4, 1), (5, 1)\}$

Clearly f is neither one-to-one nor onto.

(*iii*) None exists. Reason is that as A and B contains equal number of elements. So if we define one-one function from A to B, then it will be onto also.

(*iv*) None exists. Again A and B contains equal number of elements. So if we define onto function from A to B, then it will be one-one also.

Example 6. For a function $g : R \to R$, determine whether the following functions are one-to-one and onto. If the function is not onto, determine range g (R).

(*i*) $g(x) = x + 7$ (*ii*) $g(x) = x^2 + x$.

Sol. $g : R \to R$

(*i*) $g(x) = x + 7$

One-one : Let $x_1, x_2 \in R$ such that $g(x_1) = g(x_2)$

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

$\therefore$ g is one-one.

Onto : Let $y \in R$

such that $y = g(x)$

$\Rightarrow$ $y = x + 7 \Rightarrow x = y - 7$

so $\forall y \in R \; \exists x \in R$ such that $y = g(x)$

Hence g is onto.

(ii). $g(x) = x^2 + x$

g is not one-one as $g(0) = 0^2 + 0 = 0$, $g(-1) = (-1)^2 + (-1) = 0$

But $0 \neq -1$

Again let $y \in R$ such that $y = g(x)$

$\Rightarrow$ $y = x^2 + x \Rightarrow x^2 + x - y = 0$

For $y = -2$ we have $x^2 + x + 2 = 0$.

Hence $D = b^2 - 4ac = 1 - 4 \times 1 \times 2 = -7 < 0$

So x will be imaginary so g is not onto.

Range of g : we have $x^2 + x - y = 0$

y should be such that $D \geq 0$

$$1 - 4 \times 1 \times (-y) \geq 0 \Rightarrow 1 + 4y \geq 0 \text{ or } y \geq -\frac{1}{4} \quad y \in R.$$

$$\therefore \quad R_g = \left\{ y \in R, y \geq -\frac{1}{4} \right\}$$

Example 7. Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$ how many functions $f : A \to B$ satisfy $f(1) = f(2)$ Give reason.

Sol. $A = \{1, 2, 3, 4\}$, $B = \{x, y, z\}$

Since $f(1) = f(2) = x$

We know in a function $f: A \to B$

Every element of A is uniquely associated to an element of B.

It is given that image of 1 and 2 is x.

Image of 3 can be x or y or z.

Similarly image of 4 can be x or y or z,

i.e. 3 and 4 can have image in 3 ways each.

So, total number of functions $= 1 \times 1 \times 3 \times 3 = 9$.

Example 8. Consider $f: N \to Z_{10}$ defined by $f(a)$ = the remainder after dividing 10 into a. what is $f(23)$? Describe the set of elements of N whose image is zero.

Sol. $f: N \to Z_{10}$ defined by $f(a)$ = the remainder after dividing 10 into a.

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

$f(23) = 3$ [because when we divide 23 by 10, we get 3 as remainder]

The set of elements of N whose image is zero is

$\{10, 20, 30, ...\} = 10k, k \in N$.

Example 9. Under that condition a constant function can be (*i*) one-to-one (*ii*) an onto function.

Sol. (*i*) For $f: A \to B$ to be one-one, different elements of A must have different images in B which is possible iff A contains only one element. So, f is one-one iff domain contains single element.

(*ii*) Also for $f: A \to B$ to be onto, every element of B must be an image of at least one element of A, which is true iff B contains only one element. So, condition for onto is that co-domain contains only one element.

Example 10. Prove that the function $f: C \to \mathbf{R}$, defined by $f(z) = |z|$ is neither one-one nor onto.

Sol. $f: C \to \mathbf{R}$

$f(z) = |z|$

Let $z_1 = 2 + 3i, z_2 = 2 - 3i \Rightarrow z_1 \neq z_2$

$f(z_1) = |z_1| = \sqrt{4+9} = \sqrt{13}$ $\quad [z = x + iy, \ |z| = \sqrt{x^2 + y^2}\ ]$

$f(z_2) = |z_2| = \sqrt{4+9} = \sqrt{13}$

Here $f(z_1) = f(z_2)$.

But $z_1 \neq z_2$

so, f is not one-one.

Onto : again let $-3 \in \mathbf{R}$.

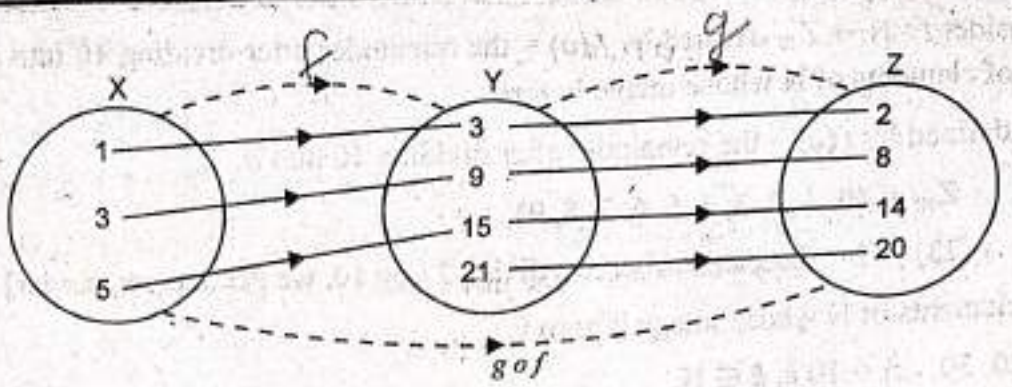
But there does not exist any complex number such that $f(z) = -3$.

So, f is not onto.

1.34. Composition of Functions

Let f be a function from X to Y and let g be a function from Y to Z. Let $X \in X$. Then the image of x under f *i.e.*, $f(x)$ is in Y. Now $g: Y \to Z$ and $f(x) \in Y$, therefore we can find the image of $f(x)$ under g *i.e.*, we can find $g[f(x)]$ which will be in Z. Also $f(x)$ is unique and consequently $g[f(x)]$ is unique. Thus we have a rule which assigns to element $x \in X$ a unique element $g[f(x)] \in Z$. In this way, we have a function from X to Z. This function is called the function of a function or composite function of g and f and is denoted by $g \circ f$.

Let $X = \{1, 3, 5\}$, $Y = \{3, 9, 15, 21\}$, $Z = \{2, 8, 14, 20\}$



Let f be a function from X to Y and g be a function from Y to Z such that

$$f = \{(1, 3), (3, 9), (5, 15)\}, g = \{(3, 2), (9, 8), (15, 14), (21, 20)\}$$

then $g \circ f = \{(1, 2), (3, 8), (5, 14)\}$

It must be noted that

(*i*) $g \circ f$ is defined only when $R_f \subset D_g$.

(*ii*) It is possible that one of fog may be defined while the other may not be defined.

(*iii*) $g \circ f$ and $f \circ g$ both may be defined but may not be equal.

Composite Function : Let f be a function with domain X and range in Y and let g be a function domain Y and range in Z. The function with domain X and range in Z which maps an element $x \in X$, $g(f(x))$, is called the composite of the functions f and g and is written as $g \circ f$.

Properties of composite functions.

Let f, g, h be three functions and α be a real number, then

(*i*) $(f \circ g) \circ h = f \circ (g \circ h)$ (Associative Law)

(*ii*) $f \circ (g + h) = f \circ g + f \circ h$ (Distributive Law)

(*iii*) $(\alpha f) \circ g = \alpha . (f \circ g)$ (Scalar multiplication)

(iv) $f \circ g \neq g \circ f$ (Non – Commutative)

1.35. Equality of Maps

Two maps f and g are called equal maps if

(*i*) Domain of f = Domain of g

(*ii*) $f(x) = g(x)\ \forall\ x \in$ common domain of f and g

1.36. Show that the composition of maps is associative.

Proof. Let $f: A \to B$, $g: B \to C$, $h: C \to D$ be mapping then $h \circ (g \circ f)$ and $(h \circ g) \circ f$ are both maps from A to D

$\therefore$ domain of $h \circ (g \circ f)$ = domain of $(h \circ g) \circ f$ [Each A]

Let $x \in A$

then $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$

and $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$

$\therefore$ $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$ $\forall\ x \in A$ ...(2)

$\therefore$ from (1) and (2) we get,

$h \circ (g \circ f) = (h \circ g) \circ f$

Hence composition of maps is associative.

1.37. If $f: A \to B$ and $g: B \to C$ are both one - one maps, then $g \circ f$ is also one- one.

Proof. Since $f: A \to B$ and $g: B \to C$ are maps therefore $g \circ f$ is a map from A to C. Let $x_1, x_2 \in A$ such that

$(g \circ f)(x)_1 = (g \circ f)(x)_2 \Rightarrow g(f(x_1)) = g(f(x_2))$

$\Rightarrow$ $f(x_1) = f(x_2)$, since g is one-one $\Rightarrow x_1 = x_2$ since f is one-one

$\therefore$ $g \circ f$ is a one- one map.

1.38. If $f: A \to B$ and $g: B \to C$ are both onto maps, then $g \circ f$ is also onto.

Proof. Since f, g are onto

Let $c \in C$ be any element, then $\exists\ b \in B$ such that

$g(b) = c$ ($\because$ g being onto)

Again for this $b \in B$, $\exists$ some $a \in A$ such that

$f(a) = b$ ($\therefore$ f is onto)

$\therefore$ $g \circ f(a) = g(f(a)) = g(b) = c$

Thus for $c \in C$, $\exists\ a \in A$ such that

$g \circ f(a) = c$

Hence $g \circ f: A \to C$ is onto.

1.39. If $f: A \to B$ and $g: B \to C$ are both one-one and onto maps *i.e.*, bijective maps then $g \circ f$ is also both one-one and onto *i.e.*, bijective map.

Proof : Combining 1.37 and 1.38, we get required result.

1.40. If $f: A \to B$ and $g: B \to C$ are two maps such that $g \circ f$ is one- one. Then f is one- one but g may not be one- one.

Proof. Since $f: A \to B$, $g: B \to C$ are maps

$\therefore$ $g \circ f: A \to C$ is a map. Also $g \circ f$ is given to be one- one map.

If possible, suppose that f is not one-one

$\therefore$ $\exists\ x_1, x_2 \in A$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$.

But $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow g \circ f(x_1) = g \circ f(x_2)$

$\therefore$ $x_1, x_2 \in A$ such that $x_1 \neq x_2$, but $(g \circ f)(x_1) = (g \circ f)(x_2)$

$\therefore$ $g \circ f$ is not one-one, which is against the given hypothesis that $g \circ f$ is one-one.

Thus our supposition is wrong

$\therefore$ f is one-one

We, now give an example to illustrate that if $g o f$ is one- one, then g may not be one-one.

Let $A = \{1, 2\}, B = \{4, 5, 6\}, C = \{7, 8, 9, 10\}$

Let $f = \{(1, 4), (2,6)\}$ and $g = \{(4,7), (5,8), (6,8)\}$

then f and g are functions from A to B and from B to C respectively.

Have $R_f = \{4, 6\} \subseteq D_g = \{4, 5, 6\}$

$\therefore$ $R_f \subseteq D_g$

$\Rightarrow$ $g o f$ is defined and $D_{g o f} = D_f = A = \{1, 2\}$

$g o f(1) = g(f(1)) = g(4) = 7$

$g o f(2) = g(f(2)) = g(6) = 8$

$\therefore$ $g o f = \{(1, 7), (2, 8)\}$

Here, $g o f$ is one-one map since different elements of A have different image.

But g is not one-one since

$g(5) = g(6) = 8$. But $5 \neq 6$

1.41. If $f: A \to B$ and $g: B \to C$ are two maps such that $g o f$ is onto then g is onto but f may not be onto

Proof. Since $f: A \to B$ and $g: B \to C$ are maps, so $g o f$ is a map from A to C. We are given that $g o f: A \to C$ is onto. We now prove that g is onto

Let $z \in C$.

Since $g o f: A \to C$ is onto, so $\exists\, x \in A$ such that $g o f(x) = z$

$\Rightarrow$ $g(f(x)) = z \Rightarrow g(y) = z$ where $y = f(x)$

Since $x \in A$ and f is a map from A to B

Therefore $f(x) \in B$

$\Rightarrow$ $y \in B$

for given $z \in C$, we have determined $y \in B$ such that $g(y) = z$

$\therefore$ $g: B \to C$ is onto

Now, we show by an example that if $g o f$ is onto, then f may not be onto

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

Let $f = \{(1, 4), (2, 6)\}$ and $g = \{(4, 7), (5, 7), (6, 7)\}$

Then f is a function from A to B and g is a function from B to C

$\therefore$ $g o f$ is a function from A to C such that $g o f = \{(1, 7), (2, 7)\}$

Here, $g o f$ is onto. But f is not onto since 5 belonging to B has no pre-image in A under the map f.

1.42. If $f: A \to B$ and $g: B \to C$ are two maps such that $g o f: A \to C$ is both one-one and onto map f is one-one and g is onto.

Proof. Combining 1.40, and 1.42, we get required result.

1.43. Invertible Function

A function f defined from X to Y is said to be invertible if there exists a function g from Y to X such that $g o f = I_X$ and $f o g = I_Y$, where I_X is an identity mapping on X and I_Y is an identity mapping on Y.

Note : f and g are called inverse of each other.

1.44. Let $f: X \to Y$. Then $f \circ I_X = f = I_Y \circ f$.

Proof. Let x be any element of X and let $f(x) = y, y \in Y$

Since $f: X \to Y$ and $I_Y : Y \to Y$

$\therefore$ $I_X \circ f: X \to Y$

Now $(I_Y \circ f)(x) = I_Y(f(x)) = I_Y(y) = y = f(x) \; \forall x \in X$

$\therefore$ $I_Y \circ f = f$

Again $I_X : X \to X$ and $f: X \to Y$

$\therefore$ $f \circ I_X : X \to Y$

Now $(f \circ I_X)(x) = f(I_X(x)) = f(x) \; \forall x \in X$

$\therefore$ $f \circ I_X = f$.

1.45. Let $f: X \to Y$ be one-one onto. Then the inverse map of f is unique.

Proof. Let $g: Y \to X$ and $h: Y \to X$ be two inverse maps of f.

Let y be an arbitrary element of Y.

Let $g(y) = x_1$ and $h(y) = x_2$

Since g is an inverse map of f

$\therefore$ $g(y) = x_1$

$\Rightarrow$ $f(x_1) = y$ ...(1)

Again h is an inverse map of f

$\therefore$ $h(y) = x_2$

$\Rightarrow$ $f(x_2) = y$ ...(2)

From (1) and (2), we get, $f(x_1) = f(x_2)$

$\because$ f is one-one

$\therefore$ $f(x_1) = f(x_2)$

$\Rightarrow$ $x_1 = x_2 \Rightarrow g(y) = h(y) \; \forall y \in Y$

$\therefore$ $g = h$

$\therefore$ inverse map of f is unique.

1.46. A function $f: X \to Y$ is invertible iff f is one-one and onto.

Proof. (*i*) Assume that $f: X \to Y$ is invertible

$\therefore$ $\exists$ a function $g: Y \to X$ such that $f \circ g = I_Y$ and $g \circ f = I_X$

We will prove that f is one-one and onto.

To prove that f is one-one

Let $x_1 \in X, x_2 \in X$

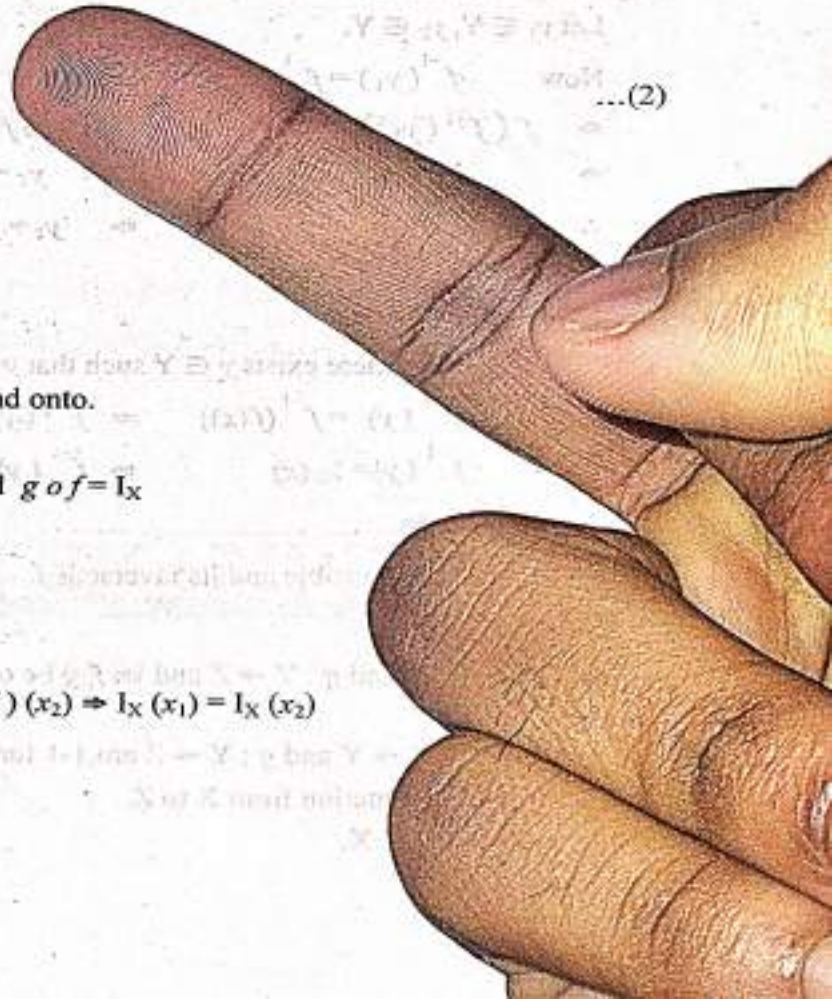
Now $f(x_1) = f(x_2)$

$\Rightarrow$ $g(f(x_1)) = g(f(x_2)) \Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow I_X(x_1) = I_X(x_2)$

$\Rightarrow$ $x_1 = x_2$

$\therefore$ $f(x_1) = f(x_2) \Rightarrow x_1 = x_2 \; \forall x_1, x_2 \in X$

$\therefore$ f is one-one.



To prove f is onto

To each $y \in Y$, there exists $x \in X$ such that $g(y) = x$.

$\Rightarrow f(g(y)) = f(x) \Rightarrow (f \circ g)(y) = f(x) \Rightarrow I_Y(y) = f(x) \Rightarrow y = f(x)$

$\therefore$ f is onto.

(*ii*) Assume that $f: X \to Y$ is one-one and onto. We are to show that f is invertible.

Since f is one-one and onto

$\therefore$ to each $y \in Y$, there exists one and only one $x \in X$ such that $f(x) = y$.

$\therefore$ we can define a function $g: Y \to X$ such that $g(y) = x$ iff $f(x) = y$

Now $(g \circ f)(x) = g(f(x)) = g(y) = x, \forall x \in X$

$\therefore$ $g \circ f = I_X$

Again $(f \circ g)(y) = f(g(y)) = f(x) = y, \forall y \in Y$

$\therefore$ $f \circ g = I_Y$

$\therefore$ f is invertible and g is inverse of f.

1.47. If a function $f: X \to Y$ be one-one and onto then f^{-1} is also one-one and onto.

Proof. $\because$ $f: X \to Y$ is one-one and onto

$\therefore$ $f^{-1}: Y \to X$ exists and $f^{-1} \circ f = I_X, f \circ f^{-1} = I_Y$

To prove f^{-1} is one-one

Let $y_1 \in Y, y_2 \in Y$.

Now $f^{-1}(y_1) = f^{-1}(y_2)$

$\Rightarrow f(f^{-1}(y_1)) = f(f^{-1}(y_2)) \Rightarrow (f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$

$\Rightarrow I_Y(y_1) = I_Y(y_2) \Rightarrow y_1 = y_2$

$\therefore$ $f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow y_1 = y_2 \; \forall y_1, y_2 \in Y$

$\therefore$ f^{-1} is one-one.

To prove f^{-1} is onto

To each $x \in X$, there exists $y \in Y$ such that $y = f(x)$

$\Rightarrow f^{-1}(y) = f^{-1}(f(x)) \Rightarrow f^{-1}(y) = (f^{-1} \circ f)(x)$

$\Rightarrow f^{-1}(y) = I_X(x) \Rightarrow f^{-1}(y) = x$

$\therefore$ f^{-1} is onto

Cor. $\because$ f^{-1} is invertible and its inverse is f.

$\therefore$ $(f^{-1})^{-1} = f$.

1.48. Let $f: X \to Y$ and $g: Y \to Z$ and let f, g be one-one onto. Then $g \circ f: X \to Z$ is also one-one onto $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. (*i*) Here $f: X \to Y$ and $g: Y \to Z$ are 1-1 functions.

Now $g \circ f$ is a function from X to Z.

Let $x_1 \in X, x_2 \in X$.

Now $(g\,o\,f)(x_1) = (g\,o\,f)(x_2)$

$\Rightarrow$ $g(f(x_1)) = g(f(x_2))$ [$\because$ g is one-one]

$\Rightarrow$ $f(x_1) = f(x_2)$ [$\because$ f is one-one]

$\Rightarrow$ $x_1 = x_2$

$\therefore$ $(g\,o\,f)(x_1) = (g\,o\,f)(x_2) \Rightarrow x_1 = x_2 \; \forall \, x_1, x_2 \in X$

$\therefore$ $g\,o\,f$ is $1-1$.

(*ii*) Here $f: X \to Y$ and $g: Y \to Z$ are onto functions.

$\therefore$ $g\,o\,f$ is defined from X to Z

$\because$ g is an onto mapping from $Y \to Z$

$\therefore$ to each $z \in Z$, there exists $y \in Y$ such that $g(y) = z$.

Again as f is an onto mapping from X to Y.

$\therefore$ to each $y \in Y$, there exists $x \in X$ such that $f(x) = y$

$\therefore$ to each $z \in Z$, there exists $x \in X$ such that

$z = g(y) = g(f(x)) = (g\,o\,f)(x)$.

$\therefore$ $g\,o\,f$ is onto.

(*iii*) Now $f: X \to Y$ and $g: Y \to Z$ are one-one and onto.

$\therefore$ $f^{-1}: Y \to X$ and $g^{-1}: Z \to Y$ exist and the function $f^{-1}\,o\,g^{-1}$ is defined from Z to X.

Also $g\,o\,f: X \to Z$ is one-one and onto.

$\therefore$ $(g\,o\,f)^{-1}$ exists and is defined from Z to X.

Now $(f^{-1}\,o\,g^{-1})\,o\,(g\,o\,f) = f^{-1}\,o\,(g^{-1}\,o\,g)\,o\,f = f^{-1}\,o\,I_Y\,o\,f = f^{-1}\,o\,(I_Y\,o\,f) = f^{-1}\,o\,f = I_X$

Again $(g\,o\,f)\,o\,(f^{-1}\,o\,g^{-1}) = g\,o\,(f\,o\,f^{-1})\,o\,g^{-1} = g\,o\,I_Y\,o\,g^{-1} = (g\,o\,I_Y)\,o\,g^{-1} = g\,o\,g^{-1} = I_Z$

$\therefore$ $(f^{-1}\,o\,g^{-1})\,o\,(g\,o\,f) = I_X$ and $(g\,o\,f)\,o\,(f^{-1}\,o\,g^{-1}) = I_Z$

$\therefore$ $(g\,o\,f)^{-1} = f^{-1}\,o\,g^{-1}$

ILLUSTRATIVE EXAMPLES

Example 1. Let $A = \{1, 2, 3, 4, 5\}$. Let $f: A \to A$ and $g: A \to A$ be defined by

$f(1) = 3, f(2) = 5, f(3) = 3, f(4) = 1, f(5) = 2,$

$g(1) = 4, g(2) = 1, g(3) = 1, g(4) = 2, g(5) = 3.$

Find $(g\,o\,f)$ and $(f\,o\,g)$.

Sol. $(f\,o\,g)(1) = f(g(1)) = f(4) = 1$

$(f\,o\,g)(2) = f(g(2)) = f(1) = 3$

$(f\,o\,g)(3) = f(g(3)) = f(1) = 3$

$(f\,o\,g)(4) = f(g(4)) = f(2) = 5$

$(f\,o\,g)(5) = f(g(5)) = f(3) = 3$

$(g\,o\,f)(1) = g(f(1)) = g(3) = 1$

$(g\,o\,f)(2) = g(f(2)) = g(5) = 3$

$(g\,o\,f)(3) = g(f(3)) = g(3) = 1$

$(g\,o\,f)(4) = g(f(4)) = g(1) = 4$

$(g\,o\,f)(5) = g(f(5)) = g(2) = 1$

$\therefore$ $f\,o\,g$ and $g\,o\,f$ are not equal in general.

Example 2. If $f, g : \mathbf{R} \to \mathbf{R}$ are defined respectively by $f(x) = x^2 + 3x + 1$, $g(x) = 2x - 3$ find formu for $(i)\, f\,o\,g$ $(ii)\, g\,o\,f$ $(iii)\, f\,o\,f$ $(iv)\, g\,o\,g$.

Sol. Here $f(x) = x^2 + 3x + 1, g(x) = 2x - 3$

(i) $(f\,o\,g)(x) = f(g(x)) = f(2x-3) = (2x-3)^2 + 3(2x-3) + 1$

$= 4x^2 - 12x + 9 + 6x - 9 + 1 = 4x^2 - 6x + 1$

(ii) $(g\,o\,f)(x) = g(f(x)) = g(x^2 + 3x + 1) = 2(x^2 + 3x + 1) - 3$

$= 2x^2 + 6x + 2 - 3 = 2x^2 + 6x - 1$

(iii) $(f\,o\,f)(x) = f(f(x))$

$= f(x^2 + 3x + 1) = (x^2 + 3x + 1)^2 + 3(x^2 + 3x + 1) + 1$

$= x^4 + 9x^2 + 1 + 6x^3 + 6x + 2x^2 + 3x^2 + 9x + 3 + 1 = x^4 + 6x^3 + 14x^2 + 15x +$

(iv) $(g\,o\,g)(x) = g(g(x))$

$= g(2x-3) = 2(2x-3) - 3 = 4x - 6 - 3 = 4x - 9$

Example 3. Is $f(x) = \dfrac{x-1}{x+1}$ invertible in its domain ? If so, find f^{-1}. Further verify that $(f\,o\,f^{-1})(x) = x$

Sol. Here $f(x) = \dfrac{x-1}{x+1}$

D_f = set of all reals except -1

R_f = set of all reals except 1

Let $x_1, x_2 \in D_f$ and $f(x_1) = f(x_2)$

$\Rightarrow \quad \dfrac{x_1 - 1}{x_1 + 1} = \dfrac{x_2 - 1}{x_2 + 1} \quad \Rightarrow x_1 x_2 - x_2 + x_1 - 1 = x_1 x_2 + x_2 - x_1 - 1$

$\Rightarrow \quad 2x_1 = 2x_2 \quad \Rightarrow \quad x_1 = x_2$

$\therefore \quad f(x_1) = f(x_2) \quad \Rightarrow x_1 = x_2$

$\therefore \quad f(x)$ is $1-1$ in D_f.

$\forall\, y \in R_f \;\; \exists \;\; x = \dfrac{1+y}{1-y} \in D_f$ (where $y \neq 1$)

$$\text{s.t. } f(x) = f\left(\frac{1+y}{1-y}\right) = \frac{\dfrac{1+y}{1-y} - 1}{\dfrac{1+y}{1-y} + 1} = \frac{\dfrac{1+y-1+y}{1-y}}{\dfrac{1+y+1-y}{1-y}} = \frac{2y}{2} = y$$

$\therefore$ the mapping f is onto

$\therefore$ f is both $1-1$ and onto $\Rightarrow$ f^{-1} exists

Now to find f^{-1},

Let $\quad y = f(x) = \dfrac{x-1}{x+1}$ (Cross Multiplying)

$\therefore \quad xy + y = x - 1 \quad \Rightarrow x - xy = y + 1$

$\Rightarrow \quad x(1-y) = 1 + y \quad \Rightarrow x = \dfrac{1+y}{1-y}$,

$\therefore \quad f^{-1}(y) = \dfrac{1+y}{1-y} \Rightarrow f^{-1}(x) = \dfrac{1+x}{1-x}$

and $D_{f^{-1}}$ = Set of all reals except 1

Verification :

$$(f o f^{-1})(x) = f(f^{-1}(x)) = \frac{f^{-1}(x) - 1}{f^{-1}(x) + 1} = \frac{\dfrac{1+x}{1-x} - 1}{\dfrac{1+x}{1-x} + 1} = \frac{\dfrac{1+x-1+x}{1-x}}{\dfrac{1+x+1-x}{1-x}} = \frac{2x}{2} = x$$

$(f o f^{-1})(x) = x$.

Example 4. Let $f: R \times R \to R \times R$ be defined by $f(x, y) = (x + y, x - y)$. Show that f is bijection.

Sol. $f: R \times R \to R \times R$ such that $f(x, y) = (x + y, x - y)$

Let $f(x, y) = f(u, v)$

$\therefore \quad (x + y, x - y) = (u + v, u - v)$

$\therefore \quad x + y = u + v$ ...(1)

and $x - y = u - v$ ...(2)

Adding (1) and (2), $\quad 2x = 2u \quad \Rightarrow \quad x = u$

Subtracting (2) from (1), $\; 2y = 2v \quad \Rightarrow \quad y = v$

$\therefore \quad (x, y) = (u, v)$

$\therefore \quad f$ is one-one *i.e.*, f is injective.

Let (s, t) be an element of the codomain R × R. We determine (x, y) such that

$$f(x, y) = (s, t) \Rightarrow (x + y,\ x - y) = (s, t)$$

$$x + y = s \quad \ldots(3)$$

and $x - y = t \quad \ldots(4)$

Adding (3) and (4), $2x = s + t \Rightarrow x = \frac{s+t}{2} \in R$

Subtracting (4) from (3), $2y = s - t \Rightarrow y = \frac{s-t}{2} \in R$

Since $\left(\frac{s+t}{2}, \frac{s-t}{2}\right)$ is in the domain of f

$\therefore \quad f$ is onto

$\therefore \quad f$ is one-one and onto

$\therefore \quad f$ is a bijection.

Example 5. Prove that the set, 2P of even positive integers has the same cardinality as the set P of positive integers.

Sol. We know that two sets have the same cardinality if there exists a bijection between them.

$\therefore$ for proving the required result, we must find a map from P to 2P and show that this map is a bijection.

Define f: P → 2P such that $f(x) = 2x$

Let $x_1, x_2 \in$ P and $f(x_1) = f(x_2)$

$\therefore \quad 2x_1 = 2x_2 \Rightarrow x_1 = x_2$

$\therefore \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore \quad f$ is one-one map.

Let $y \in$ 2P. We will show that there exists an element $x \in$ P such that $y = f(x)$.

Since $y \in$ 2P, $\therefore \ y = 2p$ for some $p \in$ P

$\therefore \quad f(p) = 2p = y$

$\therefore$ each element of 2P comes from some element of P

$\therefore \quad f$ is onto

$\therefore \quad f$ is both 1-1 and onto

$\therefore \quad f$ is bijection

Hence the result.

Example 6. Prove that P, set of positive integers, is countable.

Sol. A set is said to be countable if it has same cardinality as set of natural numbers N.

Let f: N $\to$ P such that $f(x) = x + 1$

Let $x_1, x_2 \in$ N such that

$f(x_1) = f(x_2) \Rightarrow x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$

$\therefore$ f is one-one map

Let $y \in$ P. Let $y = f(x)$

Then $x + 1 = y \Rightarrow x = y - 1 \in$ N

Now $f(x) = f(y - 1) = y - 1 + 1 = y$

$\therefore$ for each $y \in$ P, there exist $x \in$ N such that $f(x) = y$

$\therefore$ f is onto

$\therefore$ f is both 1 – 1 and onto

$\therefore$ f is a bijective map

$\therefore$ N and P have same cardinality

$\Rightarrow$ P is countable.

Example 7. Let f: A $\to$ B and g : B $\to$ C be two functions such that $g\,o\,f$: A $\to$ C is a bijective map. Then f is injective and g is surjective.

Sol. Since f: A $\to$ B, g : B $\to$ C are maps

$\therefore$ $g\,o\,f$: A $\to$ C is a map. Also $g\,o\,f$ is given to be bijective *i.e.*, $g\,o\,f$ is one-one, onto map

If possible, let f be not injective *i.e.*, f is not one-one map

$\therefore$ $\exists$ $x_1, x_2 \in$ A such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$

But $f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (g\,o\,f)(x_1) = (g\,o\,f)(x_2)$

$\therefore$ $x_1, x_2 \in$ A such that $x_1 \neq x_2$ but $(g\,o\,f)(x_1) = (g\,o\,f)(x_2)$

$\Rightarrow$ $g\,o\,f$ is not one-one mapping which is against the given hyothesis that $g\,o\,f$ is one-one

$\therefore$ f is injective

Now, we show that g is surjective.

Let $z \in$ C be any element. Since $g\,o\,f$: A $\to$ C is onto

So, $\exists$ $x \in$ A such that $(g\,o\,f)(x) = z$

$\Rightarrow$ $g(f(x)) = z \Rightarrow g(y) = z$, where $y = f(x)$

Since $x \in$ A and f is a map from A to B

$\therefore$ $f(x) \in$ B *i.e.*, $y \in$ B

$\therefore$ for given $z \in$ C, we have determined $y \in$ B such that

$g(y) = z$

$\therefore$ g : B $\Rightarrow$ C is onto *i.e.*, g is surjective.

Example 8. Let $f: R \to R$ be real valued function defined by $f(x) = x^2, x \in R$. Is f invertible ? Give reasons.

Sol. First we check weather f is a bijection or not.

For this let us check f to be one-one.

Let $x_1, x_2 \in R$

such that $f(x_1) = f(x_2)$

$\Rightarrow$ $x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2$

$x_1 = x_2$ or $x_1 = -x_2$.

So f is not 1-1.

Hence f is not a bijection $\therefore$ f is not invertible.

Example 9. Let $X = Y = Z = R$ and let $f: X \to Y$ and $g: Y \to Z$ are such that $f(x) = 2x + 1$ and $g(y) = y/3$. Verify that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Sol. $f: x \to y$ $f(x) = 2x + 1$

$$g(y) = \frac{y}{3}$$

L.H.S. : $g \circ f(x) = g(f(x)) = g(2x + 1) = \frac{2x+1}{3}$

Now we find $(g \circ f)^{-1}$

Let $g \circ f(x) = y$

then $y = \frac{2x+1}{3}$

$$x = \frac{3y - 1}{2}$$

$\Rightarrow$ $(g \circ f)^{-1} y = \frac{3y-1}{2}$ or $(g \circ f)^{-1} x = \frac{3x-1}{2}$

R.H.S. : $f(x) = 2x + 1$

$\Rightarrow$ $y = 2x + 1 \Rightarrow x = \frac{y-1}{2} \Rightarrow f^{-1}(y) = \frac{y-1}{2}$ or $f^{-1}(x) = \frac{x-1}{2}$

Again $g(y) = \frac{y}{3}$

$$x = \frac{y}{3}$$

$$y = 3x$$

$$g^{-1}(x) = 3x \text{ or } g^{-1}(y) = 3y$$

Now $f^{-1} o g^{-1}(x) = f^{-1}(g^{-1}(x)) = f^{-1}(3x) = \frac{3x-1}{2}$

so $(g o f)^{-1} = f^{-1} o g^{-1}$.

Example 10. Let $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = ax + b$, $a, b, x \in \mathbf{R}$ and $a \neq 0$. Show that f is invertible and find the inverse of f.

Sol. $f(x) = ax + b,\ a, b \in \mathbf{R}, a \neq 0$

One-one : Let $x_1, x_2 \in \mathbf{R}$

such that $f(x_1) = f(x_2) \Rightarrow ax_1 + b = ax_2 + b \Rightarrow ax_1 = ax_2$

$\Rightarrow$ $x_1 = x_2$ [$\because a \neq 0$]

$\therefore$ f is one-one.

Onto : Let $y \in \mathbf{R}$

such that $y = f(x)$

$\Rightarrow$ $y = ax + b$

$\Rightarrow$ $x = \frac{y-b}{a}$ ...(*i*)

as $a \neq 0$ $\therefore$ $\forall\ y \in \mathbf{R}$

$\exists$ $x \in \mathbf{R}$

such that $y = f(x)$

Hence f is onto.

Since f is one-one and onto so f is invertible.

Now we find inverse of f.

By definition $x = f^{-1}(y)$ iff $y = f(x)$

$\Rightarrow$ $\frac{y-b}{a} = f^{-1}(y)$ [using (*i*)]

or $f^{-1}(x) = \frac{x-b}{a}$.

Example 11. Let f and g be functions from $\mathbf{R}$ to $\mathbf{R}$ defined by $f(x) = [x]$ and $g(x) = |x|$. Determine whether $f o g = g o f$.

Sol. Given $f(x) = [x]$ and $g(x) = |x|$

$f o g(x) = f[g(x)] = f(|x|) = [|x|]$

$g o f(x) = g[f(x)] = g([x]) = |[x]|$

Now $f o g \neq g o f$.

As $f o g(-3.2) = f[g(-3.2)] = f(3.2) = 3$

$g o f(-3.2) = g[f(-3.2)] = g(-4) = 4$.

Example 12. Let $f: R \to R$ and $g: R \to R$ be real valued functions defined by $f(x) = 2x^3 - 1, x \in R$ and $g(x) = \left[\frac{1}{2}(x+1)\right]^{1/3}, x \in R$. Show that f and g are bijective and each is inverse of other.

Sol. First we show f and g both are one-one

Let $x_1, x_2 \in R$ such that

$f(x_1) = f(x_2)$ and $g(x_1) = g(x_2)$

$\Rightarrow \quad 2x_1^3 - 1 = 2x_2^3 - 1$ and $\left[\frac{1}{2}(x_1+1)\right]^{1/3} = \left[\frac{1}{2}(x_2+1)\right]^{1/3}$

$\Rightarrow \quad 2x_1^3 - 1 - 2x_2^3 + 1 = 0$ and $\frac{1}{2}(x_1+1) = \frac{1}{2}(x_2+1)$ (By Cubing

$\Rightarrow \quad 2(x_1^3 - x_2^3) = 0$ and $x_1 + 1 = x_2 + 1$

$\Rightarrow \quad x_1^3 - x_2^3 = 0$ and $x_1 + 1 - x_2 - 1 = 0$

$\Rightarrow \quad x_1^3 = x_2^3$ and $x_1 - x_2 = 0$

$\Rightarrow \quad x_1 = x_2$ and $x_1 = x_2$

$\therefore$ f and g both are one-one functions

Now we show f and g both are onto functions for this let $y \in R$

such that $y = f(x)$ and $y = g(x)$

$\Rightarrow \quad y = 2x^3 - 1$ and $y = \left[\frac{1}{2}(x+1)\right]^{1/3}$

$\Rightarrow \quad x^3 = \frac{y+1}{2}$ and $y^3 = \frac{1}{2}(x+1)$

$\Rightarrow \quad x = \left(\frac{y+1}{2}\right)^{1/3}$ ...(1) and $x = 2y^3 - 1$ ...(2

so $\forall\, y \in R$ we have $x \in R$ such that $y = f(x)$

also $\forall\, y \in R$ we have, $x \in R$ such that $y = g(x)$

$\therefore$ f and g both are onto.

Hence f and g both are bijective and $\therefore$ Invertible.

From (1) $x = \left(\frac{y+1}{2}\right)^{1/3}$

$\Rightarrow \quad f^{-1}(y) = \left(\frac{y+1}{2}\right)^{1/3}$

[Since $y = f(x)$ $\therefore x = f^{-1}(y)$

or $f^{-1}(x) = \left(\frac{x+1}{2}\right)^{1/3} = g(x)$

Similarly we can how $g^{-1}(x) = f(x)$.

Example 13. Prove that if A is a set then identity function I on A is one-one onto.

Sol. $I : A \to A$ is defined by $I(x) = x, \ \forall \ x \in A$

I is one-one :

Let $x_1, x_2 \in A$

such that $I(x_1) = I(x_2) \Rightarrow x_1 = x_2$

$\therefore$ I is one-one.

I is onto :

Let $y \in A$

If possible, let $x \in A$

such that $y = I(x) \Rightarrow y = x$

or $x = y$

so $\forall \ y \in A, \ \exists \ x = y \in A$

such that $y = I(x)$

$\therefore$ I is onto.

Hence I is one-one onto.

Example 14. Is function $f : R \to R$ defined by $f(x) = \frac{1}{x}$ is bijective in its domain.

Sol. $f : R \to R, \quad f(x) = \frac{1}{x}$

$D_f = R - \{0\} \quad R_f = R - \{0\}$

Let $x_1, x_2 \in R \ (x_1 \neq 0, \ x_2 \neq 0)$

s.t. $f(x_1) = f(x_2) \Rightarrow \frac{1}{x_1} = \frac{1}{x_2} \Rightarrow x_1 = x_2$

so f is one-one.

Let $y \in R$

If possible, $y = f(x) \Rightarrow y = \frac{1}{x}$

or $x = \frac{1}{y}$.

Now $\forall \quad y \in R \quad (y \neq 0)$

$\exists \quad x \in R$ s.t. $y = f(x)$

so f is onto.

f is one-one and onto.

so f is bijective in its domain.

Example 15. $f(a) = a + 1 \; g(a) = \begin{cases} \frac{a}{2} & \text{if } a \text{ is even} \\ \frac{a-1}{2} & \text{if } a \text{ is odd} \end{cases}$. Find $f o g$ and $g o f$.

Sol. $f o g(a) = f(g(a)) = \begin{cases} \frac{a}{2}+1 & \text{if } a \text{ is even} \\ \frac{a-1}{2}+1 & \text{if } a \text{ is odd} \end{cases} = \begin{cases} \frac{a+2}{2} & \text{if } a \text{ is even} \\ \frac{a+1}{2} & \text{if } a \text{ is odd} \end{cases}$

$g o f(a) = g(f(a))$

$= \begin{cases} \frac{f(a)}{2} & \text{if } f(a) \text{ is even} \\ \frac{f(a)-1}{2} & \text{if } f(a) \text{ is odd} \end{cases} = \begin{cases} \frac{a+1}{2} & \text{if } a+1 \text{ is even} \\ \frac{a+1-1}{2} & \text{if } a+1 \text{ is odd} \end{cases}$

$= \begin{cases} \frac{a+1}{2} & \text{if } a \text{ is odd} \\ \frac{a}{2} & \text{if } a \text{ is even} \end{cases}$

Example 16. f, g, h are functions from N to N $\cup$ {0} defined as

$f(n) = n + 1, \; g(n) = 2n, \; h(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$. Find $f o h, (f o g) o h$.

Sol. $f(n) = n + 1 \;, \quad h(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$

$f o h(n) = f(h(n)) = h(n) + 1 = \begin{cases} 0+1 & \text{if } n \text{ is even} \\ 1+1 & \text{if } n \text{ is odd} \end{cases} = \begin{cases} 1 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd} \end{cases}$

$f o g(n) = f(g(n)) = f(2n) = 2n + 1$

$(f og) oh = f o g(h(n)) = 2h(n) + 1 = \begin{cases} 2.0+1 & \text{if } n \text{ is even} \\ 2.1+1 & \text{if } n \text{ is odd} \end{cases} = \begin{cases} 1 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd} \end{cases}$

Example 17. Let $f: R \to R$ and $g: R \to R$ be two functions on real number defined as $f(x) = 2x + 3$, $g(x) = x^2$ show that $fog \neq gof$

Sol. $f(x) = 2x + 3 \qquad g(x) = x^2$

$fog(x) = f(g(x)) = f(x^2) = 2x^2 + 3$

$gof(x) = g(f(x)) = g(2x + 3) = (2x + 3)^2$

$fog \neq gof$

Example 18. Let $A = \{1, 2, 3\}$. Define $f: A \to A$ by $f(1) = 2$, $f(2) = 1$, $f(3) = 3$. Find f^2, f^4.

Sol. $f^2(1) = f(f(1)) = f(2) = 1$

$f^2(2) = f(f(2)) = f(1) = 2$

$f^2(3) = f(f(3)) = f(3) = 3$

$f^2 : \{(1, 1), (2, 2), (3, 3)\}$

$f^4(1) = f^2(f^2(1)) = f^2(1) = 1$

$f^4(2) = f^2(f^2(2)) = f^2(2) = 2$

$f^4(3) = f^2(f^2(3)) = f^2(3) = 3$

$f^4 : \{(1, 1), (2, 2), (3, 3)\}$

EXERCISE 1.7

1. Let a map $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$. Prove that f is neither one-one nor onto.
2. Let a function $f: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x + 3 \ \forall x \in R$. Prove that f is one-one and onto.
3. Prove that a function $f: \mathbf{R} \to \mathbf{R}$, defined by $f(x) = x^3$ is one-one onto.
4. Let $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$ and define $f: A \to B$ by $f(1) = b, f(2) = c, f(3) = a$. Then show that f is injective.
5. Consider the function $f(x) = 2^x$ and $g(x) = x^2$. Determining which of the two function are one to one. Justify your answer.
6. $f: A \to B$ is a constant function. Can f be
   (*i*) 1 – 1 function (*ii*) Onto function ?
7. If $f(x) = \dfrac{x-4}{4x-1}$ for all $x \neq \dfrac{1}{4}$, find $f(f(x))$.
8. If $f: \mathbf{R} \to \mathbf{R}$ is defined by $f(x) = x^2 - 3x + 2$, find $f(f(x))$.
9. If $y = f(x) = \dfrac{x+2}{x-1}$, then show that $x = f(y)$.
10. If $f(x) = x^2 - 1$, $g(x) = 3x + 1$, then describe the following functions :
    (*i*) $g\,o\,f$ (*ii*) $f\,o\,g$ (*iii*) $g\,o\,g$ (*iv*) $f\,o\,f$
11. (*a*) (*i*) Given $f(x + 1) = 3x + 5$, evaluate $f(2x)$.
    (*ii*) $f(x) = x + 1$, $g(x) = x^2 + 1$, $h(x) = 3x - 2$ verify $(f\,o\,g)\,o\,h = f\,o(g\,o\,h)$
    (*iii*) If a vertical line cuts a graph in two points then graph does not represent a function. Why ?

    (*b*) Let $f(x) = x + 2$, $g(x) = x - 2$, $h(x) = 3x$. For $x \in R$, where R is a set of real numbers, Find $g\,o\,f$, $f\,o\,f$, $h\,o\,g$.

12. Define composition of two functions. let f and g be two functions from R → R defined $f(x) = x^2 + 3x + 2$ and $g(x) = 4x - 1$. Find $f \circ g$ and $g \circ f$. Also calculate $(g \circ f)(-1)$ and $(f \circ$ (-1). Is composition commutative ?

13. Let $f: R \times R \to R \times R$ be defined by $f(x, y) = (x + 2y, y - x)$. Let $g: R \to R \times R$ be defined $g(t) = (3t, t^2)$. Let $h = R \times R \to R$ be defined by $h(x, y) = x + 2y$. Find $f \circ g$, $h \circ f$, $h \circ (f \circ g$

14. If f: $\mathbf{R} \to \mathbf{R}$ is given by $f(x) = 3x - 1$, find f^{-1}.

15. The function $f(x) = 2^x, x > 0$ has an inverse. Why ?

16. Is the function $f(x) = \dfrac{x}{x+1}$ invertible in its domain ? If so, find the inverse function.

17. Let A = {– 2, – 1, 0, 1, 2, 3}, B = {0, 1, 2,.....,10} and f : A → B be a function defined $f(x) = x^2$ for all $x \in$ A, find f^{-1} (C) where C = {0, 1, 2, 4}

18. Prove that each of the following function is a bijection :
   (*a*) $f: R \times R \to R \times R$ defined by $f(x, y) = (x + y, 2x - y)$
   (*b*) $f: Z \times Z \to Z \times Z$ defined by $f(m, n) = (2n + m, n + m)$

19. If S is a set containing finite number of elements and f is a function from S into S, then prove following
   (*i*) If f is one-one, then f is onto
   (*ii*) If f is onto, then f is one-one.

20. Prove that if f is a bijection then $(f^{-1})^{-1} = f$.

21. Prove that $f(x) = 2^x, x > 0$ is invertible.

22. Let f and g be functions from R to R defined by $f(x) = [x]$ and $g(x) = |x|$. Determine whe $f \circ g = g \circ f$.

23. If #A and #B are both finite, how many different function are there from A into B.

ANSWERS

5. f is one-one , g is not one-one

6. (*i*) Not one-one (*ii*) onto 7. x 8. $x^4 - 6x^3 + 10x^2 - 3$

10. (*i*) $3x^2 - 2$ (*ii*) $9x^2 + 6x$ (*iii*) $9x + 4$ (*iv*) $x^4 - 2x^2$

11. (*a*) (*i*) $6x + 2$ (*ii*) Two images correspond to same point
   (*b*) x ; $x + 4$; $3x - 6$

12. $16x^2 + 4x$; $4x^2 + 12x + 7$; -1 , 12 ; no

13. $(3t + 2t^2, t^2 - 3t)$, $4y - x$, $4t^2 - 3t$ 14. $\dfrac{x+1}{3}$

15. Since f is one-one and onto 16. Yes ; $f^{-1}(x) = \dfrac{x}{1-x}$ 17. $\{0, -1, 1, -2, 2\}$

SECTION-IV
COUNTABLE AND UNCOUNTABLE SETS

1.49. Introduction

It is well known to every one that an infinite set has infinite number of elements. Is there any connection between two infinite sets ?

For example : Is there any relationship between the set of natural numbers N, set of integers **Z**, set of real numbers **R**, set of rational numbers **Q** etc. ? In this direction the concept of **equivalent sets** is being introduced and consequently the concept of countable set and uncountable set comes into picture. In this chapter we will study countable set and uncountable set and some of their properties.

1.50. Equivalent Sets

A set A is called **equivalent** to a set B, written as $A \sim B$, if there exists a function $f: A \to B$ which is one-one and onto.

Example 1. Show that the following sets are equivalent

(*i*) $A = \{2n : n \in \mathbb{Z}\}$ and $B = \{2n - 1 : n \in \mathbb{Z}\}$

(*ii*) $A = \{n : n \in \mathbb{N}\}$ and $B = \{2n : n \in \mathbb{N}\}$

(*iii*) $A = \{n : n \in \mathbb{N}\}$ and $B = \{n : n \in \mathbb{Z}\}$

(*iv*) $A = \{x : x \in \mathbb{R}$ such that $0 \le x \le 1\}$ and $B = \{x : x \in \mathbb{R}$ such that $3 \le x \le 7\}$

(*v*) $A = \{x : x \in \mathbb{R}$ such that $-1 < x < 1\}$ and $B = \{x : x \in \mathbb{R}\}$

Sol. (*i*) Define a function $f: A \to B$ as $f(x) = x - 1, \forall x \in A$

We show that f is bijective.

For one-one Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$\Rightarrow \quad x_1 - 1 = x_2 - 1 \Rightarrow x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto Let $y \in B$ be any element

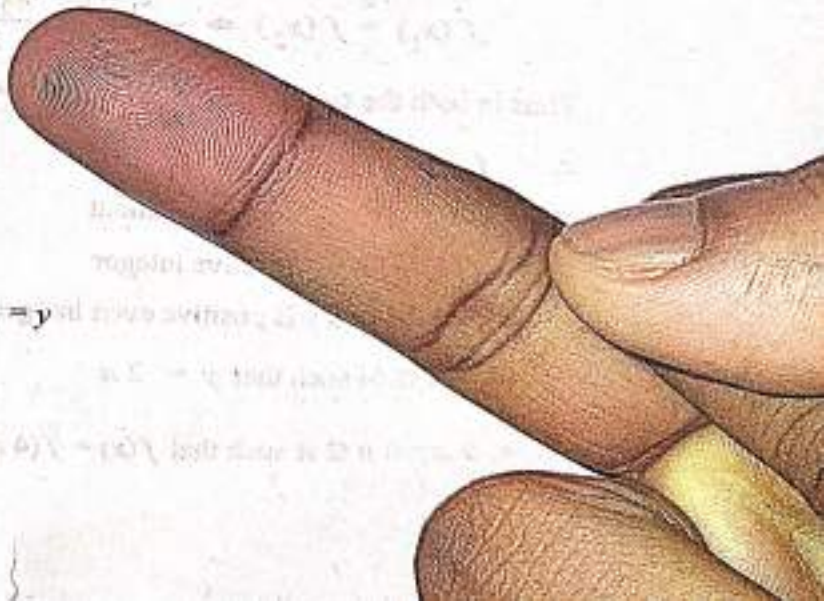
$\therefore$ $\exists$ some $n \in \mathbb{Z}$ such that $y = 2n - 1$

Thus $\exists\, x = 2n \in A$ such that $f(x) = f(2n) = 2n - 1 = y$

$\therefore$ f is onto.

So, f is one-one and onto

Hence $A \sim B$.



(*ii*) Define a function $f: A \to B$ as $f(x) = 2x, \ \forall\ x \in A$

we show that f is bijective

For one-one : Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$\Rightarrow \quad 2x_1 = 2x_2 \Rightarrow x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one

For onto Let $y \in B$ be any element $\therefore \exists$ some $n \in \mathbb{N}$ such that $y = 2n$

Thus $\exists\ x = n \in A$ such that $f(x) = f(n) = 2n = y$

$\therefore$ f is onto

So, f is one-one and onto

Hence $A \sim B$.

(*iii*) Define a finction $f: A \to B$ as follow

$$f(x) = \begin{cases} \dfrac{x}{2} & \text{if } x \text{ is even natural number} \\ -\dfrac{x-1}{2} & \text{if } x \text{ is odd natural number} \end{cases}$$

We show f is bijective.

For one-one Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

Case (*i*) When both $f(x_1)$ and $f(x_2)$ are positive integers, then

$$f(x_1) = f(x_2) \Rightarrow \frac{x_1}{2} = \frac{x_2}{2} \Rightarrow x_1 = x_2$$

Case (*ii*) When both $f(x_1)$ and $f(x_2)$ are negative integer, then

$$f(x_1) = f(x_2) \Rightarrow -\frac{x_1 - 1}{2} = \frac{x_2 - 1}{2} \Rightarrow x_1 = x_2$$

Thus in both the cases we see that $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto Let $y \in B$ be any element

Case (*i*) When y is a positive integer

Subcase (*a*) When y is positive even integer, then

$\exists\ n \in \mathbb{N}$ such that $y = 2n$

Now, $\exists\ x = 4n \in A$ such that $f(x) = f(4n) = -\dfrac{4n}{2} = 2n = y$

Subcase (*b*) When y is positive odd integer, then

$\exists\ n \in \mathbb{N}$ such that $y = 2n-1$

Now, $\exists\ x = 4n-2 \in A$ such that $f(x) = f(4n-2) = \frac{4n-2}{2} = 2n-1 = y$

Case (*ii*) When y is a negative integer

Subcase (*a*) When y is negative even integer, then

$\exists\ n \in \mathbb{N}$ such that $y = -2n$

Now, $\exists\ x = 4n+1 \in A$ such that $f(x) = f(4n+1) = -\frac{4n+1-1}{2} = -2n = y$

Subcase (*b*) When y is negative odd integer, then

$\exists\ n \in \mathbb{N}$ such that $y = -2n+1$

Now, $\exists\ x = 4n-1 \in A$ such that $f(x) = f(4n-1) = -\frac{4n-1-1}{2} = -2n+1 = y$

Thus in all the cases we notice that for every $y \in B, \exists\ x \in A$ such that $f(x) = y$

$\therefore$ f is onto.

Thus f is one-one and onto.

Hence $A \sim B$.

(*iv*) Define a function $f: A \to B$ as

$f(x) = 4x+3\ \forall\ x \in A$

We show that f is bijective.

For one-one Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$\Rightarrow\ 4x_1 + 3 = 4x_2 + 3 \Rightarrow x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

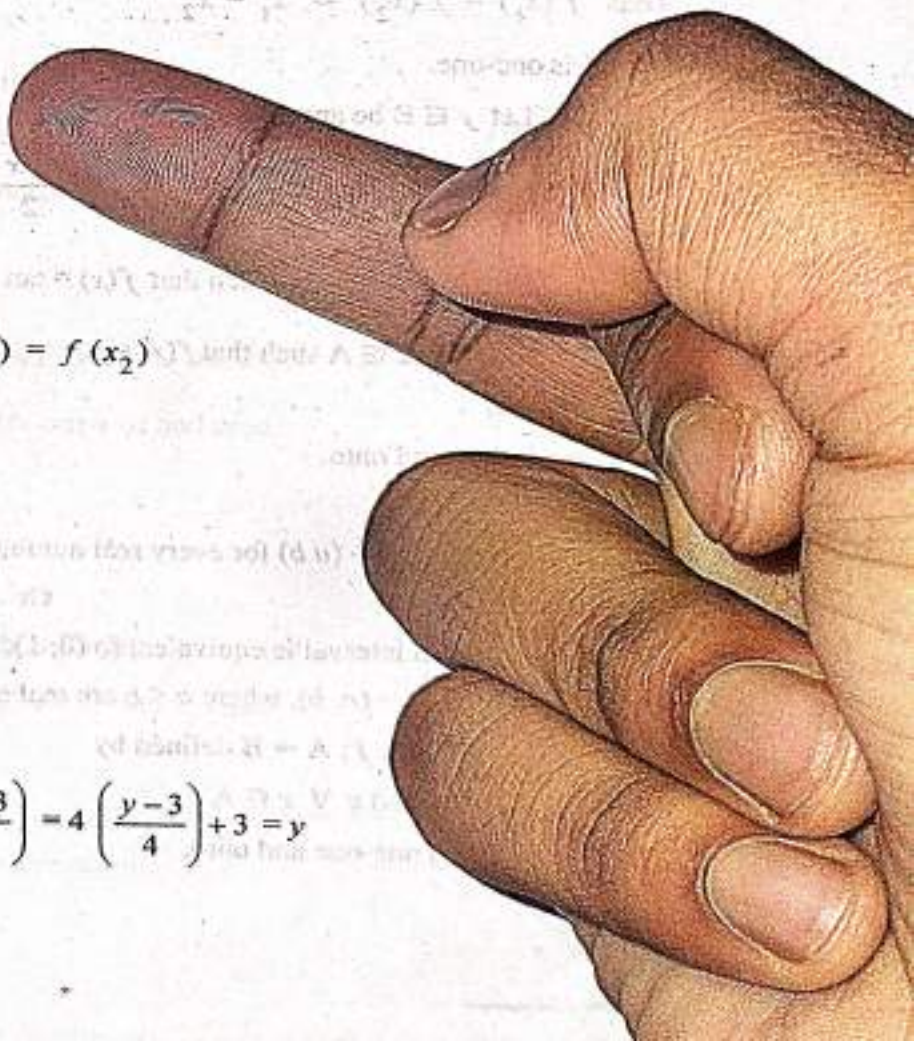
$\therefore$ f is one-one.

For onto Let $y \in B$ be any element

$\therefore\ 3 \le y \le 7$

$\Rightarrow\ 0 \le y-3 \le 4 \Rightarrow 0 \le \frac{y-3}{4} \le 1$

Let $x = \frac{y-3}{4} \in A$ such that $f(x) = f\left(\frac{y-3}{4}\right) = 4\left(\frac{y-3}{4}\right)+3 = y$



Thus $\forall\ y \in B,\ \exists\ x \in A$ such that $f(x) = y$

$\therefore$ f is on to

So, f is one-one and onto

Hence $A \sim B$.

(v) Define the function $f: A \to B$ as

$$f(x) = \tan \frac{\pi x}{2} \quad \forall\ x \in A$$

We show that f is bijective.

For one-one Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$$\Rightarrow \quad \tan \frac{\pi x_1}{2} = \tan \frac{\pi x_2}{2} \Rightarrow \frac{\pi x_1}{2} = \frac{\pi x_2}{2} + n\pi,\ \forall\ n \in \mathbb{Z}$$

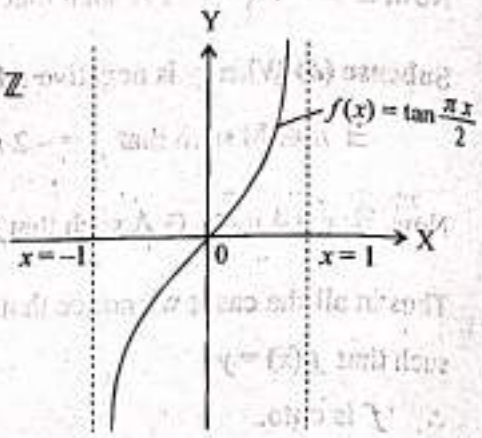
$$\Rightarrow \quad x_1 = x_2 + 2n, \forall\ n \in \mathbb{Z} \Rightarrow x_1 - x_2 = 2n, \forall\ n \in \mathbb{Z}$$

But $x_1, x_2 \in A = (-1, 1) \Rightarrow |x_1, x_2| < 1$

$\therefore$ $n = 0 \Rightarrow x_1 - x_2 = 0$ *i.e.* $x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.



For onto Let $y \in B$ be any real number. Then

for $y \geq 0\ \exists\ x \in [0, 1)$ such that $f(x) = \tan \frac{\pi x}{2} = y$.

and for $y < 0\ \exists\ x \in (-1, 0)$ such that $f(x) = \tan \frac{\pi x}{2} = y$

Thus $\forall\ y \in B,\ \exists\ x \in A$ such that $f(x) = y$

$\therefore$ f is onto

So, f is one-one and onto.

Hence $A \sim B$.

Example 2. Show that $(0, 1) \sim (a\ b)$ for every real number a and b, where $a < b$

Or

Show that any open interval is equivalent to $(0, 1)$.

Sol. Let $A = (0, 1)$ and $B = (a, b)$, where $a < b$ are real numbers

Consider the mapping $f: A \to B$ defined by

$$f(x) = a + (b - a)x \quad \forall\ x \in A$$

We show that f is one-one and onto.

For one-one Let $x_1, x_2 \in A$ be any elements such that $f(x_1) = f(x_2)$

$\Rightarrow \quad a+(b-a)x_1 = a+(b-a)x_2 \Rightarrow x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto Let $y \in B$ be any element

$\therefore \quad a<y<b$

$\Rightarrow \quad 0<y-a<b-a \Rightarrow 0<\dfrac{y-a}{b-a}<1$

Let $x = \dfrac{y-a}{b-a}$, then $0<x<1$ *i.e.* $x \in A$

Now $f(x) = f\left(\dfrac{y-a}{b-a}\right) = a+\dfrac{y-a}{b-a}(b-a) = y$

$\therefore$ f is onto.

Thus f is one-one and onto. So, f is bijective

Hence $A \sim B$ *i.e.* $(0, 1) \sim (a, b)$.

1.51. Prove that the equivalent relation $\sim$ is an equivalence relation.

Proof : (*i*) Since the identity mapping $I : A \to A$ defined by

$I(x) = x, \ \forall \ x \in A$ is both one-one and onto

$\therefore \quad A \sim A, \ \forall$ set A.

Hence $\sim$ is reflexive.

(*ii*) Let $A \sim B \Rightarrow \exists$ a map $f : A \to B$, which is both one-one and onto

$\Rightarrow \exists$ inverse map $f^{-1} : B \to A$, which is also one-one and onto.

$\therefore \quad B \sim A.$

Hence $\sim$ is symmetric.

(*iii*) Let $A \sim B$ and $B \sim C$

$\Rightarrow \exists$ maps $f : A \to B$ and $g : B \to C$ which are both one-one and onto.

$\therefore$ The composite map $h = gof : A \to C$ is also one-one and onto.

$\therefore \quad A \sim C$

Hence $\sim$ is transitive.

Thus, the equivalent relation $\sim$ is an equivalence relation.

1.52. Prove that any two open intervals are equivalent *i.e.* $(a, b) \sim (c, d)$.

Proof. Define a map $f : (a, b) \to (c, d)$ by

$$f(x) = c + \frac{d-c}{b-a}(x-a) \; \forall \; x \in (a, b)$$

We first show that f is well-defined map.

Let $x \in (a, b)$ be any element

$$\Rightarrow \quad a < x < b \;\Rightarrow\; 0 < x-a < b-a$$

$$\Rightarrow \quad 0 < \frac{x-a}{b-a} < 1 \;\Rightarrow\; 0 < \frac{x-a}{b-a}(d-c) < d-c$$

$$\Rightarrow \quad c < c + \frac{d-c}{b-a}(x-a) < d \;\; \text{i.e.} \;\; c < f(x) < d$$

$\therefore$ f is well-defined map.

For one-one

Let $x_1, x_2 \in (a, b)$ such that $f(x_1) = f(x_2)$

$$\Rightarrow \quad c + \frac{d-c}{b-a}(x_1 - a) = c + \frac{d-c}{b-a}(x_2 - a) \Rightarrow x_1 = x_2$$

$\therefore$ f is one-one.

For onto Let $y \in (c, d)$ be any number, then

$$c < y < d \;\Rightarrow\; 0 < y-c < d-c$$

$$\Rightarrow \quad 0 < \frac{y-c}{d-c} < 1 \;\Rightarrow\; 0 < \frac{b-a}{d-c}(y-c) < b-a$$

$$\Rightarrow \quad a < a + \frac{b-a}{d-c}(y-c) < b$$

Let $x = a + \dfrac{b-a}{d-c}(y-c) \in (a, b)$ such that

$$f(x) = c + \frac{d-c}{b-a}\left[a + \frac{b-a}{d-c}(y-c) - a\right] = y$$

$\therefore$ f is onto

Thus f is a bijection

Hence $(a, b) \sim (c, d)$.

Aliter Hint : Show that $(0, 1) \sim (a, b)$ and $(0, 1) \sim (c, d)$ (See Example 2). Then $(a, b) \sim (c, d)$ follows by 1.51.

Example 3. Give an example of a proper subset A of a set B such that $A \sim B$.

Sol. Consider the sets $A = (0, 1)$ and $B = (-1, 1)$

Define a function $f: A \to B$ by $f(x) = 2x - 1, \forall\ x \in A$

We show that f is one-one and onto.

For one-one : Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$$\Rightarrow \quad 2x_1 - 1 = 2x_2 - 1 \Rightarrow 2x_1 = 2x_2 \Rightarrow x_1 = x_2$$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto : Let $y \in B$ be any element

$$\therefore \quad -1 < y < 1 \Rightarrow 0 < 1 + y < 2 \Rightarrow 0 < \frac{1+y}{2} < 1$$

Let $x = \frac{1+y}{2} \in (0, 1) = A$ such that

$$f(x) = f\left(\frac{1+y}{2}\right) = 2\left(\frac{1+y}{2}\right) - 1 = y$$

$\therefore$ f is onto

So, f is one-one and onto. Therefore $A \sim B$.

Also, A is a proper subset of B.

Thus A is a proper subset of the set B such that $A \sim B$.

Example 4. Prove that any open interval (a, b) and the set of real numbers **R** are equivalent.

Sol. Let us define the map $f: (a, b) \to \mathbf{R}$ by

$$f(x) = \tan\left(\frac{x - \frac{a+b}{2}}{b-a}\right)\pi\ ;\ \forall\ x \in (a, b)$$

First, we show that f is well-defined map

Let $x \in (a, b)$ be any point. Then $a < x < b$

$$\Leftrightarrow \quad a - \frac{a+b}{2} < x - \frac{a+b}{2} < b - \frac{a+b}{2}$$

$$\Leftrightarrow \quad \frac{a-b}{2} < x - \frac{a+b}{2} < \frac{b-a}{2}$$

$$\Leftrightarrow \quad -\frac{1}{2} < \frac{x - \frac{a+b}{2}}{b-a} < \frac{1}{2}$$

$$\Leftrightarrow \quad -\frac{\pi}{2} < \left(\frac{x-\frac{a+b}{2}}{b-a}\right)\pi < \frac{\pi}{2}$$

$$\Leftrightarrow \quad -\infty < \tan\left(\frac{x-\frac{a+b}{2}}{b-a}\right)\pi < \infty \quad i.e.\ f(x) = \tan\left(\frac{x-\frac{a+b}{2}}{b-a}\right)\pi \in \mathbf{R}$$

$\therefore$ f is well-defined map.

Next, we show that f is bijective map.

For one-one. Let $x_1, x_2 \in (a, b)$ be any two points such that $f(x_1) = f(x_2)$.

$$i.e. \quad \tan\left(\frac{x_1-\frac{a+b}{2}}{b-a}\right)\pi = \tan\left(\frac{x_2-\frac{a+b}{2}}{b-a}\right)\pi$$

$$\Rightarrow \quad \left(\frac{x_1-\frac{a+b}{2}}{b-a}\right)\pi = \left(\frac{x_2-\frac{a+b}{2}}{b-a}\right)\pi \qquad [\because \text{of}$$

$$\Rightarrow \quad x_1 = x_2$$

$\therefore$ f is one-one map.

For onto Let $y \in \mathbf{R}$ be any real number such that $f(x) = y$

$$i.e. \quad y = \tan\left(\frac{x-\frac{a+b}{2}}{b-a}\right)\pi$$

$$\tan^{-1} y = \left(\frac{x-\frac{a+b}{2}}{b-a}\right)\pi \qquad [\because \text{of}$$

$$x = \frac{a+b}{2} + \frac{b-a}{\pi}\tan^{-1} y$$

Then $-\infty < y < \infty$

$\Rightarrow \quad -\frac{\pi}{2} < \tan^{-1} y < \frac{\pi}{2} \Rightarrow -\frac{\pi}{2}\left(\frac{b-a}{\pi}\right) < \frac{b-a}{\pi}\tan^{-1} y < \frac{\pi}{2}\left(\frac{b-a}{\pi}\right)$

$\Rightarrow \quad \frac{a-b}{2} < \frac{b-a}{\pi}\tan^{-1} y < \frac{b-a}{2} \Rightarrow \frac{a+b}{2} + \frac{a-b}{2} < \frac{a+b}{2} + \frac{b-a}{2}\tan^{-1} y < \frac{b-a}{2} + \frac{a+b}{2}$

$\Rightarrow \quad a < x < b \quad i.e. \quad x \in (a, b)$

$\therefore$ f is onto.

Thus f is bijective map. Hence $(a, b) \sim \mathbf{R}$.

Example 5. Show that $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \sim \mathrm{R}$.

Sol. Let $\mathrm{A} = \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ and $\mathrm{B} = \mathrm{R}$

Consider the function $f: \mathrm{A} \to \mathrm{B}$ defined as

$$f(x) = \tan x \ \forall \ x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$$

We show that f is bijective.

For one-one Let $x_1, x_2 \in \mathrm{A}$ be such that $f(x_1) = f(x_2)$

$\Rightarrow \quad \tan x_1 = \tan x_2$

$\Rightarrow \quad x_1 = x_2 + n\pi$, where $n \in \mathbb{Z}$

$x_1 - x_2 = n\pi$, where $n \in \mathbb{Z}$

But $x_1, x_2 \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \quad \therefore \quad |x_1 - x_2| < \frac{\pi}{2}$

$\therefore \quad x_1 - x_2 = n\pi \Rightarrow n = 0$ *i.e.* $x_1 = x_2$

$\therefore$ f is one –one.

For onto For any $y \in \mathrm{R}$ there exists $x = \tan^{-1} y \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$

such that $f(x) = y$

$\therefore$ f is onto

Thus f is one-one and onto.

So, f is bijective.

Hence $\mathrm{A} \sim \mathrm{B}$ *i.e.* $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \sim \mathrm{R}$.

ILLUSTRATIVE EXAMPLES

Example 1. Prove that the set of even integers is equivalent to the set of odd integers.

Sol. Let $A = \{2n : n \in \mathbb{Z}\}$ and $B = \{2n+1 : n \in \mathbb{Z}\}$ be the set of even integers and the set of odd integers

Define a function $f: A \to B$ as $f(x) = x + 1, \forall x \in A$

We show that f is bijective.

For one-one : Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$

$\Rightarrow \quad x_1 + 1 = x_2 + 1 \Rightarrow x_1 = x_2$

Thus $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto : Let $y \in B$ be any element

$\therefore$ $\exists$ some $n \in \mathbb{Z}$ such that $y = 2n + 1$

Thus $\exists\ x = 2n \in A$ such that $f(x) = f(2n) = 2n + 1 = y$

$\therefore$ f is onto

So, f is one-one and onto

Therefore f is bijective. Hence $A \sim B$.

Example 2. Define equivalent sets. Prove that open intervals (3, 7) and (5, 9) are equivalent sets.

Sol. Def : A set A is **equivalent** to a set B if there exists a function $f: A \to B$ which is 1 – 1 and onto.

Define a map $f: (3, 7) \to (5, 9)$ by

$$f(x) = 5 + \frac{9-5}{7-3}(x-3) \ \forall\ x \in (3\ 7) = x + 2$$

We first show f is well defined map

Let $x \in (3\ 7)$ be any element

$\Rightarrow\ 3 < x < 7 \Rightarrow 3 + 2 < x + 2 < 7 + 2 \Rightarrow 5 < f(x) < 9 \Rightarrow f(x) \in (5, 9)$

$\therefore$ f is well defined map

For one-one :

Let $x_1, x_2 \in (a, b)$ such that

$f(x_1) = f(x_2)$

$\Rightarrow\ x_1 + 2 = x_2 + 2 \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto : Let $y \in (5, 9)$ be any number,

Then $5 < y < 9 \Rightarrow 5 - 2 < y - 2 < 9 - 2$

$\Rightarrow\ 3 < y - 2 < 7$

Let $x = y - 2 \in (3\ \ 7)$ such that

$f(x) = f(y-2) = y - 2 + 2 = y$

$\therefore$ f is onto

Thus f is a bijection

Hence $(3, 7) \sim (5, 9)$.

Example 3. Let A and B be two sets. Prove that $A \times B$ is equivalent to $B \times A$.

Sol. Consider the map $f: A \times B \to B \times A$ defined by

$$f((a, b)) = (b, a),\ \forall (a, b) \in A \times B$$

we show that f is bijective.

For one-one : Let $(a_1, b_1), (a_2, b_2) \in A \times B$ be any elements such that

$$f((a_1, b_1)) = f((a_2, b_2))$$

$\Rightarrow$ $(b_1, a_1) = (b_2, a_2) \Rightarrow b_1 = b_2$ and $a_1 = a_2$

$\Rightarrow$ $(a_1, b_1) = (a_2, b_2)$

Thus $f((a_1, b_1)) = f((a_2, b_2)) \Rightarrow (a_1, b_1) = (a_2, b_2)$

$\therefore$ f is one-one.

For onto : Let $y \in B \times A$ be any element

$\therefore$ $\exists\ b \in B$ and $a \in A$ such that $y = (b, a)$

Now, we find $x = (a, b) \in A \times B$ such that

$$f(x) = f((a, b)) = (b, a) = y$$

$\therefore$ f is onto.

So, f is one-one and onto.

Therefore f is bijective. Hence $A \times B \sim B \times A$.

Example 4. Show that $(0, 1) \sim R$.

Sol. Define the function $f(x) = \tan \pi \left(x - \frac{1}{2}\right),\ \forall\ x \in (0, 1)$

We show that f is bijective

For one-one Let $x_1, x_2 \in (0, 1)$ be such that $f(x_1) = f(x_2)$

$\Rightarrow$ $\tan \pi \left(x_1 - \frac{1}{2}\right) = \tan \pi \left(x_2 - \frac{1}{2}\right) \Rightarrow \pi \left(x_1 - \frac{1}{2}\right) = \pi \left(x_2 - \frac{1}{2}\right) + n\pi$, where $n \in \mathbb{Z}$

$\Rightarrow$ $x_1 - \frac{1}{2} = x_2 - \frac{1}{2} + n$, where $n \in \mathbb{Z} \Rightarrow x_1 - x_2 = n$, where $n \in \mathbb{Z}$

But $x_1, x_2 \in (0, 1) \therefore |x_1 - x_2| < 1$, so $n = 0$

$\therefore \quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

So, f is one-one.

For onto For any $y \in R$, we have

If $y \geq 0$ then $\exists\ x \in \left[\frac{1}{2}, 1\right)$ such that $f(x) = \tan \pi \left(x - \frac{1}{2}\right) = y$

If $y < 0$ then $\exists\ x \in \left(0, \frac{1}{2}\right)$ such that $f(x) = \tan \pi \left(x - \frac{1}{2}\right) = y$

Thus $\forall\ y \in R$, $\exists\ x \in (0, 1)$ such that $f(x) = y$

$\therefore$ f is onto .

So, f is one-one and onto

Hence $(0, 1) \sim R$.

Example 5. Show that for each $a \in R$, $(0, 1) \sim (a, a + 1)$.

Sol. Consider the map $f: (0, 1) \to (a, a + 1)$ defined by

$$f(x) = a + x, \ \forall x \in (0, 1)$$

We claim that f is a bijective map.

For one-one Let $x_1, x_2 \in (0, 1)$ be two numbers such that $f(x_1) = f(x_2)$

$\Rightarrow \quad a + x_1 = a + x_2 \Rightarrow x_1 = x_2$

$\therefore$ f is one-one.

For onto Let $y \in (a, a + 1)$ be any real number, then

$$a < y < a + 1 \Rightarrow 0 < y - a < 1$$

Take $x = y - a \in (0, 1)$ such that

$$f(x) = a + x = a + (y - a) = y$$

$\therefore$ f is onto, *i.e.* f is a bijection.

Hence $(0, 1) \sim (a, a + 1)\ \forall\ a \in R$.

Aliter Hint : Take $b = a + 1$ in Example 2.

Example 6. If A, B, P and Q be four sets such that $A \sim P$ and $B \sim Q$ and $A \cap B = \phi = P \cap Q$. Then sh that $A \cup B \sim P \cup Q$ and $A \times B \sim P \times Q$.

Sol. Given $A \sim P$ and $B \sim Q$

$\therefore$ $\exists$'s bijective functions $f : A \to P$ and $g : B \to Q$

(i) Define a function $h : A \cup B \to P \cup Q$ as

$$h(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B \end{cases}$$

We show that h is one-one and onto.

For one-one Let $x_1, x_2 \in A \cup B$ be any two element, such that $h(x_1) = h(x_2)$

Case (i) When both $x_1, x_2 \in A$ (or $x_1, x_2 \in B$)

Then $h(x_1) = h(x_2)$

$\Rightarrow \quad f(x_1) = f(x_2)$

$\Rightarrow \quad x_1 = x_2$ [$\because f$ is one-one]

The case when both $x_1, x_2 \in B$ can be handle similarly.

Case (ii) When $x_1 \in A$ and $x_2 \in B$, then $x_1 \neq x_2$ (as $A \cap B = \phi$)

Also $f(x_1) \in P$ and $g(x_2) \in Q$ and $P \cap Q = \phi$ implies

$$f(x_1) \neq g(x_2) \Rightarrow h(x_1) \neq h(x_2)$$

$\therefore \quad x_1 \neq x_2 \Rightarrow h(x_1) \neq h(x_2)$.

Thus in both the cases, we see that h is one-one.

For onto Let $y \in P \cup Q$ be any element

Since $P \cap Q = \phi$

$\therefore$ either $y \in P$ or $y \in Q$

if $y \in P$ then as $f : A \to P$ is onto

$\therefore$ $\exists$ some $a \in A$ such that

$f(a) = y$. Then

$h(a) = f(a) = y$

If $y \in Q$ then as $g : B \to Q$ is onto

$\therefore$ $\exists$ some $b \in A$ such that

$g(b) = y$. Then

$h(b) = f(a) = y$

Thus in both the cases we see that for each $y \in P \cup Q$ $\exists$ some $x \in A \cup B$ such that $h(x) = y$

$\therefore$ h is onto.

So, h is bijective. Hence $A \cup B \sim P \cup Q$.

(*ii*) Define the mapping $h' : A \times B \to P \times Q$ by

$$h'(a, b) = (f(a), g(b)) \quad \forall\ (a, b) \in A \times B$$

We show that h' is one-one and onto.

For one-one Let $(a_1, b_1), (a_2, b_2) \in A \times B$ be any element such that

$$h'(a_1, b_1) = h'(a_2, b_2)$$

$$\Rightarrow \quad (f(a_1), g(b_1)) = (f(a_2), g(b_2))$$

$$\Rightarrow \quad f(a_1) = f(a_2) \text{ and } g(b_1) = g(b_2)$$

[$\because$ both f and g are

$$\Rightarrow \quad a_1 = a_2 \text{ and } b_1 = b_2$$

$$\Rightarrow \quad (a_1, b_1) = (a_2, b_2)$$

$\therefore$ h' is one-one.

For onto Let $(y_1, y_2) \in P \times Q$ be any element

Where $y_1 \in P$ and $y_2 \in Q$.

As $f : A \to P$ and $g : B \to Q$ onto

$\therefore$ $\exists\ x_1 \in A$ and $x_2 \in B$ such that $f(x_1) = y_1$ and $g(x_2) = y_2$

$\therefore$ $h'(x_1, x_2) = (f(x_1), g(x_2)) = (y_1, y_2)$

Thus $\forall\ (y_1, y_2) \in P \times Q, \exists\ (x_1, x_2) \in A \cup B$ such that

$$h'(x_1, x_2) = (y_2, y_2)$$

$\therefore$ h' is onto.

Hence h' is one-one and onto.

So $A \times B \sim P \times Q$.

Example 7. *Show that if* $A \sim B$, then $P(A) \sim P(B)$.

Sol. *Since* $A \sim B$. *Let* $f : A \to B$ be the bijection between A and B.

Define a mapping $F : P(A) \to P(B)$ by

$$F(X) = \{f(a) : \forall\ a \in X\}, \forall\ X \subseteq A$$

we show that F is bijective.

For one-one : *Let* $X_1, X_2 \in P(A)$ such that $F(X_1) = F(X_2)$

$$\Rightarrow \quad \{f(a) : \forall\ a \in X_1\} = \{f(b) : \forall\ b \in X_2\}$$

$\therefore$ *for each* $a_1 \in X_1$, *let the element* $f(a_1) = f(b_1)$ *for some* $b \in X_2$

But $f : A \to B$ is bijective

$\therefore \quad f(a_1) = f(b_1) \Rightarrow a_1 = b_1$

$\therefore \quad X_1 \subseteq X_2$

Similarly, for each $b_2 \in X_2$, let the element $f(b_2) = f(a_2)$ for some $a \in X_1$

But $f : A \to B$ is bijective

$\therefore \quad f(b_2) = f(a_2) \Rightarrow b_2 = a_2$

$\therefore \quad X_2 \subseteq X_1$

Thus $X_1 = X_2$

So, $F(X_1) = F(X_2) \Rightarrow X_1 = X_2$.

Therefore F is one-one.

For onto : Let $Y \in P(B)$ be any element

$\Rightarrow$ Y is a subset of B $\therefore$ $F^{-1}(Y) \subseteq A$, where

$F^{-1}(Y) = \{a \in A : f(a) \in Y\} = X$ (say)

$\Rightarrow$ $F(X) = Y$. So F is onto

Therefore F is one-one and onto

Hence $P(A) \sim P(B)$.

EXERCISE 1.8

1. Show that the sets

   $A = \{x : x \in R$ such that $2 \le x \le 3\}$ and $B = \{x : x \in R$ such that $5 \le x \le 7\}$ are equivalent.

2. For a set A, let P(A) denote the collection of all subsets of A. Prove that if $n(A) = n$, then $n(P(A)) = 2^n$.

3. Give an example of a set S such that there is an injection from S to S but no surjection from R (set of real numbers) to the set S.

4. Prove that there is no surjection from a set A to P(A).

1.53. Finite and Infinite set

A set A is said to be **finite** iff either $A = \phi$ or there exist a positive integer n such that $A \sim \{1, 2, 3, ..., n\}$, otherwise A is said to be an **infinite** set. In other words, A is said to be **infinite set** if $\exists$ a **injection** $f : A \to A$ such that $f(A) \neq A$.

Remark : (*i*) If a set $A \sim \{1, 2, 3, ..., n\}$, then we say that A is a finite set having n elements.

(*ii*) In case of finite sets, two sets are equivalent iff they have the same number of elements.

(*iii*) If B is infinite and $B \subset A$, then A is infinite *i.e.* superset of infinite set is infinite.

1.54. Definitions

(*i*) Countably infinite set (or Denumerable or Enumerable set) : An infinite set A is said countably infinite set or denumerable or enumerable set iff $A \sim \mathbb{N}$.

(*ii*) Countable set : A set A is said to be countable if A is either finite set or a countably infinite s

(*iii*) Almost Countable : A set A is said to be atmost countable if A is either a finite set or a countable

(*iv*) Uncountable set : An infinite set, which is not countably infinite (or denumerable) set is sa be uncountable set.

1.55. A set A is countably infinite or denumerable iff its elements can be put in the form of an inf sequence of distinct elements.

Proof : Let A be a countably infinite set. Then by definition $A \sim \mathbb{N}$.

Therefore, $\exists$ a function $f: \mathbb{N} \to A$ which is bijective

i.e. $\forall\ n \in \mathbb{N}, \exists$'s $a_n \in A$ such that $f(n) = a_n$ and

$f(n_1) = f(n_2) \Rightarrow n_1 = n_2$ [or $n_1 \neq n_2 \Rightarrow f(n_1) \neq f(n_2)$]

Thus $A = \{a_1, a_2, \ldots, a_n, \ldots\}$, where $a_1, a_2, \ldots a_n, \ldots$ are distinct elements of A

Conversely, let every elements of A can be put in the form of an infinite sequence

Let $A = \{a_1, a_2, \ldots, a_n, \ldots\}$ where $a_1, a_2, \ldots, a_n \ldots$ are distinct elements of A.

Define a function $g: \mathbb{N} \to A$ as $g(n) = a_n \quad \forall\ n \in \mathbb{N}$

Then we claim g is a bijective function.

For one-one Let $n_1 \neq n_2 \in \mathbb{N} \Rightarrow a_{n_1} \neq a_{n_2} \Rightarrow f(n_1) \neq f(n_2)$

$\therefore \quad n_1 \neq n_2 \Rightarrow f(n_1) \neq f(n_2)$

So, f is one-one.

For onto Let $y \in A$ be any element

$\therefore \quad \exists\ a_n \in A$ such that $y = a_n$

Thus $\exists\ n \in \mathbb{N}$ such that $g(n) = a_n = y$

$\therefore$ g is onto.

Thus g is bijective function.

Hence $A \sim \mathbb{N}$ *i.e.*, A is countably infinite set.

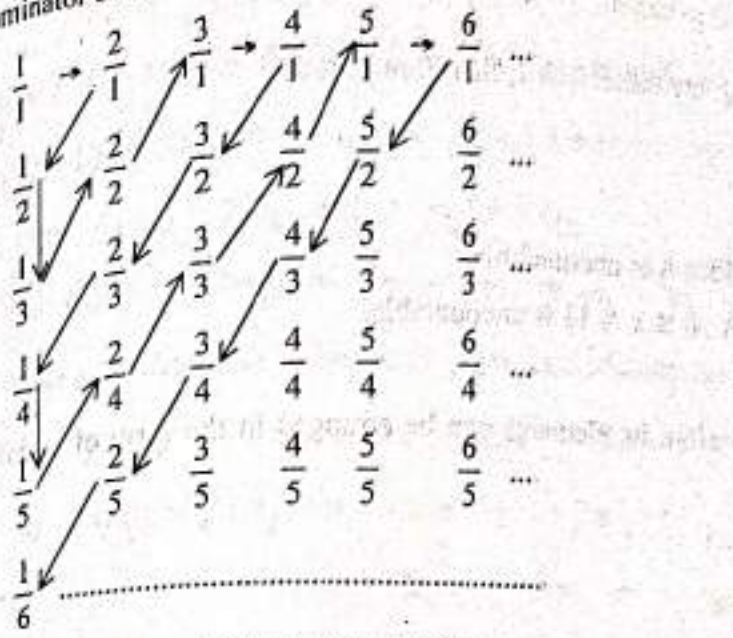
Remark : Every infinite set contains a denumerable set.

1.56. Prove that the set of rational numbers is denumerable.

Or

Find a bijection between the set of rational numbers and the set of all positive integers.

Proof : Firstly, we will take positive rational numbers only and write them all in the order of magnitude *i.e.* all numbers whose denominator is 1, then all fraction with denominator is 2, then all fraction with denominator 3 and so on as shown below by the arrow.



[Here arrow follows the **addition of numerator and denominator** in each fraction as 2, 3, 4, ...]

If we write down numbers in the order of succession indicated by arrow after leaving out those numbers, which have already appeared, then every positive rational number can be written as the sequence $\left\{\frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{1}{3}, \frac{3}{1}, \frac{4}{1}, \frac{3}{2}, \frac{2}{3}, \frac{1}{4}, \ldots\right\}$ and if we denote the sequence by $\{s_1, s_2, s_3, \ldots\}$, then

Clearly,

$$\mathbf{Q} = \{0, -s_1, s_1, -s_2, s_2, -s_3, \ldots\}$$

Thus, the set of rational numbers can be written as an infinite sequence with distinct elements.

Then we can define a bijection map $f : \mathbf{N} \to \mathbf{Q}$ as $f(1) = 0$ and

$$f(n) = \begin{cases} s_{\frac{n}{2}} & ; \text{ if } n \text{ is even} \\ -s_{\frac{n-1}{2}} & ; \text{ if } n \text{ is odd} \end{cases}$$

$\mathbf{N} \sim \mathbf{Q}$.

Hence Q is denumerable.

Example 1. Prove that the set of all sequences whose elements are either zero or one is not countable.

Sol. Let A be the set of all sequences with elements 0 and 1 only.

For example the sequence $< 0, 1, 0, 1, 0, 1, \ldots\ldots\ldots > \in A$.

Suppose that A is countable. Then A can be written $\{f_1, f_2, f_3, \ldots\ldots\ldots\}$ where each $f_i, i \in \mathbf{N}$ is a sequence such that $f_i(n) = 0$ or 1 ; $\forall\, n \in \mathbf{N}, i \in \mathbf{N}$.

Consider the sequence f such that

$$f(n) = \begin{cases} 1 & \text{if } f_n(n) = 0 \\ 0 & \text{if } f_n(n) = 1 \end{cases}$$

Since all the elements of the sequence f are either 0 or 1, therefore $f \in A$.

But $f \neq f_n$, $\forall n \in \mathbf{N}$ (∵ of

So, we arrive at a contradiction.

Hence our supposition is wrong. Therefore A is uncountable.

Example 2. Prove that the set $[0, 1] = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$ is uncountable.

Sol. Let $A = [0, 1] = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$

If possible, let A be denumerable, therefore its elements can be arranged in the form of an infini sequence with distinct elements.

∴ Let $A = \{x_1, x_2, x_3, ..., x_n, ...\}$

Expanding each x_i in decimals, we have

$x_1 = 0 . a_{11}\ a_{12}\ a_{13}\ a_{14}$ .....

$x_2 = 0 . a_{21}\ a_{22}\ a_{23}\ a_{24}$ .....

$x_3 = 0 . a_{31}\ a_{32}\ a_{33}\ a_{34}$ .....

.....

.....

$x_n = 0 . a_{n1}\ a_{n2}\ a_{n3}\ a_{n4}$ .....

.....

.....

where each $a_{ij} \in \{0, 1, 2, 3, ..., 9\}$ and each decimal contains an infinite number of non-zero digi

[*e.g.* $1 = 0 \cdot \overline{9}$, $\frac{1}{2} = 0 \cdot 4\overline{9}$, $\frac{1}{5} = 0 \cdot 1\overline{9}$ etc.]

Now, we construct a real number y as follows

$y = 0.b_1\ b_2\ b_3\ b_4\ .....b_n$ ....., where each $b_i \in \{0, 1, 2, ..., 9\}$

∴ $0 \leq y \leq 1$ $\Rightarrow$ $y \in A$

Let $b_1 \neq a_{11}, b_2 \neq a_{22}, ..., b_n \neq a_{nn}, ...$

$\Rightarrow$ $y \neq x_1, y \neq x_2, ..., y \neq x_n, ...$

∴ y is distinct from each x_n $\{n \in \mathbf{N}\}$ in alteast one decimal place and hence $y \notin A$, which contradiction ∴ our supposition is wrong.

Hence, [0, 1] is uncountable.

Example 3. Show that Z is countable *i.e.* the set of integers is countable.

Sol. We define a mapping $f: Z \to N$ as

$f(0) = 1,\ f(m) = 2m,\ f(-m) = 2m + 1$ where $m \in Z^+$

To show f is 1-1 Take $f(m_1) = f(m_2)$ for $m_1, m_2 \in Z$

Case (i) When both $f(m_1)$ and $f(m_2)$ are even integers

Then $f(m_1) = 2m_1$ and $f(m_2) = 2m_2$

So $f(m_1) = f(m_2) \Rightarrow 2m_1 = 2m_2 \Rightarrow m_1 = m_2$

Case (ii) When both $f(m_1)$ and $f(m_2)$ are odd (except 1)

Then $f(m_1) = -2m_1 + 1$ and $f(m_2) = -2m_2 + 1$

So $f(m_1) = f(m_2) \Rightarrow -2m_1 + 1 = -2m_2 + 1$

$\Rightarrow -2m_1 = -2m_2 \Rightarrow m_1 = m_2$

Case (iii) When $f(m_1) = 1 = f(m_2)$

Then $m_1 = 0$ and $m_2 = 0$ so $m_1 = m_2$

$\therefore$ in each case $f(m_1) = f(m_2) \Rightarrow m_1 = m_2$

$\therefore$ f is $1-1$

To show f is onto Let $m \in N$

If m is odd except 1, then $m = 2n + 1$ for some $n \in N \subseteq Z$

and $f(-n) = 2n + 1 = m$

If $m = 1$ then $f(0) = 1 = m$

and if m is even, then $m = 2n$ for some $n \in N \subseteq Z$

and $f(n) = 2n = m$

so that f is onto

$\therefore$ $Z \sim N \Rightarrow Z$ is countable.

Example 4. Prove that the set $\left\{\ldots 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3 \ldots\right\}$ is countable.

Sol. Given set $= \left\{\ldots 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3 \ldots\right\} = A$ (say)

i.e. $A = \left\{2^m \mid m \text{ is an integer}\right\}$

We define a mapping $f: Z \to A$ (Z is set of integers) as $f(m) = 2^m$

To show f is 1 – 1 Let $f(m_1) = f(m_2)$, for $m_1, m_2 \in Z$

$\Rightarrow \quad 2^{m_1} = 2^{m_2} \Rightarrow m_1 = m_2$

so f is 1 – 1

To show f is onto For each $y = 2^m \in A$, $\exists\ m \in Z$

such that $f(m) = 2^m = y$ (by def. of f)

$\therefore$ f is onto

$\therefore$ $Z \sim A$

Also we know $Z \sim N$

So that $A \sim N \Rightarrow$ A is countable.

Cor. 1. The set $[a, b] = \{x \in R : a \le x \le b\}$ is uncountable.

Proof : As $f: [0, 1] \to [a, b]$ defined by $f(x) = a + (b - a)x$ is one-one and onto.

$\therefore$ $[0, 1] \sim [a, b]$

But the set [0, 1] is uncountable $\therefore$ $[a, b]$ is uncountable.

1.57. Prove that every subset of a denumerable set is countable.

Proof : Let A be a denumerable set. Then A can be written as an infinite sequence with distinct elements.
Let $A = \{a_1, a_2, a_3, ..., a_n, ...\}$.

Let $B \subseteq A$. If $B = \phi$, then B is finite set and hence countable.

And, if $B \neq \phi$, let k_1 be the least positive integer such that $a_{k_1} \in B$.

Consider, the set $B_1 = B - \{a_{k_1}\}$.

If $B_1 = \phi$, then $B = \{a_{k_1}\}$, is finite and hence countable.

If $B_1 \neq \phi$, let k_2 be the least positive integer such that $a_{k_2} \in B_1$.

Consider, the set $B_2 = B - \{a_{k_1}, a_{k_2}\}$, where $k_1 < k_2$.

If $B_2 = \phi$, then $B = \{a_{k_1}, a_{k_2}\}$, is finite and hence countable.

If $B_2 = \phi$, then continuing in this way, we get

$B_{m-1} = B - \{a_{k_1}, a_{k_2}, ..., a_{k_{m-1}}\}$

If $B_{m-1} = \phi$, then $B = \{a_{k_1}, a_{k_2}, ..., a_{k_{m-1}}\}$, is finite and hence countable.

The above process may or may not stop, according as B is finite or infinite. If B is finite, then B is countable and if B is infinite, let k_m be the least positive integer greater than k_{m-1} such that $a_{k_m} \in B$. Then

$$B = \{a_{k_1}, a_{k_2}, a_{k_3}, ..., a_{k_m}, ...\}$$

where $k_1 < k_2 < k_3 < .... < k_{m-1} < k_m < ....$

Let $f: N \to B$ be the map definited by $f(m) = a_{k_m}, \forall\, m \in N$

Clearly, f is one-one and onto $\therefore$ $N \sim B$

So, B is denumerable.

Thus, either B is finite or denumerable. Hence B is countable.

Cor. Every infinite subset of denumerable set is denumerable.

Remark 1. The set of prime numbers is denumerable.

Proof : Since the set of prime numbers P is subset of set of natural number which is denumerable. Also P is infinite set. Hence by above corollary P is denumerable.

Remark 2. The set of real numbers **R** is uncountable.

Proof : If possible, let **R**, be denumerable. Also we know that infinite subset of a denumerable is denumerable. Therefore $[0, 1] \subset \mathbf{R}$, implies that [0, 1] is denumerable set. Which is a contradiction to the fact that [0, 1] is uncountable.

Hence, **R**, the set of real numbers is uncountable.

Remark 3. The set of irrational numbers is uncountable.

Proof. Let **P** be a the set of irrational numbers. If possible, let **P** be denumerable. But the set Q of rational numbers is denumerable.

$\Rightarrow$ $\mathbf{P} \cup \mathbf{Q}$ is also denumerable [$\because$ Union of two denumerable set is denumerable]

$\Rightarrow$ **R**, is denumerable [$\because \mathbf{R} = \mathbf{P} \cup \mathbf{Q}$], which is a contradiction.

Hence, the set **P**, of irrational numbers is uncountable.

1.58 Prove that the union of denumerable collection of denumerable sets is denumerable.

Proof : Let $E = \{E_1, E_2, E_3, ...\}$ be a denumerable collection of denumerable sets.

Let $E_1 = \{e_{11}, e_{12}, e_{13}, ...\}$

$E_2 = \{e_{21}, e_{22}, e_{23}, ...\}$

$E_3 = \{e_{31}, e_{32}, e_{33}, ...\}$

.....

.....

$E_n = \{e_{n_1}, e_{n_2}, e_{n_3}, ...\}$

.....

.....

Now, we list the elements of $\bigcup_{n\in N} E_n$ as follows :

$$e_{11}$$

$$e_{12}\ e_{21}$$

$$e_{13}\ e_{22}\ e_{31}$$

$$e_{14}\ e_{23}\ e_{32}\ e_{41}$$

$$e_{15}\ e_{24}\ e_{33}\ e_{42}\ e_{51}$$

.....

.....

Here, first row contain all elements e_{pq}, where $p+q=2$. Second row contains all the elemen e_{pq} with $p+q=3$ and so on, of course, we remove any element e_{ij} if it has already occured. In this wa every elements of $\bigcup_{n\in N} E_n$ occurs one and only once and it occupies a definite position. Further, E_1 $\bigcup_{n\in N} E_n$ and E_1 is infinite, therefore $\bigcup_{n\in N} E_n$ is an infinite set. Thus the elements of $\bigcup_{n\in N} E_n$ has bee arranged in the form of an infinite sequence with distinct elements.

Hence $\bigcup_{n\in N} E_n$ is a denumerable set.

1.59. Prove that the set $\mathbf{N}\times\mathbf{N}$ is denumerable.

Proof. Since $\mathbf{N}\times\mathbf{N}=\{(a, b) : a, b\in\mathbf{N}\}$

Let $A_1=\{(1,1),(1,2),(1,3),(1,4),\ldots\ldots\}$

$A_2=\{(2,1),(2,2),(2,3),(2,4),\ldots\ldots\}$

$A_3=\{(3,1),(3,2),(3,3),(3,4),\ldots\ldots\}$

_____

_____

$A_n=\{(n,1),(n,2),(n,3),(n,4),\ldots\ldots\}$

_____

_____

then, clearly $\bigcup_{n\in N} A_n=\mathbf{N}\times\mathbf{N}$

Let $f: A_n\to\mathbf{N}$ be a mapping defined by $f(n,b)=b$, $\forall\, b\in\mathbf{N}$

Then, f is one-one and onto

$\therefore$ $A_n\sim\mathbf{N}$ *i.e.* A_n is denumerable for $n=1,2,3,\ldots\ldots$

$\therefore$ $\mathbf{N}\times\mathbf{N}=\bigcup_{n\in N} A_n$, is the union of denumerable sets.

Hence, $\mathbf{N}\times\mathbf{N}$ is denumerable.

Remark. Since $\mathbf{N}\times\mathbf{N}$ is denumerable.

$\therefore$ $\mathbf{N}\times\mathbf{N}\sim\mathbf{N}$.

Example 5. Prove that if A and B are two denumerable sets, then $A \times B$ is also denumerable.

Sol. Let $A = \{a_1, a_2, a_3, ...\}$ and $B = \{b_1, b_2, b_3, ...\}$ be two denumerable sets. Therefore there exists mapping $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ defined by $f(n) = a_n$ and $g(m) = b_m$, $\forall\, n, m \in \mathbb{N}$, such that both f and g are one-one and onto.

Let $h : \mathbb{N} \times \mathbb{N} \to A \times B$ be a map defined by

$$h((n, m)) = (a_n, b_n) = (f(n), g(m)), \forall\, (n, m) \in \mathbb{N} \times \mathbb{N}$$

Since f and g are both one-one and onto maps, therefore h is also one-one and onto.

$\therefore$ $\mathbb{N} \times \mathbb{N} \sim A \times B$. Also $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$

$\Rightarrow$ $A \times B \sim \mathbb{N}$.

Hence, $A \times B$ is denumerable.

Remark : Cartesian Product of finite number of countable sets is countable.

Example 6. Give are example to show that countable Cartesian product of countable sets need not be countable.

Sol. For each $n \in \mathbb{N}$, Consider the set $A_n = \{0, 1\}$. Clearly each A_n is a finite set and hence countable.

There $\{A_n : n \in \mathbb{N}\}$ be a collection of countable sets.

Let $A = \prod_{n \in \mathbb{N}} A_n$, be the Cartesian product of $\{A_n : n \in \mathbb{N}\}$.

We show that A is not countable.

If possible, let A be countable.

Let $f : \mathbb{N} \to A$ be a bijection between $\mathbb{N}$ and A

Let $f(i) = (a_{i1}, a_{i2}, ..., a_{in}, ...)$ $\forall\, i \in \mathbb{N}$.

where $a_{ij} \in \{0, 1\}$ $\forall\, i, j$

Consider an element $a \in A$ defined by

$$b = (b_1, b_2, b_3, ... b_n, ...)$$

where $b_i = \begin{cases} 1 & \text{if } a_{ii} = 0 \\ 0 & \text{if } a_{ii} = 1 \end{cases}$ $\forall\, i \in \mathbb{N}$

Clearly $b \neq f(n)$ for any $n \in \mathbb{N}$.

Which is a contradiction as f is onto.

Hence A is not countable.

1.60. Algebraic and Transcendental Numbers

Algebraic Numbers : The roots of a polynomial equation with integral coefficients are algebraic numbers.

i.e. if $p(x) = a_0 + a_1 x + a_2 x + \ldots\ldots + a_n x^n = 0$

be a polynomial equation, where each $a_i \in \mathbf{Z}$. Then the roots of $p(x)$ are algebraic numbers.

Transcendental Numbers : A number which is not an algebraic number is called transcendental number *i.e.* a number which is not a root of a polynomial equation with integral coefficient is transcendental number.

For example : e, π, log 2 etc. are transcendental numbers.

1.61. Prove that the set of algebraic numbers is countable set.

Proof : Let P = $\{p(x) : p(x)$ is polynomial with integral coefficients$\}$

where $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_m x^m$, where $a_i \in \mathbf{Z}$

We first show that the set P is countable.

For each ordered pair of natural number (m, n)

Let $P_{mn} = \{p(x) : p(x) \in P$ s.t. $|a_0| + |a_1| + |a_2| + \ldots\ldots + |a_m| = n\}$

Since degree m of a polynomial is fixed and sum of finite number of terms is finite

$\therefore$ P_{mn} is finite set and $\therefore$ P_{mn} is countable set

Now $P = \cup \{P_{mn}$: where $(m, n) \in \mathbf{N} \times \mathbf{N}\}$

= countable union of countable sets = countable set

Hence the set of all polynomial with integral coefficient is countable set.

Let E = $\{ p_i(x) = 0$; where $i \in \wedge \}$, where $\wedge$ is countable set.

For each $i \in \wedge$, let $A_i = \{x : x$ is a root of $p_i(x) = 0$, where $p_i(x) \in E\}$.

Then $A = \cup A_i$ = Set of all algebraic numbers.

Since each $p_i(x) = 0$ is of finite degree m has at most m roots.

$\therefore$ Each A_i is finite set and so countable set.

$\therefore$ $A = \bigcup_{i \in \wedge} A_i$ is the countable union of countable sets is also countable set.

Hence the set of all algebraic numbers is countable set.

Cor. If a finite number of elements be added in a countable set, then the resulting set is again countable

Proof : Let $A = \{a_1, a_2, a_3, \ldots\ldots a_n\}$ be a finite set and

$B = \{b_{n+1}, b_{n+2}, \ldots\ldots, b_{m+n}, \ldots\ldots\}$ be a countable set.

Then we can define a function $f: N \to A \cup B$ by

$$f(k) = \begin{cases} a_k & \text{if } 1 \le k \le n \\ b_k & \text{if } k > n \end{cases}$$

Clearly f is one-one and onto $\therefore$ $N \sim A \cup B$.

$\Rightarrow$ $A \cup B$ is countable.

1.62. Prove that the set of Transcendental numbers is uncountable set.

Proof : Let T = Set of all transcendental numbers and

A = Set of all algebraic numbers

If possible, let T be countable set. Then $T \cup A$ is countable set. [$\because$ union of two countable sets is countable]

Since $\mathbf{R} \subseteq A \cup T$, where $\mathbf{R}$ = set of all real numbers.

We know that subset of a countable set is countable set.

$\Rightarrow$ $\mathbf{R}$ is countable set, which is a contradiction as the set of real numbers is uncountable.

$\therefore$ our supposition is wrong.

Hence the set of all transcendental numbers is uncountable set.

ILLUSTRATIVE EXAMPLES

Example 1. If a function $f : A \to B$ is one-one and B is countable, there prove that A is atmost countable.

Sol. Let A be any set

Case (*i*) When A is a finite set, then A is almost countable

Case (*ii*) When A is infinite set.

Since $f : A \to B$ is one-one. Then $A \sim f(A)$

$\therefore$ $f(A)$ is also infinite set.

$\Rightarrow$ B is infinite set [$\because$ super set of infinite set is infinite $f(A) \subseteq B$]

As B is countable set.

$\therefore$ B is countably infinite set.

Let $B = \{b_1, b_2, b_3, ...\}$

Let n_1 be the first positive integer such that $b_{n_1} \in f(A)$

Let $n_2 > n_1$ be the next positive integer such that $b_{n_2} \in f(A)$

Continuing in this way.

We choose $n_1, n_2, \ldots\ldots, n_{k-1}, n_k \in \mathbb{N}$ such that $n_k > n_{k-1} > n_{k-2} > \ldots\ldots$

such that $b_{n_k} \in f(A)$. We get

$$f(A) = \{b_{n_1}, b_{n_2}, \ldots\ldots\}.$$

In other word the element of $f(A)$ can be arranged in the form of a sequence

$\therefore$ $f(A) \sim \mathbb{N}$ also $A \sim f(A)$

[$\because$ $\sim$ is transitive relation]

$\Rightarrow$ $A \sim \mathbb{N}$

i.e. A is countable set.

Therefore combinding the two cases, we find that either A is a finite set or a countable set.

Hence A is atmost countable.

Example 2. Prove that every infinite set is equivalent to a proper subset of itself.

Sol. Let A be infinite set

$\therefore$ by previous theorem A has a countable set (say) B.

Let $C = A - B \Rightarrow A = B \cup C$ and $B \cap C = \phi$

Since B is countable set $\therefore$ its elements can be arranged in the form of an infinite sequence with distinct elements.

Let $B = \{b_1, b_2, b_3, \ldots\ldots\}$ be countable set.

We take another set $B_1 = \{b_2, b_3, b_4, \ldots\ldots\}$.

$\therefore$ B_1 is a proper subset of B.

Define a function $\phi : B \to B_1$ by $\phi(b_i) = b_{i+1}$.

Clearly ϕ is one-one and onto $\therefore$ $B \sim B_1$

Let $A_1 = B_1 \cup C$

Since B_1 is a proper subset of B $\therefore$ $B_1 \cup C$ is a proper subset of $B \cup C$.

$\Rightarrow$ A_1 is a proper subset of A.

But $B \sim B_1$ and $B \cap C = \phi$

Also $C \sim C$ and $B_1 \cap C = \phi$

implies that $B \cup C \sim B_1 \cup C$ *i.e.* $A \sim A_1$

where A_1 is a proper subset of A.

Hence every infinite set is equivalent to a proper subset of itself.

Example 3. Prove that the set of rational numbers is denumerable.

Sol. We know that the set of integers is a denumerable set as $\exists$ a bijection $f: \mathbf{N} \to \mathbf{Z}$ defined by

$$f(n) = \begin{cases} \frac{n}{2} & ; \text{ if } n \text{ is even} \\ -\frac{n-1}{2} & ; \text{ if } n \text{ is odd} \end{cases}$$

i.e. $\mathbf{N} \sim \mathbf{Z}$

Let for each $n \in \mathbf{N}$, Define the set

$$A_n = \left\{ \frac{m}{n} : m \in \mathbf{Z} \right\}$$

Then $A_n \sim \mathbf{Z}$ for $\exists$ a bijection $g: \mathbf{Z} \to A_n$ by

$$g(m) = \frac{m}{n} \; ; \forall m \in \mathbf{Z}$$

$$\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} \left\{ \frac{m}{n} : m \in \mathbf{Z} \right\} = \mathbf{Q}$$

Since each A_n is denumerable set and countable union of dennumerable sets is denumerable set

implies that $\bigcup_{n=1}^{\infty} A_n$ is denumerable set.

Example 4. Prove that cartesians product of two countable sets is a countable set.

Sol. Let A and B be two countable sets

$\therefore$ $\exists$'s bijection $f: \mathbf{N} \to \mathrm{A}$ and $g: \mathbf{N} \to \mathrm{B}$

Let us defined a map $h: \mathbf{N} \times \mathbf{N} \to \mathrm{A} \times \mathrm{B}$ by

$$h(m, n) = (f(m), g(n))$$

For one-one Let $h(m_1, n_1) = h(m_2, n_2)$

$\Rightarrow$ $(f(m_1), g(n_1)) = (f(m_2), g(n_2))$

$\Rightarrow$ $f(m_1) = f(m_2)$ and $g(n_1) = g(n_2)$

$\Rightarrow$ $m_1 = m_2$ and $n_1 = n_2$ ($\because$ both f and g are one-one)

$\therefore$ $(m_1, n_1) = (m_2, n_2)$

so h is one-one.

For onto. Let $(a, b) \in \mathrm{A} \times \mathrm{B}$ be any element where $a \in \mathrm{A}$ and $b \in \mathrm{B}$.

As f and g are onto maps $\therefore$ $\exists\, m \in \mathbf{N}$ and $n \in \mathbf{N}$ such that $f(m) = a$ and $g(n) = b$

Thus $\exists\ (m, n) \in \mathbf{N} \times \mathbf{N}$ such that

$$h(m, n) = (f(m), g(n)) = (a, b)$$

$\therefore$ h is onto

Hence h is a bijection between $\mathbf{N} \times \mathbf{N}$ to $\mathrm{A} \times \mathrm{B}$

$\therefore$ $\mathbf{N} \times \mathbf{N} \sim \mathrm{A} \times \mathrm{B}$

As $\mathbf{N} \times \mathbf{N}$ is countable set $\therefore$ $\mathrm{A} \times \mathrm{B}$ is also countable set.

Thus the product of two countable sets is a countable set.

Example 5. Prove that union of finite number of countable sets is a countable set.

Sol. Let $\mathrm{E} = \{\mathrm{E}_1, \mathrm{E}_2, \mathrm{E}_3, \ldots\ldots, \mathrm{E}_m\}$ be a finite collection of countable sets

Let $\mathrm{E}_1 = \{e_{11}, e_{12}, e_{13}, \ldots\ldots\}$

$\mathrm{E}_2 = \{e_{21}, e_{22}, e_{23}, \ldots\ldots\}$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\mathrm{E}_m = \{e_{m_1}, e_{m_2}, e_{m_3}, \ldots\ldots\}$

Take, the union $\bigcup_{i=1}^{m} \mathrm{E}_i$ the element of which are as follows :

e_{11}

$e_{12}\ \ e_{21}$

$e_{13}\ \ e_{22}\ e_{31}$

$e_{14}\ \ e_{23}\ \ e_{32}\ \ e_{41}$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$\ldots\ldots\ldots\ldots\ldots\ldots$

$e_{1m}\ \ e_{2\overline{m-1}}\ e_{3\overline{m-3}}\ \ldots\ldots\ldots\ldots\ e_{m1}$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Here, first row contain all element e_{pq}, where $p + q = 2$. Second row contains all the elements e_{pq} with $p + q = 3$ and so on and the mth row contains all the elements e_{pq} with $p + q = m + 1$, of course, we remove any element e_{ij} if it has already occurred. In this way every element of $\bigcup_{i=1}^{m} \mathrm{E}_i$ occurs one and only once and it occupies a definite position. Further, $\mathrm{E}_1 \subseteq \bigcup_{i=1}^{m} \mathrm{E}_i$ and E_1 is infinite, therefore $\bigcup_{i=1}^{m} \mathrm{E}_i$ is

an infinite set. Thus the element of $\bigcup_{i=1}^{m} E_i$ has been expressed in the form of an infinite sequence with distinct elements. Here $\bigcup_{i=1}^{m} E_i$ is a countable set.

Example 6. Prove that every subset of a countable set is atmost countable.

Sol. Let A be a subset of a countable set B.

Since B is a countable set. Therefore there exist a bijection mapping $f: B \to \mathbb{N}$

Let $g = f|_A$ be the restriction of the mapping f to the set A

i.e., $g: A \to \mathbb{N}$ defined by $g(x) = f(x), \forall\ x \in A$

Clearly, the mapping g is one-one, for let $x_1, x_2 \in A$ such that

$$g(x_1) = g(x_2) \Rightarrow f(x_1) = f(x_2)$$

$$\Rightarrow \quad x_1 = x_2 \qquad \text{[As } f \text{ is bijective function]}$$

$\exists$ some $x_n \in B$ such that $f(x_n) = n$

As f is onto $\therefore$ for each $n \in \mathbb{N}$

Also because $A \subseteq B$, then x_n may or may not belong to A

If $x_n \in A$ then $g(x_n) = f(x_n) = n$ implies g is onto

If $x_n \notin A$ then A is a finite subset of B

Thus either A is a finite subset of B or A is countable.

Hence A is atmost countable.

EXERCISE 1.9

1. Prove that every finite set is equivalent to $N_R = \{1, 2, 3, ..., k\}$ for some $k \in N$.
2. If B is countable subset of an uncountable set A, then show that A – B is uncountable.
3. If A and B are disjoint countably infinite sets, then prove that A ∪ B is a countably infinite set.
4. Show that the set of all intervals with rational end points is a countable set.
5. Prove that union of two denumerable sets is denumerable set.
6. Prove that the set of complex number is uncountable.
7. If A is a countable set and $A \sim B$, then show that that B is also countable.
8. (*i*) If A is a countable set and $f: A \to B$ be a surjective map. Then prove that B is also countable set.

   (*ii*) If $f: A \to B$ and the range of f is uncountable, then prove that the domain of f is uncountable.

1.60. Cantor's diagonal Argument : (Diagonalisation argument, diagonal slash argument or diagonal method)

Cantor's diagonal argument was published in 1891 by Georg Cantor as a mathematical proof that there are infinite sets which cannot be put into one-to-one correspondence with the infinite set of natural numbers. Such sets are now known uncountable sets.

1.61. Working of Cantor's diagonal argument

Theorem : Cantor considered the set T of all infinite sequences of binary digits (i.e. each digit is 0 or 1).

If $s_1, s_2, ..., s_n, ...$ is any enumeration of elements from T, then there is always an element and of T which corresponds to no S_n in the enumeration.

Proof : $s_1, s_2, ..., s_n, ...$ is any enumeration of elements from T,

We can consider $s_1 = (0, 0, 0, 0, 0, 0, 0, ...)$

$s_2 = (1, 1, 1, 1, 1, 1, 1, ...)$

$s_3 = (0, 1, 0, 1, 0, 1, 0, ...)$

$s_4 = (1, 0, 1, 0, 1, 0, 1, ...)$

$s_5 = (1, 1, 0, 1, 0, 1, 1, ...)$

$s_6 = (0, 0, 1, 1, 0, 1, 1, ...)$

$s_7 = (1, 0, 0, 0, 1, 0, 0, ...)$

.....

.....

Next a sequence s is constructed by choosing the 1st digit as complementary to the 1st digit of s_1 (swapping 0's for 1's and vice versa), the 2nd digit as complementary to the 2nd digit of s_2, the 3rd digit as complementary to the 3rd digit of s_3 and generally for every n, the n^{th} digit as complementary to the n^{th} digit of s_n. This yields

$s = (1, 0, 1, 1, 1, 0, 1, ...)$

(s obtained by taking complement of diagonal entries in $[s_i]$)

by construction s differs from each s_n, since their n^{th} digit differ. Hence and cannot occur in the enumeration

Example : Prove by Cantor's diagonal argument, set of real no. is uncountable.

Sol. We will firstly prove interval

$(0, 1) = \{x \in R : 0 < x < 1\}$ is uncountable by contradiction.

Assume there is a bijective function f such that $f : N \to (0, 1)\ \forall\ n \in N$

$f(n) = \cdot a_{n1}\ a_{n2}\ a_{n3}\ a_{n4} \ldots\ldots$

such that a_{nk} represent k^{th} digit of n^{th} real number in decimal representation

$N \leftrightarrow (0, 1)$

1. $f(1) = \cdot a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15} \ldots$
2. $f(2) = \cdot a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25} \ldots$
3. $f(2) = \cdot a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35} \ldots$
4. $f(2) = \cdot a_{41}\ a_{42}\ a_{43}\ a_{44}\ a_{45} \ldots$
5. $f(2) = \cdot a_{51}\ a_{52}\ a_{53}\ a_{54}\ a_{55} \ldots$

⋮ .....

⋮ .....

Let us define a new number

$x = \cdot b_1\ b_2\ b_3\ b_4\ b_5 \ldots$

where $b_n = \begin{cases} 7 & , a_{nn} \neq 7 \\ 5 & , a_{nn} = 7 \end{cases}$

Clearly $x \in (0, 1)$ and $x \neq f(1)$, $x \neq f(2)$

$x \neq f(3)$, $x \neq f(4)$, $x \neq f(5)$ .....

So we can't find $i \in N$ such that

$x = f(i)$

$\therefore$ f is not surjective

a contradiction

$\therefore$ $\nexists\ f : N \to (0, 1)$ which is bijective

$\therefore$ $(0, 1) = \{x \in R / 0 < x < 1\}$ is uncountable

and $(0, 1) \subseteq R$

$\therefore$ R is uncountable.

Theorem : Cantor's Power set theorem (Power set theorem)

Statement : If S is any set, then there is an injection from S to P (S) but no bijection, So $|S| < |P(S)|$.

Proof : For any set S, the map $P : S \to P(S)$ defined as $p(s) = \{s\}$ $\forall$ $s \in S$

Clearly this map is well defined and injection from S to P (S)

$\therefore$ $\exists$ an injection from S to P (S).

Now we shall prove that $\nexists$ any bijection from S to P (S)

Let $q : S \to P(S)$ be a map

Put $Y = \{x \in S : x \notin q(x)\}$

Clearly Y is well defined subset of S we will prove that $\nexists$ $y \in S$ such that $q(y) = Y$

Suppose the contrary so there is $y \in S$ with $q(y) = Y$

If $y \in q(y) = Y$, then $y \notin q(y)$ is false, so by definition of Y we have $y \notin Y$, a contradiction.

If $y \notin q(y) = Y$, then $y \notin q(y)$ is true, so by definition of Y we have $y \in Y$, a contradiction so we get contradiction in both the cases $y \in Y$ and $y \notin Y$.

So the assumption that $q(y) = Y$ for $y \in S$ leads to a contradiction.

So no such y exists

So $Y \notin$ range of function q But $Y \in P(S)$

S q is not surjective

Thus we have proved that for any set S, there is no surjection from $S \to P(S)$, so no bijection.

Example : If N is set of natural number, then P (N), *i.e.* power set of N is uncountable.

Sol. If possible let P (N) is countable, $\therefore$ $\exists$ *a* map $f : N \to P(N)$ which is one-one and onto (i.e. bijective).

But by Cantor's power set theorem $\nexists$ map $S \to P(S)$ which is bijection. Which contradiction.

$\therefore$ our supposition is wrong

$\therefore$ P (N) is uncountable.

Theorem : Schroeder-Bernstein Theorem (Cantor-Schroeder Bernstein Theorem)

Statement : If A and B are sets and there are injections $f : A \to B$ and $g : B \to A$ then there is a bijection $h : A \to B$.

Proof : We call an element b of B lonely if there is no element $a \in A$ such that $f(a) = b$. We call an element b_1 of B is a descendent of an element b_0 of B if there is a natural number such that $b_1 = (f \circ g)^n (b_0)$.

We define the function $h : A \to B$ as follows :

$$h(a) = \begin{cases} g^{-1}(a) & , \text{ if } f(a) \text{ is the descendent of a lonely point} \\ f(a) & , \text{ otherwise} \end{cases}$$

Note that $f(a)$ cannot be lonely itself. If $f(a)$ is descendent of a lonely point, then

$f(a) = f \circ g(b)$ for some b ; since g is injective, the element $g^{-1}(a)$ is well defined. Thus h is also well defined, we claim that it is a bijection from A to B.

We first prove that h is surjective. Indeed if $b \in B$ is descendent of a lonely point then $h(g(b)) = b$; and if b is not descendent of a lonely point, then b is not lonely, so there is some $a \in A$ such that $f(a) = b$: by definition of h, $h(a) = b$. Thus h is surjective.

Now we will prove h is injective, we first note that for any $a \in A$, the point $h(a)$ is descendent of a lonely point iff $f(a)$ is a descendent of a lonely point. Now suppose that we have two elements $a_1, a_2 \in A$ such that

$$h(a_1) = h(a_2)$$

We consider two cases :

Case I : If $f(a_1)$ is descendent of a lonely point then so is $f(a_2)$.

$\Rightarrow \quad g^{-1}(a_1) = h(a_1) = h(a_2) = g^{-1}(a_2)$

$\Rightarrow \quad g^{-1}(a_1) = g^{-1}(a_2)$

Since g is well defined $\Rightarrow \quad a_1 = a_2$

Case II : If $f(a_2)$ is not descendent of a lonely point then neither is $f(a_2)$

$\Rightarrow \quad f(a_1) = h(a_1) = h(a_2) = f(a_2)$

$\Rightarrow \quad f(a_1) = f(a_2)$

Since f is injective

$\Rightarrow \quad a_1 = a_2$

Thus h is injective. Since h is surjective and injective, h is bijective, as desired.

Note : If A and B are finite sets

$f : A \to B$ is injection , $\therefore \; |A| \leq |B|$

and $g : B \to A$ is injection, $\therefore \; |B| \leq |A|$

$\therefore \quad |A| = |B|$

$\Rightarrow \quad \exists$ is a bijection from A to B.

SECTION-V
PRINCIPLES OF MATHEMATICS INDUCTION

1.62. Statement of Principle of Mathematical Induction

Let P (n) be a statement such that

(a) P (1) is true

(b) P $(r+1)$ is true whenever P (r) is true where $n = r$.

Then P (n) is true for all natural numbers n.

The Well-Ordering Principle

Every nonempty set of non-negative integers has a least element.

Recursive Definition : Sometimes we find it difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called recursion.

We can use recursion to define sequence, functions, and sets. In previous discussions, we specified the terms of a sequences using an explicit formula.

For example : We define recursively defined functions : We use two steps to define a function with the set of nonnegative integers as its domain :

Basic step : Specify the value of the function at zero.

Recursive step : Give a rule for finding its value at an integer from its value at smaller integers.

ILLUSTRATIVE EXAMPLES

Example 1. Prove that $9^n - 8^n - 1$ is divisible by 8.

Sol. Let $P(n) = 9^n - 8^n - 1$

$\therefore$ $P(1) = 9 - 8 - 1 = 0$, which is divisible by 8

$\therefore$ result is true for $n = 1$

Assume that result is true for $n = k$

$\therefore$ $P(k) = 9^k - 8^k - 1$ is divisible by 8.

Let $9^k - 8^k - 1 = 8l$, where l is an integer

$\therefore$ $9^k = 8l + 8^k + 1$ ...(1)

Now $P(k+1) = 9^{k+1} - 8^{k+1} - 1 = 9 \cdot 9^k - 8^{k+1} - 1$

$= 9(8l + 8^k + 1) - 8^{k+1} - 1$ [$\because$ of (1)]

$= 72l + 9 \cdot 8^k + 9 - 8 \cdot 8^k - 1 = 72l + 8^k + 8$

$= 8(9l + 8^{k-1} + 1)$, which is divisible by 8.

$\therefore$ result is true for $n = k+1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k+1$.

But the result is true for $n = 1$.

$\therefore$ by the method of induction, the result is true for all $n \in N$.

Example 2. Prove that $5^{2n+2} - 24n - 25$ is a multiple of 576.

Sol. Let $P(n) = 5^{2n+2} - 24n - 25$

$\therefore$ $P(1) = 5^4 - 24 - 25 = 625 - 24 - 25 = 576$, which is a multiple of 576.

$\therefore$ result is true for $n = 1$.

Assume that result is true for $n = k$.

$\therefore$ $P(k) = 5^{2k+2} - 24k - 25$ is a multiple of 576.

Let $5^{2k+2} - 24k - 25 = 576\,l$, where l is an integer

$\therefore$ $5^{2k+2} = 576\,l + 24k + 25$ ...(1)

Now $P(k+1) = 5^{2(k+1)+2} - 24(k+1) - 25 = 5^2 \cdot 5^{2k+2} - 24k - 24 - 25$

$= 25(576\,l + 24k + 25) - 24k - 24 - 25$ [$\because$ of (1)]

$= 25 \cdot 576\,l + 25 \cdot 24k + 625 - 24k - 24 - 25 = 576 \cdot 25\,l + 576k + 576$

$= 576(25\,l + k + 1)$, which is a multiple of 576.

$\therefore$ result is true for $n = k+1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k+1$.

But the result is true for $n = 1$.

$\therefore$ by the method of induction, the result is true for all $n \in N$.

Example 3. Use the principle of mathematicel induction to prove that

$$1^3 + 2^3 + 2^3 + \ldots\ldots\ldots + n^3 = \frac{n^2(n+1)^2}{4} \quad \forall\, n \in N.$$

Sol. We have to prove that

$$1^3 + 2^3 + 2^3 + \ldots\ldots\ldots + n^3 = \frac{n^2(n+1)^2}{4} \quad \ldots(1)$$

For $n = 1$,

L.H.S. $= 1^3 = 1$

R.H.S. $= \frac{1^2(1+1)^2}{4} = \frac{1 \times 4}{4} = 1$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ result (1) is true for $n = 1$.

Assume that result (1) is true for $n = k$

$$\therefore \quad 1^3 + 2^3 + 2^3 + \ldots\ldots + k^3 = \frac{k^2(k+1)^2}{4}$$

Adding $(k+1)^3$ to both sides of (2), we get

$$1^3 + 2^3 + 2^3 + \ldots\ldots + k^3 + (k+1)^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3$$

$$= (k+1)^2\left[\frac{k^2}{4} + (k+1)\right] = (k+1)^2\left[\frac{k^2 + 4k + 4}{4}\right]$$

$$\therefore \quad 1^3 + 2^3 + 2^3 + \ldots\ldots + k^3 + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4}$$

$\therefore$ result is true for $n = k + 1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k + 1$.

But the result is true for $n = 1$.

$\therefore$ by method of induction, the result is true for all $n \in \mathbf{N}$.

Example 4. By mathematical induction, prove that $1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \forall n \in \mathbf{N}$.

Sol. We are to prove that

$$1^2 + 2^2 + 3^2 + \ldots\ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \forall n \in \mathbf{N}.$$

For $n = 1$,

L.H.S. $= 1^2 = 1$

R.H.S. $= \frac{1(1+1)(2+1)}{6} = \frac{1 \times 2 \times 3}{6} = \frac{6}{6} = 1$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ result (1) is true for $n = 1$

Assume that result (1) is true for $n = k$

$$\therefore \quad 1^2 + 2^2 + 3^2 + \ldots\ldots + k^2 = \frac{k(k+1)(2k+1)}{6} \qquad \ldots(2$$

Adding $(k+1)^2$ to both sides of (2), we get

$$1^2 + 2^2 + 3^2 + \ldots\ldots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$$

$$= (k+1)\left[\frac{k(2k+1) + 6(k+1)}{6}\right] = \frac{(k+1)}{6}[k(2k+1) + 6(k+1)] = \frac{(k+1)}{6}[2k^2 + k + 6k + 6$$

$$= \frac{(k+1)}{6}[2k^2+7k+6] = \frac{(k+1)}{6}[2k^2+3k+4k+6] = \frac{(k+1)}{6}[k(2k+3)+2(2k+3)]$$

$$= \frac{(k+1)}{6}[(k+2)(2k+3)] = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$\therefore \quad 1^2+2^2+3^2+.....+k^2+(k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

$\therefore$ result is true for $n = k+1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k+1$.

But the result is true for $n = 1$.

$\therefore$ by method of induction, the result is true for all $n \in N$.

Note. We have added $(k+1)^2$ to both sides of (2). This is obtained by changing n to $k+1$ in the last term of L.H.S. of (1).

Example 5. Use the principle of mathematical induction to prove that

$$1\cdot3+2\cdot4+3\cdot5+.....+n(n+2) = \frac{n(n+1)(2n+7)}{6} \quad \forall n \in N.$$

Sol. We have to prove that

$$1\cdot3+2\cdot4+3\cdot5+.....+n(n+2) = \frac{n(n+1)(2n+7)}{6} \qquad ...(1)$$

For $n = 1$,

L.H.S. $= 1\cdot3 = 3$

R.H.S. $= \frac{1(1+1)(2+7)}{6} = \frac{1\times2\times9}{6} = 3$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ result (1) is true for $n = 1$.

Assume that result (1) is true for $n = k$.

$$\therefore \quad 1\cdot3+2\cdot4+3\cdot5+.....+k(k+2) = \frac{k(k+1)(2k+7)}{6} \qquad ...(2)$$

Adding $(k+1)(k+3)$ to both sides of (2), we get

$$1\cdot3+2\cdot4+3\cdot5+.....+k(k+2)+(k+1)(k+3)$$

$$= \frac{k(k+1)(2k+7)}{6} + (k+1)(k+3) = (k+1)\left[\frac{k(2k+7)}{6}+k+3\right]$$

$$= (k+1)\left[\frac{k(2k+7)+6k+18}{6}\right] = (k+1)\left[\frac{2k^2+13k+18}{6}\right] = (k+1)\left[\frac{(k+2)(2k+9)}{6}\right]$$

$$\therefore \quad 1\cdot3+2\cdot4+3\cdot5+.....+k(k+2)+(k+1)(k+3) = \frac{(k+1)(k+2)(2k+9)}{6}$$

$\therefore$ result is true for $n = k+1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k+1$.

But the result is true for $n = 1$.

$\therefore$ by method of induction, the result is true for all $n \in N$.

Example 6. Use the principle of mathematical induction to prove that

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\frac{1}{5\cdot7}+\ldots\ldots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1} \quad \forall n \in N.$$

Sol. We have to prove that

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\frac{1}{5\cdot7}+\ldots\ldots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1} \quad \ldots(1)$$

For $n = 1$,

$$\text{L.H.S.} = \frac{1}{1\cdot3} = \frac{1}{3}$$

$$\text{R.H.S.} = \frac{1}{2+1} = \frac{1}{3}$$

$\therefore$ L.H.S. = R.H.S.

$\therefore$ result (1) is true for $n = 1$.

Assume that result (1) is true for $n = k$.

$$\therefore \quad \frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\frac{1}{5\cdot7}+\ldots\ldots+\frac{1}{(2k-1)(2k+1)}=\frac{k}{2k+1} \quad \ldots(2)$$

Adding $\dfrac{1}{[2(k+1)-1][2(k+1)+1]}$ *i.e.* $\dfrac{1}{(2k+1)(2k+3)}$ to both sides of (2), we get

$$\frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\frac{1}{5\cdot7}+\ldots\ldots+\frac{1}{(2k-1)(2k+1)}+\frac{1}{(2k+1)(2k+3)}$$

$$=\frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)}=\frac{1}{2k+1}\left[\frac{k}{1}+\frac{1}{2k+3}\right]$$

$$=\frac{1}{2k+1}\left[\frac{2k^2+3k+1}{2k+3}\right]=\frac{1}{2k+1}\left[\frac{(k+1)(2k+1)}{2k+3}\right]$$

$$\therefore \quad \frac{1}{1\cdot3}+\frac{1}{3\cdot5}+\frac{1}{5\cdot7}+\ldots\ldots+\frac{1}{(2k+1)(2k+1)}+\frac{1}{(2k+1)(2k+3)}=\frac{k+1}{2k+3}$$

$\therefore$ result is true for $n = k+1$

$\therefore$ if the result is true for $n = k$, then it is also true for $n = k+1$.

But the result is true for $n = 1$.

$\therefore$ by method of induction, the result is true for all $n \in N$.

EXERCISE 1.10

1. Use the principle of mathematical induction to prove that
   (i) $2^{3n}-1$ is divisible by 7 $\forall n \in N$ (ii) $10^{2n-1}+1$ is divisible by 11 $\forall n \in N$
   (iii) $3^{2n+2}-8n-9$ is divisible by 64 $\forall n \in N$

2. Use the principle of mathematical induction to prove that
   (i) $3^{2n}-1$ is divisible by 8 $\forall n \in N$. (ii) $10^n+3\cdot 4^{n+2}+5$ is divisible by 9 $\forall n \in N$.
   (iii) $6^{n+2}+7^{2n+1}$ is divisible by 43 $\forall n \in N$.

3. Use the principle of mathematical induction to prove that
   $$x+4x+7x+\ldots\ldots+(3n-2)x=\frac{1}{2}n(3n-1)x \quad \forall n \in N.$$

4. By mathematical induction, prove that $1^2+3^2+5^2+\ldots\ldots+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$ $\forall n \in N$

5. Prove by induction that $1+\frac{1}{1+2}+\frac{1}{1+2+3}+\ldots\ldots+\frac{1}{1+2+3+\ldots\ldots+n}=\frac{2n}{n+1}$ $\forall n \in N$.

1.63. Division Algorithm

Statement. For any two integers a and b, with $a>0$, there exist unique integers q and r such that
$$b=aq+r,\ 0 \le r<|a|$$

Proof. When $b=0$

Taking $q=0,\ r=0$, we have
$$0=a(0)+0,\ 0=r<|a| \quad \text{or} \quad b=aq+r,\ 0 \le r<|a|$$
Hence the result.

When $b \neq 0$

Consider the infinite sequence of multiples of a *i.e.* $\ldots,-2a,-a,0,a,2a,\ldots$

Let aq be the greatest multiple of a such that
$$b \ge aq \quad \text{and} \quad b<(q+1)a$$
$\therefore \quad aq \le b<a(q+1) \Rightarrow 0 \le b-aq<a$

Put $b-aq=r$

$\therefore \quad 0 \le r<a$

$\therefore \quad b=aq+r,\ 0 \le r<|a|$ ...(1) $[\because a>0]$

Uniqueness

If possible, let there exist another set of integers q_1 and r_1 such that
$$b=aq_1+r_1,\ 0 \le r_1<|a| \qquad \ldots(2)$$

From (1) and (2), we get

$$aq + r = aq_1 + r_1$$

$\therefore \quad r - r_1 = a(q_1 - q)$

$\Rightarrow \quad a$ divides $r - r_1$

But $\quad |r - r_1| < a \qquad [\because \ 0 \le r < a, 0 \le r_1 <$

$\therefore \quad r - r_1 = 0 \Rightarrow r_1 = r$

$\therefore$ from (3), $a(q_1 - q) = 0 \Rightarrow q_1 - q = 0$ as $a \neq 0$

$\therefore \quad q_1 = q$

$\therefore$ for any two integers a and b, with $a > 0$, there exist unique integers q and r such that $b = aq + r, 0 \le r < |a|$.

Cor 1. If a and b are any integers, with $a \neq 0$, then there exist unique integers q and r such that

$$b = aq + r, 0 \le r < |a|$$

Proof. We have proved the result for $a > 0$

If $\quad a < 0$, then $|a| > 0$

$\therefore$ there exists unique integers q_2 and r such that

$$b = q_2|a| + r, \quad 0 \le r < |a| = q_2(-a) + r, \quad 0 \le r < |a|$$

$$= (-q_2)a + r, \quad 0 \le r < |a|$$

$$= qa + r, \ 0 \le r < |a| \text{ where } q = -q_2 \in Z,$$

$\therefore \qquad b = aq + r, \ 0 \le r < |a|$

Hence the result.

Cor. 2. If a and b are integers with $a \neq 0$, then there exists unique integers q and r such that

$$b = aq + r, \ -\frac{|a|}{2} \le r < \frac{|a|}{2}.$$

Proof : By Division algorithm, for any integers $a \neq 0$ and b, $\exists$ unique integers q_1, r_1 such that

$$b = aq_1 + r_1, \ 0 \le r_1 < |a|. \qquad ...(1$$

Now $\ 0 \le r_1 < |a| \Rightarrow 0 \le r_1 < \frac{|a|}{2}$ or $\frac{|a|}{2} \le r_1 < |a|$.

If $\quad 0 \le r_1 < \frac{|a|}{2}$, on taking $q_1 = q$, $r_1 = r$ in (1), we have

$$b = aq + r, \ 0 \le r < \frac{|a|}{2} \qquad ...(2$$

If $\frac{|a|}{2} \le r_1 < |a|$, then

$$\frac{|a|}{2} - |a| \le r_1 - |a| < |a| - |a|$$

$$-\frac{|a|}{2} \le r_1 - |a| < 0$$

$$-\frac{|a|}{2} \le r < 0 \qquad \text{where } r = r_1 - |a| \text{ or } r_1 = r + |a|.$$

$\therefore$ from (1), $b = aq_1 + r + |a|, \; -\frac{|a|}{2} \le r < 0$

$$= aq_1 + |a| + r$$

$$= a(q_1 \pm 1) + r \qquad [\because |a| = \pm a]$$

$$= aq + r \text{ (say)}, \; -\frac{|a|}{2} \le r < 0 \qquad \ldots(3)$$

Combining (2) and (3), we have

$$b = aq + r, \; -\frac{|a|}{2} \le r < \frac{|a|}{2}.$$

As q_1, r_1 are unique so q, r are also unique.

Hence the result.

Note : (*i*) In $b = aq + r, 0 \le r < |a|$

b, a, q, r are called **dividend, divisor, quotient, remainder** respectively.

(*ii*) The remainder is zero iff a divides b.

ILLUSTRATIVE EXAMPLES

Example 1. Prove that fourth power of any integer is either of the form $5k$ or $5k + 1$.

Sol. Let b be any integer, divide b by a

By division algorithm, we have

$$b = aq + r, \; 0 \le r < a, \text{ for } q, r \in Z$$

Put $a = 5$

$\therefore \quad b = 5q + r, \; 0 \le r < 5$

$\therefore \quad b = 5q, 5q + 1, 5q + 2, \; 5q + 3, 5q + 4$

$\therefore$ Every integer is of form $5q, 5q + 1, 5q + 2, 5q + 3, 5q + 4$

If $b = 5q$ then $b^4 = 625\, q^4 = 5(125\, q^4) = 5k; \; k = 125q^4 \in Z.$

If $b = 5q + 1$ then $b^4 = (5q+1)^4$

$= {}^4C_0 (5q)^4 + {}^4C_1 (5q)^3 + {}^4C_2 (5q)^2 + {}^4C_3 (5q) + {}^4C_4$

$= 5({}^4C_0 5^3 q^4 + {}^4C_1 5^2 q^3 + {}^4C_2 5q^2 + {}^4C_3 q) + 1$

$= 5k + 1$ (say), $k \in Z$.

If $b = 5q + 2$ then $b^4 = (5q+2)^4$

$= {}^4C_0 (5q)^4 + {}^4C_1 (5q)^3 (2)^1 + {}^4C_2 (5q)^2 (2)^2 + {}^4C_3 (5q) 2^3 + {}^4C_4 2^4$

$= 5({}^4C_0 5^3 q^4 + {}^4C_1 (25)(2q^3) + {}^4C_2 (20) q^2 + {}^4C_3\, 8q + 3) + 1 = 5k + 1$ (say), $k \in Z$.

If $b = 5q + 3$ then $b^4 = (5q+3)^4$

$= {}^4C_0 (5q)^4 + {}^4C_1 (5q)^3 (3) + {}^4C_2 (5q)^2 3^2 + {}^4C_3 (5q) 3^3 + {}^4C_4 3^4$

$= 5({}^4C_0 5^3 q^4 + {}^4C_1 5^2 q^3 (3) + {}^4C_2 5q^2 (9) + {}^4C_3\, q(27) + 16) + 1 = 5k + 1$ (say), $k \in Z$.

If $b = 5q + 4$ then $b^4 = (5q+4)^4$

$= {}^4C_0 (5q)^4 + {}^4C_1 (5q)^3 (4) + {}^4C_2 (5q)^2 4^2 + {}^4C_3 (5q) 4^3 + {}^4C_4 4^4$

$= 5({}^4C_0 5^3 q^4 + {}^4C_1 5^2 q^3 (4) + {}^4C_2 5q^2 (16) + {}^4C_3\, q(64) + 51) + 1 = 5k + 1$ (say), $k \in Z$.

Hence fourth power of any integer is either of the form $5k$ or $5k + 1$.

Example 2. Prove that if a and b are integers, with $b > 0$, then there exists unique integers q and r satisfying $a = bq + r$, where $2b \le r < 3b$.

Sol. Given a and b are integers with $b > 0$.

By division algorithm, we have

$a = bq' + r'$ where q' and r' are integers

and $0 \le r' < b$

$\Rightarrow$ $a = b(q' - 2 + 2) + r'$

$= b(q' - 2) + 2b + r' = bq + r$ where $q = q' - 2$ and $r = 2b + r'$ are integers

and q', r' are unique.

Also $0 \le r' < b$

$\Rightarrow$ $2b \le r' + 2b \le 3b \Rightarrow 2b \le r < 3b$

$\therefore$ there exists unique q and r such that

$a = bq + r$, where $2b \le r < 3b$.

Example 3. Show every integer is of form

(*i*) $3k - 1, 3k, 3k + 1$ (*ii*) $-4k - 2, 4k - 1, 4k, 4k + 1,$

(*iii*) $5k - 2, 5k - 1, 5k, 5k + 1, 5k + 2$

(*iv*) $6k - 3, 6k - 2, 6k - 1, 6k, 6k + 1, 6k + 2$, where $k \in Z$

Sol. Let b be any integer

We have $b = aq + r, -\frac{|a|}{2} \le r < \frac{|a|}{2}, r \in Z$ ...(I)

(i) Putting $a = 3$ and $q = k$ in (I), we have

$$b = 3k + r, -\frac{3}{2} \le r < \frac{3}{2}$$

$$b = 3k + r, \ r = -1, 0, 1$$

$\Rightarrow$ $b = 3k - 1, 3k, 3k + 1, k \in Z$

$\Rightarrow$

$\therefore$ every integer is of form $3k - 1, 3k, 3k + 1$.

(ii) Putting $a = 4$ and $q = k$ in (I), we have

$$b = 4k + r, -\frac{4}{2} \le r < \frac{4}{2}$$

$$b = 4k + r, \ r = -2, -1, 0, 1$$

$\Rightarrow$ $b = 4k - 2, 4k - 1, 4k, 4k + 1, k \in Z$

$\Rightarrow$

$\therefore$ every integer is of form $4k - 2, 4k - 1, 4k, 4k + 1$.

(iii) Putting $a = 5$ and $q = k$ in (I), we have

$$b = 5k + r, -\frac{5}{2} \le r < \frac{5}{2}$$

$$b = 5k + r, \ r = -2, -1, 0, 1, 2$$

$\Rightarrow$ $b = 5k - 2, 5k - 1, 5k, 5k + 1, 5k + 2, \ k \in Z$

$\therefore$ every integer is of form $5k - 2, 5k - 1, 5k, 5k + 1, 5k + 2$.

(iv) Putting $a = 6$ and $q = k$ in (I), we have

$$b = 6k + r, -\frac{6}{2} \le r < \frac{6}{2}$$

$$b = 6k + r, \ r = -3, -2, -1, 0, 1, 2$$

$\Rightarrow$ $b = 6k - 3, 6k - 2, 6k - 1, 6k, 6k + 1, 6k + 2, \ k \in Z$.

$\therefore$ every integer is of form $6k - 3, 6k - 2, 6k - 1, 6k, 6k + 1, 6k + 2$.

Example 4. If m is an integer not divisible by 2 or 3 show that $24 \mid m^2 + 23$.

Sol. Firstly, divide m by 6 and let q be quotient and r be remainder.

so that $m = 6q + r, \ 0 \le r < 6$

But $r \neq 0, 2, 3, 4$ [$\because$ m is not divisible by 2 or 3]

$\therefore$ $r = 1, 5$

so that $m = 6q + 1$ or $6q + 5$

When $m = 6q + 1$, Then

$$m^2 + 23 = (6q+1)^2 + 23$$

$$= 36q^2 + 12q + 1 + 23 = 36q^2 + 12q + 24 = 12(3q^2 + q + 2) = 12(q^2 + q + 2q^2 + 2)$$

$$= 12[q(q+1) + 2(q^2+1)] \quad \text{...(1)}$$

$\because$ $q, q+1$ are consecutive integers.

$\Rightarrow$ $q(q+1)$ is even integer $\Rightarrow$ $q(q+1) + 2(q^2+1)$ is also even integer

$\therefore$ $2 \mid q(q+1) + 2(q^2+1)$

$\Rightarrow$ $12.2 \mid 12(q(q+1) + 2(q^2+1)) \Rightarrow 24 \mid m^2 + 23$ [$\because$ of (1)]

When $m = 6q + 5$, Then

$$m^2 + 23 = (6q+5)^2 + 23$$

$$= 36q^2 + 60q + 25 + 23 = 36q^2 + 60q + 48$$

$$= 12(3q^2 + 5q + 4) = 12(q^2 + q + 2q^2 + 4q + 4)$$

$$= 12(q(q+1) + 2(q^2 + 2q + 2)) \quad \text{...(2)}$$

$\because$ $q, q+1$ are consecutive integers $\Rightarrow$ $q(q+1)$ is even integer

$\Rightarrow$ $q(q+1) + 2(q^2 + 2q + 2)$ is also even integer.

$\Rightarrow$ $2 \mid q(q+1) + 2(q^2 + 2q + 2) \Rightarrow 12.2 \mid 12(q(q+1) + 2(q^2 + 2q + 2))$

$\Rightarrow$ $24 \mid m^2 + 23$ [$\because$ of (2)]

Hence the result.

Example 5. Show that $\frac{n(n^2+2)}{3}$ is an integer for all $n \in N$.

Sol. By division algorithm, if n is divided by 3, then

$$n = 3q + r, \quad 0 \le r < 3, \quad q, r \in Z$$

$\Rightarrow$ $n = 3q + r, \quad r = 0, 1, 2 \Rightarrow n = 3q, \; 3q+1, 3q+2$

When $n = 3q$, Then $\frac{n(n^2+2)}{3} = \frac{3q(9q^2+2)}{3} = q(9q^2+2) =$ An integer [$\because$ $q \in Z$]

When $n = 3q + 1$, Then $\frac{n(n^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3}$

$$= \frac{(3q+1)(9q^2+6q+3)}{3} = \frac{(3q+1)3(3q^2+2q+1)}{3}$$

$$= (3q+1)(3q^2+2q+1)$$

= An integer [$\because$ $q \in Z$]

When $n = 3q+2$, Then $\frac{n(n^2+2)}{3} = \frac{(3q+2)((3q+2)^2+2)}{3}$

$$= \frac{(3q+2)(9q^2+12q+6)}{3} = \frac{(3q+2)3(3q^2+4q+2)}{3}$$

$$= (3q+2)(3q^2+4q+2)$$

= An integer $[\because q \in Z]$

Hence $\frac{n(n^2+2)}{3}$ is an integer for all $n \in N$.

EXERCISE 1.11

1. Show that every integer is of form :
   (i) $2q, 2q+1$ (ii) $3q, 3q+1, 3q+2$
   (iii) $4q, 4q+1, 4q+2, 4q+3$ (iv) $5q, 5q+1, 5q+2, 5q+3, 5q+4$
   (v) $6q, 6q+1, 6q+2, 6q+3, 6q+4, 6q+5$ where $q \in Z$
2. Show that b^2 leaves the remainder 0 or 1 when divided by 4 for any integer b.
3. Find remainder r, when 1059, 1417, 2312 are divided by $p > 1$.

ANSWERS

3. 164.

1.64. Common Divisor, Greatest Common Divisor

Common Divisor : If $c \mid a$ and $c \mid b$, then c is called a common divisor of a and b.

Note : As there is only a finite number of divisors of any non zero integer so there is only a finite number of common divisors of a and b except when $a = b = 0$. If atleast one of a and b is non zero, then the greatest among their common divisors is known as greatest common divisor of a and b.

Greatest Common Divisor : Let a and b be two integers such that atleast one of them is non zero. Then positive integer d is the **Greatest Common Divisor** of a and b if

(i) $d \mid a, d \mid b$ *i.e.* d is a common divisor of a and b.

(ii) $c \mid a, c \mid b \Rightarrow c \leq d$ for any positive integer c.

Notation : (i) The g.c.d. of a and b is denoted by g.c.d. (a, b) or simply (a, b).

(ii) (a, b) is defined for each pair of integers a and b except when $a = 0, b = 0$.

(iii) $(a, b) \geq 1$.

For example : To find g.c.d. of -12 and 48.

The positive divisors of -12 are 1, 2, 3, 4, 6, 12

The positive divisors of 48 are 1, 2, 3, 4, 6, 8, 12, 16, 24, 48

$\therefore$ the common divisors are 1, 2, 3, 4, 6, 12

so that g.c.d. of -12 and 48 is 12 *i.e.* $(-12, 48) = 12$.

1.65. If a and b are any two integers, not both zero, then prove that g.c.d of a and b exists and is unique.

Proof : Firstly, we shall prove that g.c.d. (a, b) exists.

W.l.o.g. assume that a and b both are positive and $b \geq a$

[$\because$ g.c.d. (a, b) is not affected by signs of a and

$\therefore$ by division algorithm

$$b = aq_1 + r_1 \text{ where } 0 \leq r_1 < a$$

If $r_1 = 0$ then $b = aq_1 \Rightarrow a \mid b$ and g.c.d. $(a, b) = a$

$\Rightarrow$ g.c.d. (a, b) exists.

If $r_1 \neq 0$, again by division algorithm

$$a = r_1 q_2 + r_2,\ 0 \leq r_2 < r_1$$

If $r_2 = 0$, then $a = r_1 q_2 \Rightarrow r_1 \mid a$

Putting value of a in (1), we have

$$b = (r_1 q_2) q_1 + r_1 = r_1 (q_2 q_1 + 1)$$

$\Rightarrow r_1 \mid b$

Thus $r_1 \mid a$ and $r_1 \mid b$

Take $p \mid a$ and $p \mid b$. Then $p \mid b - aq_1$

$\Rightarrow p \mid r_1$ [$\because$ of (

$\Rightarrow p \leq r_1$

Hence g.c.d. $(a, b) = r_1$ [$\because$ of (3) and (

so that g.c.d. (a, b) exists.

If $r_2 \neq 0$, we repeat the above process, which ends after n steps (say) and we get the remainder ze after nth step.

So, we get a sequence of integers r_j $(1 \leq j \leq n)$ such that

$$0 \leq r_n < r_{n-1} < \ldots\ldots < r_2 < r_1 < a$$

and $$r_{n-2} = r_{n-1} q_n + r_n \ ;\ n \geq 3$$

$$r_{n-1} = r_n q_{n+1}$$

$\therefore\ r_n \mid r_{n-1}, r_n \mid r_{n-2}, \ldots\ldots, r_n \mid a$ and $r_n \mid b$

Further, if p is a common divisor of a and b then

$p \mid b, p \mid a \Rightarrow p \mid b - aq_1 \Rightarrow p \mid r_1$ [$\because$ of (

$\Rightarrow p \mid r_2, \ldots\ldots, p \mid r_n$

so that g.c.d. $(a, b) = r_n$.

Hence g.c.d. (a, b) exists.

Secondly, we want to show g.c.d. (a, b) is unique.

If possible, let d_1 as well as d_2 be g.c.d. (a, b).

$\Rightarrow$ d_1 and d_2 are also common divisors of a and b.

$\Rightarrow$ $d_1 \geq d_2$ [$\because$ d_1 = g.c.d. (a, b) and d_2 is divisor of a, b]

and $d_2 \geq d_1$ [$\because$ d_2 = g.c.d. (a, b) and d_1 is divisor of a, b]

Hence $d_1 = d_2$

$\therefore$ g.c.d. (a, b) is unique.

1.66. If $d = (a, b)$ where a, b not both zero, then prove that $\exists$ integers x and y such that $d = ax + by$ and d is the least positive value of $xa + yb$.

Proof : Consider the set

$$A = \{ax + by \mid ax + by > 0 ;\ x, y \in I\}$$

As a, b are not both zero

W.l.o.g. let $a \neq 0 \Rightarrow |a| > 0$

and $|a| = a \cdot x + b \cdot 0$ where $x = \begin{cases} 1 & \text{if } a > 0 \\ -1 & \text{if } a < 0 \end{cases}$

$\Rightarrow$ $|a| \in A$

$\therefore$ $A \neq \phi$

$\therefore$ by well ordering principle, A has a least element say d.

Thus $d = ax + by$ for some integers x, y.

We claim d = g.c.d. $(a\ b)$

Divide a by d, so by division algorithm $\exists$ $q, r \in I$ such that

$a = qd + r,\ 0 \leq r < d$

$\Rightarrow$ $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$

$= ax_1 + by_1$ where $1 - qx = x_1,\ -qy = y_1$.

If $r > 0$ then $r \in S$ which is a contradiction to the choice of d.

$\therefore$ $r = 0$ so that $a = qd$

$\Rightarrow$ $d \mid a$

Similarly on dividing b by d, we get $d \mid b$

$\therefore$ d is a common divisor of a and b.

Consider c be any other positive common divisor of a and b

$\therefore$ $c \mid a$ and $c \mid b$

$\Rightarrow$ $c \mid ax + by \Rightarrow c \mid d \Rightarrow |c| \leq |d| \Rightarrow c \leq d$

Hence d = g.c.d. (a, b).

Now we will prove that d is the least positive value of $x\,a + y\,b$.

Let $m\,a + n\,b$ be any other member of the form $x\,a + y\,b$.

Since $(a, b) = d$

$\therefore$ $d \mid a$ and $d \mid b \Rightarrow d \mid (m\,a + n\,b) \Rightarrow d \leq (m\,a + n\,b)$

$\Rightarrow$ d is the least positive value of $x\,a + y\,b$.

Cor. 1. If a and b are two integers not both zero, then prove that a positive integer d = g.c.d.(a, b) iff (*i*) $d \mid a$, $d \mid b$ (*ii*) If $c \mid a$ and $c \mid b$ then $c \mid d$

Proof : Firstly, let d = g.c.d. $(a, b) \Rightarrow d \mid a$ and $d \mid b$.

And as $c \mid a$ and $c \mid b$ so that

$$a = p\,c \text{ and } b = q\,c \text{ where } p, q \in Z$$

Let $d = (a, b)$ so $\exists\ x, y \in Z$ such that

$$d = a\,x + b\,y = p\,c\,x + q\,c\,y$$

$$= c\,(p\,x + q\,y) = c\,r \text{ where } r = p\,x + q\,y \in Z$$

$\therefore$ $d = c\,r \Rightarrow c \mid d \Rightarrow c \mid (a, b)$.

Conversely : Let d be positive integer satisfying conditions (*i*) and (*ii*)

By condition (*ii*) if c is a common divisor of a and b, then

$c \mid d \Rightarrow c \leq d \Rightarrow d \geq c \Rightarrow d$ is g.c.d. of a and b.

Hence the result.

Cor. 2. If a and b are given integers, not both zero, then prove that the set $B = \{a\,x + b\,y \mid x, y \in Z\}$ consists of all multiplies of g.c.d. (a, b).

Proof : Let d = g.c.d. (a, b)

$\Rightarrow$ $d \mid a$ and $d \mid b \Rightarrow d \mid a\,x + b\,y$ for all $x, y \in Z$

$\Rightarrow$ d is a divisor of each element of B

i.e. Each element of B is a multiple of d ...(1)

As d is the smallest positive integer of the form $a\,x + b\,y$.

$\therefore$ $\exists$ integers x_1, y_1 such that $d = a\,x_1 + b\,y_1$

For any integer m,

$$m\,d = m\,(a\,x_1 + b\,y_1) = a\,(m\,x_1) + b\,(m\,y_1) = a\,x_2 + b\,y_2 \text{ (say)}$$

$\Rightarrow$ $m\,d \in B$ where $x_2, y_2 \in Z$

$\therefore$ each multiple of d is an element of B ...(2)

Combining (1) and (2), we see that the set B consists of all multiples of d.

Hence the result.

1.67. Other Definition of G.C.D.

Def. For integers a, b not both zero, the g.c.d.(a, b) is defined as the smallest positive integer of type $ax + by$; $x, y \in Z$.

Def. For integers a, b not both zero, the g.c.d.$(a, b) = d$ where d is positive integer satisfying

(i) $d \mid a,\ d \mid b$ (ii) If $c \mid a,\ c \mid b$ Then $c \mid d$.

Result : If $a \mid k$ and $b \mid k$. Then $(a, b) \mid k$

Proof : Let $d = (a, b) \Rightarrow d \mid a,\ d \mid b$

Given $a \mid k,\ b \mid k$

so that $d \mid k \Rightarrow (a, b) \mid k$.

Def. If $a_1, a_2, \ldots\ldots, a_m$ are m integers, not all zero, then g.c.d. of $a_1, a_2, \ldots\ldots, a_m$ is positive integer d satisfying

(i) $d \mid a_i$ for $1 \le i \le m$ (ii) If $c \mid a_i$ for $1 \le i \le m$, then $c \mid d$.

Note : G.C.D. of $a_1, a_2, \ldots\ldots, a_m$ is denoted as $d = (a_1, a_2, \ldots\ldots, a_m)$.

1.68. Prove that $(a, b) = (a, b + ax) = (a + by, b)\ \forall x, y \in Z$.

Proof : Let $(a, b) = d$ and $(a, b + ax) = d_1$

$\because$ $(a, b) = d \Rightarrow d \mid a$ and $d \mid b \Rightarrow d \mid ax$ and $d \mid b\ \forall x \in Z$

$\Rightarrow d \mid (b + ax) \Rightarrow d \mid a$ and $d \mid (b + ax)$

$\Rightarrow d \mid (a, b + ax)$

$\Rightarrow d \mid d_1$ ...(1)

And $(a, b + ax) = d_1$

$\Rightarrow d_1 \mid a$ and $d_1 \mid (b + ax) \Rightarrow d_1 \mid ax$ and $d_1 \mid (b + ax)$

$\Rightarrow d_1 \mid ((b + ax) - ax) \Rightarrow d_1 \mid b$

$\therefore d_1 \mid a$ and $d_1 \mid b \Rightarrow d_1 \mid (a, b)$

$\Rightarrow d_1 \mid d$ ...(2)

From (1) and (2), we get

$$d = d_1$$

or $$(a, b) = (a, b + ax)\ \forall x \in Z$$

Further to prove $(a, b) = (a + by, b)\ \forall y \in Z$

Let $(a + by, b) = d_2$

$\therefore$ $(a, b) = d \Rightarrow d \mid a$ and $d \mid b \Rightarrow d \mid a$ and $d \mid by\ \forall y \in Z$

$\Rightarrow d \mid a + by \Rightarrow d \mid a + by$ and $d \mid b \Rightarrow d \mid (a + by, b)$

$\Rightarrow d \mid d_2$ ...(3)

and $(a+by, b) = d_2$

$\Rightarrow$ $d_2 \mid a+by$ and $d_2 \mid b$ $\Rightarrow$ $d_2 \mid a+by$ and $d_2 \mid by$

$\Rightarrow$ $d_2 \mid a+by-by$ and $d_2 \mid a$

$\therefore$ $d_2 \mid a$ and $d_2 \mid b$ $\Rightarrow$ $d_2 \mid (a, b)$ $\Rightarrow$ $d_2 \mid d$ ...(4)

From (3) and (4), we get

$$d = d_2$$

$\Rightarrow$ $(a, b) = (a+by, b)\ \forall\ y \in Z.$

$\therefore$ $(a, b) = (a, b+ax) = (a+by, b)\ \forall x, y \in Z.$

1.69. For a, b any two integers, not both zero, prove that

$(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

Proof : Let $d = (a, b)$ and $d_1 = (-a, b)$

As $d = (a, b)$ $\Rightarrow$ $d \mid a$ and $d \mid b$

$\Rightarrow$ $d \mid -a$ and $d \mid b$

$\Rightarrow$ $d \mid (-a, b)$ $\Rightarrow$ $d \mid d_1$ ...(1)

Further, as $d_1 = (-a, b)$

$\Rightarrow$ $d_1 \mid -a$ and $d_1 \mid b$

$\Rightarrow$ $d_1 \mid a$ and $d_1 \mid b$

$\Rightarrow$ $d_1 \mid (a, b)$ $\Rightarrow$ $d_1 \mid d$ ...(2)

From (1) and (2), $d = d_1$ $\Rightarrow$ $(a, b) = (-a, b)$

Similarly $(a, b) = (a, -b)$.

Further to show $(a, b) = (-a, -b)$

Let $d = (a, b)$ and $d_2 = (-a, -b)$

As $d = (a, b)$ $\Rightarrow$ $d \mid a$ and $d \mid b$

$\Rightarrow$ $d \mid -a$ and $d \mid -b$

$\Rightarrow$ $d \mid (-a, -b)$

$\Rightarrow$ $d \mid d_2$ ...(3)

And as $d_2 = (-a, -b)$

$\Rightarrow$ $d_2 \mid -a$ and $d_2 \mid -b$

$\Rightarrow$ $d_2 \mid a$ and $d_2 \mid b$

$\Rightarrow$ $d_2 \mid (a, b)$ $\Rightarrow$ $d_2 \mid d$ ...(4)

From (3) and (4) $d = d_2$ $\Rightarrow$ $(a, b) = (-a, -b)$

Hence $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

70. For a, b any two integers, not both zero and m any positive integer, prove that

$$(m\,a, m\,b) = m(a, b)$$

Proof: Let $d = (a, b)$ and $d_1 = (m\,a, m\,b)$

We want to prove $d_1 = m\,d$.

As $d = (a, b)$

$\Rightarrow$ $d \mid a$ and $d \mid b$

$\Rightarrow$ $m\,d \mid m\,a$ and $m\,d \mid m\,b$

$\Rightarrow$ $m\,d \mid (m\,a,\ m\,b)$

$\Rightarrow$ $m\,d \mid d_1$ ...(1)

Further as $d = (a, b)$ so there exist integers x, y such that

$$d = a\,x + b\,y$$

$$m\,d = m\,(a\,x + b\,y)$$

$\Rightarrow$ $$m\,d = (m\,a)\,x + (m\,b)\,y$$ ...(2)

$\Rightarrow$ $$d_1 = (m\,a,\ m\,b)$$

Also $$d_1 \mid m\,a \text{ and } d_1 \mid m\,b$$

$\Rightarrow$ $$d_1 \mid (m\,a)\,x + (m\,b)\,y$$

$\Rightarrow$ $$d_1 \mid m\,d$$ ...(3)

[$\because$ of (2)]

From (1) and (3), we get

$$d_1 = m\,d$$

$\therefore$ $$(m\,a, m\,b) = m\,(a, b)$$

Hence the result.

Cor. 1. For any non zero integer m, prove that $(m\,a, m\,b) = |m|\,(a, b)$.

Proof: If $m > 0$, we have

$$(m\,a, m\,b) = m\,(a, b)$$

$\Rightarrow$ $$(m\,a, m\,b) = |m|\,(a, b)$$ [$\because$ $m > 0 \Rightarrow m = |m|$]

If $m < 0$, then $-m > 0$

$\therefore$ $$(m\,a, m\,b) = (-m\,a, -m\,b)$$

$$= -m\,(a, b)$$

$$= |m|\,(a, b)$$ [$\because$ $m < 0 \Rightarrow -m = |m|$]

$\therefore$ for $m \neq 0$, we have

$$(m\,a, m\,b) = |m|\,(a, b).$$

Cor. 2. If $d \mid a$, $d \mid b$ and $d > 0$. Prove $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$.

Further more if $d_1 = (a, b)$. Prove $\left(\frac{a}{d_1}, \frac{b}{d_1}\right) = 1$.

Proof : Since $(m\,a, m\,b) = m(a, b)$ for positive integer m.

$$\left[d\left(\frac{a}{d}\right), d\left(\frac{b}{d}\right)\right] = d\left(\frac{a}{d}, \frac{b}{d}\right)$$

$$\Rightarrow \quad (a, b) = d\left(\frac{a}{d}, \frac{b}{d}\right)$$

$$\Rightarrow \quad \left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) \qquad (1)$$

Hence the result.

Further given $d_1 = (a, b) \Rightarrow d_1 > 0$.

Putting $d = d_1$ in (1), we get

$$\left(\frac{a}{d_1}, \frac{b}{d_1}\right) = \frac{1}{d_1}(a, b) = \frac{1}{d_1}(d_1) = 1$$

$$\Rightarrow \quad \left(\frac{a}{d_1}, \frac{b}{d_1}\right) = 1.$$

Hence the result.

1.71. If a, b, c are any integers, no two of which are zero and $d = (a, b, c)$.

Prove $d = (a, b, c) = ((a, b), c) = (a, (b, c)) = ((a, c), b)$.

Proof : Let $d = (a, b, c)$ and $e = ((a, b), c)$

$\Rightarrow \quad d \mid a,\ d \mid b,\ d \mid c$

$\Rightarrow \quad d \mid (a, b)$ and $d \mid c$

$\Rightarrow \quad d \mid ((a, b), c) \Rightarrow d \mid e$

Further as $e \mid ((a, b), c)$

$\Rightarrow \quad e \mid (a, b)$ and $e \mid c$

$\Rightarrow \quad e \mid a,\ e \mid b$ and $e \mid c$

$\Rightarrow \quad e \mid (a, b, c) \Rightarrow e \mid d$

From (1) and (2) $d = e$

$\Rightarrow$ $(a, b, c) = ((a, b), c)$

Similarly $(a, b, c) = (a, (b, c)) = ((a, c), b)$

Hence the result.

ILLUSTRATIVE EXAMPLES

Example 1. If $a = b q + r$, then show that $(a, b) = (b, r)$.

Sol. Let $(a, b) = d_1$, $(b, r) = d_2$

$\because$ $(a, b) = d_1$

$\because$ $d_1 / a,\ d_1 / b \Rightarrow d_1 / (a - b q) \Rightarrow d_1 / r$

Now d_1 / b and d_1 / r

$\therefore$ d_1 is a common divisor of b and r

$\therefore$ d_1 / d_2 as d_2 is the g.c.d. of b and r.

Similarly d_2 / d_1

Now d_1 / d_2, d_2 / d_1 and d_1, d_2 are natural numbers.

$\therefore$ $d_1 = d_2$

$\Rightarrow$ $(a, b) = (b, r)$.

Note. If $(a, b) = 1$, then $(b, r) = 1$.

Example 2. $(a, m n) = 1$ if and only if $(a, m) = 1$ and $(a, n) = 1$.

Sol. (i) Assume that $(a, m) = 1$, $(a, n) = 1$

$\because$ $(a, m) = 1$

$\therefore$ there exist integers x and y such that

$$a x + m y = 1 \qquad \ldots(1)$$

$\because$ $(a, n) = 1$

$\therefore$ there exist integers z and t such that

$$a z + n t = 1$$

Or

$$a z + n t(1) = 1$$

$\therefore$

$$a z + n t(a x + m y) = 1 \qquad [\because \text{of } (1)]$$

$\Rightarrow$

$$a z + a n t x + n m t y = 1$$

$\Rightarrow$

$$a(z + n t x) + m n(t y) = 1$$

$\therefore$

$$a r + (m n) s = 1 \text{ where } r = z + n t x, s = t y$$

$$(a, m n) = 1$$

(*ii*) Assume that $(a, mn) = 1$

$\therefore$ there exist integers u and v such that

$$au + (mn)v = 1$$

$$\therefore \quad au + m(nv) = 1$$

$$\Rightarrow \quad (a, m) = 1$$

Similarly $(a, n) = 1$

Note. Let $(a, m) = 1$

$\therefore$ we have $(m, a) = 1, (m, a) = 1$

$\Rightarrow$ $(m, a^2) = 1 \Rightarrow (a^2, m) = 1$

Now $(m, a^2) = 1, (m, a) = 1$

$\Rightarrow$ $(m, a^3) = 1$

and so on.

Proceeding in this way, we get

$$(m, a^r) = 1 \quad \text{or} \quad (a^r, m) = 1$$

$\therefore$ if $(a, m) = 1$, then

$$(a^2, m) = 1, (a^3, m) = 1, \ldots\ldots, (a^r, m) = 1.$$

Example 3. If a / b, c / d and $(b, d) = 1$, then prove that $(a, c) = 1$.

Sol. Since a / b, c / d.

$\therefore$ there exist integers m, n such that

$$b = am, \; d = cn \qquad \ldots(1)$$

$\because$ $(b, d) = 1$

$\therefore$ there exist integers x and y such that

$$bx + dy = 1$$

$\therefore$ $amx + cny = 1$ [$\because$ of (1)]

$\Rightarrow$ $a(mx) + c(ny) = 1$

$\Rightarrow$ $(a, c) = 1$

Example 4. If $(a, b) = 1$ and $c \mid (a + b)$, then prove that $(c, a) = (c, b) = 1$.

Sol. Let $(c, a) = d$

$\Rightarrow$ $d \mid c$ and $d \mid a$

Given $c \mid a + b$

$\therefore$ $d \mid a + b$ and $d \mid a$

$\Rightarrow$ $d \mid a + b - a \Rightarrow d \mid b$

$d \mid a$ and $d \mid b$

$\therefore$ $d \mid (a, b) \Rightarrow d \mid 1 \Rightarrow d = \pm 1$

so that

But d is positive so that $d = 1 \Rightarrow (c, a) = 1$.

Further let $(c, b) = e$

$e \mid c$ and $e \mid b$

$\Rightarrow$ $c \mid a + b$

Given $e \mid a + b$ and $e \mid b$

$\therefore$ $e \mid a + b - b \Rightarrow e \mid a$

$\Rightarrow$ $e \mid (a, b) \Rightarrow e \mid 1 \Rightarrow e = \pm 1$

so that

But e is positive

so that $e = 1 \Rightarrow (c, b) = 1$.

$\therefore$ $(c, a) = (c, b) = 1$.

Hence the result.

Example 5. If $(c, a) = 1$, then prove that $(a, bc) = (a, b)$.

Sol. Let $(a, b) = d$ and $(a, bc) = e$

$\therefore$ $d \mid a$, $d \mid b$ and $e \mid a$, $e \mid bc \Rightarrow d \mid a$, $d \mid bc$

$\Rightarrow$ $d \mid (a, bc)$ ...(1)

$\Rightarrow$ $d \mid e$

$\because$ $e \mid a$ and $(c, a) = 1$

$\therefore$ $(e, c) = 1$.

$\therefore$ $e \mid bc \Rightarrow e \mid b$ ...(2)

$\therefore$ $e \mid a$ and $e \mid b \Rightarrow e \mid (a, b) \Rightarrow e \mid d$

From (1) and (2), we get $e = d$

$\Rightarrow$ $(a, bc) = (a, b)$

Hence the result.

Example 6. Prove that there are infinitely many pairs x, y satisfying

$x + y = 100$ and $(x, y) = 5$.

Sol. Given $x + y = 100$ ...(1)

Let $x = 5p$ where p is odd integer such that $(p, 5) = 1$.

From (1), $y = 100 - x = 100 - 5p = 5(20 - p)$.

We claim $(x, y) = 5$

Let $(x, y) = d \Rightarrow d \geq 5$ [$\because$ $5 \mid x$ and $5 \mid y$]

If possible, suppose $d > 5$

Now $(x, y) = d \Rightarrow d \mid x,\ d \mid y$

$\Rightarrow d \mid x + y$

$\Rightarrow d \mid 100$

$\Rightarrow d = 10, 20, 25, 50, 100.$

As $d \mid x$ and x is odd

$\Rightarrow$ d must be odd

$\therefore$ $d = 25$

$\therefore$ $d \mid x \Rightarrow 25 \mid 5p$

$\Rightarrow 5 \mid p$

which is impossible as $(p, 5) = 1$

$\therefore$ our supposition is wrong so that $d = 5 \Rightarrow (x, y) = 5$.

As there are infinitely many p such that $(p, 5) = 1$

$\therefore$ there are infinitely many x and so infinitely many pairs x, y satisfying $x + y = 100$ and $(x, y) = 5$.

Example 7. For any integers a, b, c, prove that $(a, bc) = (a, (a, b)c)$.

Sol. Let $(a, bc) = d$ and $(a, (a, b)c) = e$

$\therefore$ $d \mid a$ and $d \mid bc \Rightarrow d \mid ac$ and $d \mid bc$

$\Rightarrow d \mid (ac, bc) \Rightarrow d \mid (a, b)c$

$\therefore$ $d \mid a$ and $d \mid (a, b)c \Rightarrow d \mid (a, (a, b)c)$

$\Rightarrow d \mid e$ ...(1)

As $(a, (a, b)c) = e$

$\Rightarrow e \mid a,\ e \mid (a, b)c \Rightarrow e \mid a,\ e \mid (ac, bc) \Rightarrow e \mid a,\ e \mid bc$

$\Rightarrow e \mid (a, bc) \Rightarrow e \mid d$ ...(2)

From (1) and (2), $d = e \Rightarrow (a, bc) = (a, (a, b)c)$.

Example 8. Prove for any integer m, $30 \mid (m^5 - m)$.

Sol. Here $m^5 - m = m(m^4 - 1)$

$= m(m^2 - 1)(m^2 + 1)$

$= (m^3 - m)(m^2 + 1)$.

As $6 \mid (m^3 - m)$ [$\because$ $m^3 - m = (m - 1)m(m + 1)$ and $m - 1, m, m + 1$ are three consecutive integers and their product is divisible by $\lfloor 3 \rfloor$]

$\Rightarrow 6 \mid (m^3 - m)(m^2 + 1) \Rightarrow 6 \mid (m^5 - m)$ ...(1)

Also $m^5 - m = (m^3 - m)(m^2 + 1) = (m^3 - m)(m^2 - 4 + 5)$

$= (m^3 - m)(m^2 - 4) + 5(m^3 - m) = m(m^2 - 1)(m^2 - 4) + 5(m^3 - m)$

$= (m-2)(m-1)m(m+1)(m+2) + 5(m^3 - m)$ ...(2)

As $m-2, m-1, m, m+1, m+2$ are 5 consecutive integer so that

$\therefore \quad 5 \mid (m-2)(m-1)m(m+1)(m+2)$

$5 \mid 5(m^3 - m)$

Also

$\Rightarrow \quad 5 \mid (m-2)(m-1)m(m+1)(m+2) + 5(m^3 - m)$

[$\because$ of (2)]

$\Rightarrow \quad 5 \mid m^5 - m$ ...(3)

From (1) and (3), we get

$6 \times 5 \mid m^5 - m$ as $(6, 5) = 1$ [$\because a \mid n, b \mid n \Rightarrow ab \mid n$ where $(a, b) = 1$]

$\Rightarrow \quad 30 \mid (m^5 - m)$.

Hence the result.

Example 9. If $(a, b) = 1$, prove that $(a^2, ab, b^2) = 1$.

Sol. $(a, b) = 1 \Rightarrow (a^2, ab) = a$

$\therefore \quad (a^2, ab, b^2) = (a, b^2)$ [$\because (a^2, ab) = a$]

$= 1$ [$\because (a, b) = 1 \Rightarrow (a, b^2) = 1$]

Example 10. For any integer p, show that

(*i*) $(2p+1, 9p+4) = 1$ (*ii*) $(5p+2, 7p+3) = 1$ (*iii*) $(3p, 3p+2) = 1$ for odd p.

Sol. (*i*) Let $(2p+1, 9p+4) = d$

$\therefore \quad d \mid 2p+1$ and $d \mid 9p+4$

$\Rightarrow \quad d \mid 2(9p+4) - 9(2p+1)$

$\Rightarrow \quad d \mid 8 - 9$

$\Rightarrow \quad d \mid -1$

$\Rightarrow \quad d = \pm 1$

But d is positive

$\therefore \quad d = 1$.

$\Rightarrow \quad (2p+1, 9p+4) = 1$.

(*ii*) Let $(5p+2, 7p+3) = d$

$\therefore$ $d \mid 5p+2$ and $d \mid 7p+3$

$\Rightarrow$ $d \mid 5(7p+3) - 7(5p+2)$

$\Rightarrow$ $d \mid 1 \Rightarrow d = \pm 1$

But d is positive

$\therefore$ $d = 1 \Rightarrow (5p+2, 7p+3) = 1.$

(*iii*) Given p be odd so let $p = 2k+1,\ k \in I$

$\therefore$ $3p = 3(2k+1) + 1 = 6k+4$

and $3p+2 = 3(2k+1) + 2 = 6k+5$

Let $(3p, 3p+2) = d$

i.e. $(6k+4, 6k+5) = d$

$\Rightarrow$ $d \mid 6k+4$ and $d \mid 6k+5$

$\Rightarrow$ $d \mid (6k+5) - (6k+4)$

$\Rightarrow$ $d \mid 1 \Rightarrow d = \pm 1$

But d is positive.

$\therefore$ $d = 1 \Rightarrow (3p, 3p+2) = 1.$

EXERCISE 1.12

1. If $(a, b) = 1$ and c / a, then $(c, b) = 1$.
2. If a and b are relatively prime, then any common divisor of $a\,c$ and b is a divisor of c.
3. If $(a, b) = 1$, then $(a\,c, b) = (c, b)$
4. If $(a, c) = d$, a / b and c / b, then show that $a\,c / b\,d$.
5. Show that $(a, b) = (a + b, b)$.
6. If $(a, b) = 1$, then $(a, b + k\,a) = 1$.
7. If $(a, m) = 1$, then $(m - a, m) = 1$.
8. If $(a, 4) = 2$ and $(b, 4) = 2$, then prove that $(a + b, 4) = 4$.
9. If $a > 1$ and n is positive integer such that $b \mid (a^n - 1)$, then prove that $(a, b) = 1$.
10. Prove that there are no pair of integers x, y satisfying $x + y = 100$ and $(x, y) = 3$.
11. Prove that $(a^2, b^2) = (a, b)^2$.
12. If x and y are prime to 3, then prove that $x^2 + y^2$ can not be a perfect square.
13. Let d and g be two positive integers. Prove that there are integers x and y satisfying $x + y = g$ and $(x, y) = d$ iff $d \mid g$.
14. Let d and p be two positive integers. Prove that there are integers x and y satisfying $x\,y = p$ and $(x, y) = d$ iff $d^2 \mid p$.

15. For all positive integers p and q where p is odd, show that $(2^p - 1, 2^q + 1) = 1$.

16. If $(a, b) = 1$, then prove that
    (i) $(a+b,\ a-b) = 1$ or 2
    (ii) $(a+b,\ ab) = 1$
    (iii) $(a+b,\ a^2+b^2) = 1$ or 2
    (iv) $(2a+b,\ a+2b) = 1$ or 3
    (v) $(a+b,\ a^2-ab+b^2) = 1$ or 3

17. If $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

18. If $c \mid a,\ c \mid b,\ \left(\frac{a}{c}, \frac{b}{c}\right) = 1$, then $(a, b) = c$.

19. Prove that every two consecutive integers are coprime.

20. Prove that one of any three consecutive integers is divisible by 3.

21. Let $\frac{a}{b}$ and $\frac{c}{d}$ be fractions such that $(a, b) = (c, d) = 1$. Prove if $\frac{a}{b} + \frac{c}{d}$ is an integer, then $|b| = |d|$.

22. If $a_1, a_2, \ldots, a_m$ are integers which are relatively prime in pairs, then prove that $(a_1, a_2, \ldots, a_m) = 1$. Is converse true ?

23. Prove
    (i) If g.c.d. (a, b) = g.c.d. $(a, c) = 1$, then g.c.d. $(a, bc) = 1$.
    (ii) If g.c.d. $(a, b) = 1$ and $c \mid a$ then g.c.d. $(b, c) = 1$.
    (iii) If g.c.d. $(a, b) = 1$, then g.c.d. (ac, b) = g.c.d. (c, b).
    (iv) If g.c.d. $(a, b) = 1$, $d \mid ac$ and $d \mid bc$ then $d \mid c$.

24. If a and b are non zero integers, prove that g.c.d. $(2a - 3b, 4a - 5b)$ divides b and hence g.c.d. $(2a+3, 4a+5) = 1$.

ANSWERS

22. Not true.

1.72. Euclidean Algorithm

For any two positive integers a and b, on applying the division algorithm repeatedly to obtain a set of remainders $r_1, r_2, \ldots, r_n$ defined successively by the following relations :

$$\left.\begin{array}{ll} b = aq_1 + r_1, & 0 \le r_1 < a \\ a = r_1 q_2 + r_2, & 0 \le r_2 < r_1 \\ r_1 = r_2 q_3 + r_3, & 0 \le r_3 < r_2 \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 \le r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} & \end{array}\right] \quad \ldots(1)$$

Then, show r_n, the last non zero remainder in the above process is g.c.d. of a and b.

Proof : We have for any integers x, y

$$(a, b) = (a, b + a x) = (a + b y, b)$$

Using equations (1)

$$(a, b) = (a, b - a q_1)$$

$$= (a, r_1) = (a - r_1 q_2, r_1)$$

$$= (r_2, r_1) = (r_2, r_1 - r_2 q_3) = (r_2, r_3)$$

Continuing like this, we get

$$(a, b) = (r_2, r_1) = (r_1, r_2) = (r_2, r_3)$$

.....

.....

$$= (r_{n-1}, r_n)$$

$$= (r_n, 0) = r_n$$

$\therefore$ r_n, the last non zero remainder is g.c.d. of a, b.

Cor. 1. Express G.C.D. of a and b as a linear combination of a and b.

Proof : From Euclidean Algorithm, we have

$$b = a q_1 + r_1 \qquad 0 \le r_1 < a$$

$$a = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$$

....

....

$$r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} \qquad 0 \le r_{n-2} < r_{n-3}$$

$$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} \qquad 0 \le r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1} q_n + r_n \qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1}$$

Rewrite above equations as

$$r_n = r_{n-2} - r_{n-1} q_n$$

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$$

$$r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$$

....

....

$$r_3 = r_1 - r_2 q_3$$

$$r_2 = a - r_1 q_2$$

$$r_1 = b - a q_1$$

Now
$$(a, b) = r_n = r_{n-2} - r_{n-1} q_n$$

$$= r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n$$

$$= (1 + q_{n-1} q_n) r_{n-2} + (-q_n) r_{n-3} \quad ...(1)$$

$$= (1 + q_{n-1} q_n)(r_{n-4} - r_{n-3} q_{n-2}) + (-q_n) r_{n-3}$$

$$= (1 + q_{n-1} q_n) r_{n-4} + (-q_n - q_{n-2} - q_{n-2} q_{n-1} q_n) r_{n-3} \quad ...(2)$$

$\therefore$ equation (1) gives r_n as linear combination of r_{n-2} and r_{n-3}

Equation (2)gives r_n as linear combination of r_{n-3} and r_{n-4}

Continuing like this, we go on eliminating the remainders $r_{n-1}, r_{n-2}, r_{n-3}, \ldots\ldots r_3, r_2, r_1$ until r_n is expressed as a linear combination of a and b.

1.73. Common Multiple, Least Common Multiple

Common Multiple. If a and b are non zero integers such that $a \mid n, b \mid n$. Then n is called a common multiple of a and b.

Least Common Multiple. Let a and b be non zero integers. Then a positive integer l is the least common multiple (L.C.M.) of a and b if

(i) $a \mid l,\ b \mid l$ *i.e.* l is a common multiple of a and b.

(ii) $a \mid n,\ b \mid n \Rightarrow l \leq n$ for any positive integer n.

Notation : The L.C.M. of a and b is denoted by L.C.M. (a, b) or $[a, b]$.

Important Results :

1. If $a \mid n,\ b \mid n$, then $[a, b] \mid n$.
2. Prove $[k a,\ k b\} = k\,[a, b]$ for positive integer k.
3. Let a, b be two positive integers.

   Prove that (g.c.d. (a, b)) (l.c.m. $[a, b]$) $= a b$.

   Or

   $(a, b)\,[a, b] = a b$.

1.74. If $a b = c^n$ and $(a, b) = 1$, then each of a and b is an exact nth power.

Proof. We are given that

$$a b = c^n \quad ...(1)$$

and
$$(a, b) = 1$$

Let $(a, c) = \alpha$

$\therefore$ we can take

$$a = \alpha\beta, c = \alpha\gamma \quad \ldots(2)$$

where $(\beta, \gamma) = 1$

$\therefore$ from (1), we get

$$\alpha\beta b = \alpha^n\gamma^n$$

$$\therefore \quad \beta b = \alpha^{n-1}\gamma^n \quad \ldots(3)$$

$\because$ $(\beta, \gamma) = 1$

$\therefore$ $(\beta, \gamma^n) = 1$

$\therefore$ from (3), γ^n / b $[\because \gamma^n / \beta b$ and $(\gamma^n, \beta) = 1]$

$\therefore$ we take $b = \gamma^n\delta$ $\ldots(4)$

From (3) and (4), we get,

$$\beta\gamma^n\delta = \alpha^{n-1}\gamma^n$$

$$\Rightarrow \quad \beta\delta = \alpha^{n-1} \quad \ldots(5)$$

$\because$ $(a, b) = 1$ and α / a, δ / b

$\therefore$ $(\alpha, \delta) = 1 \Rightarrow (\alpha^{n-1}, \delta) = 1$

$\therefore$ from (5), α^{n-1} / β

$\therefore$ we can take $\beta = \alpha^{n-1}\lambda$ $\ldots(6)$

From (5) and (6), we get,

$$\alpha^{n-1}\lambda\delta = \alpha^{n-1}$$

$$\Rightarrow \quad \lambda\delta = 1 \Rightarrow \lambda = 1, \delta = 1$$

$\therefore$ from (6), $\beta = \alpha^{n-1}$ as $\lambda = 1$

From (2), $a = \alpha\beta = \alpha \cdot \alpha^{n-1} = \alpha^n$

From (4), $b = \gamma^n$ as $\delta = 1$

$\therefore$ each of a and b is an exact nth power.

1.75. Explain the method of finding g.c.d. of three numbers a, b, c.

Proof. Let $(a, b) = d$ $\ldots(1)$

and $(d, c) = D$ $\ldots(2)$

We shall prove that $(a, b, c) = D$.

$\because$ $(d, c) = D$

$\therefore$ D / d and D / c

$\therefore$ D / d and $(a, b) = d$

$\therefore$ D / d and $d / a,\ d / b$

$\therefore$ $D / a,\ D / b$

$\therefore$ we have $D / a, D / b, D / c$

$\therefore$ D is a common divisor of a, b, c.

$\therefore$ Let D' be any other common divisor of a, b, c.

$\therefore$ $D' / a, D' / b \Rightarrow D' / (a, b) \Rightarrow D' / d$

Now $D' / d, D' / c \Rightarrow D' / (d, c) \Rightarrow D' / D$

$\therefore$ $(a, b, c) = D$

$\Rightarrow$ D is g.c.d. of a, b, c.

1.76. Prove that $(m a, m b, m c) = m(a, b, c)$.

Proof. Let $(a, b) = d$ and $(d, c) = D$

$\therefore$ $(a, b, c) = D$ ...(1)

Also $(m a, m b) = m d$

and $(m d, m c) = mD$

$\therefore$ $(m a, m b, m c) = mD$ ...(2)

From (1) and (2), we get

$(m a, m b, m c) = m(a, b, c)$

Cor. If $m / a, m / b, m / c$, then $\left(\frac{a}{m}, \frac{b}{m}, \frac{c}{m}\right) = \frac{(a, b, c)}{m}$

Proof is quite simple.

ILLUSTRATIVE EXAMPLES

Example 1. Find g.c.d. of 24 and 138 and express it as linear combination of these numbers.

Sol. Here $138 = 24(5) + 18$

$24 = 18(1) + 6$

$18 = 6(3) + 0$

$\therefore$ $6 =$ g.c.d. $(24, 138)$

And $6 = 24 - 18$

$= 24 - (138 - 24(5))$

$= 6 \times 24 - 138 = 6 \times 24 + (-1) \times 138$

$= 24x + 138y$ where $x = 6,\ y = -1$.

$$
\begin{array}{r}
5 \\
24 \overline{)\ 138} \\
120 \\
\hline
18 \overline{)\ 24\ (1} \\
18 \\
\hline
6 \overline{)\ 18\ (3} \\
18 \\
\hline
\times
\end{array}
$$

Example 2. Find integers x and y so that $12378x + 3054y = 6$.

Sol. Firstly show g.c.d. $(12378, 3054) = 6$.

Here $12378 = 3054(4) + 162$

$3054 = 162(18) + 138$

$162 = 138(1) + 24$

$138 = 24(5) + 18$

$24 = 18(1) + 6$

$18 = 6(3) + 0$

$\Rightarrow$ g.c.d. $(12378, 3054) = 6$

and $6 = 24 - 18$

$= 24 - (138 - 24(5))$

$= 6(24) - 138$

$= 6(162 - 138) - 138$

$= -7 \times 138 + 6 \times 162$

$= -7 \times (3054 - 162 \times 18) + 6 \times 162$

$= 132 \times 162 - 7 \times 3054$

$= 132(12378 - (3054)4) - 7 \times 3054$

$= -535 \times 3054 + 132 \times 12378$

$= 12378x + 3054y$ where $x = 132$ and $y = -535$

$\Rightarrow$ $12378x + 3054y = 6$ for $x = 132$ and $y = -535$.

4
3054) 12378
12216
162) 3054 (18
162
1434
1296
138) 162 (1
138
24) 138 (5
120
18) 24 (1
18
6) 18 (3
18
×

Example 3. Use the Euclidean Algorithm to find integers x and y such that

g.c.d. $(1769, 2378) = 1769x + 2378y$

Sol. Here $2378 = 1769(1) + 609$

$1769 = 609(2) + 551$

$609 = 551(1) + 58$

$551 = 58(9) + 29$

$58 = 29(2) + 0$

$\therefore$ g.c.d. $(1769, 2378) = 29$

and $29 = 551 - 58(9)$

$= 551 - (609 - 551)(9)$

$= 10 \times 551 - 609 \times 9$

$= 10 \times (1769 - 609 \times 2) - 609 \times 9$

$= 10 \times 1769 - 29 \times 609$

$= 10 \times 1769 - 29(2378 - 1769)$

$= 39 \times 1769 - 29 \times 2378$

$= 1769x + 2378y$ where $x = 39, y = -29$.

1
1769) 2378
1769
609) 1769 (2
1218
551) 609 (1
551
58) 551 (9
522
29) 58 (2
58
×

Example 4. Find x, y such that $71x - 50y = 1$.

Sol. Firstly, we shall prove $(71, -50) = 1$.

Here
$$71 = 50(1) + 21$$
$$50 = 21(2) + 8$$
$$21 = 8(2) + 5$$
$$8 = 5(1) + 3$$
$$5 = 3(1) + 2$$
$$3 = 2(1) + 1$$
$$2 = 1(2) + 0$$

$\therefore$ g.c.d. $(71, 50) = 1$

$\Rightarrow$ g.c.d. $(71, -50) = 1$ $[\because (a, b) = (a, -b)]$

Now
$$1 = 3 - 2 = 3 - (5 - 3) = 2 \times 3 - 5$$
$$= 2 \times (8 - 5) - 5 = -3 \times 5 + 2 \times 8$$
$$= -3 \times (21 - 8(2)) + 2 \times 8$$
$$= -3 \times 21 + 8 \times 8 = -3 \times 21 + 8 \times (50 - 21(2))$$
$$= 8 \times 50 - 19 \times 21 = 8 \times 50 - 19 \times (71 - 50)$$
$$= -19 \times 71 + 27 \times 50 = 71(-19) - 50(-27)$$
$$= 71x - 50y \text{ where } x = -19, y = -27.$$

$\therefore$ $71x - 50y = 1$ for $x = -19, y = -27$.

Example 5. Evaluate g.c.d. $(198, 288, 512)$ and express it as a linear combination of x, y, z (integers).

Sol. Here g.c.d. $= (198, 288, 512) =$ g.c.d. (g.c.d.$(198, 288), 512)$

Here
$$288 = 198(1) + 90$$
$$198 = 90(2) + 18$$
$$90 = 18(5) + 0$$

$\therefore$ $(198, 288) = 18$.
$$= 198 - 90(2)$$
$$= 198 - (288 - 198)(2)$$
$$= 3(198) - 2(288) \quad \ldots(1)$$

Now g.c.d. $(198, 288, 512) =$ g.c.d. $(18, 512)$

Here
$$512 = 18(28) + 8$$
$$18 = 8(2) + 2$$
$$8 = 2(4) + 0$$

$\therefore$ g.c.d. $(18, 512) = 2$.

Hence g.c.d. $(198, 288, 512) = 2$.

$\therefore$
$$2 = 18 - 8(2)$$
$$= 18 - (512 - 18(28))2$$

$$= 18 \times 57 - 2 \times 512$$

$$= (3\,(198) - 2(288))\,57 - 2 \times 512$$

$$= -2 \times 512 - 114 \times 288 + 171 \times 198$$

$$= 512\,(-2) + 288\,(-114) + 198\,(171)$$

$$= 512\,x + 288\,y + 198\,z \text{ where } x = -2, y = -114 \text{ and } z = 171$$

g.c.d. $= 2 = 512\,x + 288\,y + 198\,z.$

Example 6. Evaluate l.c.m. [306, 657].

Sol. Firstly find g.c.d. (657, 306)

By Euclidean algorithm

$$657 = 306\,(2) + 45$$

$$306 = 45\,(6) + 36$$

$$45 = 36\,(1) + 9$$

$$36 = 9\,(4) + 0$$

$\therefore$ g.c.d. (657, 306) = 9.

Now using $(a, b)\,[a, b] = a\,b$

we have $$[a, b] = \frac{a\,b}{(a, b)}$$

$\Rightarrow$ $$[306, 657] = \frac{306 \times 657}{9} = 34 \times 657 = 22338.$$

EXERCISE 1.13

1. Find the g.c.d. of 595 and 252 and express d in the form $252\,m + 595\,n$.
2. Find the g.c.d. of 726 and 275 and express it in the form $726\,x + 276\,y$.
3. Find the g.c.d. of 858 and 325, and express it in the form $858\,x + 325\,y$.
4. Find the g.c.d. of 1109 and 4999, and express it in the form $1109\,x + 4999\,y$.
5. Find the g.c.d. of 826 and 1890, and express it in the form $826\,x + 1890\,y$.
6. Find x, y (integers) satisfying

   (*i*) $6409\,x + 42823\,y = 17$ (*ii*) $256\,x + 1166\,y = 2$ (*iii*) $119\,x + 272\,y = 17$

   (*iv*) $68\,x + 710\,y = 2$ (*v*) $657\,x + 963\,y = 9$
7. Find x, y such that $3587\,x + 1819\,y = 17$.
8. If $a = 780$, $b = 728$ and $c = 585$, find (a, b, c).
9. Evaluate g.c.d. (228, 342, 420) and find x, y, z (integers) so that

   g.c.d. $(228, 342, 420) = 228\,x + 342\,y + 420\,z$
10. Find l.c.m. [1819, 3587].

ANSWERS

1. $7, 7 = 252m + 595m$ 2. $11, 11 = 726x + 275y$ 3. $13, 13 = 858x + 325y$
4. $1, 1 = 1109x + 4999y$ 5. $14, 14 = 826x + 1890y$
6. (i) $x = 147, y = -22$ (ii) $x = 41, y = -9$ (iii) $x = 7, y = -3$
   (iv) $x = 94, y = -9$ (v) $x = 22, y = -15$
7. $x = -36, y = 71$ 8. $(a, b, c) = 13$. 9. $x = 11, y = -11, z = 3$ 10. 383809

1.17. Prime Number

Any positive integer greater than 1 is called a prime number if it has no proper divisor.

Or

Any positive integer > 1 is called prime number if it has only two divisors 1 and itself

2, 3, 5, 7, 11, 13, 17, 19, ... are prime numbers.

Composite Number. Any positive integer greater than 1, which is not prime, is called a composite number.

4, 6, 8, 9, 10, ... are composite numbers.

Now we can divide natural numbers into three classes :

(i) Unity

(ii) Prime Numbers

(iii) Composite Numbers

Note 1. 1 is neither prime nor composite.

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

Note 3. Any number, which is not prime, is not necessarily composite.

Two prime numbers are called **twin-primes** if there is only one composite number between them.

e.g., for any odd integer p ; p and $p + 2$ are **Twin Primes.**

e.g., 3, 5 ; 5, 7 ; 11, 13 ; 17, 19 are twin primes.

1.18. Prove that the least divisor (other than 1) of a composite number is a prime.

Proof : Let us take n be any given composite number.

$\therefore$ there is atleast one divisor of n other than 1 so n has a least divisor q such that $1 < q < n$.

If q is a composite number, then it has atleast one divisor q other than 1 and q so that $1 < q_1 < q$.

Now $q_1 \mid q$ and $q \mid n \Rightarrow q_1 \mid n$ which is a contradiction to the fact that q is the least divisor of n.

$\therefore$ q is not a composite number *i.e.* q is prime.

Note : Thus each integer > 1 has a prime factor.

1.79. If p is any prime and m any integer, then prove that either $(p, m) = 1$ or $p \mid m$.

Proof : Let us take g.c.d. $(p, m) = d \Rightarrow d \mid p$ and $d \mid m$

Now $d \mid p \Rightarrow d = 1$ or p ($\because p$ is p

If $d = 1$, then g.c.d. $(p, m) = 1$

If $d = p$, then $d \mid m \Rightarrow p \mid m$

Hence either g.c.d. $(p, m) = 1$ or $p \mid m$.

1.80. If p is a prime and $p \mid a\,b$, then prove that $p \mid a$ or $p \mid b$.

Proof : Given that $p \mid a\,b$

$\Rightarrow$ $p \mid a$, then theorem is proved.

If $p \nmid a$ then g.c.d. $(p, a) = 1$

$\therefore$ $p\,x + a\,y = 1$ for some integers x, y.

Multiplying both sides by b, we get

$$b\,p\,x + b\,a\,y = b$$

Given $p \mid a\,b \Rightarrow p \mid a\,b\,y$

Also $p \mid p \Rightarrow p \mid b\,p\,x$

$\therefore$ $p \mid (b\,p\,x + a\,b\,y) \Rightarrow p \mid b$ [$\because$ o

Hence either $p \mid a$ or $p \mid b$.

Cor. 1. If $p \mid a_1 a_2 \ldots\ldots a_n$ then prove $p \mid a_t$ for some t, $1 \le t \le n$ *i.e.* p divides atleast one factor a_t

Proof : We shall prove this result by induction on n.

Step 1. If $n = 1$, then $p \mid a_1$ and there is nothing to prove.

If $n = 2$, then $p \mid a_1 a_2 \Rightarrow p \mid a_1$ or $p \mid a_2$

$\therefore$ result is true for $n = 1, 2$

Step 2. Suppose result is true for $n = k$

i.e. $p \mid a_1 a_2 \ldots\ldots a_k \Rightarrow p \mid a_t$ for some t, $1 \le t \le k$.

Step 3. Suppose $p \mid a_1 a_2 \ldots\ldots a_k\, a_{k+1}$

$\Rightarrow$ $p \mid b\, a_{k+1}$ where $b = a_1 a_2 \ldots\ldots a_k \Rightarrow p \mid b$ or $p \mid a_{k+1}$

$\Rightarrow$ $p \mid a_1 a_2 \ldots\ldots a_k$ or $p \mid a_{k+1}$

$\Rightarrow$ $p \mid a_t$ or $p \mid a_{k+1}$ for some t, $1 \le t \le k$ ($\because$ of st

$\Rightarrow$ $p \mid a_t$ for some t, $1 \le t \le k+1$

$\therefore$ result is true for $n = k + 1$

Hence by mathematical induction, result is true for all n.

Remark : The above **result holds only if** p is prime *e.g.* $6 \mid 12$ *i.e.* $6 \mid 2^2 \times 3$. But $6 \nmid 3$ and $6 \nmid 4$.

Cor. 2. Given $p, p_1, p_2 \ldots\ldots p_n$ are all prime numbers and $p \mid p_1 p_2 \ldots\ldots p_n$ then prove that p for some t, $1 \le t \le n$.

Proof : Given $p \mid p_1 p_2 \ldots\ldots\ldots p_n$

Then by cor 1, $p \mid p_t$ for some t, $1 \le t \le n$

As p_t is prime so its only divisors are 1, p_t

But $p > 1$ so that $p = p_t$

Hence proved.

1.81. Euclid's Theorem

Prove that number of primes is infinite

i.e. there is no end to the sequence of primes 2, 3, 5, 7, 11, 13, 17, ...

Proof. If possible, suppose that number of primes is finite. Let p be the greatest prime.

Consider an integer N defined as

$$N = (2 \times 3 \times 5 \times \ldots\ldots \times p) + 1$$

If N is prime, then $N > p$.

If N is composite, then it has atleast one prime factor. But none of primes from 2 to p divides N.

$\therefore$ N has at least one prime factor greater than p.

$\therefore$ in both the cases, $\exists$ a prime which is greater than p, which is impossible.

$\therefore$ our supposition is wrong.

$\therefore$ number of primes is infinite.

Note 1. The above theorem can be set as "Out side any given set of primes, there is another one".

Note 2. The product of two numbers of the form $4n + 1$ is again of the same form.

$$(4n+1)(4n'+1) = 16nn' + 4n + 4n' + 1$$
$$= 4[4nn' + n + n'] + 1$$
$$= 4k + 1, \text{ where } k = 4nn' + n + n'$$

Note 3. Any number of type $4k - 1$ is of type $4k + 3$

$$p = 4k - 1 = 4k - 4 + 4 - 1 = (4k - 4) + 4 - 1$$
$$= 4(k - 1) + 3$$
$$= 4k' + 3$$

1.82. Prove that primes of the form $4k + 3$ are infinite.

Proof. If possible, suppose that number of primes of the form $4k + 3$ is finite.

Let p be the greatest prime of this type.

Consider a number N defined as

$$N = 2^2(3 \times 5 \times 7 \times \ldots\ldots\ldots \times p) - 1$$

Clearly N is of the type $4k - 1$ and hence of $4k + 3$ type.

If N is a prime number, then certainly $N > p$ and N is of type $4k + 3$.

If N is composite, then it has a prime factor of $4k + 3$ type.

[$\because$ product of two numbers of the form $4k + 1$ is again of the same f

But none of the primes 2, 3, 5, ..., p divides N.

$\therefore$ this prime divisor of N is greater than p.

$\therefore$ in both the cases, we have got a prime which is of form $4k + 3$ and is greater than p, whic impossible.

$\therefore$ our supposition is wrong.

$\therefore$ number of primes of the form $4k + 3$ is infinite.

Cor. Prove that number of primes of the form $4k - 1$ are infinite.

Proof. Primes of the form $4k - 1$ are of the form $4k + 3$.

1.83. Prove that primes of the form $6k + 5$ are infinite.

Proof. If possible, suppose that, primes of the form $6k + 5$ are finite, and let p be the greatest prime of type.

Let $N = 2 \times 3 \times 5 \times \ldots\ldots\ldots \times p - 1$

Clearly N is of $6k - 1$ type and hence of $6k + 5$ type.

If N is prime, then certainly N is of type $6k + 5$ and $> p$.

If N is composite, then it has at least one prime factor of $6k + 5$ type.

But none of the primes 2, 3, 5, ..., p divides N.

$\therefore$ N has got a prime factor of $6k + 5$ type and which is $> p$.

$\therefore$ in both the cases, there is a prime of $6k + 5$ type and $> p$, which is impossible.

$\therefore$ our supposition is wrong.

$\therefore$ number of primes of the type $6k + 5$ is infinite.

Cor. Primes of the form $6k - 1$ are infinite.

Proof. Primes of the form $6k - 1$ are clearly of the form $6k + 5$.

Note 1. If a and b have no common divisor > 1, then every odd prime factor of $a^2 + b^2$ is of $4n + 1$ type

Example. Take $a = 5, b = 12$

$\therefore$ a and b have no common factor > 1

$$a^2 + b^2 = 25 + 144 = 169 = 13 \times 13 = (4k' + 1)(4k' + 1)$$
$$= 4n + 1$$

Note 2. Prove that square of every odd +ve number is of $8k + 1$ type.

Proof. Let n be any odd + ve integer.

$\therefore$ $n = 2\lambda + 1$

$\Rightarrow$ $n^2 = 4\lambda^2 + 4\lambda + 1 = 4\lambda(\lambda + 1) \times 1$

Now either λ is even or $\lambda+1$ is even

$\therefore$ $\lambda(\lambda+1)$ is even

Let $\lambda(\lambda+1)=2k$

$\therefore$ $n^2=4(2k)+1=8k+1$.

184. Prove that there are infinitely many prime numbers of the form $8k+1$.

Proof: Let, if possible, set of primes of the form $8k+1$, $k\in Z$ be finite.

Let p be the largest possible prime of the form $8k+1$, $k\in Z$. Consider N be any integer

$$N=2^3\cdot3^2\cdot5^2\cdot7^2\cdot11^2\cdot13^2\ldots\ldots p^2+1$$

Since square of every odd integer is of the form $8k+1$ and product of integers of the form $8k+1$ is again an integer of the form $8k+1$.

$\therefore$ $3^2\cdot5^2\cdot7^2\cdot11^2\cdot13^2\ldots\ldots p^2$ is of the form $8k+1$ and let it be k'.

$\Rightarrow$ $2^3(3^2\cdot5^2\cdot7^2\cdot11^2\cdot13^2\ldots\ldots p^2)$ is of the form $8k'$.

$\Rightarrow$ N is of the form $8k'+1$

Now either N is a composite number or N is a prime number.

If N is a composite number, then clearly none of the odd primes 3, 5, 7, 11, 13, ... p divides N. Also as N is an odd number, not divisible by 2.

$\Rightarrow$ N has odd prime factor $>p$ of the form $8k+1$.

Further if N is a prime number, again we get a prime number $>p$.

$\therefore$ in both the cases, we get a contradiction *i.e.* our supposition is wrong.

Hence the set of primes of the form $8k+1$, $k\in Z$ is not finite.

$\therefore$ there are infinite many primes of the form $8k+1$.

185. Prove that primes of the form $8k+5$ are infinite.

Proof. If possible, suppose that number of primes of type $8k+5$ is finite and let p be the greatest prime of this type.

Consider $N=3^2\cdot5^2\cdot7^2\ldots\ldots p^2+2^2$

$\because$ square of every odd number is of $8k+1$ type.

$\therefore$ each of $3^2, 5^2, 7^2, \ldots\ldots, p^2$ is of $8k+1$ type.

$\therefore$ $3^2\cdot5^2\cdot7^2\ldots\ldots p^2$ is of type $8k+1$

$\therefore$ $3^2\cdot5^2\cdot7^2\ldots\ldots p^2+2^2$ is of type $8k+5$.

If N is prime, then clearly $N > p$ and N is of type $8k + 5$.

If N is composite, then N has at least one prime factor of type $4k + 1$

[Take $a = 3 \cdot 5 \cdot 7 \ldots\ldots p$, $b = 2$

$\therefore \quad (a, b) = 1$

Also $N = a^2 + b^2$

$\therefore$ N has atleast one prime factor of $4k + 1$ type.]

$\therefore$ N has at least prime factor of $8k + 1$ or $8k + 1$ type.

[$\because$ every number of type $4k + 1$ is of type $8k + 1$ or $8k + 5$ as k is even or

But the product of any number of primes of $8k + 1$ type is again of the same type.

Since N is of $8k + 5$ type.

$\therefore$ N has atleast one prime factor of $8k + 5$ type and it is $> p$ as none of primes 3, 5, 7, ... divides N.

$\therefore$ in both the cases, there is a prime of $8k + 5$ type which is $> p$, which is impossible.

$\therefore$ our supposition is wrong.

$\therefore$ number of primes of type $8k + 5$ is infinite.

Cor. Prove that the number of primes of the form $8k - 3$ is infinite.

Proof. The primes of the form $8k - 3$ are primes of the form $8k + 5$.

1.86. Fundamental Theorem of Arithmetic

Or

Unique Factorisation Theorem

Statement : Every integer $n > 1$ can be expressed as product of primes and factorisation is u apart from the order in which the factors occur.

Proof. Let $n > 1$ be any positive integer.

If n is prime, then the result is proved.

If n is composite, it has divisors between 1 and n.

Let p_1 be its smallest factor > 1.

Then p_1 is certainly prime.

[$\because$ otherwise if p_1 is composite, then $\exists\ l$ such that $1 < l < p_1$ and $l \mid p_1$

$\because$ $p_1 \mid n$, $\therefore l \mid n$, which contradicts the definition of p_1.

$\therefore$ p_1 is not composite.]

$\therefore \quad n = p_1 n_1$

where $1 < n_1 < n$

Again if n_1 is prime, theorem is complete.

If n_1 is composite, let p_2 be its smallest proper divisor. Then as above, p_2 is prime.

...(2)

Let $n_1 = p_2 n_2$

where $1 < n_2 < n_1$

From (1) and (2), $n = p_1 p_2 n_2$, where $1 < n_2 < n_1 < n$

If n_2 is prime, theorem is complete.

If n_2 is composite, proceed as above.

Repeating this argument, we get a sequence of decreasing numbers

$n, n_1, n_2, \ldots\ldots, n_{k-1}$ (say), all > 1.

Ultimately, we shall have to accept that n_{k-1} is prime $= p_k$ (say)

$\therefore$ $n = p_1 p_2 p_3 \ldots\ldots p_{k-1} p_k$, where p_i's are primes not necessarily distinct.

$\therefore$ every positive integer > 1 is the product of primes.

If we arrange the above primes in the increasing order and associate set of equal primes into single factor, then we can represent n as $p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$, where α's and p's are distinct.

Uniqueness

Let n be any positive integer > 1.

If possible, let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_s^{\beta_s}$

where α's > 0, β's > 0 and

p's are primes in the increasing order,

q's are primes in the increasing order.

$\because$ p_1 divides $p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_p}$

$\therefore$ p_1 divides $q_1^{\beta_1} q_2^{\beta_2} \ldots\ldots q_s^{\beta_s}$

$\therefore$ p_1 is one of q's.

Similarly $p_2, p_3, \ldots\ldots, p_k$ are present in q's.

Similarly $q_1, q_2, \ldots\ldots, q_s$ are present in p's.

$\therefore$ p's and q's are the same primes, though not necessarily in same order and $k = s$

$\therefore$ $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k} = p_1^{\gamma_1} p_2^{\gamma_2} \ldots\ldots p_k^{\gamma_k}$

$$\therefore \quad \frac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}}{p_1^{\gamma_1} p_2^{\gamma_2} \ldots\ldots p_k^{\gamma_k}} = 1$$

$$\Rightarrow \quad p_1^{\alpha_1-\gamma_1} p_2^{\alpha_2-\gamma_2} \ldots\ldots p_k^{\alpha_k-\gamma_k} = 1$$

$$\Rightarrow \quad \alpha_1 - \gamma_1 = 0,\ \alpha_2 - \gamma_2 = 0, \ldots\ldots, \alpha_k - \gamma_k = 0$$

$$\Rightarrow \quad \alpha_1 = \gamma_1, \alpha_2 = \gamma_2, \ldots\ldots, \alpha_k = \gamma_k$$

$\therefore$ every natural number > 1 is represented as product of primes in just one way.

Example : (*i*) $720 = 8 \times 90 = 16 \times 45 = 16 \times 9 \times 5 = 2^4 \times 3^2 \times 5$

(*ii*) $5040 = 16 \times 315 = 16 \times 9 \times 35 = 2^4 \times 3^2 \times 5 \times 7$

(*iii*) $10395 = 9 \times 1155 = 9 \times 3 \times 385 = 3^3 \times 5 \times 77 = 3^3 \times 5 \times 7 \times 11$

(*iv*) $40425 = 3 \times 13475 = 3 \times 25 \times 539 = 3 \times 25 \times 49 \times 11 = 3 \times 5^2 \times 7^2 \times 11$

Another statement.

Every positive integer is normal.

ILLUSTRATIVE EXAMPLES

Example 1. Show that every prime except 2 and 3 is of the form $6m + 1$ or $6m + 5$; $m \in Z$.

Sol. We know any integer can be put in the form $6m$, $6m + 1$, $6m + 2$, $6m + 3$, $6m + 4$, $6m + 5$.

For $m = 0$, $6m + 2 = 2$ and $6m + 3 = 3$.

Also $6m$, $6m + 2 = 2(3m + 1)$, $6m + 3 = 3(2m + 1)$, $6m + 4 = 2(3m + 2)$ are composite numb for each non zero integer.

$\therefore$ every prime except 2 and 3 is of the form $6m + 1$ or $6m + 5$.

Example 2. Show that any prime of the form $3k + 1$ is of the form $6k + 1$.

Sol. We know any integer can be put in the form $6m$, $6m + 1$, $6m + 2$, $6m + 3$, $6m + 4$, $6m + 5$.

And $6 \mid 6m$, $2 \mid 6m + 2$, $3 \mid 6m + 3$, $2 \mid 6m + 4$

$\Rightarrow$ $6m$, $6m + 2$, $6m + 3$, $6m + 4$ are all composite so prime is of the form $6m + 1$ or $6m + 5$.

If possible, suppose $p = 3k + 1 = 6m + 5$

$\therefore$ $3k - 6m = 4 \Rightarrow 3(k - 2m) = 4$

Now $3 \mid$ L.H.S. but $3 \nmid 4 =$ R.H.S.

$\therefore$ (1) is absurd.

Thus a prime $p = 3k + 1$ must of the form $6m + 1$ or $6k + 1$.

Example 3. Show that for each prime $p \geq 5$, p^2+2 is a composite number.

Sol. As p is prime so it is of form $3m+1$ or $3m+2$ for some integer m.

($\because$ every integer is of form $3m$, $3m+1$ or $3m+2$. But $3m$ is a composite number)

If $p = 3m+1$, then $p^2+2 = (3m+1)^2+2$

$= 9m^2+6m+1+2 = 9m^2+6m+3$

$= 3(3m^2+2m+1)$

$\Rightarrow$ p^2+2 is a composite number.

If $p = 3m+2$, then $p^2+2 = (3m+2)^2+2$

$= 9m^2+12m+4+2$

$= 3(3m^2+4m+2)$

$\Rightarrow$ p^2+2 is a composite number.

Hence p^2+2 is a composite number for all $p \geq 5$, prime.

Note: For $p=2$, $p^2+2 = 4+2 = 6$ is composite but for $p=3$, $p^2+2 = 9+2 = 11$ is prime.

Example 4. If p, q are primes such that $p-q=2$

show that p^p+q^q is divisible by $p+q$

i.e. p^p+q^q is a composite number. ...(1)

Sol. Given p, q are primes such that $p-q=2$ ...(2)

Now $p^p+q^q = (p^p-1)+(q^q+1)$

Here $p^p-1 = p^p-1^p = (p-1)(p^{p-1}+p^{p-2}+\ldots\ldots+p+1)$

$= (p-1)(2l+1)$ (say)

($\because$ $p^{p-1}+p^{p-2}+\ldots\ldots+p$ is even for prime p)

and $q^q+1 = q^q+1^q = (q+1)(q^{q-1}-q^{q-2}+q^{q-3}\ldots\ldots-q+1)$

$= (q+1)(2m+1)$ ($\because$ $q^{q-1}-q^{q-2}+\ldots\ldots-q$ is even)

$\therefore$ from (2), $p^p+q^q = (p-1)(2l+1)+(q+1)(2m+1)$

$= (q+1)(2l+1)+(q+1)(2m+1) = (q+1)(2l+1+2m+1)$ [$\because$ of (1)]

$= 2(q+1)(l+m+1) = (2q+2)(l+m+1)$

$= (2q+p-q)(l+m+1)$ [$\because$ of (1)]

$= (p+q)(l+m+1)$

$\Rightarrow$ p^p+q^q is divisible by $p+q$

i.e. p^p+q^q is a composite number.

Example 5. For any prime $p > 3$, prove $p^2 - 1$ is divisible by 24.

Sol. Any integer is of the form $6l, 6l+1, 6l+2, 6l+3, 6l+4, 6l+5$

out of which $6l, 6l+2, 6l+3, 6l+4$ are composite

$(\because 6|6l,\ 2|6l+2,\ 3|6l+3, 2|6l+$

$\therefore$ any prime $p > 3$ is of form $6l+1$ or $6l+5$

If $p = 6l+1$, then $p^2 - 1 = (6l+1)^2 - 1 = 36l^2 + 12l$

$= 12l(3l+1)$

If $p = 6l+5$, then $p^2 - 1 = (6l+5)^2 - 1 = 36l^2 + 60l + 25 - 1 = 36l^2 + 60l + 24$

$= 12(3l^2 + 5l + 2) = 12(3l+2)(l+1)$

If l is even, then $l = 2m$

$\therefore \quad p^2 - 1 = 12(2m)(6m+1) = 24m(6m+1)$

or

$p^2 - 1 = 12(6m+2)(2m+1) = 24(3m+1)(2m+1)$

$\Rightarrow \quad p^2 - 1$ is divisible by 24.

If l is odd, then $l = 2m+1$

$\therefore \quad p^2 - 1 = 12(2m+1)(3(2m+1)+1) = 12(2m+1)(6m+4)$

$= 24(2m+1)(3m+2)$

or

$p^2 - 1 = 12(6m+3+2)(2m+1+1) = 12(6m+5)(2m+2)$

$= 24(6m+5)(m+1)$

$\Rightarrow \quad p^2 - 1$ is divisible by 24.

Hence the result.

Example 6 If p is prime, then prove that

(*i*) $p|a$ and $p|a^2 + b^2 \Rightarrow p|b$ (*ii*) $p|a^7 \Rightarrow p|a$

(*iii*) $p|a^2 + b^2,\ p|b^2 + c^2 \Rightarrow p|a^2 - c^2$

Sol. (*i*) Given p is prime and $p|a$

Then $p|a^2$

Also given $p|a^2 + b^2$

$\Rightarrow \quad p \mid a^2 + b^2 - a^2 \Rightarrow p|b^2$

$\Rightarrow \quad p|b$ $(\because p$ is prir

(ii) Given p is prime and $p \mid a^7$

$\Rightarrow$ $p \mid a.a.a.a.a.a.a$

Then p must divide at least one of the factors and here each factor is a

$\therefore$ $p \mid a$

(iii) Given p is prime and $p \mid a^2+b^2$, $p \mid b^2+c^2$

$\Rightarrow$ $p \mid (a^2+b^2)-(b^2+c^2)$

$\Rightarrow$ $p \mid a^2-c^2$

Example 7. (a) If 2^n-1 is a prime number, show that n is prime.

(b) If $n>1$, a positive integer and a^n-1 is prime show $a=2$.

Sol. (a) If possible, suppose that n is not a prime

$\therefore$ let $n=pq$, where $1<p, q<n$

Now $2^n-1 = 2^{pq}-1$

$= (2^p)^q-1 = a^q-1$ where $a=2^p$

We claim $a-1 \mid a^q-1$

Since $a^q-1 = (a-1)(a^{q-1}+a^{q-2}+\ldots\ldots+1)$

$\Rightarrow$ $a-1 \mid a^q-1$ $(\because a^q-1=2^n-1)$

$\Rightarrow$ $2^p-1 \mid 2^n-1$

which contradicts that 2^n-1 is a prime

$\therefore$ our supposition is wrong.

Hence n must be a prime.

(b) If $a=1$ then $a^n-1=1-1=0$, not a prime number so that $a \neq 1$

$\therefore$ $a \geq 2$

If possible suppose that, $a>2 \Rightarrow a-1>1$

for $n>1$, $a<a^n$

$\Rightarrow$ $a-1<a^n-1$

And $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\ldots\ldots+1)$

$\Rightarrow$ $a-1$ divides a^n-1 where $1<a-1<a^n-1$

$\Rightarrow$ a^n-1 is composite, contrary to given

so $a=2$. Hence proved.

EXERCISE 1.14

1. If p, q are twin primes, prove that $p+q$ is divisible by 12 if $p > 3$, odd.
2. For any integer $n > 1$, prove $n^4 + 4^n$ is composite.
3. For any integer $n > 1$, show that $n^4 + 4$ is a composite number.
4. For any integer $n \geq 1$, show that $8^n + 1$ is a composite number.
5. If p and q are twin primes, show that $pq + 1$ is a perfect square.
6. For any integer $n > 1$, show that $n^4 + n^2 + 1$ is a composite number.
7. (*i*) Show that only prime of the form $n^3 - 1$ is 7.

   (*ii*) Show that only prime of the form $n^2 - 4$ is 5.
8. If p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.
9. Prove each integer $n > 11$ can be written as a sum of two composite numbers.
10. If $2^n + 1$ is an odd prime, show n is equal to a power of 2.

MODULE-2

MODULE-2

1

PERMUTATIONS AND COMBINATIONS

1.1. Factorial Notations

The product of all the positive integers from 1 to n is called *factorial* n and is denoted by the symbol $\lfloor n$ or $n!$. For example,

$$\lfloor 6 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$$

and $$1 \cdot 2 \cdot 3 \cdot 4 \ldots 20 = \lfloor 20$$

An Important result

$$\lfloor n = n(n-1)(n-2)(n-3) \ldots 3 \cdot 2 \cdot 1 = n[(n-1)(n-2)(n-3) \ldots\ldots 3 \cdot 2 \cdot 1] = n \lfloor n-1$$

$$= n(n-1) \lfloor n-2 = n(n-1)(n-2) \lfloor n-3$$

.....

Also $n \lfloor n-1 = n(n-1)(n-2) \ldots\ldots 3 \cdot 2 \cdot 1$

$\therefore \quad n \lfloor n-1 = \lfloor n$

Similarly $(n+2)(n+1) \lfloor n = \lfloor n+2$

Note 1. Since $\lfloor n = n \lfloor n-1$

Put $n = 1$

$\therefore \quad \lfloor 1 = 1 \lfloor 0$

$\therefore \quad 1 = (1)(\lfloor 0) \quad \Rightarrow \quad \lfloor 0 = 1$

We will also prove at a later stage that $\lfloor 0 = 1$

Note 2. Factorial of proper fraction and negative integer is not defined.

ILLUSTRATIVE EXAMPLES

Example 1. Compute (*i*) $\dfrac{\lfloor 7}{\lfloor 5}$ (*ii*) $\dfrac{\lfloor 12}{\lfloor 10 \lfloor 2}$

Sol. (*i*) $\dfrac{\lfloor 7}{\lfloor 5} = \dfrac{7 \times 6 \times \lfloor 5}{\lfloor 5} = 42$

(*ii*) $\dfrac{\lfloor 12}{\lfloor 10 \lfloor 2} = \dfrac{12 \times 11 \times \lfloor 10}{\lfloor 10 \times (2 \times 1)} = 66$

Example 2. Evaluate $\frac{\lfloor n}{\lfloor r \lfloor n-r}$, when

(*i*) $n=6, r=2$, (*ii*) $n=7, r=4$ (*iii*) $n=15, r=12$

Sol. (*i*) When $n=6, r=2$

$$\frac{\lfloor n}{\lfloor r \lfloor n-r} = \frac{\lfloor 6}{\lfloor 2 \lfloor 6-2} = \frac{\lfloor 6}{\lfloor 2 \lfloor 4} = \frac{6\times 5\times \lfloor 4}{(2\times 1)\lfloor 4} = 15$$

(*ii*) When $n=7, r=4$

$$\frac{\lfloor n}{\lfloor r \lfloor n-r} = \frac{\lfloor 7}{\lfloor 4 \lfloor 7-4} = \frac{\lfloor 7}{\lfloor 4 \lfloor 3} = \frac{7\times 6\times 5\times \lfloor 4}{\lfloor 4\times(3\times 2\times 1)} = 35$$

(*iii*) When $n=15, r=12$

$$\frac{\lfloor n}{\lfloor r \lfloor n-r} = \frac{\lfloor 15}{\lfloor 12 \lfloor 15-12} = \frac{\lfloor 15}{\lfloor 12 \lfloor 3} = \frac{15\times 14\times 13\times \lfloor 12}{\lfloor 12\times(3\times 2\times 1)} = 455$$

Example 3. If $\frac{1}{\lfloor 6} + \frac{1}{\lfloor 7} = \frac{x}{\lfloor 8}$, find x.

Sol. $$\frac{1}{\lfloor 6} + \frac{1}{\lfloor 7} = \frac{x}{\lfloor 8}$$

$$\Rightarrow \quad \frac{1}{\lfloor 6} + \frac{1}{7\times \lfloor 6} = \frac{x}{8\times 7\times \lfloor 6} \Rightarrow 1 + \frac{1}{7} = \frac{x}{56} \Rightarrow \frac{8}{7} = \frac{x}{56}$$

$$\therefore \quad x = \frac{8}{7}\times 56 = 64$$

Example 4. If $\lfloor n+2 = 2550 \lfloor n$, find n.

Sol. $\lfloor n+2 = 2250 \lfloor n \Rightarrow (n+2)(n+1)\lfloor n = 2550 \lfloor n$

$\Rightarrow (n+2)(n+1) = 2550 \Rightarrow n^2 + 3n - 2548 = 0$

$$\Rightarrow \quad n = \frac{-3\pm\sqrt{9+10192}}{2} = \frac{-3\pm\sqrt{10201}}{2} = \frac{-3\pm 101}{2} \Rightarrow n = 49, -52$$

Rejecting $n=-52$ as n cannot be negative, we get $n=49$.

Example 5. If $\frac{\lfloor n}{2\lfloor n-2}$ and $\frac{\lfloor n}{\lfloor 4 \lfloor n-4}$ are in the ratio 2 : 1, find the value of n.

Sol. Here $\frac{\lfloor n}{2\lfloor n-2} : \frac{\lfloor n}{\lfloor 4 \lfloor n-4} = 2:1$

$$\frac{\lfloor n}{2\lfloor n-2}\times\frac{\lfloor 4\lfloor n-4}{\lfloor n}=\frac{2}{1} \Rightarrow \frac{\lfloor 4\lfloor n-4}{2\lfloor n-2}=\frac{2}{1}$$

$$\frac{4.3.2.1\lfloor n-4}{2(n-2)(n-3)\lfloor n-4}=\frac{2}{1} \Rightarrow \frac{6}{(n-2)(n-3)}=\frac{1}{1}$$

$$(n-2)(n-3)=6 \Rightarrow (n-2)(n-3)=(3)(2)$$

$$n-2=3, \text{ or } n=5$$

EXERCISE 1.1

1. Evaluate (*i*) $\lfloor 8$ (*ii*) $\lfloor 4-\lfloor 3$.
2. Compute $\frac{\lfloor 8}{\lfloor 6\lfloor 2}$.
3. Is $\lfloor 3+\lfloor 4=\lfloor 7$?
4. Compute $\lfloor 4\lfloor 2$. Is $\lfloor 4\lfloor 2=\lfloor 8$?
5. Evaluate $\frac{\lfloor n}{\lfloor r\lfloor n-r}$, when $n=5$, $r=2$.
6. Evaluate $\frac{\lfloor n}{\lfloor n-r}$, when (*i*) $n=6$, $r=2$ (*ii*) $n=9$, $r=5$
7. If $\frac{1}{\lfloor 8}+\frac{1}{\lfloor 9}=\frac{x}{\lfloor 10}$, find x.
8. If $\frac{1}{\lfloor 9}+\frac{1}{\lfloor 10}=\frac{x}{\lfloor 11}$; find x.
9. If $\lfloor n+1=60\lfloor n-1$, find n.
10. Prove that $\frac{\lfloor 2n}{\lfloor n}=1.3.5.....(2n-1).2^n$.

1.2. Basic Counting Principles

There are mainly two counting principles namely

(*i*) Sum Rule (*ii*) Product Rule

These two principles form the basis of permutations and combinations and so are known as basic counting principles.

Sum Rule

If there are two operations such that they can be performed independently in m and n ways, then number of ways in which either of the two operations can be performed is $m+n$.

Product Rule

If there are two operations such that one of them can be performed in m ways and when it performed, second operations can be performed in n ways, then the two operations can be performed ways.

Product rule is Also known as Fundamental Principle of Counting *i.e.* FPC

Fundamental Principle of Counting *i.e.* FPC

If one operation can be performed in 'm' different ways and if corresponding to each of these of performing the first operation, there are 'n' different ways of performing the second operation, number of different ways of performing the two operations taken together is $m \times n$.

Extension. If corresponding to each of the $m \times n$ ways of performing the two operations taken there are 'p' different ways of performing the third operation then the number of different performing the three operations taken together is $m \times n \times p$ and so on.

Note : Fundamental Principle of Counting is known as Fundamental Principle of Associa Multiplication Principle.

We give some example to illustrate the above principle.

ILLUSTRATIVE EXAMPLES

Example 1. Find the number of 4 letter words, with or without meaning, which can be formed ou letters of the word ROSE, where the repetition of the letters is not allowed.

Sol. ROSE

Number of letters = 4

Number of places to be filled up = 4

The first place can be filled up in 4 ways as any one of the 4 letters can be placed there. After up the first place in any one of the 4 ways, there are 3 different ways of filling up the second place, one of the remaining 3 letters can be placed there. Therefore, by the principle of counting, the two taken together can be filled up in 4 ×3 ways. After filling the two places in 4 × 3 ways, the third pla be filled up in 2 ways as any one of the remaining two letters can be placed there. So, the three taken together can be filled up in 4 × 3 × 2 ways. After filling the three places in 4 × 3 × 2 wa fourth place can be filled up in 1 ways as the remaining 1 letter can be placed there.

$\therefore$ required number of words = $4 \times 3 \times 2 \times 1 = 24$

Example 2. In how many ways can 3 people be seated in a row containing 7 seats ?

Sol. First person can be seated in 7 ways

Second person can be seated in 6 ways

and the third person can be seated in 5 ways.

By the fundamental principle of counting total number of ways in which three persons can be sea seven seats in a row

$= 7 \times 6 \times 5 = 210$

Example 3. How many 3-digit numbers can be formed from the digits 1, 2, 3, 4 and 5 assuming that (*i*) repetition of the digits is allowed ? (*ii*) repetition of the digits is not allowed ?

Sol. Given digits are 1, 2, 3, 4, 5

∴ number of given digits = 5

Number of places to be filled = 3

(*i*) There are 5 ways of filling up the first place , 5 ways for the second place and 5 ways for the third place.

∴ by fundamental principle of counting,

total number of 3-digit numbers = 5 × 5 × 5 = 125

(*ii*) There are 5 ways of filling up the first place, 4 ways for the second place and 3 ways for the third place.

∴ by fundamental principle of counting,

total number of 3-digit numbers = 5 × 4 × 3 = 60

Example 4. How many numbers can be formed from the digits 1, 2, 3, 9 if repetition of digits is not allowed ?

Sol. (*a*) **Numbers with one digit :** There are four digits, hence four numbers of one digit can be formed with the help of these digits.

Hence, number of one digit numbers = 4.

(*b*) **Numbers with two digits :** First place of two digit number can be filled in 4 ways and the second place can be filled in 3 ways.

Hence, number of two digit numbers = 4 × 3 = 12.

(*c*) **Numbers with three digits :**

Number of three digits number = 4 × 3 × 2 = 24.

(*d*) **Number with four digits :**

Number of four digits numbers = 4 × 3 × 2 × 1 = 24.

Hence, total number of digits formed with the given digits = 4 + 12 + 24 + 24 = 64.

Example 5. Find the number of different signals that can be generated by arranging at least two flags in order (one below the other) on a vertical staff, if five different flags are available.

Sol. Number of flags = 5

A signal can be formed by using two, three, four or five flags.

Number of ways of forming signal using two flags = 5 × 4 = 20

Number of ways of forming signal using three flags = 5 × 4 × 3 = 60

Number of ways of forming signal using four flags = 5 × 4 × 3 × 2 = 120

Number of ways of forming signal using five flags = 5 × 4 × 3 × 2 × 1 = 120

∴ total numbers of signals formed = 20 + 60 + 120 + 120 = 320.

Example 6. Find the number of different signals that can be made by arranging at least three flags in ord on a vertical pole, if 6 different flags are available.

Sol. Number of flags = 6

(*a*) **Number of signals with three flags**

First place can be filled in 6 ways

Second place can be filled in 5 ways

Third place can be filled in 4 ways

$\therefore$ total number of signals = $6 \times 5 \times 4 = 120$ ways.

(*b*) **Number of signals with four flags**

Four places can be filled in 6, 5, 4, 3 ways

$\therefore$ total number of signals formed = $6 \times 5 \times 4 \times 3 = 360$

(*c*) **Number of signals with five flags**

Five places can be filled in 6, 5, 4, 3, 2 ways

$\therefore$ total number of signals formed = $6 \times 5 \times 4 \times 3 \times 2 = 720$

(*d*) **Number of signals with six flags**

Six places can be filled in 6, 5, 4, 3, 2, 1 ways

$\therefore$ total number of signals formed = $6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$

$\therefore$ required number of signals = $120 + 360 + 720 + 720 = 1920$

EXERCISE 1.2

1. Ram proposes to go to his friend Ali's house in a town which is connected with his village by three different routes. From there he will go to the city where his uncle lives. The city is connected with the town by two different routes. List out the various possible routes which Ram can choose from his village to go to the city.
2. If there are 20 steamers playing between places A and B, in how many ways could the round trip from A be made if the return was made on
   (*i*) the same steamer, (*ii*) a different steamer ?
3. A coin is tossed 3 times and the outcomes are recorded. How many possible outcomes are there ?
4. How many 4-letter codes can be formed using the first 10 letters of the English alphabet, if no letter can be repeated ?
5. How many 3-letter code words are possible using the first 10 letters of English alphabet if
   (*i*) no letter can be repeated ? (*ii*) letters are repeated ?
6. How many 5-digit telephone numbers can be constructed using the digits 0 to 9 if each number starts with 67 and no digit appears more than once ?
7. How many 3-digit even numbers can be formed from the digits 1, 2, 3, 4, 5, 6 if the digits can be repeated ?

8. A class consists of 40 girls and 60 boys. In how many ways can a president, vice president, treasurer and secretary be chosen if the treasurer must be a girl, the secretary must be a boy and a student may not hold more than one office ?

9. Eight children are to seated on a bench.
   (*i*) In how many ways can the children be seated ?
   (*ii*) How many arrangement are possible if the youngest child sits at the left hand end of the bench ?

10. Given 5 flags of different colours, how many different signals can be generated if each signal requires the use of 2 flags, one below the other ?

1.3. Permutation

It is an arrangement that can be made by taking some or all of a number of given things.

Meaning of ^nP_r : ^nP_r means the number of permutations of n different things taken r at a time.

Illustrations. Consider three letters *a, b, c.*

(*i*) The permutations of three letters taken two at a time are :

a b, b c, c a

b a, c b, a c

∴ The number of arrangements of three letters taken two at a time is 6 *i.e.*, $^3P_2 = 6$.

Note. ^nP_r is also written as P (n, r).

1.4. Combination

It is a group (or selection) that can be made by taking some or all of a number of a given things at a time.

Meaning of ^nC_r : ^nC_r means the number of combinations of n different things taken r at a time.

Illustration. Consider three letters *a, b, c.*

The groups of these 3 letters taken two at a time are *a b, b c, c a.*

As far as group is concerned *a c* or *c a* is the same group, as in a group we are concerned with the number of things contained, whereas in the case of arrangement we have to take into consideration the order of things.

Note. ^nC_r is also written as C (n, r).

1.5. Find the number of permutation of n different things taken r at a time *i.e.*, find the value of ^nP_r.

Proof : We know that the number of permutations of n different things taken r at a time is the same as the number of ways in which r places in a line can be filled up with n persons.

The first place can be filled up in n different ways as any one of the n persons can be placed there, After filling up the first place in any one of n ways, there are $(n-1)$ different ways of filling up the second place, as any one of the remaining $(n-1)$ persons can be placed there. Therefore, by the principle of association, the two places taken together can be filled up in $n(n-1)$ ways. After the two places have been filled up in any of the $n(n-1)$ ways, the third place can be filled up in $(n-2)$ ways as any one of the remaining $(n-2)$ persons can be placed there. Therefore the three places taken together can be filled up in $n(n-1)(n-2)$ ways.

Proceeding in this ways, we see that

(*i*) Whenever a place is filled up, a new factor is introduced.

(*ii*) The factors begin with n and go on diminishing by unity.

$\therefore$ rth factor $= n-(r-1) = n-r+1$

$\therefore$ number of ways of filling up r places $= n(n-1)(n-2)\ldots(n-r+1)$

$\therefore$ $${}^{n}P_r = n(n-1)(n-2)\ldots(n-r+1) = \frac{n(n-1)(n-2)\ldots(n-r+1)(n-r)\ldots3.2.1}{(n-r)\ldots3.2.1}$$

$\therefore$ $${}^{n}P_r = \frac{\lfloor n}{\lfloor n-r}$$

Cor. We know that ${}^{n}P_r = n(n-1)(n-2)\ldots(n-r+1)$ ...(1)

and $${}^{n}P_r = \frac{\lfloor n}{\lfloor n-r}$$ ...(2)

Putting $r = n$ in (1) and (2),

$${}^{n}P_n = n(n-1)(n-2)\ldots(n-n+1)$$

$$= n(n-1)(n-2)\ldots1 = \lfloor n$$ ...(3)

and $${}^{n}P_n = \frac{\lfloor n}{\lfloor 0}$$ ...(4)

From (3) and (4), we get,

$$\lfloor n = \frac{\lfloor n}{\lfloor 0} \Rightarrow \lfloor 0 = 1.$$

ILLUSTRATIVE EXAMPLES

Example 1. Prove that

(*i*) ${}^{n}P_n = 2 \cdot {}^{n}P_{n-2}$ (*ii*) ${}^{10}P_3 = {}^{9}P_3 + 3 \times {}^{9}P_3$

Sol. (*i*) L.H.S. $= {}^{n}P_n = \lfloor n$

$$\text{R.H.S.} = 2 \cdot {}^{n}P_{n-2} = 2 \times \frac{\lfloor n}{\lfloor n-(n-2)} = 2 \times \frac{\lfloor n}{\lfloor 2} = 2 \times \frac{\lfloor n}{2\times1} = \lfloor n$$

$\therefore$ L.H.S. = R.H.S.

(*ii*) L.H.S. $= {}^{10}P_3 = 10 \times 9 \times 8 = 720$

R.H.S. $= {}^{9}P_3 + 3 \cdot {}^{9}P_2 = 9 \times 8 \times 7 + 3(9 \times 8) = 504 + 216 = 720$

$\therefore$ L.H.S. = R.H.S.

Example 2. Find r, if $5 \cdot {}^4P_r = 6 \cdot {}^5P_{r-1}$.

Sol. $\because \quad 5 \cdot {}^4P_r = 6 \cdot {}^5P_r$

$$5\frac{\lfloor 4}{\lfloor 4-r} = 6\frac{\lfloor 5}{\lfloor 5-(r-1)} \quad \Rightarrow \quad \frac{\lfloor 5}{\lfloor 4-r} = \frac{6\times\lfloor 5}{\lfloor 6-r}$$

$$\therefore \quad \frac{1}{\lfloor 4-r} = \frac{6}{(6-r)\ (5-r)\lfloor 4-r}$$

$$\frac{1}{1} = \frac{6}{(6-r)(5-r)} \quad \Rightarrow \quad (6-r)\ (5-r) = 6$$

$$\therefore \quad r^2 - 11r + 24 = 0 \quad \Rightarrow \quad (r-8)(r-3) = 0$$

$$\therefore \quad r = 8, 3$$

Rejecting $r = 8$ [$\because\ r \le 5$], we get, $r = 3$

Example 3. Find n if $P(9, 5) + 5P(9, 4) = P(10, n)$.

Sol. Since $P(9, 5) + 5P(9, 4) = P(10, n)$

$$\therefore \quad {}^9P_5 + 5\,{}^9P_4 = {}^{10}P_n$$

$$\Rightarrow \quad \frac{\lfloor 9}{\lfloor 9-5} + 5\times\frac{\lfloor 9}{\lfloor 9-4} = \frac{\lfloor 10}{\lfloor 10-n} \quad \Rightarrow \quad \frac{\lfloor 9}{\lfloor 4} + 5\times\frac{\lfloor 9}{\lfloor 5} = \frac{10\times\lfloor 9}{\lfloor 10-n}$$

$$\Rightarrow \quad \frac{\lfloor 1}{\lfloor 4} + \frac{\lfloor 1}{\lfloor 4} = \frac{10}{\lfloor 10-n} \quad \Rightarrow \quad \frac{1}{24} + \frac{1}{24} = \frac{10}{\lfloor 10-n} \qquad [\because \lfloor 4 = 24]$$

$$\Rightarrow \quad \frac{1}{12} = \frac{10}{\lfloor 10-n} \quad \Rightarrow \quad \lfloor 10-n = 120$$

$$\Rightarrow \quad \lfloor 10-n = \lfloor 5 \quad \Rightarrow \quad 10-n = 5$$

$$\Rightarrow \quad n = 5.$$

Example 4. Find r if $P(10, r+1) : P(11, r) = 30 : 11$.

Sol. Since $P(10, r+1) : P(11, r) = 30 : 11$

$$\therefore \quad {}^{10}P_{r+1} : {}^{11}P_r = 30 : 11 \quad \Rightarrow \quad \frac{{}^{10}P_{r+1}}{{}^{11}P_r} = \frac{30}{11}$$

$$\Rightarrow \quad \frac{\dfrac{\lfloor 10}{\lfloor 10-r-1}}{\dfrac{\lfloor 11}{\lfloor 11-r}} = \frac{30}{11} \quad \Rightarrow \quad \frac{\lfloor 10}{\lfloor 9-r}\times\frac{\lfloor 11-r}{\lfloor 11} = \frac{30}{11}$$

$$\Rightarrow \quad \frac{\lfloor 10}{\lfloor 11}\times\frac{\lfloor 11-r}{\lfloor 9-r} = \frac{30}{11} \quad \Rightarrow \quad \frac{\lfloor 10}{11\times\lfloor 10}\times\frac{(11-r)(10-r)\lfloor 9-r}{\lfloor 9-r} = \frac{30}{11}$$

$$\Rightarrow \quad (11-r)(10-r) = 6\times 5$$

$$\Rightarrow \quad 11-r = 6 \quad \Rightarrow \quad r = 5$$

EXERCISE 1.3

1. Find n if $P(n, 4) = 20\ P(n, 2)$.
2. Find n if $P(2n, 3) = 100\ P(n, 2)$.
3. Find n if $30\ P(n, 6) = P(n+2, 7)$.
4. Find the value of n such that

   (*i*) ${}^nP_5 = 42\ {}^nP_3,\ n > 4$ (*ii*) $\frac{{}^nP_4}{{}^{n-1}P_4} = \frac{5}{3},\ n > 4$

5. Find r if :

   (*i*) ${}^5P_r = 2\ {}^6P_{r-1}$ (*ii*) ${}^5P_r = {}^6P_{r-1}$

6. Find n if ${}^{n-1}P_3 : {}^nP_4 = 1 : 9$.
7. If ${}^{56}P_{r+6} : {}^{54}P_{r+3} = 30800 : 1$, find r.

1.6. Practical Problems involving Permutation

Now we will apply the formula

$P(n, r) = n(n-1)(n-2) \ldots (n-r+1) = \frac{\lfloor n}{\lfloor n-r}$ to practical problems.

ILLUSTRATIVE EXAMPLES

Example 1. How many 3-letter words can be made using the letters of the words ORIENTAL ?

Sol. Given word is ORIENTAL

$\therefore$ number of letters = 8

Number of letters to be taken at a time = 3

$\therefore$ required number of words = ${}^8P_3$

$= 8 \times 7 \times 6 = 336$

Example 2. Find the number of different 8-letter words formed from the letters of the word TRIANGLE if each word is to

(*i*) begin with T (*ii*) end with E (*iii*) begin with T and end with E.

Sol. The given word is TRIANGLE

Number of letters = 8

Number of letter to be taken at a time = 8

(*i*) Since each word is to begin with T

$\therefore$ fix T in the beginning

$\therefore$ 7 letters are to be arranged in 7 places

$\therefore$ required numbers of words = ${}^7P_7 = \lfloor 7 = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5040$

(*ii*) Since each word is to end with E

$\therefore$ fix E in the end

$\therefore$ 7 letters are to be arranged in 7 places

$\therefore$ required number of words $= {}^7P_7 = \lfloor 7 = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 5040$

(*iii*) Since each word is to begin with T and end with E

$\therefore$ fix T in the beginning and E in the end

$\therefore$ 6 letters are to be arranged in 6 places

$\therefore$ required number of words $= {}^6P_6 = \lfloor 6 = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$

Example 3. How many words (with or without dictionary meaning) can be made from the letters in the word MONDAY, assuming that no letter is repeated, if

(*i*) 4 letters are used at a time ? (*ii*) all letters used at a time ?

(*iii*) all letters are used but the first is a vowel ?

Sol. The given word is MONDAY.

Number of letters = 6

(*i*) Number of letters to be taken at a time = 4

$\therefore$ required number of words $= {}^6P_4 = 6 \times 5 \times 4 \times 3 = 360$

(*ii*) Number of letters to be taken at a time = 6

$\therefore$ required number of words $= {}^6P_6 = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$

(*iii*) First place with 2 vowels O and A can be filled in 2 ways.

Now remaining 5 places can be filled up with 5 letters in ${}^5P_5$ ways.

$\therefore$ required number of words $= 2 \times {}^5P_5$

$= 2 \times (5 \times 4 \times 3 \times 2 \times 1) = 2 \times 120 = 240$

Example 4. It is required to seat 5 men and 4 women in a row so that the women occupy the even places. How many such arrangements are possible ?

Sol. Number of men = 5

Number of women = 4

Nine places are to be filled. In these 9 places, only four are even. Therefore, 4 even places can be filled with 4 women in ${}^4P_4 = \lfloor 4$ ways. Also remaining 5 places can be filled up with 5 men in ${}^5P_5 = \lfloor 5$ ways.

$\therefore$ required number of arrangements $= \lfloor 4 \times \lfloor 5 = (4 \times 3 \times 2 \times 1) \times (5 \times 4 \times 3 \times 2 \times 1)$

$= 24 \times 120 = 2880$

Example 5. Find the number of different 8-letter words formed from the letters of the word TRIANGLE if each word is to have vowels occupying odd places.

Sol.

T	R	I	A	N	G	L	E
1	2	3	4	5	6	7	8
×		×		×		×	

∵ vowels occupy odd places.

∴ the three vowels can be arranged in four × marked places in ${}^4P_3$ ways.

Also the five consonants can be arranged among themselves in $\lfloor 5$ ways.

∴ required number of words = ${}^4P_3 \times \lfloor 5$

$= (4 \times 3 \times 2) \times (5 \times 4 \times 3 \times 2 \times 1) = 24 \times 120 = 2880.$

Example 6. How many words, with or without meaning, can be formed using all the letters of the word EQUATION at a time so that the vowels and consonants occur together ?

Sol. EQUATION

Consonants are Q, T, N

Vowels are E, U, A, I, O

Consider 3 consonants as one letter and also 5 vowels as one letter.

∴ two letters can be arranged in $\lfloor 2$ ways.

Also 3 consonants can be arranged among themselves in $\lfloor 3$ ways and 5 vowels in themselves in $\lfloor 5$ ways.

∴ required number of words = $\lfloor 2 \times \lfloor 3 \times \lfloor 5$

$= (2 \times 1) \times (3 \times 2 \times 1) \times (5 \times 4 \times 3 \times 2 \times 1) = 2 \times 6 \times 120 = 1440$

Example 7. In how many ways can 5 girls and 3 boys be seated in a row so that no two boys are together.

Sol. Let 5 girls be G_1, G_2, G_3, G_4, G_5

$\times\ G_1 \times G_2 \times G_3 \times G_4 \times G_5 \times$

∵ no two boys are together

∴ 3 boys can be arranged in 6 'X' marked places in ${}^6P_3$ ways.

Also 5 girls can be arranged among themselves in $\lfloor 5$ ways.

∴ required number of ways = ${}^6P_3 \times \lfloor 5$

$= (6 \times 5 \times 4) \times (5 \times 4 \times 3 \times 2 \times 1) = 120 \times 120 = 14400$

Example 8. How many 4-digit numbers can be formed by using the digits 1 to 9 if repetition of digits is not allowed ?

Sol. Digits are 1, 2, 3, 4, 5, 6, 7, 8, 9

∴ total number of digits = 9

Number of digits to be taken = 4

∴ numbers formed = ${}^9P_4 = 9 \times 8 \times 7 \times 6 = 3024$

Example 9. How many numbers lying between 100 and 1000 can be formed with the digits 0, 1, 2, 3, 4, 5, if the repetition of the digits is not allowed ?

Sol. Numbers between 100 and 1000 consist of three digits.

Given digits are 0, 1, 2, 3, 4, 5

$\therefore$ number of given digits = 6

Number of digits to be taken at a time = 3

$\therefore$ numbers formed of three digits = ${}^6P_3 = 6 \times 5 \times 4 = 120$

But these include those numbers which have '0' on their extreme left and these will be numbers of 2 digits and not of three digits.

$\therefore$ we have to exclude these from the total.

In order to find numbers which have 0 on the extreme left position, we fix 0 in that position and fill up the remaining two places out of five digits at our disposal which can be done in ${}^5P_2$ ways *i.e.* 5×4 *i.e.* 20 ways.

$\therefore$ required numbers = $120 - 20 = 100$

Example 10. How many odd numbers greater than 80000 can be formed using the digits 2, 3, 4, 5 and 8 if each digit is used only once in a number ?

Sol. Given digits are 2, 3, 4, 5, and 8.

$\therefore$ number of given digits = 5

Number of digits to be taken at a time = 5

Since number is to greater than 80000

$\therefore$ first digit from left should be 8

$\therefore$ fix 8 in the beginning.

Now 4 places are to be filled with 4 digits.

Again numbers are odd

$\therefore$ numbers should have either 3 or 5 in the end

$\therefore$ end's place can be filled in 2 ways.

Remaining 3 places with 3 digits can be filled in ${}^3P_3$ ways

$\therefore$ required numbers $= 1 \times 2 \times {}^3P_3 = 1 \times 2 \times (3 \times 2 \times 1) = 12$

Example 11. How many different signals can be formed with five given flags of different colours ?

Number of flags = 5

A signal may formed by hoisting any number of flags at a time.

Number of signals by hoisting one flags at a time = ${}^5P_1$

Number of signals by hoisting two flags at a time = ${}^5P_2$

Number of signals by hoisting three flags at a time = ${}^5P_3$

Number of signals by hoisting four flags at a time = ${}^5P_4$

Number of signals by hoisting five flags at a time = ${}^5P_5$

$\therefore$ total number of signals formed

$= {}^5P_1 + {}^5P_2 + {}^5P_3 + {}^5P_4 + {}^5P_5$

$= 5 + 5 \times 4 + 5 \times 4 \times 3 + 5 \times 4 \times 3 \times 2 + 5 \times 4 \times 3 \times 2 \times 1$

$= 5 + 20 + 60 + 120 + 120 = 325.$

EXERCISE 1.4

1. (*i*) Ten horses are running a race. In how many ways can these horses come in the first, second an third place, assuming no ties ?

   (*ii*) Seven songs are to be rendered in a programme. In how many different orders could they be rendered ?

   (*iii*) There are six candidates contesting for a certain office in a municipal election. In how many ways can their names be listed on a ballot ?

   (*iv*) Four books, one each in Chemistry, Physics, Biology and Mathematics are to be arranged in a shelf. In how many ways can this be done ?

   (*v*) How many different signals can be generated from 6 flags of different colours if each signal makes use of all the flags at a time, placed one below the other ?

2. How many words, with or without meaning, can be formed using all the letters of the word EQUATION, using each letter exactly once ?

3. There are 6 items in column A and 6 items in column B. A student is asked to match each item in column A with an item in column B. How many possible answers (correct or incorrect) are there to the question ?

4. (*a*) From a committee of 8 persons, in how many ways can we choose a chairman and vice chairman assuming one person cannot hold more than one position ?

   (*b*) From a pool of 12 candidates, in how many ways can we select president, vice president, secretary and a treasurer if each of the 12 candidates can hold any office ?

5. How many different 5-letters words can be formed out of the letters of the word 'DELHI' ? How many of these will begin with D and end with E ?

6. The letters of the word TUESDAY are arranged in a line, each arrangement ending with letter S. How many different arrangements are possible ? How many of them start with letter D ?

7. Find the number of different 8-letters words formed from the letters of the word TRIANGLE if each word to have T and E at the end places.

8. Find the number of different 8- letters words formed from the letters of the word EQUATION, if each word is to start with a vowel.

9. In how many ways can 6 boys and 5 girls be arranged for a group photograph if the girls are to sit on chairs in a row and the boys are to stand, in row, behind them ?

10. Find the number of different 8-letter words formed from the letters of the word TRIANGLE if each word is to have vowels occupying the second, third and fourth places.
11. In how many ways can 4 boys and 3 girls be seated in a row of 7 chairs if boys and girls alternate ?
12. If there are six periods in each working day of a school, in how many ways can one arrange 5 subjects such that each subject is allowed at least one period ?
13. In how many way can the letters of the word 'PENCIL' be arranged so that N is always next to E ?
14. Find the number of different 8-letter words formed from the letters of the word TRIANGLE if each word is to have consonants never together.
15. Find the number of different 8-letter arrangements that can be made from the letters of the word DAUGHTER so that all vowels never occur together.
16. In how many ways can 5 books on Chemistry and 4 books on Physics be arranged on a shelf so that the books on same subject remain together ?
17. There are 8 students appearing in an examination, of which 3 have to appear in a mathematics paper and the remaining 5 in different subjects. In how many ways can they be made to sit in a row if the candidates in mathematics cannot sit next to each other ?
18. In how many ways can 4 boys and 3 girls be seated in a row so that two girls are together ?
19. Three married couples are to be seated in a row having six seats in a cinema hall. If spouses are to be seated next to each other, in how many ways can they be seated ? Find also the number of ways of their seating if all the ladies sit together.
20. Find the number of different 8 letter words formed from the letters of the word TRIANGLE if each word is to
    (*i*) have no two vowel together
    (*ii*) have both consonants and vowels together
    (*iii*) have the relative position of the vowels and consonants unaltered.
21. How many 3-digit numbers can be formed by using the digits 1 to 9 if no digit is repeated ?
22. How many different 4-digit numbers can be formed from the digits 2, 3, 4 and 6 if each digit is used only once in a number ? Further, how many of these numbers
    (*i*) end in *a* 4 ? (*ii*) end in *a* 3 ? (*iii*) end in *a* 3 or 6 ?
23. Find the number of 4-digit numbers that can be formed using the digits 1, 2, 3, 4, 5 if no digit is repeated. How many of these will be even ?
24. How many different numbers between 100 and 1000 can be formed from the digits 0, 1, 2, 3, 4, 5 and 6, assuming that in a number, the digits cannot be repeated ? How many of these will be divisible by 5 ?
25. How many 6-digit numbers can be formed from the digits 0, 1, 3, 5, 7 and 9 which are divisible by 10 and no digit is repeated ?
26. How many 4-digit numbers are there with no digit repeated ?
27. How many 3-digit even numbers can be made using the digits 1, 2, 3, 4, 6, 7, if no digit is repeated ?
28. How many numbers greater than 40000 can be formed using the digits 1, 2, 3, 4 and 5 if each digit is used only once in each number ?
29. How many of the natural numbers from 1 to 1000 have none of their digits repeated ?

1.7. Find the number of permutations of n things taken all at a time when p of them are alike and of one kind, q of them are alike and of a second kind, all others being different.

Proof. Let n things be denoted by n letters, p of them being alike and denoted by 'a', q of them being alike and denoted by 'b' and the remaining being all different and denoted by $c, d, e, f \ldots$

Let x be the required number of permutations. Take any one of these permutations and replace p alike letters 'a' by 'p' different letters $a_1, a_2, \ldots a_p$. These new p letters can be arranged among themselves in $\lfloor p$ new arrangements, when a's are considered different. And, therefore, if such a change is made in all the x permutations, then the total number of permutations will be $x \times \lfloor p$.

Now, consider one of these $x \times \lfloor p$ arrangements, and replace q like letters by q different letters, $b_1, b_2 \ldots, b_q$. These q letters can be arranged among themselves in $\lfloor q$ ways.

$\therefore$ one such permutation will give rise to $\lfloor q$ permutation and if such a change is made to all the $x \times \lfloor p$ permutations then the total number of permutations will be $x \times \lfloor p \times \lfloor q$

But number of permutations of n different things taken all at a time is $= \lfloor n$

$\therefore$ we have $x \times \lfloor p \times \lfloor q = \lfloor n \quad \Rightarrow \quad x = \dfrac{\lfloor n}{\lfloor p \times \lfloor q}$

Extension. This rule can be extended if in addition to the above r things are alike and of a third kind and so on.

ILLUSTRATIVE EXAMPLES

Example 1. Find the number of permutations of the letters of the word ALLAHABAD.

Sol. ALLAHABAD

Total number of given letters = 9

Number of A's = 4

Number of L's = 2

$\therefore$ required number of words $= \dfrac{\lfloor 9}{\lfloor 4 \,.\, \lfloor 2} = \dfrac{9 \times 8 \times 7 \times 6 \times 5 \times \lfloor 4}{\lfloor 4 \times (1 \times 2)} = 7560$

Example 2. In how many ways can 5 flags, in which 3 are red, one is white and one is blue, be arranged on a staff, one blow the other, if flags of one colour are not distinguishable ?

Sol. Total number of flags = 5

Number of red flags = 3

Number of white flags = 1

Number of blue flags = 1

$\therefore$ required number of arrangements $= \dfrac{\lfloor 5}{\lfloor 3 \cdot \lfloor 1 \cdot \lfloor 1} = \dfrac{5 \times 4 \times \lfloor 3}{\lfloor 3 \times 1 \times 1} = 20$

Example 3. In how many ways can the letters of the word ASSASSINATION be arranged so that all the S's are together ?

Sol. ASSASSINATION

Number of given letters = 13

Number of A's = 3

Number of S's = 4

Number of I's = 2

Number of N's = 2

Consider the four S's as one letter

$\therefore$ 10 letters can be arranged in $\frac{\lfloor 10}{\lfloor 3 . \lfloor 2 . \lfloor 2}$

Also four S's can be arranged among themselves in $\frac{\lfloor 4}{\lfloor 4}$ ways.

$\therefore$ required number of ways in which four S's are always together

$$= \frac{\lfloor 10}{\lfloor 3 . \lfloor 2 . \lfloor 2} \times \frac{\lfloor 4}{\lfloor 4} = \frac{10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times \lfloor 3}{\lfloor 3 \times (2 \times 1) \times (2 \times 1)} \times 1 = 151200$$

Example 4. Find the number of arrangements of the letters of the word INDEPENDENCE. In how many of these arrangements

(*i*) do the words start with P

(*ii*) do all the vowels always occur together

(*iii*) do the vowels never occur together

(*iv*) do the words begin with I and end in P ?

Sol. INDEPENDENCE

Number of given letters = 12

Number of N's = 3

Number of E's = 4

Number of D's = 2

$\therefore$ required number of arrangements = $\frac{\lfloor 12}{\lfloor 3 \times \lfloor 4 \times \lfloor 2}$

$$= \frac{12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times \lfloor 4}{(3 \times 2 \times 1) \times \lfloor 4 \times (2 \times 1)} = 1663200$$

(*i*) Since each word is to start with P

$\therefore$ fix P in the beginning.

Remaining 11 letters can be arranged in $\frac{\lfloor 11}{\lfloor 3 \times \lfloor 4 \times \lfloor 2}$

$$= \frac{11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times \lfloor 4}{(3 \times 2 \times 1) \times \lfloor 4 \times (2 \times 1)} = 138600$$

(*ii*) Consider five vowels as one letter.

$\therefore$ 8 letters can be arranged in $\frac{\lfloor 8}{\lfloor 3 \cdot \lfloor 2}$ ways

Also five vowels can be arranged in themselves in $\frac{\lfloor 5}{\lfloor 4}$ ways.

$\therefore$ number of arrangements in which vowels are always together

$$= \frac{\lfloor 8}{\lfloor 3 \cdot \lfloor 2} \times \frac{\lfloor 5}{\lfloor 4} = \frac{8 \times 7 \times 6 \times 5 \times 4 \times \lfloor 3}{\lfloor 3 \times (1 \times 2)} \times \frac{5 \times \lfloor 4}{\lfloor 4} = 3360 \times 5 = 16800$$

(*iii*) Required number of arrangements = 1663200 – 16800 = 1646400

(*iv*) Fix I in the beginning and P in the end.

$\therefore$ required number of arrangements = $\frac{\lfloor 10}{\lfloor 3 \cdot \lfloor 4 \cdot \lfloor 2}$

$$= \frac{10 \times 9 \times 8 \times 7 \times 6 \times 5 \times \lfloor 4}{(3 \times 2 \times 1) \times \lfloor 4 \times (2 \times 1)} = 12600$$

Example 5. How many numbers greater than 1000000 can be formed by using the digits 1, 2, 0, 2, 4, 2, 4

Sol. Given digits are 1, 2, 0, 2, 4, 2, 4

$\therefore$ total number of digits = 7

Number of 2's = 3

Number of 4's = 2

Number of digits to be taken at a time = 7

$\therefore$ numbers formed = $\frac{\lfloor 7}{\lfloor 3 \times \lfloor 2} = \frac{7 \times 6 \times 5 \times 4 \times \lfloor 3}{\lfloor 3 \times (1 \times 2)} = 420$

These numbers also include those numbers which have 0 at the extreme left position.

Numbers having 0 at the extreme left position = $\frac{\lfloor 6}{\lfloor 3 \times \lfloor 2} = \frac{6 \times 5 \times 4 \times \lfloor 3}{\lfloor 3 \times (1 \times 2)} = 60$

$\therefore$ required number of numbers = 420 – 60 = 360

EXERCISE 1.5

1. How many permutations of the letter of word APPLE are there ?
2. In how many ways can 4 red, 3 yellow and 2 green discs be arranged in a row if the discs of the same colour are indistinguishable ?
3. There are 3 white, 4 red and 1 blue marbles in bag. They are drawn one by one and arranged in a row. Assuming that all the 8 marbles are drawn, determine the number of different arrangements if marbles of same colour are indistinguishable.
4. In how many distinct ways can the product $x^1y^2z^2$ be written without using exponents ?
5. In how many distinct permutations of the letters in MISSISSIPPI do the four I's not come together ?
6. In how many different ways, the letters of the word ALGEBRA can be arranged in a row if
   (*i*) the two A's are together ? (*ii*) the two A's are not together ?
7. Find how many arrangements can be made with the letters of the word 'MATHEMATICS' ? In how many of them
   (*i*) consonants occur together (*ii*) vowels do not occur together ?
8. If the different permutations of all the letters of the word EXAMINATION are listed as in a dictionary, how many words are there in this list before the first word starting with E ?
9. In how many ways can the letters of the word PERMUTATIONS be arranged if the
   (*i*) words start with P and end with S,
   (*ii*) vowels are all together
   (*iii*) there are always 4 letters between P and S ?
10. How many 5-digit even numbers can be formed using the digits 1, 2, 5, 5, 4 ?

1.8. Circular Permutations

Find the number of ways in which n persons can be arranged at a round table.

Proof. When n persons are sitting around a circular table, then there is no first and last person. Let us fix the position of one person. The remaining $(n-1)$ persons can now be arranged in the remaining $(n-1)$ places in ${}^{n-1}P_{n-1}$ *i.e.*, $\lfloor n-1$ ways.

$\therefore$ required number of ways $= \lfloor n-1$.

1.9. Clockwise and Anti-clockwise Permutations

The total number of circular permutations can be divided into two types :

(*i*) Clockwise (*ii*) Anti-clockwise.

In two such arrangements each person has the same neighbour though in the reverse order and either of these arrangements can be obtained from the other by just over-turning the circle. If in this case, no distinction is made between clockwise and anti-clockwise arrangements then the two such arrangements are considered as only one distinct arrangement.

Hence the number of circular permutations in such cases $= \frac{1}{2}\lfloor n-1$

Note. Questions on necklaces with beads if different colours are to be tackled by the above formula, as in this case also there is no difference between clockwise and antiwise arrangements.

ILLUSTRATIVE EXAMPLES

Example 1. In how many ways can 6 beads of different colours form a necklace ?

Sol. Number of beads = 6

$\therefore$ required number of necklaces $= \frac{1}{2} \lfloor 6-1 = \frac{1}{2} \cdot \lfloor 5 = \frac{1}{2} \times (5 \times 4 \times 3 \times 2 \times 1) = 60.$

Example 2. Four persons A, B, C and D are to be seated at a circular table. In how many ways can they be seated ?

Sol. Number of given persons = 4

Number of ways of seating them in a circular table $= \lfloor 4-1 = \lfloor 3 = 3 \times 2 \times 1 = 6$

Example 3. In how many ways can 5 boys and 5 girls be seated at a round table, so that no two girls sit together ?

Sol. Let the boys be seated firstly leaving one seat vacant in between each of two boys .

[$\because$ no two girls are to sit together]

This can be done in $\lfloor 5-1$ *i.e.*, in $\lfloor 4$ ways.

Now 5 girls can be arranged in 5 vacant seat ${}^5P_5$ *i.e.*, $\lfloor 5$ ways.

$\therefore$ required number of ways $= \lfloor 4 \times \lfloor 5$

$= (4 \times 3 \times 2 \times 1) \times (5 \times 4 \times 3 \times 2 \times 1) = 24 \times 120 = 2880.$

EXERCISE 1.6

1. In how many ways can 8 girls be seated at a round table provided Parveen and Vipul are not to sit together ?
2. In how many ways 4 boys and 4 girls be seated at a round table provided each boy is to be between two girls ?
3. The Principals of six colleges seat themselves round a table to discuss the student's unrest problem. In how many arrangements, Principals of X-college and Y-college will not sit together?

1.10. Combination

In combination, we are not interested in arranging, but only in selecting r objects from n objects. In fact, we do not want to specify the ordering of these selected objects.

Differences between a permutation and a combination :

1. In a combination only a selection is made whereas in a permutation not only a selection is made, but also an arrangement in a definite order.
2. In a combination, the ordering of the selected objects is immaterial whereas in a permutation, this ordering is essential.

1.11. Find the number of combinations of n dissimilar things taken r at time (by using the value of ${}^nP_r$).

Proof : Let the required number of combinations of n things taken r at a time be x.

$\because$ each combination contains r things, which can be arranged among themselves in $\lfloor r$ ways.

$\therefore$ corresponding to each combination, we get $\lfloor r$ permutations.

$\therefore$ total number of permutations due to x combinations $= x\lfloor r$

But number of permutations of n things taken r at a time $= {}^nP_r$.

$\therefore$ we have, $x\lfloor r = {}^nP_r$ or $x = \dfrac{{}^nP_r}{\lfloor r}$

i.e., $${}^nC_r = \frac{{}^nP_r}{\lfloor r} \Rightarrow {}^nC_r = \frac{\lfloor n}{\lfloor r \lfloor n-r}$$

Cor. $${}^nC_r = \frac{{}^nP_r}{\lfloor r} = \frac{n(n-1)(n-2)\ldots(n-r+1)}{\lfloor r}$$

1.12. Complimentary Combination

Prove that $\boxed{{}^nC_r = {}^nC_{n-r}}$

Proof. L.H.S. $= {}^nC_r = \dfrac{\lfloor n}{\lfloor r \cdot \lfloor n-r}$

$$\text{R.H.S.} = {}^nC_{n-r} = \frac{\lfloor n}{\lfloor n-r \lfloor n-(n-r)} = \frac{\lfloor n}{\lfloor n-r \cdot \lfloor r}$$

$\therefore$ L.H.S. = R.H.S.

Another method. (*From first Principles*)

We know that ${}^nC_r$ means the number of combinations of n things taken r at a time. Whenever we form a group of r things out of n things, $(n-r)$ things are left which themselves form a group.

$\therefore$ number of groups of n things taken r at a time is the same as the number of groups of n things taken $(n-r)$ at a time.

i.e., ${}^nC_r = {}^nC_{n-r}$

Note. We will apply this formula in problems in which $r > \dfrac{n}{2}$.

1.13. Prove that $\boxed{{}^nC_r + {}^nC_{r-1} = {}^{n+1}C_r}$.

Proof. **[From first Principles]**

We know that,

${}^{n+1}C_r$ = number of combinations of $(n+1)$ things taken r at a time

= number of combinations which include a particular thing

+ number of combinations which exclude that particular thing.

= number of combinations of n things taken $(r-1)$ at a time.

+ number of combinations of n things taken r at a time.

$\therefore \quad {}^{n+1}C_r = {}^{n}C_{r-1} + {}^{n}C_r$

or $\quad {}^{n}C_r + {}^{n}C_{r-1} = {}^{n+1}C_r$

Another method

$$\text{R.H.S.} = {}^{n+1}C_r = \frac{\lfloor n+1}{\lfloor r \, \lfloor n-r+1}$$

$$\text{L.H.S.} = {}^{n}C_{r-1} + {}^{n}C_r$$

$$= \frac{\lfloor n}{\lfloor r-1 \, \lfloor n-r+1} + \frac{\lfloor n}{\lfloor r \, \lfloor n-r} = \frac{\lfloor n}{\lfloor r-1 . (n-r+1) . \lfloor n-r} + \frac{\lfloor n}{r \lfloor r-1 \lfloor n-r}$$

$$= \frac{\lfloor n}{\lfloor r-1 \, \lfloor n-r}\left[\frac{1}{n-r+1} + \frac{1}{r}\right] = \frac{\lfloor n}{\lfloor r-1 \, \lfloor n-r}\left[\frac{r+n-r+1}{r(n-r+1)}\right]$$

$$= \frac{\lfloor n}{\lfloor r-1 \, \lfloor n-r}\left[\frac{n+1}{r(n-r+1)}\right] = \frac{(n+1)\lfloor n}{(r \lfloor r-1)(n-r+1) \lfloor n-r} = \frac{\lfloor n+1}{\lfloor r \, \lfloor n-r+1}$$

$\therefore \quad$ L.H.S. = R.H.S.

1.14. Find the total number of combinations of n different things by taking some or all at a time.

OR

Find the value of ${}^{n}C_1 + {}^{n}C_2 + {}^{n}C_3 + \ldots + {}^{n}C_n$

Proof : Here each thing can be dealt in two ways. Either it is included or excluded from a selection.

Hence each thing can be disposed in 2 ways.

But each way of dealing with a thing is associated with each way of dealing with the other.

$\therefore$ total number of ways of dealing with n things

$= 2 \times 2 \times 2 \times \ldots\ldots n$ items $= 2^n$

But these include the case where none of the things is selected.

$\therefore$ the required number of ways $= 2^n - 1$

Again, we may select 1 or 2 or 3 or 4 ...or n things out of the given n different things.

$\therefore$ the required number of ways $= {}^{n}C_1 + {}^{n}C_2 + {}^{n}C_3 + \ldots + {}^{n}C_n = 2^n - 1.$

ILLUSTRATIVE EXAMPLES

Example 1. Verify that $C(8, 4) + C(8, 3) = C(9, 4)$.

Sol. L.H.S. $= C(8, 4) + C(8, 3) = {}^8C_4 + {}^8C_3$

$$= \frac{8 \times 7 \times 6 \times 5}{1 \times 2 \times 3 \times 4} + \frac{8 \times 7 \times 6}{1 \times 2 \times 3} = 70 + 56 = 126$$

R.H.S. $= C(9, 4) = {}^9C_4 = \frac{9 \times 8 \times 7 \times 6}{1 \times 2 \times 3 \times 4} = 126$

$\therefore$ L.H.S. = R.H.S.

Example 2. Evaluate ${}^{50}C_{47}$, $C(15, 14)$.

Sol. Here ${}^{50}C_{47} = {}^{50}C_3$ $[\because {}^nC_r = {}^nC_{n-r}]$

$$= \frac{50 \times 49 \times 48}{1 \times 2 \times 3} = 19600$$

Again $C(15, 14) = {}^{15}C_{14} = {}^{15}C_1$ $[\because {}^nC_r = {}^nC_{n-r}]$

$$= \frac{15}{1} = 15$$

Example 3. Determine n if

$${}^{2n}C_3 : {}^nC_3 = 11 : 1$$

Sol. $$\frac{{}^{2n}C_3}{{}^nC_3} = \frac{11}{1} \Rightarrow \frac{\frac{(2n)(2n-1)(2n-2)}{1.2.3}}{\frac{n(n-1)(n-2)}{1.2.3}} = \frac{11}{1}$$

$$\therefore \frac{(2n)(2n-1)(2n-2)}{n(n-1)(n-2)} = \frac{11}{1} \Rightarrow \frac{4(2n-1)(n-1)}{(n-1)(n-2)} = \frac{11}{1}$$

$$\therefore \frac{4(2n-1)}{n-2} = \frac{11}{1} \Rightarrow 11n - 22 = 8n - 4$$

$$\Rightarrow 3n = 18 \Rightarrow n = 6$$

Example 4. If ${}^nC_9 = {}^nC_8$, find ${}^nC_{17}$.

Sol. Here ${}^nC_9 = {}^nC_8$

$\therefore$ either $9 = 8$ which is impossible | or $n = 9 + 8$, $\therefore$ $n = 17$

$\therefore$ ${}^nC_{17} = {}^{17}C_{17} = 1$

Example 5. Find the value of $^{47}C_4 + \sum_{r=1}^{5} {}^{52-r}C_3$

Sol. Consider $^{47}C_4 + \sum_{r=1}^{5} {}^{52-r}C_3$

$= {}^{47}C_4 + {}^{51}C_3 + {}^{50}C_3 + {}^{49}C_3 + {}^{48}C_3 + {}^{47}C_3 = ({}^{47}C_3 + {}^{47}C_4) + {}^{48}C_3 + {}^{49}C_3 + {}^{50}C_3 + {}^{51}C_3$

$= ({}^{48}C_4 + {}^{48}C_3) + {}^{49}C_3 + {}^{50}C_3 + {}^{51}C_3 \qquad [\because {}^{n}C_{r-1} + {}^{n}C_r = {}^{n+1}C_r]$

$= ({}^{49}C_4 + {}^{49}C_3) + {}^{50}C_3 + {}^{51}C_3 = ({}^{50}C_4 + {}^{50}C_3) + {}^{51}C_3 = {}^{51}C_4 + {}^{51}C_3 = {}^{52}C_4$

$= \frac{52 \times 51 \times 50 \times 49}{1 \times 2 \times 3 \times 4} = 270725$

Example 6. If $^{n}C_x = 56$ and $^{n}P_x = 336$, find n and x.

Sol. $^{n}C_x = 56 \Rightarrow \frac{\lfloor n}{\lfloor x \lfloor n-x} = 56$ ...(1)

$^{n}P_x = 336 \Rightarrow \frac{\lfloor n}{\lfloor n-x} = 336$ ...(2)

Dividing (2) by (1), we get,

$$\frac{\lfloor n}{\lfloor n-x} \times \frac{\lfloor x \lfloor n-x}{\lfloor n} = \frac{336}{56}$$

or $\lfloor x = 6$

$\therefore \quad \lfloor x = \lfloor 3 \Rightarrow x = 3$

Now $^{n}P_x = 336 \Rightarrow {}^{n}P_3 = 336$

$\Rightarrow \quad n(n-1)(n-2) = 8 \times 7 \times 6 \Rightarrow n = 8$

$\therefore$ we have $x = 3, n = 8$

Example 7. If $^{n-1}C_r : {}^{n}C_r : {}^{n+1}C_r = 6 : 9 : 13$, find n and r.

Sol. We have

$$^{n-1}C_r : {}^{n}C_r : {}^{n+1}C_r = 6 : 9 : 13$$

$$\therefore \quad \frac{{}^{n-1}C_r}{{}^{n}C_r} = \frac{6}{9} \Rightarrow \frac{\frac{\lfloor n-1}{\lfloor r \lfloor n-r-1}}{\frac{\lfloor n}{\lfloor r \lfloor n-r}} = \frac{2}{3}$$

$$\therefore \quad \frac{\lfloor n-1}{\lfloor r \lfloor n-r-1} \times \frac{\lfloor r \lfloor n-r}{\lfloor n} = \frac{2}{3}$$

$\therefore \quad \frac{\lfloor n-1}{\lfloor n} \times \frac{\lfloor n-r}{\lfloor n-r-1} = \frac{2}{3}$

$\therefore \quad \frac{\lfloor n-1}{n\lfloor n-1} \times \frac{(n-r)\lfloor n-r-1}{\lfloor n-r-1} = \frac{2}{3}$

$\therefore \quad \frac{n-r}{n} = \frac{2}{3} \Rightarrow 3n-3r = 2n$

$\therefore \quad n = 3r \qquad \ldots(1)$

and $\frac{{}^nC_r}{{}^{n+1}C_r} = \frac{9}{13} \Rightarrow \frac{\frac{\lfloor n}{\lfloor r \lfloor n-r}}{\frac{\lfloor n+1}{\lfloor r \lfloor n-r+1}} = \frac{9}{13}$

$\therefore \quad \frac{\lfloor n}{\lfloor r \lfloor n-r} \times \frac{\lfloor r \lfloor n-r+1}{\lfloor n+1} = \frac{9}{13} \Rightarrow \frac{\lfloor n}{(n+1)\lfloor n} \times \frac{(n-r+1)\lfloor n-r}{\lfloor n-r} = \frac{9}{13}$

$\therefore \quad \frac{\lfloor n}{\lfloor n+1} \times \frac{\lfloor n-r+1}{\lfloor n-r} = \frac{9}{13}$

$\therefore \quad \frac{n-r+1}{n+1} = \frac{9}{13}$

$\Rightarrow \quad 13n-13r+13 = 9n+9$

$\therefore \quad 4n-13r+4 = 0$

$\therefore \quad 4(3r)-13r+4 = 0 \qquad [\because \text{of (1)}]$

$\therefore \quad 12r-13r+4 = 0$

$\Rightarrow \quad -r+4 = 0 \qquad \Rightarrow r = 4$

$\therefore$ from (1), $n = 3 \times 4 = 12$

$\therefore \quad n = 12, \quad r = 4$

EXERCISE 1.7

1. Evaluate $C(19, 17) + C(19, 18)$.
2. Prove that
   (*i*) $1 + C(3, 1) + C(4, 2) = C(5, 3)$
   (*ii*) $C(2, 1) + C(3, 1) + C(4, 1) = C(3, 2) + C(4, 2)$
3. Determine n if ${}^{2n}C_3 : {}^nC_2 = 12 : 1$.
4. If ${}^nC_8 = {}^nC_2$, find ${}^nC_2$.

5. If C $(n, 10)$ = C $(n, 12)$, determine n and hence C $(n, 5)$.

6. If ${}^{15}C_{3r} = {}^{15}C_{r+3}$, find r.

7. Prove that $C(2n, n) = \dfrac{2^n [1.3.5...(2n-1)]}{\lfloor n}$.

8. If m = C $(n, 2)$, prove that C $(m, 2)$ = 3 C $(n+1, 4)$.

9. If ${}^nC_r : {}^nC_{r+1} = 1 : 2$ and ${}^nC_{r+1} : {}^nC_{r+2} = 2 : 3$, find n and r.

1.15. Practical Problems Involving Combinations

ILLUSTRATIVE EXAMPLES

Example 1. In how many ways can a committee be selected from 15 persons if the committee is to have

(*i*) 3 members. (*ii*) 13 members.

Sol. Total number of persons = 15

(*i*) Number of persons to be selected = 3

$\therefore$ required number of ways = ${}^{15}C_3 = \dfrac{15 \times 14 \times 13}{1 \times 2 \times 3} = 455$

(*ii*) Number of persons to be selected = 13

$\therefore$ required number of ways = ${}^{15}C_{13} = {}^{15}C_2 = \dfrac{15 \times 14}{1 \times 2} = 105$

Example 2. In how many ways can a student choose a programme of 5 courses if 9 courses are available and 2 courses are compulsory for every student ?

Sol. Total number of courses = 9

Number of courses to be chosen = 5

$\because$ two courses are compulsory

$\therefore$ student is to select 3 courses out of 7 courses

$\therefore$ required number of ways = ${}^7C_3 = \dfrac{7 \times 6 \times 5}{1 \times 2 \times 3} = 35$

Example 3. Determine the number of 5-card combinations out of a deck of 52 cards if atleast one of the five cards has to be a king.

Sol. Total number of cards = 52

Number of king = 4

$\therefore$ remaining cards = 48

Number of combinations of 5 cards out of 52 $= {}^{52}C_5 = \dfrac{52 \times 51 \times 50 \times 49 \times 48}{1 \times 2 \times 3 \times 4 \times 5}$

Number of combinations of 5 cards containing no king $= {}^{48}C_5 = \dfrac{48 \times 47 \times 46 \times 45 \times 44}{1 \times 2 \times 3 \times 4 \times 5}$

$\therefore$ required number of combinations

$$= \frac{52 \times 51 \times 50 \times 49 \times 48}{1 \times 2 \times 3 \times 4 \times 5} - \frac{48 \times 47 \times 46 \times 45 \times 44}{1 \times 2 \times 3 \times 4 \times 5} = 886656$$

Example 4. In how many ways can we select a cricket eleven from 17 players in which only 5 players can bowl if each cricket eleven must include exactly 4 bowlers ?

Sol. Number of bowlers = 5

Number of other players = 12

7 other players out of 12 other players can be selected on ${}^{12}C_7$ ways and 4 bowlers out of 5 bowlers can be selected in ${}^{5}C_4$ ways.

$\therefore$ required number of teams $= {}^{12}C_7 \times {}^{5}C_4 = {}^{12}C_5 \times {}^{5}C_1 = \dfrac{12 \times 11 \times 10 \times 9 \times 8}{1 \times 2 \times 3 \times 4 \times 5} \times \dfrac{6}{1} = 3960$

Example 5. A committee of 3 persons is to be constituted from a group of 2 men and 3 women. In how many ways can this be done ? How many of these committees would consist of 1 man and 2 women ?

Sol. (*i*) Number of men = 2

Number of women = 3

$\therefore$ total number of persons = 2 + 3 = 5

Number of persons to be taken in a group = 3

$\therefore$ required number of committees $= {}^{5}C_3 = {}^{5}C_2$

$$= \frac{5 \times 4}{1 \times 2} = 10$$

(*ii*) 1 man out of 2 men can be selected in ${}^{2}C_1$ ways. 2 women out of 3 women can be selected in ${}^{3}C_2$ ways.

$\therefore$ required number of committees

$= {}^{2}C_1 \times {}^{3}C_2$

$= {}^{2}C_1 \times {}^{3}C_1 = \dfrac{2}{1} \times \dfrac{3}{1} = 6$

Men	Women
2	3
1	2

Example 6 What is the number of ways of choosing 4 cards from a pack of 52 playing cards ? In how many of these

(*i*) four cards are of the same suit,

(*ii*) four cards belongs to four different suits,

(*iii*) are face cards

(*iv*) two are red cards and two are black cards,

(*v*) cards are of the same colour ?

Sol. Total number of given cards = 52

Number of cards to be selected at a time = 4

$\therefore$ required number of ways = $^{52}C_4 = \frac{52 \times 51 \times 50 \times 49}{1 \times 2 \times 3 \times 4} = 270725$

(*i*) There are four suits namely diamond, club, spade and heart. There are 13 cards in each suit.

There are $^{13}C_4$ ways of choosing 4 diamonds, $^{13}C_4$ ways of choosing 4 clubs, $^{13}C_4$ ways of choosing 4 spades and $^{13}C_4$ ways of choosing 4 hearts.

$\therefore$ required number of ways = $^{13}C_4 + {}^{13}C_4 + {}^{13}C_4 + {}^{13}C_4$

$= 4 \times {}^{13}C_4 = 4 \times \frac{13 \times 12 \times 11 \times 10}{1 \times 2 \times 3 \times 4} = 2860$

(*ii*) There are four suits and 13 cards in each suit.

There are $^{13}C_1$ ways of choosing 1 card from 13 cards of each suit.

$\therefore$ by the multiplication principle,

required number of ways = $^{13}C_1 \times {}^{13}C_1 \times {}^{13}C_1 \times {}^{13}C_1 = 13 \times 13 \times 13 \times 13 = 28561$

(*iii*) Jacks, queens and kings are face cards

$\therefore$ total number of face cards = 12

Number of cards to be selected at a time = 4

$\therefore$ required number of ways = $^{12}C_4 = \frac{12 \times 11 \times 10 \times 9}{1 \times 2 \times 3 \times 4} = 495$

(*iv*) There are 26 red cards and 26 black cards. Now 2 red cards out of 26 red cards can be selected in $^{26}C_2$ ways. Similarly 2 black cards out of 26 black cards can be selected in $^{26}C_2$ ways.

$\therefore$ required number of ways = $^{26}C_2 \times {}^{26}C_2 = \frac{26 \times 25}{1 \times 2} \times \frac{26 \times 25}{1 \times 2} = 105625$

(v) 4 red cards out of 26 red cards can be selected in ${}^{26}C_4$ ways. Also 4 black cards out of 26 black cards can be selected in ${}^{26}C_4$ ways

$\therefore$ required number of ways $= {}^{26}C_4 + {}^{26}C_4$

$$= 2 \times {}^{26}C_4 = 2 \times \frac{26 \times 25 \times 24 \times 23}{1 \times 2 \times 3 \times 4} = 29900$$

Example 7. A group consists of 4 girls and 7 boys. In how many ways can a team of 5 members be selected if the team has

(i) no girls ? (ii) at least one boy and one girl ?

(iii) at least three girls ?

Sol. Number of boys = 7

Number of girls = 4

Committee is to consist of 5

Boys	Girls
7	4
5	

(i) $\because$ committee includes no girl

$\therefore$ we are to select 5 boys out of 7 boys

$\therefore$ number of committees $= {}^{7}C_5 = {}^{7}C_5 = \frac{7 \times 6}{1 \times 2} = 21$

(ii) $\because$ committee is to include at least one boy and one girl

$\therefore$ different possibilities are

Boys	Girls
7	4
1	4
2	3
3	2
4	1

(a) 1 boy, 4 girls

(b) 2 boys, 3 girls

(c) 3 boys, 2 girls

(d) 4 boys, 1 girls

$\therefore$ required number of ways

$$= {}^{7}C_1 \times {}^{4}C_4 + {}^{7}C_2 \times {}^{4}C_3 + {}^{7}C_3 \times {}^{4}C_2 + {}^{7}C_4 \times {}^{4}C_1$$

$$= {}^{7}C_1 \times 1 + {}^{7}C_3 \times {}^{4}C_1 + {}^{7}C_3 \times {}^{4}C_2 + {}^{7}C_3 \times {}^{4}C_1$$

$$= 7 \times 1 + \frac{7 \times 6}{1 \times 2} \times \frac{4}{1} + \frac{7 \times 6 \times 5}{1 \times 2 \times 3} \times \frac{4 \times 3}{1 \times 2} + \frac{7 \times 6 \times 5}{1 \times 2 \times 3} \times \frac{4}{1}$$

$$= 7 + 84 + 210 + 140 = 441$$

(iii) $\because$ committee is to include at least three girls

$\therefore$ different possibilities are

Boys	Girls
7	4
2	3
1	4

(a) 2 boys, 3 girls

(*b*) 1 boy, 4 girls

$\therefore$ required number of ways $= {}^7C_2 \times {}^4C_3 + {}^7C_1 \times {}^4C_4$

$$= {}^7C_2 \times {}^4C_1 + {}^7C_1 \times 1 = \frac{7\times6}{1\times2} \times \frac{4}{1} + \frac{7}{1} \times 1$$

$$= 84 + 7 = 91$$

Example 8. From 5 consonants and 4 vowels, how many words can be constructed using 3 consonants and 2 vowels ?

Sol. 3 consonants out of 5 can be selected in ${}^5C_3$ ways and 2 vowels out of 4 can be selected in ${}^4C_2$ ways.

$\therefore$ total number of groups formed $= {}^5C_3 \times {}^4C_2 = \frac{5\times4\times3}{1\times2\times3} \times \frac{4\times3}{1\times2} = 10 \times 6 = 60$

Now each group contains 5 letters, which can be arranged among themselves is $\lfloor 5$ ways.

$\therefore$ required number of words formed $= 60 \times \lfloor 5 = 60 \times (5 \times 4\times3\times2\times1) = 60 \times 120 = 7200$

Example 9. How many words, with or without meaning, each of 2 vowels and 3 consonants can be formed from the letters of the word DAUGHTER ?

Sol. DAUGHTER

Consonants are D, G, H, T, R

Vowels are A, U E

Now 3 consonants out of 5 can be selected in ${}^5C_3$ ways and 2 vowels out of 3 can be selected in ${}^3C_2$ ways.

$\therefore$ total number of groups formed $= {}^5C_3 \times {}^3C_2 = {}^5C_2 \times {}^3C_1 = \frac{5\times4}{1\times2} \times \frac{3}{1} = 30$

Now each group contains 5 letters, which can be arranged among themselves in $\lfloor 5$ ways.

$\therefore$ required number of words formed $= 30 \times \lfloor 5 = 30 \times (5 \times 4 \times 3 \times 2 \times 1) = 30 \times 120 = 3600$

Example 10. There are 15 points in a plane, no three of which are in the same straight line excepting 4, which are collinear. Find the number of (*i*) straight lines (*ii*) triangles, formed by joining them.

Sol. (*i*) We know that join of any two distinct points, gives a line.

$\therefore$ number of lines got from 15 points, no three of which are collinear

$$= {}^{15}C_2 = \frac{15 \times 14}{1 \times 2} = 105$$

Lines got from 4 points $= {}^4C_2 = \frac{4 \times 3}{1 \times 2} = 6$

$\therefore$ number of lines lost due to 4 collinear points $= 6 - 1 = 5$ [$\because$ 4 collinear points do give one line]

$\therefore$ required number of lines $= 105 - 5 = 100$

(ii) We know that any three non-collinear points give a triangle.

∴ number of triangles got from, 15 points no three of which are collinear

$$= {}^{15}C_3 = \frac{15 \times 14 \times 13}{1 \times 2 \times 3} = 455$$

Triangles got from 4 points $= {}^4C_3 = {}^4C_1 = 4$

∴ number of triangles lost due to collinear points = 4

∴ required number of triangles = 455 – 4 = 451.

Example 11. The number of diagonals of a polygon is 20. Find the number of its sides.

Sol. Let number of sides of polygon $= n$

∴ Number of points $= n$

Number of lines formed $= {}^nC_2 = \frac{n(n-1)}{2}$

∴ number of diagonals $= \frac{n(n-1)}{2} - n$

From given condition, $\frac{n(n-1)}{2} - n = 20$

$\therefore \quad n^2 - n - 2n = 40 \quad \Rightarrow \quad n^2 - 3n - 40 = 0$

$\Rightarrow \quad (n-8)(n+5) = 0 \quad \Rightarrow \quad n = 8, -5$

Rejecting $n = -5$ as number of sides cannot be negative, we get, $n = 8$

∴ number of sides = 8

Example 12. In class XI examination, a candidate has to pass in all the five subjects taken in order to be declared as pass. In how many ways can he fail ?

Sol. Number of subjects = 5

Candidate will fail if he fail in one or two or three or four or five subjects.

∴ required number of ways $= {}^5C_1 + {}^5C_2 + {}^5C_3 + {}^5C_4 + {}^5C_5$

$$= \frac{5}{1} + \frac{5 \times 4}{1 \times 2} + \frac{5 \times 4}{1 \times 2} + \frac{5}{1} + 1 = 5 + 10 + 10 + 5 + 1 = 31$$

EXERCISE 1.8

1. (i) A committee of 2 boys is to be selected from 4 boys. In how many ways can this be done ?
   (ii) How many different terms of 7 players can be chosen from 10 players ?
   (iii) How many selections of 4 books can be made from 8 different books ?
   (iv) Sudha wants to choose any 9 stamps from a set of 11 different stamps. How many different selections can she make ?
2. In a meeting after every one hand shaken hands with every one else, it was found that 66 hand shakes were exchanged. How many members were present at the meeting ?

3. In an examination, a student is to answer 4 questions out of 5. Question 1 and 2 are, however, compulsory. Determine the number of ways in which the student can make the choice.
4. In an examination paper on mathematics 10 questions are set. In how many different ways can you choose 6 questions to answer ? If, however, question number 1 is made compulsory, in how many ways can you select to answer 6 questions in all ?
5. We wish to select 6 persons from 8, but if the person A is chosen, then B must be chosen. In how many ways can the selection be made ?
6. Determine the number of 5-card combinations out of a deck of 52 cards if each selection of 5 cards has exactly one king.
7. A father with eight children takes them 3 at a time to zoological garden as often as he can take without the same three children together more than once. How often will each child go ? How often will the father go ?
8. In how many ways can a cricket eleven be selected out of 15 players ?
   (*a*) In how many of them a particular player be excluded ?
   (*b*) In how many of them will he be included ?
9. Show that the total number of ways in which six '+' and four '–' signs can be arranged in a line such that no two '–' signs occur together is 35.
10. A question paper has two parts, part A and part B, each containing 10 questions. If the student has to choose 8 questions from part A and 5 from part B, in how many ways can he choose the questions ?
11. A bag contains 5 black and 6 red balls. Determine the number of ways in which 2 black and 3 red balls can be selected from lot.
12. A bookshelf contains 7 different mathematics textbooks and 5 different physics textbooks. How many groups of 3 mathematics and 3 physics textbooks can be selected ?
13. 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 ?
14. For the posts of 5 teachers, there are 23 applicants. 2 posts are reserved for SC candidates and there are 7 SC candidates among the applicants. In how many ways can the selection be made ?
15. (*a*) In how many ways can a team of 3 boys and 3 girls be selected from 5 boys and 4 girls ?
    (*b*) How many different committees each consisting of 3 girls and 2 boys, can be chosen from 7 girls and 5 boys ?
16. Find the number of ways of selecting 9 balls from 6 red balls, 5 white balls and 5 blue balls if each selection consists of 3 balls of each colour.
17. In an examination, Yamini has to select 4 questions from each part. There are 6, 7 and 8 questions in Part I, Part II and Part III, respectively. What is the number of possible combinations in which she can choose the questions ?
18. A mathematics paper consists of 10 questions divided into two parts I and II. Each part containing 5 questions. A student is required to attempt 6 questions in all, talking at least 2 questions from each part. In how many ways can the student select the questions ?
19. 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.
20. A committee of four has to be selected from among 6 boys and 5 girls. The committee is to include at least 1 boy and at least 1 girl. In how many ways can we select the committee ?

A committee of 7 has to be formed from 9 boys and 4 girls. In how many ways can this be done when the committee consists of :

(*i*) exactly 3 girls ? (*ii*) atleast 3 girls ? (*iii*) atmost 3 girls ?

In an examination, a question paper consists of 12 questions divided into two parts *i.e.*, Part I and Part II, containing 5 and 7 questions, respectively. A student is required to attempt 8 questions in all, selecting at least 3 from each part. In how many ways can a student select the questions ?

A sports team of 11 students is to be constituted, choosing at least 5 from class XI and at least 5 form class XII. If there are 20 students in each of these classes, in how many ways can the team be constituted ?

From a class of 12 boys and 8 girls, 8 students are to be chosen for a competition, at least including 4 boys and 4 girls. The 2 girls who won the prizes last year should be included. In how many ways can the selection be made ?

A boy has 3 library tickets and 8 books of his interest in the library. Of these 8, he does not want to borrow Chemistry Part II unless Chemistry Part I is also borrowed. In how many ways can he choose the three books to be borrowed ?

From a class of 25 students, 10 are to be chosen for an excursion party. There are 3 students who decide that either all of them will join or none of them will join. In how many ways can they be chosen ?

The English alphabet has 5 vowels and 21 consonants./ How many words with two different vowels and 2 different consonants can be formed from the alphabet ?

From 3 capitals, 5 consonants and 4 vowels, how many words can be formed each containing 3 consonants, 2 vowels and beginning with a capital ?

How many words, with or without meaning, each of 3 vowels and 2 consonants can be formed from the letters of the word INVOLUTE ?

A team of 8 players is to be chosen from a group of 12 players. One of the 8 is then to be elected as captain and another as vice-captain. In how many ways can the team be chosen ?

A football team consists of eleven players including its captain. In how many ways may be the captain invite one or more of them to a party ?

Find the total number of all possible selections of one or more questions from 12 given questions, each question having an alternative to it.

(*a*) How many chords can be drawn through 21 points on a circle ?

(*b*) There are 15 points in a plane, no three of which are collinear. Find the number of triangles formed by joining them.

(*i*) Seven points lie on a circle. How many chords can be drawn by joining these points ?

(*ii*) How many lines can be drawn through n points on a circle ?

How many triangles can be drawn through n points on a circle ?

(*iii*) How many diagonals does a ten-sided polygon have ? How many triangles can be got by joining its vertices ?

(*iv*) A number of points are marked on a plane and are connected pairwise by a line segment. If the total number of line segments is 10, how many points are marked on the plane ?

Ram has 5 friends. In how many ways can he invite one or one of them to a party ?

(*i*) A man has 6 friends. In how many ways can he invite one or more of them to a party ?

(*ii*) In an examination, a candidate has to pass in each of four subjects taken by him. In how many ways can he fail ?

1.16. Introduction to Elementary Combinatorics

Discrete mathematics or combinatorics deals with existence, enumeration, classification, analysis and optimisation of arrangements or selection of discrete structure.

In this section, we start with some basic counting principles which help us to count number of arrangements or selections satisfying certain constraints. We have two basic counting principles with the help of which we can do many simple countings.

1.17. Two Basic Counting Principles

(I) Sum Principle

(*a*) If $S = A_1 \cup A_2 \cup ..... \cup A_n$ and A_i are mutually disjoint sets *i.e.*

$A_i \cap A_j = \phi$ if $i \neq j$, then

$$|S| = |A_1| + |A_2| + ... + |A_n|$$

In other words, if we partition a set into n parts, then the number of elements in S is equal to the sum of numbers of elements in various parts

(*b*) An alternative way of stating this principle in terms of **Events** is as follows :

If $E_1, E_2, ..., E_n$ are mutually exclusive events (*i.e.* if E_i happen, then E_j does not happen) and E_i can happen in e_i ways, then the number of ways in which either E_1 can happen or E_2 can happen or ..... or E_n can happen is $e_1 + e_2 + ... + e_n$.

(*c*) We can also state the sum principle in terms of **CHOICES** as follows :

If an object can be choosen from one heap in e_1 ways and another object from a second heap in e_2 ways and so on, then the number of ways of selecting an object from any one of the heaps is $e_1 + e_2 + ... + e_n$.

(II) Product Rule or Principle of Sequential Counting

(*a*) If $S_1, S_2, ..., S_n$ are finite sets, then $|S_1 \times S_2 \times ..... \times S_n| = |S_1||S_2| ..... |S_n|$

(*b*) In terms of **EVENTS**, the product rule can be stated as follows :

If events $E_1, E_2, ..., E_n$ can happen in $e_1, e_2, ..., e_n$ ways respectively, then the sequence of events E_1, followed by $E_2, ...$, followed by E_n can happen in $e_1 e_2, ... e_n$ ways

(*c*) In terms of **CHOICES**, we can state the product rule as follows :

If first object can be choosen in e_1 ways, a second object in e_2 ways, ... nth object in e_n ways, then the number of ways of selecting the n objects is $e_1 e_2 ..... e_n$.

Example 1. In how many ways can we draw a

(*a*) a heart or a spade

(*b*) a numbered card or a king

(*c*) a spade or an ace

Sol. (*a*) Now a heart can be drawn in 13 ways and a spade can be drawn in 13 ways

∴ By the sum principle

Total number of ways = 13 + 13 = 26

(*b*) A numbered card can be drawn in 36 ways and a king can be drawn in 4 ways

∴ By the sum principle

Total number of ways = 36 + 4 = 40

(*c*) A spade card can be drawn in 13 ways and an ace can be drawn in 3 ways

∴ By the sum principle

Total number of ways = 13 + 3 = 16

Example 2. In how many ways can we get a sum of 4 or 8 when we two distinguishable dice are thrown ? In how many ways can we get an even sum ?

Sol. A sum of 4 can be obtained from two dices in 3 different ways e.g. [(1,3), (2, 2), (3, 1)] and a sum of 8 can be obtained in 5 different ways [*e.g.* (2, 6), (3, 5), (4, 4), (5, 3), (6, 2)]

∴ By the sum principle

Total no. of ways of obtaining a sum of 4 or 8 = 3 + 5 = 8

Further, sum of the number on both the dices is even if the sum is 2 or 4 or 6 or 8 or 10 or 12

The sum of the numbers on both the dices is 2 can be in 1 ways [*e.g.* (1, 1)]

The sum of the numbers on both the dices is 4 can be in 2 ways [(1, 3), (3, 1)]

The sum of the numbers on both the dices is 6 can be in 5 ways [*e.g.* (1, 5), (2, 4), (3, 3), (4, 2), (5, 1)]

The sum of numbers on both the dices is 8 can be in 5 ways [*e.g.* (2, 6), (3, 5), (4, 4), (5, 3), (6, 2)]

The sum of numbers on both the dices is 10 can be in 3 ways [*e.g.* (4, 6), (5, 5), (6, 4)]

The sum of numbers on both the dices is 12 can be in 1 ways [*e.g.* (6, 6)]

∴ By the sum principle

Total number of ways = 1 + 3 + 5 + 5 + 3 + 1 = 18

Example 3. If k distinguishable dices are thrown, in how many ways can they fall ?

Sol. First dice can fall in 6 different ways

Second dice can fall in 6 different ways

kth dice can fall in 6 different ways

∴ By the product principle

Total number of falls = 6.6. ..... $6 = 6^k$

Example 4. If the lincense plates of a state require 3 english letters followed by 4 digits. How many plates can be manufactured if

(*a*) repetitions of letters and digits are allowed

(*b*) letters are repeated but not digits

(*c*) No repetition are allowed.

Sol. (*a*) Three english letters can be choosen in $26\times26\times26$ ways.

Four digits can be filled in $10\times10\times10\times10$ way

$\therefore$ By the product principle

Total number of plates manufactured $= 26^3\times10^4$

(*b*) Three english letters can be choosen in $26\times26\times26$ ways.

Four digits can be filled in $10\times9\times8\times7$ ways

$\therefore$ By the product principle

Total no. of plates manufactured $= 26^3\times10\times9\times8\times7$

(*c*) Three english letters can be choosen in $26\times25\times24$ ways.

Four digits can be filled in $10\times9\times8\times7$ ways

$\therefore$ By the product principle

Total no. of plates manufactured $= 26\times25\times24\times10\times9\times8\times7$

Sometimes we need to combine the two principles to solve a problem.

Example 5. How many linsense plates are there that involve

(*a*) 1, 2 or 3 letters followed by 4 digits

(*b*) 1, 2, or 3 letters followed by 1, 2, 3, or 4 digits

Sol. (*a*) Number of plates in which there is only 1 letter followed by 4 digits $= 26\times10^4$

The number of plates in which there are 2 letters followed by 4 digits $= 26^2\times10^4$

The number of plates in which there are 3 letters followed by 4 digits $= 26^3\times10^4$

$\therefore$ By the sum principle

Total no. of plates $= 26\times10^4 + 26^2\times10^4 + 26^3\times10^4$

(*b*) The number of plates in which there are 1 or 2 or 3 english letters $= 26 + 26^2 + 26^3$

The number of plates in which there are 1 or 2 or 3 or 4 digits $= 10 + 10^2 + 10^3 + 10^4$

$\therefore$ By the product rule

Total no. of plates $= (26 + 26^2 + 26^3)(10 + 10^2 + 10^3 + 10^4)$

III. Indirect Counting

Some times, we can solve a problem by indirect counting *i.e.* by counting the elements in the complement of the set.

If $A \subseteq S$, $A^c = S \setminus A = \{x \in S : x \notin A\}$. Then

$|A| = |S| - |A^c|$ $[\because S = A \cup A^c$ and $A \cap A^c = \phi]$

Example 6. In how many ways an 10 people be seated in a row so that a certain pair of persons are not together

Sol. When there is no restriction on the selection then it can be done in $\underline{|10}$ ways

Also the number of ways in which a certain pair of person are together = $2\underline{|9}$

∴ The no. of ways in which a certain pair of persons are not together = $\underline{|10} - 2\underline{|9} = 8\underline{|9}$

Example 7. Find the number of non-negative integers $< 10^9$ which contain digit 1.

Sol. Since the number is less then 10^9. Therefore it should have at the most 9 digits.

When there is no restriction on the digits. Then

The number of numbers less then 10^9 will be 10^9

Also the number of numbers less then 10^9 which don't contain the digit $1 = 9^9$

∴ The no. of number less then 10^9 which contain the digit $1 = 10^9 - 9^9$

Example 8. We can draw a card from a deck of 52 cards and replace it before the next draw. In how many can we draw 10 cards so that the 10th card is a repetition of a previous draw.

Sol. When there is no restriction on the drawn of card.

The no. of ways of drawing 10 cards = 52^{10}

Also the no. of ways of drawing 10 cards in which the 10th card drawn is not a repeated card = 52×51^9

∴ The number of ways of drawing 10 cards in which 10th card is a repetition = $52^{10} - 52 \times 51^9$.

IV. Technique of one-one correspondence

In this we replace one problem with by another problem having the same number of objects as the given problem but in which the counting can be done easily. It is based on the principle that if : $f: A \to B$ are one-one, onto functions, then $|A| = |B|$.

Example 9. If $|S| = n$, then the number of subsets of S is 2^n.

Sol. Let $S = \{x_1, x_2, ..., x_n\}$. Let $T \subseteq S$ such that

$$T = \{x_{i_1}, x_{i_2}, ..., x_{i_r}\}$$

We correspond T to a binary number of length n, where 1 occur at the $i_1, i_2, ..., i_n$ th places and 0 every where else

i.e. $T = \{x_{i_1}, x_{i_2}, ..., x_{i_r}\} \to \{0, 0, ..., \underset{i_1}{1}, 0, ..., \underset{i_2}{1}, 0, ..., \underset{i_r}{1}, 0, 0\}$

This gives a one-one correspondence between the subsets of S and the binary numbers of n digits which are 2^n in numbers

Hence the number of subsets of $S = 2^n$.

1.18. Multi Set

A collection of objects in which objects are allowed to be repeated is called a multi set.

e.g. $S = \{a, a, a, b, b, c\} = \{3 \times a, 2 \times b, 1 \times c\}$

In general $S = \{r_1 \times a_1, r_2 \times a_2, \ldots\ldots, r_k \times a_k\}$

is a multi set in which a_1 occur r_1 times, a_2 occur r_2 times and so on, a_k occur k times

1.19. r-permutation

By an r-permutations, we mean an ordered arrangement of r elements from S. If $|S| = n$, then an n-permutation of S is just called a permutation of S.

1.20. If S is a multi set with infinite repetitions then the number of r-permutation of S is k^r, where k = number of distinct objects in S.

Proof. Since each of the r-place in the arrangement can be filled in k ways by any one of the k-distinct objects.

$\therefore$ By multiplication principle

Required number of r-permutations = k^r.

Remark : If the repetition number of each object in $S \geq r$, then also the number of r-permutations = k^r.

Example 10. Find the number of ternary numbers with atmost 4 digits.

Sol. The number of ternary numbers with atmost 4 digits

= 4-permutation with 3 objects say $\{0, 1, 2\} = 3^4$

1.21. If $S = \{n_1 \times a_1, n_2 \times a_2, \ldots\ldots, n_k \times a_k : n_i \text{ finite}\}$

i.e. $|S| = n_1 + n_2 + \ldots\ldots + n_k$. Then the number of permutations of S *i.e.* n-permutation is

$$\frac{\lfloor n}{\lfloor n_1 \lfloor n_2 \ldots\ldots \lfloor n_k}$$

Proof. First, we replace n_1 a's in ${}^nC_{n_1}$ ways

For each such choice of a_i's, the remaining elements $\{n_2 \times a_2, \ldots\ldots, n_k \times a_k\}$ can be placed in

$$\frac{(n_2 + n_3 + \ldots\ldots + n_k)!}{n_2! n_3! \ldots\ldots n_k!} \text{ ways}$$

(By induction on $n_1 + \ldots\ldots + n_k$).

So by the product rule.

Total no. of permutations = ${}^nC_{n_1} \dfrac{(n_2 + n_3 + \ldots\ldots + n_k)!}{n_2! n_3! \ldots\ldots n_k!}$

$$= \frac{n!}{n_1!(n_2 + \ldots\ldots + n_k)!} \cdot \frac{(n_2 + n_3 + \ldots\ldots + n_k)!}{n_2! n_3! \ldots\ldots n_k!} = \frac{n!}{n_1! n_2!, \ldots\ldots n_k!}$$

ample 11. Find the number of ways 23 books can be given to 5 students, so that 2 students will have 4 oks each and the other 3 students will have 5 books each.

l. Here $S = \{n_1 \times a_1, n_2 \times a_2\} = \{2 \times 4, 3 \times 5\}$

where $n_1 = 2,\ n_2 = 3,\ a_1 = 4,\ a_2 = 3, |S| = n = n_1 + n_2 = 2 + 3 = 5$

$\therefore$ Required number of ways $= {}^5C_2 \times \dfrac{23!}{4!4!5!5!5!}$

ample 12. In how many ways can 7 women and 3 men be arranged in a row if 3 men must be together.

l. Regarding 3 men as a group of one. Then 7 women and 1 group of men can be arranged in ${}^8P_8 = 8!$ ys.

But 3 men is the group can be arranged them selves in ${}^3P_3 = 3!$ ways

$\therefore$ Total no. of arrangement = 8 ! 3 !

Remark : (*i*) If $r < n$, the number of r-permutations of a multi set with repetitions is not easy. The solution n this case is obtained by means of **generating functions** as will be discussed later on.

(*ii*) The number of circular permutations of n objects is $\underline{|n-1}$.

For multi sets with infinite repetitions, the number of r-combinations is given by the following heorem.

1.22. Combinations of Multisets

Let S be a multi set then an r-combination of S is an unordered selection of r of the objects of S. Thus n r-combination of a multi set S is itself a multi set, a sub multiple of S

e.g. If S = {2*a*, 1*b*, 3*c*}, then 3-combinations of S are

{2*a*, 1*b*}, {2*a*, 1*c*}, {1*a*, 1*b*, 1*c*}, {1*a*, 2*c*}, {1*b*, 2*c*}, {3*c*}.

1.23. Let S be a multi set with k distinct objects each with infinite repetitions. The number of r-ombinations of S is equal to $C(r + k - 1, r) = C(r + k - 1, k - 1)$.

roof : Let $a_1, a_2, \ldots, a_k$ be k-distinct objects in S so that

$$S = \{\infty \times a_1, \infty \times a_2, \ldots, \infty \times a_k\}$$

Any r combinations of S is of the form

$$\{x_1 \times a_1, x_2 \times a_2, \ldots, x_k \times a_k\ ; x_i \geq 0, x_1 + x_2 + \ldots + x_k = r\}$$

We have the possibilities

I Number of r-combinations of S = Number of solutions of

$x_1 + x_2 + \ldots + x_k = r,\ x_i \geq 0$ integers

II This is clearly equal to the number of solutions of

$y_1 + y_2 + \ldots + y_k = r + k$, with $y_i \geq 1$ integers

The theorem will therefore follows from the following Lemma.

1.24. The number of solutions of $x_1 + x_2 + \ldots\ldots + x_k = m$ with $x_i \geq 1$ integers is $C(m-1, k-1)$

Proof. There is a one-one correspondence between the above solutions and the choice of $k-1$ integers from $\{1, 2, \ldots\ldots, m-1\}$ as follows

Let $x_1 + x_2 + \ldots\ldots + x_k = m,\ x_i \geq 1$.

Let $y_1 = x_1,\ y_2 = x_1 + x_2, \ldots\ldots, y_{k-1} = x_1 + x_2 + \ldots\ldots + x_{k-1} = m - x_k$.

Then $1 \leq y_1 < y_2 < \ldots\ldots < y_{k-1} < m-1$ Since $x_k \geq 1$ ...(*)

Conversely if $y_1, y_2, \ldots\ldots, y_{k-1}$ satisfy (*), then we take

$x_1 = y_1,\ x_2 = y_2 - y_1, \ldots\ldots,\ x_r = y_r - y_{r-1},\ x_{k-1} = y_{k-1} - y_{k-2}$,

$x_k = m - y_{k-1}$.

This gives solutions of $x_1 + x_2 + \ldots\ldots + x_k = m,\ x_i \geq 1$

Clearly, the number of choices of $y_1, y_2, \ldots\ldots, y_{k-1}$ satisfying (*) is $C(m-1, k-1)$

III Another way of looking at the solutions of $x_1 + x_2 + \ldots\ldots + x_k = r,\ x_i \geq 0$ integer is to observe that this number is the same as the number of ways of placing r balls in k numbered boxes. We put x_1 balls in first box, x_2 balls in 2nd box and so on.

IV Another ways of counting number of solutions of $x_1 + x_2 + \ldots\ldots + x_k = r,\ x_i \geq 0$ is to count the binary numbers containing r zeros and $k-1$ 1's. We have one-one correspondence between the solutions of $x_1 + x_2 + \ldots\ldots + x_k = r$ and the binary numbers

$$\underbrace{0\ldots\ldots0}_{x_1}1\ \underbrace{0\ldots\ldots0}_{x_2}1\ \underbrace{0\ldots\ldots0}_{x_3}1\ \ldots\ldots\ 1\ \underbrace{0\ldots\ldots0}_{x_{k-1}}\ 1\ \underbrace{0\ldots\ldots0}_{x_k} \text{ of } r+k-1$$

digits. So we have to choose $k-1$ 1's out of a total of $r+k-1$ digits

This can be done in $C(r+k-1, k-1) = C(r+k-1, r)$ ways

Remark : The above results is valid if each objects in S has multiplicity $\geq r$. However the result is complicated if some objects have multiplicity $< r$. We need the **Inclusion Exclusion Principle** to find the required number of that case.

1.25. The number of integral solutions of $x_1 + x_2 + \ldots\ldots + x_n = r$ with $x_1 \geq r_1, x_2 \geq r_2, \ldots\ldots, x_n \geq r_n$ is

$$C(n-1+r+r_1-r_2\ \ldots\ldots\ -r_n, n-1).$$

Put $x_i = y_i + r_i,\ x_i \geq r_i \Rightarrow y_i \geq 0$

$\therefore$ We need to find the number of integral solutions of $y_1 + y_2 + \ldots\ldots + y_n = m$, where $m = r - r_1 - r_2 - \ldots\ldots r_n$ and $y_i \geq 0$ which is equal to $C(n-1+m, n-1)$ *i.e.*

$C(n-1+r-r_1-r_2\ \ldots\ldots\ r_n, n-1)$.

mple 13. Find the number of integral solutions of equation $x_1+x_2+x_3+x_4=20$ e $x_1 \geq 3, x_2 \geq 1, x_3 \geq 0$ and $x_4 \geq 5$.

Given equation is

$$x_1+x_2+x_3+x_4=20 \quad \ldots(1)$$

where $x_1 \geq 3, x_2 \geq 1, x_3 \geq 0$ and $x_4 \geq 5$.

Put $y_1 = x_1-3, \quad y_2 = x_2-1, \quad y_3 = x_3, \quad y_4 = x_4-5$.

With the change of variables, equation (1) transforms to

$$y_1+y_2+y_3+y_4 = 11 \quad \ldots(2)$$

where $y_1 \geq 0, y_2 \geq 0, y_3 \geq 0, y_4 \geq 0$.

Hence number of solutions of (1) of required type

= number of non-negative integral solutions of (2) $= {}^{11+4-1}C_{11} = {}^{14}C_{11} = 364$.

mple 14. Prove that the number of ways of placing 20 similar books in 5 shelves is C (24, 4).

The required number of ways is equal to finding the number of solutions of $x_1+x_2+x_3+x_4+x_5=20$, which is C $(r+k-1, k-1)$ here $r=20, k=5$,

i.e. required no. of ways = C (20 + 5 – 1, 5 – 1) = C (24, 4)

mple 15. Prove that the number of ways of filling a box with dozen pastries choosen from 8 different ies is C (19, 7).

The required number of ways is equal to finding the number of solutions of $x_1+x_2+.....+x_8 = 12$,

Which is equal to C $(r+k-1, k-1)$

Here $r = 12, k = 8$

i.e. required no. of ways = C (12 + 8 – 1, 8 – 1) = C (19, 7)

mple 16. Find the number of integral solutions of $x_1+x_2+.....+x_5 = 5$ such that $3, x_2 \geq 0, x_3 \geq 4, x_4 \geq 2, x_5 \geq 2$

ere $r = 20, r_1 = -3, r_2 = 0, r_3 = 4, r_4 = 2, r_5 = 2, n = 5$

hen the no. of required integral solutions is C $(n-1+r-r_1-r_2.....,-r_5, n-1)$

e. C (5 – 1 + 20 + 3 – 0 – 4 – 2 – 2, 5 – 1) = C (19, 4)

mple 17. Find the number of monotonically increasing sequences of length r whose terms are taken $2, ..., k$.

he monotonically increasing sequences to be counted can be obtained by first choosing r-ations of the multiset

$S = \{\infty \cdot 1, \infty \cdot 2, ..., \infty \cdot k\}$

n arranging the elements in increasing order.

ence number of monotonically increasing sequences = number of r-combination of S $= {}^{r+k-1}C_r$.

Example 18. A shop sells 6 different flavours of ice cream. In how many ways can a customer ch ice-cream cones if

(*i*) they are all of different flavours

(*ii*) they are not necessarily of different flavours

(*iii*) they contain only 3 different flavours

(*iv*) they contain only 2 or 3 different flavours ?

Sol. Let the flavours be denoted by A, B, C, D, E and F.

(*i*) Here we want the number of ways of choosing 4 ice-cream cones of different flavours from of 6 different flavours.

Hence the required number of different flavours is ${}^6C_4 = 15$.

(*ii*) The number of 4-combinations of 6 objects when repetition is allowed $= {}^{6+4-1}C_4 = {}^9C_4 =$

(*iii*) The number of ways of choosing 4 cones of exactly 3 different flavours with repetitions

= (Number of ways of choosing 3 flavours out of 6)

× (Number of ways of choosing 4 cones

choosen flav

$= {}^6C_3 \times 3 = 60,$

Since there are ${}^6C_3$ ways of choosing 3 flavours out of 6 and for each choice, say A, B, C, there ways of choosing 4 cones of 3 chosen flavours, namely A, B, C, C or A, B, B, C or A, A, B, C.

(*iv*) As in (*iii*), the number of ways of choosing 4 cones of exactly 2 different flavours, with repeti $= {}^6C_2 \times 3 = 45$, because for each choice of 2 flavours say A, B, there are 3 ways of choosing 4 con the 2 choosen flavours, namely A, A, A, B or A, A, B, B or A, B, B, B.

Hence the ways of choosing cones of 2 or 3 flavours = 60 + 45 = 105.

Example 19. Let $S = \{10 \cdot \alpha, 10 \cdot \beta, 10 \cdot \gamma, 10 \cdot \delta\}$ with four distinct elements α, β, γ and δ. Find the num of 10 combinations of S which have the property that each of the four distinct elements occurs at least o

Sol. Here number of 10-combinatios of the required form is equal to number of positive integral solutio

$$r_1 + r_2 + r_3 + r_4 = 10$$

where r_1, r_2, r_3, r_4 represents the number of α's, β's, γ's and δ's respectively in a 10-combination of S.

We change the variables to

$$s_1 = r_1 - 1,\ s_2 = r_2 - 1,\ s_3 = r_3 - 1,\ s_4 = r_4 - 1$$

so that equation (1) becomes

$$s_1 + s_2 + s_3 + s_4 = 6.$$

$\therefore$ Required numbers of 10-combinations

= Number of positive integral solution of (1)

= Number of non-negative integral solution of (2) $= {}^{6+4-1}C_6 = {}^9C_6 = 84.$

Example 20. How many integers between 100 and 1,000,000 have sum of digits

(*i*) equal to 5 (*ii*) less than 5.

Sol. (*i*) Let x_i $(1 \le i \le 6)$ be the digits of a number with at most 6 digits.

Then the number of non-negative integral solutions of

$$x_1+x_2+x_3+x_4+x_5+x_6 = 5$$

is $$6+5-1C_6 = {}^{10}C_6 = 252.$$

But we want those numbers which are > 100.

$\therefore$ We must removed 6 numbers namely 5, 14, 41, 23, 32, 50.

Hence the required numbers = 252 − 6 = 246.

(*ii*) The number of non-negative integral solutions of

$$x_1+x_2+\ldots+x_6 = 5-k \; ; \quad 1 \le k \le 4$$

is $$6+5-k-1C_{5-k} = {}^{10-k}C_{5-k} = {}^{10-k}C_5.$$

$\therefore$ Number of integers < 1,000,000 having sum of digits less than 5

$$= \sum_{k=1}^{4} {}^{10-k}C_5 = {}^{9}C_5+{}^{8}C_5+{}^{7}C_5+{}^{6}C_5 = 209.$$

These numbers include 15 numbers namely 1,10, 2, 20, 11, 3, 30, 12, 21, 4, 40, 13, 31, 22, 100 which are ≤ 100.

Hence required numbers = 209 − 15 = 194.

1.26. Ordered and Unordered Partitions

If $S = A_1 \cup A_2 \cup \ldots\ldots \cup A_k$, where $A_i \cap A_j = \phi$ if $i \ne j$

and $|A_i| = q_i$, $q_1+q_2+\ldots\ldots+q_k = n = |S|$. Then $(A_1, A_2, \ldots\ldots, A_k)$ is called an ordered partition of S of type $(q_1, q_2, \ldots\ldots, q_k)$.

If the order of $A_1, A_2, \ldots\ldots, A_r$ is not material in the above it is called an unordered partition of S.

1.27. The number of ordered partitions of S of type $(q_1, q_2, \ldots\ldots, q_k) = \dfrac{n!}{q_1!\,q_2!\ldots\ldots q_k!}$, where $n = q_1+q_2+\ldots\ldots+q_k$.

Remark : The number of unordered partitions is more complex. However of we want all the parts to have the same number of elements, then it is easy and is given by the next theorem.

1.28. Let S be a set with $n = q\,k$ elements. Then the number of unordered partition of S of the type $(q, q, \ldots\ldots, q)$ is given by $\dfrac{n!}{k!\,(q!)^k}$.

Proof. This follows from the above theorem

Since each unordered partition give rise to $k!$ ordered partitions of the types $(q, q, \ldots, q)$ so

$k!$ (Required no. of partitions) $= \dfrac{n!}{q!q!\ldots.q!} = \dfrac{n!}{(q!)^k}$

$\therefore$ Required no. of partitions $= \dfrac{n!}{k!(q!)^k}$.

Example 1. In how many ways an 12 out of 14 people be distributed into 3 terms of which the first team has 3 members, 2nd team has 5 and the 3rd team has 4 members.

Sol. Let $S = A_1 \cup A_2 \cup A_3$, where $|A_1| = 3, |A_2| = 5, |A_3| = 4$.

$|S| = 3 + 5 + 4 = 12$

The number of ordered partitions of S of type $(3, 5, 4) = \dfrac{12!}{3!5!4!}$

Also the 12 person can be choosen out of 14 peoples in C (14, 12) ways

$\therefore$ Total number of ways $= C(14, 12) \cdot \dfrac{12!}{3!5!4!}$

Example 2. Find the number of ways of choosing 12 out of 14 persons to form 3 teams of 4 each.

Sol. Here $S = A_1 \cup A_2 \cup A_3$, where $|A_1| = |A_2| = |A_3| = 4$ and $|S| = 3 \times 4 = 12$

$\therefore$ The number of unordered partition of S of type $(4, 4, 4) = \dfrac{12!}{(4!)^3}$.

Also the 12 person can be choosen out of 14 persons in C (14, 12) ways

$\therefore$ Total number of ways $= C(14, 12) \cdot \dfrac{12!}{(4!)^3}$.

2

PIGEONHOLE PRINCIPLE

. The Pigeonhole Principle (Simple Form)

If n pigeons are assigned to m pigeonholes and $m < n$, then there is at least one pigeonhole that tains two or more pigeons.

oof : Label n pigeons with the numbers 1 to n and m pigeonholes with the numbers 1 to m. Starting with eon 1 and pigeonhole 1, assign each pigeon in order to the pigeonhole with the same number. So we can gn as many pigeons as possible to distinct pigeonholes. Since the number m of pigeonholes is less than number n of the pigeons, so $n - m$ pigeons are left that are not assigned to a pigeonhole. Therefore, there least one pigeonhole that will be assigned one or more than one pigeon again.

∴ there is at least one pigeonhole that contains two or more pigeons.

mple 1. Show that if eight people are in the room, at least two of them have birthday that occur on e day of the week.

Total number of persons = 8

Total number of days in week = 7

Consider persons as pigeons and days as pigeonholes. As number of pigeons is more so at least two ons will have same pigeonholes i.e. at least two persons will have birthday on same day of week.

mple 2. Use Pigeonhole Principle to show that if seven numbers from 1 to 12 are chosen, then two of will add upto 13.

The sets which add upto 13 are {1 , 12 }, {2, 11} , {3, 10}, {4, 9}, {5, 8} {6, 7}.

By Pigeonhole principle, if we have to choose seven numbers then we must take at least two numbers nging to one set. Thus two of the seven numbers will definitely add upto 13.

mple 3. Use Pigeonhole Principle to prove that an injection cannot exist between a finite set A and a e set B if Cardinality of A is greater than Cardinality of B.

Let $n(A) = a$ $n(B) = b$ where $a > b$

Consider elements of Set B as pigeonholes and elements of set A as pigeons. As no. of pigeons are e than pigeon holes so at least two pigeons will have same pigeonholes or we can say $\exists\ x, y \in A$ such $f(x) = f(y)$. But $x \neq y$.

So $f: A \to B$ is not injective.

mple 4. Show that if any five numbers are chosen from 1 to 8, two of them will add upto 9.

The sets which add upto 9 are {1,8} {2,7} {3,6} {4,5}. By Pigeonhole principle, if we have to choose umbers then we must take atleast two numbers belonging to one set..... thus two of five numbers will itely add upto 9.

Example 5. Show that any 11 numbers chosen from the set {1, 2, 3, 4 ..... 18, 19, 20} then one will be multiple of other

Sol. Each number can be represented by $(2^m) \times n$ where n is odd.

So now as there are only 10 odd numbers between 1 to 20, if we select 11 numbers from the set 1, 2, 3, ..., 18, 19, 20 then by Pigeon Hole Principle two of them are bound to have same odd part. Hence one of them can be divide by other. Hence proved.

Example 6. If seven points are chosen in a regular hexagon each of side 1 units then two of them must be no farther apart than 1 unit.

Sol. We must find the pigeons and the pigeonholes... So divide the hexagon into six equal regions. Each will be an equilateral triangle of length of each side as one unit. Now these are our pigeonholes and the points as our pigeons. So by Pigeon Hole Principle two points will be in the same triangle. Thus they will be at a distance less than one unit. Hence Prove.

Example 7. Shirts are numbered 1 to 20 are to be worn by the 20 members of a bowling league. When any three of three of these shirts are chosen, the league proposes to use the sum of their shirts as a code number for the team. Show that if any eight are chosen from the 20 shirts, then from these eight shirts one may form atleast two different teams having the same code number.

Sol. Number of ways of choosing a code for any selected 8 shirts is C(8, 3) = 56 different teams. Now these are our pigeons and the pigeonholes are the number of options we have. That is it will range from (1 + 2 + 3) = 6 to (18 + 19 + 20) = 57. Thus we have only 52 option. So by Pigeon Hole Principle, atleast two of them will have the same team codes.

Example 8. Show that if seven positive integers are chosen, two of them will have same remainder when divided by 6.

Sol. Seven positive integers divided by 6 will have seven remainders from 0 to 5. According to pigeonhole rule, two of these seven remainders will be same.

2.2. Pigeonhole Principle (Extended Form)

If n pigeons are assigned m pigeonholes, where n is sufficiently large as compared to m, then one of the pigeonholes must contain at least $\left[\frac{n-1}{m}\right]+1$ pigeons.

Proof : Assume that the result is false

$\therefore$ each pigeonhole does not contain more than $\left[\frac{n-1}{m}\right]$ pigeon.

$\therefore$ maximum possible number of pigeons $= \left[\frac{n-1}{m}\right] m \leq \frac{n-1}{m} \cdot m = n - 1$

This contradicts the given result that number of pigeons is n.

$\therefore$ our supposition is wrong.

Hence the result.

Example 9. Show that if 9 colours are used to paint 1000 houses, at least 112 houses will be of the same colour

Sol. Let n denote the number of given houses and m denote the number of colours.

Here $n = 1000, m = 9$

$$\therefore \left[\frac{n-1}{m}\right] + 1 = \left[\frac{1000-1}{9}\right] + 1 = \left[\frac{999}{9}\right] + 1 = 111 + 1 = 112$$

$\therefore$ at least 112 houses will be of the same colour.

Example 10. How many people among 200000 people are born at same time (hour, minute, seconds) ? Use Pigeonhole principle to find it.

Sol. Total number of persons = 200000

Total number of seconds in a day = $24 \times 60 \times 60 = 86{,}400$

Here, we have to assign a time to each person

So persons are like pigeons time is like pigeonhole.

Number of pigeons (n) = 200000

Number of pigeonholes (m) = 86,400

$$\text{Min. number of persons having same birthday} = \left[\frac{n-1}{m}\right] + 1 = \left[\frac{200000-1}{86400}\right] + 1$$

$$= \left[\frac{1{,}99{,}999}{86400}\right] + 1 = 2 + 1 = 3.$$

Example 11. Of any 26 points within a rectangle 20 cm by 15 cm, show that at least two are within 5 cm of each other.

Sol. Area of rectangle = $20 \times 15 = 300$ cm^2

Divide rectangle into 25 small rectangles of 4 cm × 3 cm. Then minimum number of points which are on or inside the smaller rectangle

$$= \left[\frac{26-1}{25}\right] + 1 = 2.$$

These points are far apart it they lie on ends of diagonal of smaller rectangle and length of diagonal is $\sqrt{4^2 + 3^2} = 5$ cm.

2.3. Third Form of Pigeonhole Principle

If the average of n positive numbers is k, then at least one of the numbers is greater than or equal to k. Further, at least one of the numbers is less than or equal to k.

Proof : Let $a_1, a_2, ..., a_n$ be the n numbers such that $\dfrac{a_1 + a_2 + ... + a_n}{n} = k$

i.e. $a_1, a_2, ..., a_n = n\,k.$ ....(1)

Thus if each of the numbers $a_1, a_2, ..., a_n$ is less than k, then the sum of these numbers would be less than $n\,k$ which contradicts (1).

Hence at least one of the numbers $a_1, a_2, \ldots, a_n$ is greater than or equal to k.

Similarly if each of the numbers $a_1, a_2, \ldots, a_n$ is greater than km, then the sum of these numbers would be greater than $n\,k$ which again contradicts (1) so that there is at least one of the numbers which is less than or equal to k.

2.4. Pigeonhole Principle (Strong Form)

Let $q_1, q_2, \ldots, q_n$ be positive integers. If $q_1 + q_2 + \ldots + q_n - n + 1$ objects are put into n boxes, then either the 1st box contains at least q_1 objects, or the 2nd box contains at least q_2 objects, ..., the nth box contains at least q_n objects.

Proof : Suppose it is not true, that is, the ith box contains at most $q_i - 1$ objects, $i = 1, 2, \ldots, n$. Then the total number of objects contained in the n boxes can be at most

$$(q_1 - 1) + (q_2 - 1) + \ldots + (q_n - 1) = q_1 + q_2 + \ldots + q_n - n,$$

which is one less than the number of objects distributed. This is a contradiction.

The simple form of the pigeonhole principle is obtained from the strong form by taking $q_1 = q_2 = \ldots = q_n = 2$.

Then $q_1 + q_2 + \ldots + q_n - n + 1 = 2n - n + 1 = n + 1$

Cor: In elementary mathematics the strong form of the pigeonhole principle is most often applied in the special case when $q_1 = q_2 = \ldots = q_n = r$. In this case the principle becomes:

- If $n(r-1) + 1$ objects are put into n boxes, then at least one of the boxes contains r or more of the objects. Equivalently,
- If the average of n nonnegative integers $a_1, a_2, \ldots, a_n$ is greater than $r - 1$, *i.e.*

$\frac{a_1 + a_2 + \ldots + a_n}{n} > r - 1$, then atleast one of the integers is greater than or equal to r.

Example 12. A basket of fruit is being arranged out of apples, bananas, and oranges. What is the smallest number of pieces of fruit that should be put in the basket in order to guarantee that either there are at least 8 apples or at least 6 bananas or at least 9 oranges?

Sol. $8 + 6 + 9 - 3 + 1 = 21$

Example 13. Given two disks, one smaller than the other. Each disk is divided into 200 congruent sectors. In the larger disk 100 sectors are chosen arbitrarily and painted red; the other 100 sectors are painted blue. In the smaller disk each sector is painted either red or blue with no stipulation on the number of red and blue sectors. The smaller disk is placed on the larger disk so that the centers and sectors coincide. Show that it is possible to align the two disks so that the number of sectors of the smaller disk whose color matches the corresponding sector of the larger disk is at least 100.

Sol. We fix the larger disk first, then place the smaller disk on the top of the larger disk so that the centers and sectors coincide. These 200 ways to place the smaller disk in such a manner. For each such alignment, some sectors of the two disks may have the same color. Since each sector of the smaller disk will match the same color sector of the larger disk 100 times among all the 200 ways and there are 200 sectors in the smaller disk, the total number of matched color sectors among the 200 ways is $100 \times 200 = 20{,}000$. Note that there are only 200 ways. Then there is at least one way that the number of matched color sectors is $\frac{20{,}000}{200} = 100$ or more.

EXERCISE 2.1

1. Suppose there are n married couples. How many of the $2n$ people must be selected in order to guarantee that a married couple is selected ?
2. How may students there must be in a class to guarantee that at least two students receive the same marks in the final exam, if the maximum marks that one can obtain is 100 ?
3. Suppose there are three men and five women at a party. Show that if these people are lined up in a row then at least two women will be next to each other.
4. Show that it any five numbers from 1 to 8 are chosen, then two of them will add to 9.
5. Ten members of a club have ₹ 1001 in their pockets. Show that at least one of them must have at least ₹ 101 in his pocket.
6. How many people must you have to guarantee that at least 12 of them will have birthdays on the same day of the week ?
7. Show that if any 30 people are selected, then one may chose a subset of five so that all five were born on same day of week.
8. Show that if 30 dictionaries in a library contain a total of 61,327 pages, then one of the dictionaries must have at least 2045 pages.
9. How many friends must you have to guarantee so that at least five of them will have birthday in the same month ?
10. Describe in brief the Pigeonhole Principle with example.
11. State three forms of Pigeonhole Principle. Give an example of use of each form of the Pigeonhole principle.

ANSWERS

1. $n+1$ 2. 2 6. 78 9. 49

ADDITIONAL MATTER

Example 1. Let (x_i, y_i) $(1 \le i \le 5)$ be a set of five distinct points with integral coordinates in xy plane. Show that the mid-point of the line joining of at least one pair of these points has integral coordinates.

Sol. Since every integer is either even or odd, therefore, every point (x_i, y_i) can be put in one of the four pigeonholes

(odd, odd), (odd, even), (even, odd), (even, even).

By pigeonhole principle, at least two of the points, say $A(x_1, y_1)$ and $B(x_2, y_2)$, must lie in the same pigeonhole.

$\therefore$ x_1, x_2 both are of same parity (*i.e.* either both are even or both are odd) and y_1, y_2 also are of same parity.

$\Rightarrow$ $x_1 + x_2$ and $y_1 + y_2$ both are even $\Rightarrow$ $\frac{x_1+x_2}{2}$ and $\frac{y_1+y_2}{2}$ are integers.

Hence mid point of line joining $A(x_1, y_1)$ and $B(x_2 y_2)$ has integral coefficients.

Example 2. If 11 integers are selected from {1, 2, 3, ..., 100} then prove that there are at least two integers, say a and b, such that $0 < \left|\sqrt{a}-\sqrt{b}\right| < 1$.

Sol. Let $x \in S = \{1, 2, 3, ..., 100\}$.

Then $1 \le \sqrt{x} \le 10 \Rightarrow 1 \le [\sqrt{x}] \le 10$, where $[\sqrt{x}]$ is the integral part of $\sqrt{x}$.

Thus for elements x of S, $[\sqrt{x}]$ must be one of 1, 2, ..., 10.

Therefore, if 11 numbers are selected from S, then by pigeonhole principle, at least two of them, say a and b, must have same integral parts.

$\Rightarrow \quad \sqrt{a} = i + f_1$ and $\sqrt{b} = i + f_2$ where $0 \le f_1, f_2 < 1 \Rightarrow 0 < \left|\sqrt{a}-\sqrt{b}\right| = |f_1 - f_2| < 1$.

Hence the proof.

Example 3. Let n be an odd integer. If $i_1, i_2, ..., i_n$ is a permutation of 1, 2, ..., n then prove that $(1 - i_1)(1-i_2)...(1-i_n)$ is an even integer.

Sol. Let $n = 2m + 1$ where m is non-negative integer.

Then the set S = {1, 2, ..., n} contains $(m + 1)$ odd numbers, namely 1, 3, ..., $2m + 1$ and m even numbers, namely 2, 4, ..., $2m$.

$\therefore$ There are $(m + 1)$ odd numbers and m even numbers in the list $i_1, i_2, ..., i_n$.

Consider the $(m + 1)$ numbers

$$1 - i_1, \quad 3 - i_3, ..., \quad n - i_n. \qquad ...(1)$$

Since i_r $(1 \le r \le n)$ is even only for m values of r and there are $(m + 1)$ numbers in list (1), therefore, by pigeonhole principle, one of $i_1, i_3, ..., i_n$, say i_t, is odd.

$\therefore \quad t - i_t$ is even [$\because t$ is also odd]

Hence product $(1 - i_1)(2 - i_2) ....(n - i_n)$ is even.

Example 4. Prove that when a rational number $\frac{p}{q}$, in lowest form is expressed as a decimal then the decimal expression must be either terminating or recurring.

Sol. If decimal expression of $\frac{p}{q}$ is $x \cdot x_1 x_2 x_3$ ....

then
$$p = x\,q + r, \quad 0 \le r < q,$$
$$10\,r = x_1\,q + r_1, \quad 0 \le r_1 < q,$$
$$10\,r_1 = x_2\,q + r_2, \quad 0 \le r_2 < b$$
$$10\,r_2 = x_3 q + r_3, \quad 0 \le r_3 < b$$
.....
.....

Now if the decimal expression does not terminate, then we must obtain a non-zero remainder at each stage.

But there are only $q-1$ possible different non-zero remainders, therefore, by pigeonhole principle, therefore, some remainder must be repeated after at most q steps.

Hence the expression will recur from that point onwards.

Example 5. Given m integers $a_1, a_2, ..., a_m$, show that there exist integers k, s with $0 \le k < s \le m$ such that $a_{k+1} + a_{k+2} + ... + a_s$ is divisible by m.

Sol. Consider the sequence

$$a_1, a_1 + a_2, a_1 + a_2 + a_3, ..., a_1 + a_2 + ... + a_m.$$

If anyone of these m sums is divisible by m then we are through.

Otherwise, let none of these be divisible by m.

$\Rightarrow$ Each leaves a non-zero remainder 1, 2, ..., $(m-1)$.

Since there are m sums and $(m-1)$ possible values of the remainders, by pigeonhole principle two of the sums leave the same remainder after division by m.

$\therefore$ let $a_1 + a_2 + ... + a_k = bm + r$ ...(1)

and $a_1 + a_2 + ... + a_s = cm + r.$ ...(2)

Subtracting (1) from (2), we get

$$a_{k+1} + a_{k+2} + ... + a_s = m(c-b). \qquad [\because k < s]$$

Hence m divides $a_{k+1} + a_{k+2} + ... + a_s$.

Example 6. Among the integers 1, 2, ..., 200, if 101 integers are choosen then show that there will be two among the choosen such that one divides the other.

Sol. Let the 101 integers choosen among 1, 2, ..., 200 be

$n_i = 2^{\alpha_i} a_i$; $i = 1, 2, ..., 101$, where a_i is an odd number.

Now a_i is the greatest odd divisor of n_i, and it is one of the 100 odd numbers 1, 3, 5, ..., 199.

Thus by pigeonhole principle, among the choosen 101 numbers n_i, at least two have equal odd parts after removing the power of 2.

$\Rightarrow$ $\exists\ n_t = 2^{\alpha_t} a_t$ and $n_s = 2^{\alpha_s} a_s$ with $a_t = a_s$.

Then if $\alpha_t < \alpha_s$ then n_t divides n_s and if $\alpha_t > \alpha_s$ then n_s divides n_t.

Example 7. A storekeeper's list consists of 115 items, each marked "available" or "unavailable". Show that if there are 60 available items then there are at least 2 available items in the list exactly 4 items apart.

Sol. Let the positions of available items be $a_1, a_2, \ldots, a_{60}$.

Since $a_{60} \leq 115$, therefore, the 120 numbers

$$a_1 < a_2 < \ldots < a_{60} \quad \ldots(1)$$

and $$a_1 + 4 < a_2 + 4 < \ldots\ldots < a_{60} + 4 \quad \ldots(2)$$

lie between 1 and 119.

$\therefore$ By pigeonhole principle, two of the numbers in (1) and (2) must be equal.

But the numbers in (1) are all distinct and similarly numbers in (2) are all distinct. Hence some number in (1) must be equal to a number in (2).

$\Rightarrow$ $\exists$ some i, j for which $a_i = a_j + 4 \Rightarrow a_i - a_j = 4$, as required.

Example 8. Each student of a class of 27 students go swimming on some of the days from Monday to Friday in a certain week. If each student goes at least twice then show that there must be at least two students who go swimming on exactly the same days.

Sol. The set {Monday, Tuesday, ..., Friday} at 5 days has ${}^5C_2 + {}^5C_3 + {}^5C_4 + {}^5C_5 = 10 + 10 + 5 + 1 = 26$ subsets each containing 2 or more days. If we treat 27 students as pigeons and these 26 subsets as pigeonholes then by pigeonhole principle, at least one pigeonhole contains at least two pigeons *i.e.* at least two students must go swimming on the same days.

Example 9. Let $n \geq 3$ be an odd number. Show that there is a number in the set $\{2^1 - 1, 2^2 - 1, \ldots\ldots, 2^{n-1} - 1\}$ which is divisible by n.

Sol. Consider n numbers $2^0, 2^1, \ldots\ldots, 2^{n-1}$.

None of these numbers is divisible by n as n is odd.

Therefore these numbers can leave only $n-1$ different remainders namely $1, 2, \ldots, n-1$ when divided by n.

Thus by pigeonhole principle, two of these numbers, say, 2^r and 2^s where $0 \leq s < r \leq n-1$ will leave the same remainder when divided by n.

$\therefore$ $$n \mid 2^r - 2^s \Rightarrow n \mid 2^s(2^{r-s} - 1)$$

$\Rightarrow$ $$n \mid 2^{r-s} - 1. \qquad [\because (2^s, n) = 1]$$

Hence the result, because $2^{r-s} - 1$ is among the numbers

$$2^1 - 1, 2^2 - 1, \ldots\ldots, 2^{n-1} - 1.$$

Example 10. Let k be a given positive integer. Show that there exists a positive integer n such that $k \mid n$ and the only digits in n are 0's and 1's.

Sol. Consider $9k+1$ numbers $10^1, 10^2, ..., 10^{9k+1}$

These numbers when divided by $9k$, can leave only $9k$ different remainders namely $0, 1, ..., 9k-1$.

Thus by pigeonhole principle, two of these numbers, say 10^r and 10^s where $1 \le s < r \le 9k+1$ leave the same remainder when divided by $9k$.

$$\therefore \quad 9k \mid 10^r - 10^s$$

$$\Rightarrow \quad 10^r - 10^s = 9km \text{ for some } m \in Z$$

$$\Rightarrow \quad 10^s (10^{r-s} - 1) = 9km. \qquad ...(1)$$

Now the integer $10^{r-s} - 1$ consists of digit 9 only, therefore $n = 10^s\left(\frac{10^{r-s}-1}{9}\right)$ is an integer consisting of digits 0 and 1 and by (1), $k \mid n$.

Example 11. A chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day but, in order not to tire himself, he decides not to play more than 12 games during a week. Show that there exists a succession of days during which the chess master will have played exactly 21 games.

Sol. Let n_r be the number of total games played in the first r days.

Since at least one game is played each day, therefore the sequence of numbers

$$n_1, n_2, n_3, ..., n_{77}$$

is strictly monotonically increasing.

Moreover $n_1 \ge 1$ and because at most 12 games are played during any one week,

$$n_{77} \le 12 \times 11 = 132.$$

$$\therefore \quad 1 \le n_1 < n_2 < .....< n_{77} \le 132.$$

The sequence $n_1 + 21, n_2 + 21, ..., n_{77} + 21$ is also strictly monotonically increasing and

$$22 \le n_1 + 21 < n_2 + 21 < .....< n_{77} + 21 \le 153.$$

Thus each of the 154 numbers

$$n_1, n_2, ..., n_{77}, n_1 + 21, n_2 + 21, ..., n_{77} + 21$$

lie between 1 and 153.

$\therefore$ By pigeonhole principle, two of them are equal.

But no two of the numbers $n_1, n_2, ..., n_{77}$ are equal and no two of the numbers $n_1 + 21, n_2 + 21, ...$ $n_{77} + 21$ are equal.

$\Rightarrow$ $\exists\, i, j$ such that $n_i = n_j + 21$.

Hence on days $j+1, j+2, ..., i$, the chess master played a total of 21 games.

Example 12. Let numbers 1 to 20 be placed in any order around a circle. Prove that sum of some 3 consecutive numbers must be at least 32.

Sol. Let $a_1, a_2, ..., a_{20}$ be the numbers placed around circle.

Consider 20 sums

$$a_1+a_2+a_3,\ a_2+a_3+a_4,\ ....,\ a_{19}+a_{20}+a_1,\ a_{20}+a_1+a_2.$$

Mean of these sums $= \frac{1}{20}[3(a_1+a_2+....+a_{20})] = \frac{1}{20}[3(1+2+....+20)]$

$$= \frac{1}{20}\left[3\times\frac{20\times21}{2}\right] = 31\cdot5.$$

Hence by pigeonhole principle (third form), at least one of the sums must be ≥ 32.

Hence the proof.

Example 13. Let $\{a_1, a_2, ..., a_{1995}\}$ be a sequence of positive integers whose sum is 3989. Show that there exists a block of r successive a_i's ($r \geq 1$) whose sum is 95.

Sol. Let $S_r = a_1+a_2+....+a_r$; $1 \leq r \leq 1995$.

Then $1 \leq S_1 < S_2 < .....< S_{1995} = 3989$.

Let S_r's be distributed in 95 boxes labelled 0, 1, ..., 94 such that S_r is in the box j if j is the remainder obtained on dividing S_r by 95. We have two cases.

Case I : None of S_r is divisible by 95.

In this case the box labelled 0 is empty and all the 1995 S_r's are put in 94 boxes labelled 1, 2, ..., 94.

Hence by pigeonhole principle (second form), there is one box which contains at least 22 integers.

[$\because$ if all 94 boxes contain ≤ 21 integers then number of S_r's $\leq 21 \times 94 = 1974$]

Let $S_{i1} < S_{i2} < .....< S_{i22}$ be in the same box.

If $|S_{im} - S_{in}| = 95$, for some m, n then we are done.

Otherwise, $S_{i2} \geq S_{i1} + 2(95)$,

$S_{i3} \geq S_{i2} + 2(95) \geq S_{i1} + 4(95)$,

.....

.....

$S_{i22} \geq S_{i21} + 2(95) \geq S_{i1} + 42(95) \geq 3990$

which is a contradiction as $S_r \leq 3989\ \forall\ r$.

Hence there is a block of r successive a_i's ($r \geq 1$) whose sum is 95.

Case II : At least one of the S_i's is divisible by 95.

If there is one box which contains at least 22 integers then as in case I, we get a block of r successive a_i's ($r \geq 1$) whose sum is 95.

Otherwise, each box contains exactly 21 integers.

Let $S_{j1} < S_{j2} < \ldots\ldots < S_{j21}$ be in the box labelled 0.

If $S_{jk} = 95$ for some k or $|S_{jl} - S_{jm}| = 95$ for some l, m then we are done.

Otherwise, $S_{j2} \geq 2(95)$,

$S_{j2} \geq S_{j1} + 2(95) \geq 4(95)$,

.....

.....

$S_{j21} \geq S_{j20} + 2(95) \geq 42(95) \geq 3990$

which is a contradiction as $S_r \leq 3989 \ \forall r$.

Hence the proof.

Example 14. (Chinese remainder Theorem). Let m and n be co-prime integers and a, b be integers such that $0 \leq a \leq m-1$, $0 \leq b \leq n-1$. Then there exists a positive integer x such that when x is divided by m, we get remainder a and when x is divided by n, we get remainder b.

Sol. Consider n integers

$$a,\ m+a,\ 2m+a,\ \ldots,\ (n-1)m+a \qquad \ldots(1)$$

each of which gives remainder a when divided by m.

Let two of the integers in list (1) give the same remainder when divided by n.

$\Rightarrow$ $\exists\ 0 \leq i < j \leq n-1$ such that

$im + a = q_i n + r$ and $jm + b = q_j n + r$ for integers q_i, q_j.

$\Rightarrow$ $(im+a) - (jm+b) = (q_i n + r) - (q_j n + r) \Rightarrow (j-i)m = (q_j - q_i)n$

$\Rightarrow$ $n \mid (j-i)m$

$\Rightarrow$ $n \mid j-i$ $\quad [\because (m, n) = 1]$

which is not possible as $0 < j - i \leq n-1$.

Therefore, no two of the integers in the list (1) give the same remainder when divided by n.

$\therefore$ By pigeonhole principle each of n number 0, 1, ..., $n-1$ occurs as a remainder.

$\Rightarrow$ $\exists$ some $0 \leq p \leq n-1$ such that $pm + a$ gives the remainder b. $\quad [\because\ 0 \leq b \leq n-1]$

$\Rightarrow$ $x = pm + a$ gives remainder b when divided by n

$\Rightarrow$ $x = qn + b$ for some integer q.

Hence $x = pm + a$ and $x = qn + b$ *i.e.* x gives remainder a when divided by m and remainder b when divided by n.

Example 15. If 8 composite integers are selected from the first 360 natural numbers then show that there will always be two which are not relatively prime.

Sol. Let $n_1, n_2, \ldots\ldots, n_8$ be the eight composite numbers selected from the numbers 1, 2, 3, ..., 360.

Now $\forall\ 1 \leq i \leq 8$, $n_i \leq 360 < 361 = 19^2$.

Thus if p is the smallest prime divisor of any n_i, then

$$p \leq \sqrt{n_i} < 19.$$

But there are only 7 primes namely 2, 3, 5, 7, 11, 13, 17 which are less than 17.

Hence by pigeonhole principle, there are at least two n_i's which have a common prime divisor which means there are at least two composite numbers which are not relatively prime.

Example 16. If every point on a straight line is coloured with one of two colours then show that there is a segment whose ends and mid point have the same colour.

Sol. Let every point of the straight line be coloured with two colours red and black.

Then there exist 2 points, say A and B, with the same colour, say red.

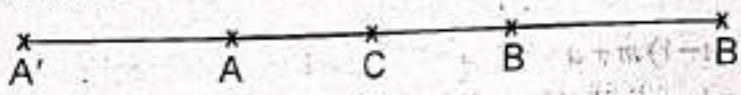
Let C be the mid-point of AB.

We have two cases

Case I : When C is red.

In this case ACB is the required segment.

Case II. When C is black.



In this case take point A′ on the A-side of C such that AA′ = AB and a point B′ on the B-side of C such that BB′ = AB.

If A′ and B′ both are black then A′C′B′ is required segment.

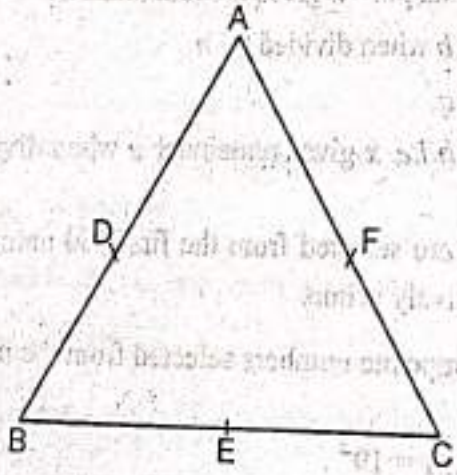
If A′ is red then A′AB is the required segment.

If B′ is red then ABB′ is the required segment.

Example 17. If the points of a plane are coloured in two colours then show that there exist three points of same colour which are vertices of an equilateral triangle.

Sol. Let the points of a plane be coloured with two colours red and black.

Then as in preceding example, there exists a segment ADB such that D is mid point of AB and A, D, B all are of same colour, say red.



Consider an equilateral triangle ABC.

Let E, F be the mid points of BC and AC respectively.

If E is red then ΔBDE is the required triangle.

If F is red then ΔADF is the required triangle.

If both E and F are blue, and C is red then ΔABC is required triangle.

If both E and F are blue, and C is blue then Δ CEF is the required triangle.

Example 18. Let S be any set containing ten 2-digit numbers. Show that there always exist 2 non-empty, disjoint subsets A and B such that sum of elements in A equals the sum of elements in B.

Sol. Let T be a non-empty subset of S and $s(T)$ denotes the sum of numbers in T.

Since the largest number in S is 99, therefore

$$s(T) \leq 90 + 91 + ... + 99 = 945.$$

But the number of non-empty subsets of $S = 2^{10} - 1 = 1023$.

Therefore by pigeonhole principle, there exist two distinct non-empty subsets A and B of S such that $s(A) = s(B)$.

If A and B are disjoint then they are the required subsets.

If $A \cap B \neq \phi$ then we remove the common part from each to get the required subsets.

Example 19. Show that every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of length $n + 1$ which is either monotonically increasing or decreasing.

Sol. Let $a_1, a_2, ..., a_{n^2+1}$ be a sequence of $n^2 + 1$ distinct real numbers.

Let there be no monotonically increasing subsequence of length $n + 1$.

For each $k = 1, 2, ..., n^2 + 1$, let l_k be the length of the longest monotonically increasing subsequence which begins with a_k.

Then $l_k \leq n \ \forall \ k = 1, 2, ..., n^2 + 1$.

$\Rightarrow$ $l_1, l_2, ..., l_{n^2+1}$ are $n^2 + 1$ integers lying between 1 and n.

$\therefore$ By strong form of pigeonhole principle, $n + 1$ of the numbers $l_1, l_2, ..., l_{n^2+1}$ are equal.

[See cor. of theorem 4.21]

Let $l_{k_1} = l_{k_2} = ... = l_{k_{n+1}}$ where $1 \leq k_1 < k_2 < ..... < k_{n+1} \leq n^2 + 1$. ...(1)

If possible let $a_{k_i} < a_{k_{i+1}}$ for some $i = 1, 2, ..., n$.

Then we can take longest monotonically increasing subsequence beginning with $a_{k_{i+1}}$ and put a_{k_i} in front to get monotonically increasing subsequence beginning with a_{k_i}.

$\Rightarrow \quad l_{k_i} > l_{k_{i+1}}$ for some $i = 1, 2, ..., n$

which contradicts (1).

$\therefore \quad a_{k_i} \geq a_{k_{i+1}} \quad \forall\, i = 1, 2, ..., n.$

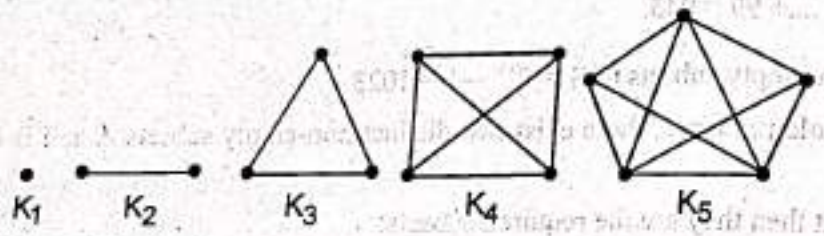
Hence $a_{k_1}, a_{k_2}, ..., a_{k_{n+1}}$ is a decreasing subsequence of length $n + 1$.

A Theorem of Ramsey

The most popular and easily understood instance of Ramsey's theorem is the following :

Example 20. Assume that in a group of six people, each pair of individuals consists of two friends or two enemies. Show that there are either three mutual friends or three mutual enemies in the group.

Sol. To prove the result, we define K_n as a set of n objects and all of the pairs of these objects. For example



picture of K_3 is that of a triangle.

We distinguish between friend pairs and enemy pairs by colouring edges red for friend and black for enemy. Three mutually friends now mean a K_3 each of whose edges a coloured red *i.e.* a red K_3. Similarly, three mutually enemies form a black K_3.

Let's formulate an expression

$$K_6 \rightarrow K_3, K_3$$

which means no matter how the edges of K_6 are coloured with the colour red and black, there is aiways a red K_3 or a black K_3 (*i.e.*a monochromatic triangle).

Now to prove $K_6 \rightarrow K_3, K_3$, let edges of K_6 be coloured red or black in any way. Consider one point P of K_6 where five edges meet. Since each of the five edges is coloured red or black, by strong form of pigeonhole principle, either at least 3 of them are coloured red or at least 3 of them are coloured black. Let 3 of the 5 edges meeting at P be red and these be PA, PB, PC.

Consider the edges which join A, B, C in pairs.

If all of these are black then A, B, C determines a black K_3.

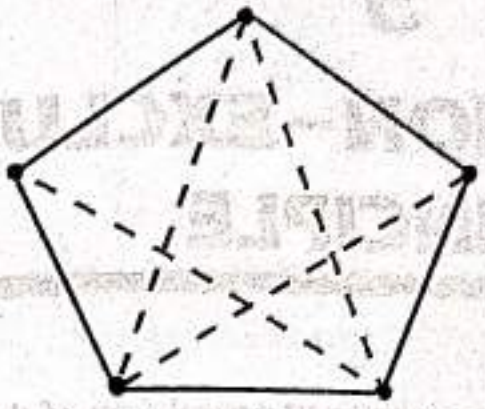
If one of them, say AB is red then P, A, B determines a red K_3.

Thus we are guaranteed to get a red K_3 or a black K_3.

Similarly if 3 of the 5 edges meeting at P are black then we will get a red K_3 or a black K_3.

Hence there are either three mutual friends or three mutual enemies in the group.

Remark 1. The expression $K_5 \to K_3, K_3$ is not true.



This can be shown by the pentagon whose solid edges are black and the dashed edges are red.

2. More generally, Ramsey's theorem, not in its full generality, states that if $m \geq 2$ and $n \geq 2$ are integers then there exists a positive integer p such that

$$K_p \to K_m, K_n$$

i.e. if the edges of K_p are coloured red or black then either there is a red K_m or there is a black K_n.

3. If $K_p \to K_m, K_n$ then $K_q \to K_m, K_n$ for any integer $q \geq p$.

Note : Ramsey Number : $r(m, n)$ is defined as the smallest integer p such that $K_p \to K_m, K_n$.

e.g. $r(3, 3) = 6$ as proved in above example and remark 1.

Example 21. Show that $r(2, n) = n = r(n, 2)$

Sol. If we colour the edges of K_n either red or black, then either some edge is coloured red (and hence we have a red K_2) or all edges are black (and hence we get a black K_2).

Then $r(2, n) \leq n$. ...(1)

Again if we colour all the edges of K_{n-1} black then we have neither red K_2 nor a black K_n.

Thus $r(2, n) > n - 1$ ...(2)

From (1) and (2), we get

$$r(2, n) = n.$$

By interchanging the colours red and black in above argument, we shall get

$$r(n, 2) = n.$$

Hence $r(2, n) = n = r(n, 2)$.

Remark : Ramsey's theorem generalizes to any number of colours according to which if n_1, n_2 and n_3 are integers greater than or equal to 2 then there exists an integer p such that

$$K_p \to K_{n_1}, K_{n_2}, K_{n_3}.$$

3

THE INCLUSION–EXCLUSION PRINCIPLE

3.1. The Inclusion–Exclusion Principle

The **principle of inclusion and exclusion** is the most general form of the addition principle for enumeration. Let A and B be two subsets of a set S, then to count the number of elements in $A \cup B$ is to count the number of elements of A and those of $B-A$ and add.

But $|B-A| = |B| - |A \cap B|$.

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

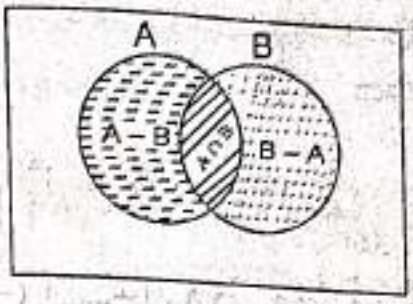
In other words, while counting elements of A and of B separately, elements common to both A and B are counted twice and so in order to nullify this double counting one has to remove $A \cap B$ count once from $|A| + |B|$.

We know that number of elements of a finite set A is denoted by $n(A)$ or $|A|$. Following results of number of elements should be kept in mind for doing problems :

1. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
2. $n(A \cup B) = n(A) + n(B) \Leftrightarrow$ A, B are disjoint sets.
3. $n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B)$
4. $n(A) = n(A - B) + n(A \cap B)$
5. $n(B) = n(B - A) + n(A \cap B)$
6. $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(C \cap A) + n(A \cap B \cap C)$
7. $n(A' \cup B') = n((A \cap B)') = n(U) - n(A \cap B)$
8. $n(A' \cap B') = n((A \cup B)') = n(U) - n(A \cup B)$
9. $n(A \cap B' \cap C') = n(A) - n(A \cap B) - n(A \cap C) + n(A \cap B \cap C)$

Proof : (1) We know that $A \cup B$ is the union of three disjoint sets

$A - B$, $A \cap B$ and $B - A$.



A – B is shaded like

A ∩ B is shaded like

B – A is shaded like

$\therefore \quad n(A \cup B) = n(A - B) + n(B - A) + n(A \cap B)$ ...(1)

Again A is union of A – B and A ∩ B

which are disjoint sets

$\therefore \quad n(A) = n(A - B) + n(A \cap B)$ ...(2)

Similarly $n(B) = n(B - A) + n(A \cap B)$ ...(3)

Adding (2) and (3), we get

$$n(A) + n(B) = n(A - B) + n(B - A) + 2n(A \cap B)$$
$$= [n(A - B) + n(B - A) + n(A \cap B)] + n(A \cap B)$$

$\therefore \quad n(A) + n(B) = n(A \cup B) + n(A \cap B)$ [$\because$ of (1)]

$\Rightarrow \quad n(A \cup B) = n(A) + n(B) - n(A \cap B)$

(2) Since A and B are disjoint sets

$\therefore \quad A \cap B = \phi \quad \Rightarrow \quad n(A \cap B) = 0$

$\therefore \quad n(A \cup B) = n(A) + n(B) - 0$

or $n(A \cup B) = n(A) + n(B)$.

(6) L.H.S. $= n(A \cup B \cup C) = n[(A \cup (B \cup C)] = n(A) + n(B \cup C) - n[A \cap (B \cup C)]$

$$= n(A) + n(B) + n(C) - n(B \cap C) - n[(A \cap B) \cup (A \cap C)]$$
$$= n(A) + n(B) + n(C) - n(B \cap C) - [n(A \cap B) + n(A \cap C) - n[(A \cap B) \cap (A \cap C)]$$
$$= n(A) + n(B) + n(C) - n(B \cap C) - n(A \cap B) - n(A \cap C) + n(A \cap B \cap C)$$

$\therefore n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(C \cap A) + n(A \cap B \cap C)$

3.2. General Principle of Inclusion – Exclusion

Let $A_1, A_2, \ldots A_n$ be n finite sets. Then

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Proof : We prove the result by induction on n.

For $n = 1$, the result is obviously true.

For $n = 2$, the result becomes

$$|A_1 \cup A_2| = \sum_{i=1}^{2} |A_i| - \sum_{i<j} |A_i \cap A_j|$$

i.e. $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

which is true.

Let the result be true for sets less than n.

Now $|A_1 \cup A_2 \cup \ldots \cup A_n| = |(A_1 \cup A_2 \cup \ldots \cup A_{n-1}) \cup A_n|$

$= |B \cup A_n|$ where $B = A_1 \cup A_2 \cup \ldots \cup A_{n-1}$

$= |B| + |A_n| - |B \cap A_n|$. ...(1)

By induction hypothesis,

$$|B| = |A_1 \cup A_2 \cup \ldots \cup A_{n-1}| = \sum_{i=1}^{n-1} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n-1} |A_i \cap A_j \cap A_k| - \ldots + (-1)^n (A_1 \cap A_2 \cap \ldots \cap A_{n-1}) \quad \ldots(2)$$

Also $|B \cap A_n| = |A_n \cap B|$

$= |A_n \cap (A_1 \cup A_2 \cup \ldots \cup A_{n-1})| = |(A_n \cap A_1) \cup (A_n \cap A_2) \cup \ldots \cup (A_n \cap A_{n-1})|$

$$= \sum_{1 \le i \le n-1} |A_n \cap A_i| - \sum_{1 \le i < j \le n-1} |A_n \cap A_i \cap A_j| + \ldots + \ldots + (-1)^n |A_n \cap A_1 \cap A_2 \cap \ldots \cap A_{n-1}| \quad \ldots(3)$$

Using (2) and (3) in (1), we get

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

llary 1. If $A_1, A_2, ..., A_n$ are subsets of a finite set S then number of elements of S not belonging to f the sets $A_1, A_2, ..., A_n$ is given by

$$|\bar{A}_1 \cap \bar{A}_2 \cap .... \cap \bar{A}_n| = \left|\bigcap_{i=1}^{n} \bar{A}_i\right| = |S| - \left|\bigcup_{i=1}^{n} A_i\right| \quad \text{[By De-Morgan's law]}$$

$$\text{i.e. } |\bar{A}_1 \cap \bar{A}_2 \cap .... \cap \bar{A}_n| = |S| - \sum_{i=1}^{n} A_i + \sum_{1 \le i < j \le n} |A_i \cap A_j|$$

$$- ..... + (-1)^n |A_1 \cap A_2 \cap .... \cap A_n|. \quad ...(4)$$

(4) is sometimes also called the **general principle of inclusion-exclusion.**

ILLUSTRATIVE EXAMPLES

mple 1. A computer company must hire 25 programmers to handle system programming jobs 40 programmers for application programming. Of those hired 10 will be expected to perform of both types. How many programmers must be hired ?

Let A denote the set of system programmers hired and B denote the set of applications grammers hired.

$\therefore$ $n(A) = 25, n(B) = 40, n(A \cap B) = 10$

Now $n(A \cup B) = n(A) + n(B) - n(A \cap B) = 25 + 40 - 10 = 55$

$\therefore$ 55 programmers must be hired.

mple 2. A sample of 80 people have revealed that 24 like cinema and 62 like television grammes. Find the number of people who like both cinema and television programmes.

Let A denote the set of people who like cinema and B denote the set of people who like vision programmes.

$\therefore$ $n(A) = 24, n(B) = 62, n(A \cup B) = 80$

Now $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

$\Rightarrow$ $80 = 24 + 62 - n(A \cap B) \Rightarrow n(A \cap B) = 24 + 62 - 80$

$\therefore$ $n(A \cap B) = 6$

$\therefore$ 6 people like both cinema and television programmes.

mple 3. In a school there are 20 teachers who teach mathematics or physics. Of these, 12 ch mathematics and 4 teach physics and mathematics. How many teach physics ?

Sol. Let M denote the set of teachers who teach mathematics and P denote the set of teachers w teach physics.

$\therefore \quad n(M \cup P) = 20, n(M) = 12, n(M \cap P) = 4$

Now $n(M \cup P) = n(M) + n(P) - n(M \cap P)$

$\Rightarrow \quad 20 = 12 + n(P) - 4 \Rightarrow n(P) = 20 - 12 + 4$

$\therefore \quad n(P) = 12$

$\therefore$ 12 teachers teach physics.

Example 4. There are 200 individuals with a skin disorder, 120 had been exposed to the chemic C_1, 50 to chemical C_2, and 30 to both the chemicals C_1 and C_2. Find the number of individua exposed to

(*i*) Chemical C_1 but not chemical C_2

(*ii*) Chemical C_2 but not chemical C_1

(*iii*) Chemical C_1 or chemical C_2

Sol. Let U denote the universal set consisting of individuals suffering from the skin disorder, denote the set of individuals exposed to the chemical C_1 and B denote the set of individua exposed to the chemical C_2.

$\therefore \quad n(U) = 200, n(A) = 120, \ n(B) = 50, \ n(A \cap B) = 30$

(*i*) Now $n(A) = n(A - B) + n(A \cap B)$

$\Rightarrow \quad 120 = n(A - B) + 30 \Rightarrow n(A - B) = 90$

$\therefore$ number of individuals exposed to chemical C_1 but not to chemical C_2 is 90.

(*ii*) Again $n(B) = n(B - A) + n(A \cap B)$

$\Rightarrow \quad 50 = n(B - A) + 30 \Rightarrow n(B - A) = 20$

$\therefore$ number of individuals exposed to chemical C_2 but not to chemical C_1 is 20.

(*iii*) The number of individuals exposed either to chemical C_1 or to chemical C_2

$= n(A \cup B) = n(A) + n(B) - n(A \cap B) = 120 + 50 - 30 = 140$

Example 5. A class has a strength of 70 students. Out of it 30 students have taken Mathemati and 20 have taken Mathematics but not Statistics. Find

(*a*) The number of students who have taken Mathematics and Statistics ?

(*b*) How many of them have taken Statistics but not Mathematics ?

Sol. Let M denote the set of students who have taken Mathematics, S the set of students wh have taken Statistics.

$\therefore$ $n(M) = 30,\ n(M \cap S^c) = 20,\ n(M \cup S) = 70$

Now $n(M) = n(M \cap S^c) + n(M \cap S) \Rightarrow 30 = 20 + n(M \cap S) \Rightarrow n(M \cap S) = 10$

Again $n(M \cup S) = n(M) + n(S) - n(M \cap S) \Rightarrow 70 = 30 + n(S) - 10 \Rightarrow n(S) = 50$

Also $n(S) = n(M \cap S) + n(M^c \cap S) \Rightarrow 50 = 10 + n(M^c \cap S) \Rightarrow n(M^c \cap S) = 40$

$\therefore$ number of students taken Mathematics and Statistics = 10

and number of students taken Statistics but not Mathematics = 40.

Example 6. In a group of 120 students studying computer course, 84 can program in 'Pascal' and 66 can program in 'C'. If 45 can program in both 'Pascal' and 'C', how many of the students cannot program in either of these languages ?

Sol. Let U denote the set of students in computer course, A denote the set of students of 'Pascal' programming and B denote the set of students of 'C' programming

$\therefore$ $n(A) = 84, n(B) = 66, n(A \cap B) = 45, n(U) = 120$

Now $n(A \cup B) = n(A) + n(B) - n(A \cap B) = 84 + 66 - 45 = 105$

Number of students who cannot program in either language

$= n((A \cup B)') = n(U) - n(A \cup B) = 120 - 105 = 15$

$\therefore$ there are 15 students who cannot program in either of these languages.

Example 7. In a town with a population of 3000 ; 2200 persons read The Tribune, 1000 read the Indian Express and 300 read both. How many read neither ?

Sol. Let U denote the set of population of town, T denote the set of people reading Tribune and I the set of people reading Indian Express.

$\therefore$ $n(U) = 3000, n(T) = 2200, n(I) = 1000, n(T \cap I) = 300$

Number of people reading neither paper $= n(T' \cap I') = n(T \cup I)'$

$= n(U) - n(T \cup I) = n(U) - [n(T) + n(I) - n(T \cap I)]$

$= n(U) - n(T) - n(I) + n(T \cap I) = 3000 - 2200 - 1000 + 300$

$= 3300 - 3200 = 100.$

Example 8. In a group of 50 persons, 14 drink tea but not coffee and 30 drink tea. Find

(*i*) How many drink both tea and coffee ?

(*ii*) How many drink coffee but not tea ?

Sol. Let T denote the set of persons drinking tea and C denote the set of persons drinking coffee.

$\therefore$ $n(T \cup C) = 50, n(T) = 30, n(T \cap C^c) = 14$

(*i*) Now $n(T \cap C^c) = n(T) - n(T \cap C)$

$\therefore \quad 14 = 30 - n(T \cap C) \quad \Rightarrow \quad (T \cap C) = 16$

$\therefore$ number of persons drinking both tea and coffee = 16

(*ii*) Also $n(T \cup C) = n(T) + n(C) - n(T \cap C)$

$\therefore \quad 50 = 30 + n(C) - 16$

$\therefore \quad n(C) = 36$

$\therefore$ number of persons drinking coffee but not tea

$= n(C \cap T^c) = n(C) - n(C \cap T) = n(C) - n(T \cap C) = 36 - 16 = 20$

Example 9. A town has a total population of 60000. Out of it 32000 read 'The Hindustan Times' paper and 35000 read 'Times of India' paper, while 7500 read both the newspapers. Indicate how many read neither the Hindustan Times nor Times of India.

Sol. Let U denote the set of population of town, H denote the set of people reading Hindustan Times and T the set of people of reading Times of India.

$\therefore \quad n(U) = 60000, n(H) = 32000, \ n(T) = 35000, n(H \cap T) = 7500$

Number of people reading neither Hindustan Times nor Times of India

$$= n(H' \cap T') = n(H \cup T)' = n(U) - n(H \cup T)$$

$$= n(U) - [n(H) + n(T) - n(H \cap T)] = 60000 - [32000 + 35000 - 7500]$$

$$= 60000 - 59500 = 500$$

Example 10. The students in dormitory were asked whether they had a dictionary (D) or a thesaurus (T) in their rooms. The results showed that 650 students had a dictionary, 150 did not have a dictionary, 175 had a thesaurus and 50 had neither dictionary nor a thesaurus. Find number of students who : (*i*) live in the dormitory, (*ii*) have both a dictionary and a thesaurus and (iii) have only a thesaurus.

Sol. Let A, B denote the sets of dictionary, thesaurus respectively.

$\therefore \quad n(A) = 650, n(A^c) = 150, n(B) = 175, \ n(A^c \cap B^c) = 50$

Now $n(U) = n(A) + n(A^c) = 650 + 150 = 800$

(*i*) Number of students living in dormitory $= n(A \cup B)$

$$= n(U) - n\left((A \cup B)^c\right) = 800 - n(A^c \cap B^c) = 800 - 50 = 750$$

(*ii*) Number of students having both a dictionary and a thesaurus

$$= n(A \cap B) = n(A) + n(B) - n(A \cup B) = 650 + 175 - 750 = 75$$

(*iii*) Number of students who have only a thesaurus

$$= n(B \cap A^c) = n(B) - n(B \cap A) = n(B) - n(A \cap B) = 175 - 75 = 100$$

Example 11. In a hostel 15 members take tea, 8 members take coffee and 6 members take milk. If 5 members take tea and coffee both, 4 members take tea and milk both and none of them take coffee and milk both or all the three beverages, find the number of members in the hostel, assuming that every member takes at least one or the other beverages.

Sol. Let T, C and M denote the set of members taking tea, coffee and milk respectively.

$\therefore$ $n(T) = 15,\ n(C) = 8,\ n(M) = 6,\ n(T \cap C) = 5,\ n(T \cap M) = 4,$

$n(C \cap M) = 0,\ n(T \cap C \cap M) = 0$

Number of members in the hostel $= n(T \cup C \cup M)$

$= n(T) + n(C) + n(M) - n(T \cap C) - n(C \cap M) - n(M \cap T) + n(T \cap C \cap M)$

$= 15 + 8 + 6 - 5 - 0 - 4 + 0 = 20$

Example 12. It is known that in university 60% of professors play tennis, 50% of them play bridge, 70% jog, 20% play tennis and bridge, 40% play bridge and jog and 30% play tennis and jog. If someone claimed that 20% professors jog and play tennis and bridge, would you believe his claim ? Why ?

Sol. Let T, B, J denote the sets of professors who play tennis, play bridge, jog respectively.

$\therefore$ % of professors playing tennis $= n(T) = 60$

% of professors playing bridge $= n(B) = 50$

% of professors jogging $= n(J) = 70$

Also $n(T \cap B) = 20,\ n(B \cap J) = 40,\ n(T \cap J) = 30$ and $n(T \cup B \cup J) = 100$

Now. $n(T \cup B \cup J) = n(T) + n(B) + n(J) - n(T \cap B) - n(B \cap J) - n(T \cap J) + (T \cap B \cap J)$

$\therefore$ $100 = 60 + 50 + 70 - 20 - 40 - 30 - n(T \cap B \cap J)$

$\therefore$ $n(T \cap B \cap J) = 100 + 20 + 40 + 30 - 60 - 50 - 70 = 10$

$\therefore$ 10% of professors jog and play tennis and bridge.

$\therefore$ if some one claims that 20% of them jog and play tennis and bridge, his claim is wrong.

Example 13. A survey of 500 television watchers produced the following information :

285 watch football, 195 watch hockey, 115 watch basketball, 45 watch football and basketball, 70 watch football and hockey, 50 watch hockey and basketball, 50 do not watch any of the three games.

How many watch all the three games ? How many watch exactly one of the three games ?

Sol. Let F, H, B denote the sets of viewers who watch football, hockey, basketball respectively.

$\therefore$ $n(F) = 285,\ n(H) = 195,\ n(B) = 115,\ n(F \cap B) = 45,$

$n(F \cap H) = 70,\ n(H \cap B) = 50,\ n(F \cup H \cup B)^c = 50$

Also total number of viewers = 500

Now $n(F \cup H \cup B)^c = 50$

$\Rightarrow 500 - n(F \cup H \cup B) = 50 \Rightarrow n(F \cup H \cup B) = 450$

$\Rightarrow n(F) + n(H) + n(B) - n(F \cap H) - n(H \cap B) - n(B \cap F) + n(F \cap H \cap B) = 450$

$\Rightarrow 285 + 195 + 115 - 70 - 50 - 45 + n(F \cap H \cap B) = 450 \Rightarrow n(F \cap H \cap B) = 20$

$\therefore$ number of viewers watching all the three games = 20.

Number of viewers watching football alone $= n(F \cap H^c \cap B^c)$

$= n(F) - n(F \cap H) - n(F \cap B) + n(F \cap H \cap B) = 285 - 70 - 45 + 20 = 190$

Number of viewers watching hockey alone $= n(H \cap F^c \cap B^c)$

$= n(H) - n(H \cap F) - n(H \cap B) + n(F \cap H \cap B) = 195 - 70 - 50 + 20 = 95$

Number of viewers watching basket- ball alone $= n(B \cap H^c \cap F^c)$

$= n(B) - n(B \cap H) - n(B \cap F) + n(F \cap H \cap B) = 115 - 50 - 45 + 20 = 40$

$\therefore$ number of viewers watching exactly one of the three games

$= 190 + 95 + 40 = 325$

Example 14. In a survey of 260 college students, the following data were obtained :

64 had taken a Mathematics course.

94 had taken a computer science course.

58 had taken a business course.

28 had taken both mathematics and business course.

26 had taken both mathematics and computer science course.

22 had taken both computer science and Business course.

14 had taken all three types of courses.

(*i*) How many students were surveyed who had taken none of the three types of courses?

(*ii*) Of the students surveyed, how many had taken only a computer science course ?

Sol Let A denote the set of Mathematics students,

B denote the set of computer science students

and C denote the set of Business course.

Let U denote the set of student surveyed.

$\therefore \quad n(A) = 64, n(B) = 94, n(C) = 58, n(U) = 260$

$n(A \cap B) = 26, n(B \cap C) = 22, n(A \cap C) = 28, n(A \cap B \cap C) = 14$

(i) Now $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$

$= 64 + 94 + 58 - 26 - 22 - 28 + 14 = 154$

$\therefore$ number of students who have not taken any one of the subjects

$= n((A \cup B \cup C)') = n(U) - n(A \cup B \cup C) = 260 - 154 = 106$

(ii) Number of students who have taken only computer science course

$= n(B) - n(B \cap A) - n(B \cap C) + n(A \cap B \cap C)$

$= 94 - 26 - 22 + 14 = 60$

Example 15. Suppose that 100 of the 120 mathematics students at a college take at least one of the languages French, German and Russian. Also suppose 65 study French,

20 study French and German,

45 study German,

25 study French and Russian,

42 study Russian,

15 study German and Russian,

(a) Find the number of students who study all three languages.

(b) Fill in the correct number of students in each of the eight regions of Venn diagram.

Here F, G and R denote the sets of students studying French, German and Russian respectively.

(c) Determine the number of students who study

(i) exactly one language

(ii) exactly two languages

Sol. Here $n(F) = 65$, $n(G) = 45$, $n(R) = 42$

$n(F \cap G) = 20$, $n(G \cap R) = 15$, $n(F \cap R) = 25$,

Since 100 students study at least one of the languages

$\therefore$ $n(F \cup G \cup R) = 100$

(a) Now $n(F \cup G \cup R) = n(F) + n(G) + n(R) - n(F \cup G) - n(G \cap R) - n(F \cap R) + n(F \cap G \cap R)$

$\therefore$ $100 = 65 + 45 + 42 - 20 - 15 - 25 + n(F \cap G \cap R)$

$\therefore$ $n(F \cap G \cap R) = 100 + 20 + 15 + 25 - 65 - 45 - 42$

$\therefore$ $n(F \cap G \cap R) = 8$

$\therefore$ eight students study all three languages.

(*b*) Number of students who study French and German but not Russian

$$= n(F \cup G) - n(F \cap G \cap R) = 20 - 8 = 12$$

Number of students who study German and Russian but not French

$$= n(G \cap R) - n(F \cap G \cap R) = 15 - 8 = 7$$

Number of students who study French and Russian but not German

$$= n(F \cap R) - n(F \cap G \cap R) = 25 - 8 = 17$$

Number of students studying only French

$$= n(F) - n(F \cap G) - n(F \cap R) + n(F \cap G \cap R) = 65 - 20 - 25 + 8 = 28$$

Number of students studying only German

$$= n(G) - n(G \cap R) - n(F \cap G) + n(F \cap G \cap R) = 45 - 15 - 20 + 8 = 18$$

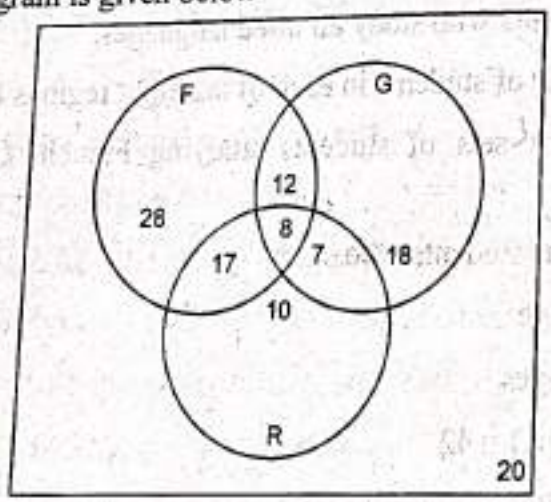
Number of students studying only Russian

$$= n(R) - n(F \cap R) - n(G \cap R) + n(F \cap G \cap R) = 42 - 25 - 15 + 8 = 10$$

Number of students who do not study any of the languages

$$= n((F \cap G \cap R)') = n(U) - n(F \cup G \cup R) = 120 - 100 = 20$$

$\therefore$ Venn Diagram is given below



(*c*) From Venn Diagram,

(*i*) number of students studying exactly one language = 28 + 18 + 10 = 56

(*ii*) number of students studying exactly two languages = 12 + 17 + 7 = 36

Example 16. Find the number of positive integer between 1 and 1000 which are divisible neither by 2 nor by 5.

Sol. Let A_1 and A_2 be sets of positive integers from 1 to 1000 which are divisible by 2 and 5 respectively.

Then $|A_1| = \left[\frac{1000}{2}\right] = 500$ and $|A_2| = \left[\frac{1000}{5}\right] = 200.$

Integers in the set $A_1 \cap A_2$ are divisible by both 2 and 5 and we know that an integer is divisible by both 2 and 5 iff it is divisible by *lcm* [2, 5] = 10.

$$\therefore \quad |A_1 \cap A_2| = \left[\frac{1000}{10}\right] = 100.$$

Thus, by inclusion–exclusion principle, the number of integers between 1 and 1000 which are divisible neither by 2 nor by 5

$$= |\overline{A}_1 \cap \overline{A}_2| = 1000 - (|A_1| + |A_2|) + |A_1 \cap A_2|$$
$$= 1000 - 500 - 200 + 100 = 400.$$

Example 17. Find how may integers between 1 and 60 are not divisible by 2 nor by 3 and nor by 5 ?

Sol. Let A, B and C be the set of integers between 1 and 60 divisible by 2, 3 and 5 respectively.

$$\therefore \quad n(A) = \left[\frac{60}{2}\right] = 30, \; n(B) = \left[\frac{60}{3}\right] = 20, \; n(C) = \left[\frac{60}{5}\right] = 12$$

and $$n(A \cap B) = \left[\frac{60}{2\times 3}\right] = 10, \; n(A \cap C) = \left[\frac{60}{2\times 5}\right] = 6, \; n(B \cap C) = \left[\frac{60}{3\times 5}\right] = 4$$

$$\therefore \quad n(A \cap B \cap C) = \left[\frac{60}{2\times 3\times 5}\right] = 2$$

Number of integers between 1 and 60 which are divisible by 2, 3 or 5 are

$$= n(A \cup B \cup C)$$
$$= n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$
$$= 30 + 20 + 12 - 10 - 6 - 4 + 2 = 44$$

$\therefore$ the number of integers between 1 and 60 that are not divisible 2, 3 or 5 = 60 – 40 = 16.

Example 18. Among integers 1 to 1000,

(*i*) How many of them are not divisible by 3 nor by 5 nor by 7 ?

(*ii*) How many are not divisible by 5 or 7 but divisible by 3 ?

Sol. Let A, B, C denote the set of numbers from 1 to 1000 that are divisible by 3, 5, 7 respectively.

$\therefore$ $n(A) = 333$, $n(B) = 200$, $n(C) = 142$

$n(A \cap B)$ = Numbers from 1 to 1000 divisible by 3 and 5 = 66

$n(B \cap C)$ = Numbers from 1 to 1000 divisible by 5 and 7 = 28

$n(A \cap C)$ = Numbers from 1 to 1000 divisible by 3 and 7 = 47

$n(A \cap B \cap C)$ = Numbers from 1 to 1000 divisible by 3, 5 and 7 = 9

Also $n(U) = 1000$, where U is the set of numbers from 1 to 1000

(*i*) $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$

$= 333 + 200 + 142 - 66 - 28 - 47 + 9 = 543$

Required numbers $= n(A^c \cap B^c \cap C^c) = n((A \cup B \cup C)^c) = n(U) - n(A \cup B \cup C)$

$= 1000 - 543 = 457$

$\therefore$ 457 numbers among 1 to 1000 are not divisible by 3 nor by 5 nor by 7.

(*ii*) Number of integers not divisible by 5 or 7 but divisible by 3

$= n(A \cap B^c \cap C^c) = n(A) - n(A \cap B) - n(A \cap C) + n(A \cap B \cap C)$

$= 333 - 66 - 47 + 9 = 229$

Example 19. Find the number of integers from 1 to 1000 which are divisible by none of 5, 6 and 8.

Sol. Let A_1, A_2, A_3 be the sets of integers from 1 to 1000 which are divisible by 5, 6 and 8 respectively.

Then $|A_1| = \left[\frac{1000}{5}\right] = 200,$

$|A_2| = \left[\frac{1000}{6}\right] = 166$ and $|A_3| = \left[\frac{1000}{8}\right] = 125.$

Integers in $A_1 \cap A_2$ are divisible by both 5 and 6 and *lcm* [5, 6] is 30.

$\therefore \quad |A_1 \cap A_2| = \left[\frac{1000}{30}\right] = 33.$

Similarly $|A_1 \cap A_3| = \left[\frac{1000}{40}\right] = 25,$ [$\because$ *lcm* [5, 8] = 40]

$|A_2 \cap A_3| = \left[\frac{1000}{24}\right] = 41$ [$\because$ *lcm* [6, 8] = 24]

and $|A_1 \cap A_2 \cap A_3| = \left[\frac{1000}{120}\right] = 8.$ [$\because$ *lcm* [5, 6, 8] = 120]

$\therefore$ By inclusion–exclusion principle, the number of integers from 1 to 1000 which are divisible by none of 5, 6 and 8

$= |\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3|$

$= 1000 - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) - |A_1 \cap A_2 \cap A_3|$

$= 1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = 600.$

Example 20. Find the number of positive integers from 1 to 500 which are
(*i*) divisible by at least one of 3, 5 and 7 (*ii*) divisible by 3 and 5 but not by 7
(*iii*) divisible by 3 but not by 5 and 7.

Sol. Let A_1, A_2 and A_3 be the sets of integers from 1 to 500 which are divisible by 3, 5 and 7 respectively.

Then $$|A_1| = \left\lfloor \frac{500}{3} \right\rfloor = 166,$$

$$|A_2| = \left\lfloor \frac{500}{5} \right\rfloor = 100,$$

$$|A_3| = \left\lfloor \frac{500}{7} \right\rfloor = 71,$$

$$|A_1 \cap A_2| = \left\lfloor \frac{500}{lcm[3,5]} \right\rfloor = \left\lfloor \frac{500}{15} \right\rfloor = 33,$$

$$|A_1 \cap A_3| = \left\lfloor \frac{500}{lcm[3,7]} \right\rfloor = \left\lfloor \frac{500}{21} \right\rfloor = 23,$$

$$|A_2 \cap A_3| = \left\lfloor \frac{500}{lcm[5,7]} \right\rfloor = \left\lfloor \frac{500}{35} \right\rfloor = 14$$

and $$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{500}{lcm[3,5,7]} \right\rfloor = \left\lfloor \frac{500}{105} \right\rfloor = 4.$$

(*i*) Number of integers from 1 to 500 which are divisible by 3, 5 and 7 $= |A_1 \cup A_2 \cup A_3|$

$$= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$= 166 + 100 + 71 - 33 - 23 - 14 + 4 = 271.$$

(*ii*) Number of integers from 1 to 500 which are divisible by 3 and 5 but not by 7

$$= |(A_1 \cap A_2) - A_3|$$

$$= |A_1 \cap A_2| - |A_1 \cap A_2 \cap A_3| \qquad [\because |A-B| = |A| - |A \cap B|]$$

$$= 33 - 4 = 29.$$

(*iii*) Number of integers from 1 to 500 which are divisible by 3 but not by 5 and 7

$$= |A_1 - (A_2 \cup A_3)|$$

$$= |A_1| - |A_1 \cap (A_2 \cup A_3)| \qquad [\because |A-B| = |A| - |A \cap B|]$$

$= |A_1| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)|$

$= |A_1| - [|A_1 \cap A_2| + |A_1 \cap A_3| - (A_1 \cap A_2) \cap (A_1 \cap A_3)]$

$= |A_1| - |A_1 \cap A_2| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3| = 166 - 33 - 23 + 4 = 114.$

EXERCISE 3.1

1. If X and Y are two sets such that X ∪ Y has 50 elements, X has 28 elements and Y ha 32 elements, how many elements does X ∩ Y have ?
2. If X and Y are two sets such that $n(X) = 17$, $n(Y) = 23$, $n(X \cup Y) = 38$, find $n(X \cap Y)$
3. In a group of students, 100 students know Hindi, 50 know English and 25 know both Each of the students knows either Hindi or English. How many students are there in the group ?
4. Let A and B be two finite disjoint sets such that $n(A \cup B) = 400$ and $n(A) = 325$, find $n(B)$
5. In a group of people, 50 speak both English and Hindi and 30 people speak English but not Hindi. All the people speak at least one of the two languages. How many people speak English ?
6. Let A and B be two finite sets such that $n(A - B) = 25$, $n(A \cup B) = 100$, $n(A \cap B) = 40$ Find $n(B)$.
7. In a class of 50 B.A. I students, 12 students have taken Economics, 8 have taken Economics but not Statistics. Find the number of students who have taken Economics and Statistics and those who have taken Statistics but not Economics.
8. In a class of 60 boys, there are 45 boys who play cards and 30 boys play carrom. How many boys play both games ? How many play cards only and how many play carrom only ?
9. In a class of 25 students, 12 have taken Economics, 8 have taken Economics but not History. Find the number of students who have taken Economics and History and those how have taken History but not Economics.
10. In a class of 53 M.A. (Eco.) students, 12 students have taken Econometrics, 8 have taken Econometrics but not Statistics. Find the number of students who have taken Econometrics and Statistics and those who have taken Statistics but not Econometrics.
11. In a joint family of 12 persons, 7 take tea, 6 take milk and 2 take neither. How many members take both tea and milk ?
12. (*a*) In a class of 30 students, 10 students take Mathematics, 15 take Physics and 10 take neither. How many students offer both subjects?

    (*b*) In survey of 600 students in a school, 150 students were found to be drinking Tea and 225 drinking Coffee, 100 were drinking both Tea and Coffee. Find how many students were drinking neither Tea nor Coffee.

13. A town has 100000 population, out of which 55000 read 'The Tribune' and 65000 read 'The Hindustan Times' while 25000 read both the newspapers. How many read neither the Tribune nor the Hindustan Times ?

14. In a town with a population of 3000 ; 2200 persons read The Tribune, 1000 read the Indian Express and 300 read both. How many read neither ?

15. In a group of 52 persons, 16 drink tea but not coffee and 33 drink tea. Find
   (*i*) How many drink tea and coffee both ?
   (*ii*) How many drink coffee but not tea ?

16. A class has a strength of 70 students. Out of it 30 students have taken Mathematics and 20 have taken Mathematics but not Statistics. Find
   (*a*) The number of students who have taken Mathematics and Statistics ?
   (*b*) How many of them have taken Statistics but not Mathematics ?

17. In certain examination, 53 percent students pass in Economics, 61% in Politics, 60% in History, 24% in Economics and Politics, 35% in Politics and History 27% in Economics and History and 5% passes in none of these subjects. How may students passed in all the three subjects ?

18. Each student in a class of 50, studies atleast one of the subject English, Mathematics and Physics. 36 study English, 32 Physics and 26 Mathematics 5 study English and Physics. 14 Mathematics and Physics and 2 English, Mathematics and Physics. Find the number of students who study (*i*) English and Mathematics (*ii*) English, Mathematics but not Physics.

19. In a class of 80 students, 50 students know English, 55 know French and 46 know German language. 37 students know English and French, 28 students know French and German, 7 students know none of the languages. Find out
   (*i*) How many students know all the 3 languages ?
   (*ii*) How many students know exactly 2 languages ?
   (*iii*) How many know only one language ?

20. In a survey it was found that 21 people liked product A, 26 liked product B and 29 liked products C. If 14 people liked products A and B; 12 people liked product C and A ; 14 people liked products B and C and 8 liked all the three products. Find how many liked product C only.

21. Out of 400 boys of a school, 112 played cricket, 120 played hockey and 168 played football. Of these, 32 played both football and hockey, 40 played cricket and football and 20 played cricket and hockey. 12 boys played all the games. How many boys did not play the game and how many played only one game ?

22. In a town of 10,000 families, it was found that 40% families buy newspaper A, 20% buy newspaper B and 10% buy newspaper C. 5 % families buy A and B, 3% buy B and C, and 4 % buy A and C. If 2% families buy all the newspapers, find the number of families which buy (*i*) A only (*ii*) B only (*iii*) none of A, B, and C.

23. In a survey of 60 people, it was found that 25 people read Newspaper H, 26 read Newspaper T, 26 read Newspaper I, 9 read both H and I, 11 read both H and T, 8 read both T and I, 3 read all three news papers. Find

(*i*) the number of people who read at least one of the newspapers.

(*ii*) the number of people who read exactly one newspaper.

24. In a survey of 100 persons, it was found that 28 read magazine A, 30 read magazine B, 42 read magazine C, 8 read both A and B, 10 read both A and C, 5 read both B and C, and 3 read all the three magazines. Find

(*i*) how many read none of the three magazines ?

and (*ii*) how many read magazine C only ?

25. A survey among 1000 people, 595 are democrats, 595 wear glasses and 550 like ice-cream. 395 of them are democrats who wear glasses, 350 of them are democrats who like ice-cream. 400 of them wear glasses and like ice-cream and 250 all the three.

(*a*) How many of them are not Democrats, do not wear glasses and do not like ice-cream ?

(*b*) How many of them are democrats who do not wear glasses and do not like ice-cream ?

26. One hundred students were asked whether they had taken course in any of three areas, sociology, anthropology and history. The results were

45 had taken sociology,

38 had taken anthropology,

21 had taken history,

18 had taken sociology and anthropology,

9 had taken sociology and history.

4 had taken history and anthropology and

23 had taken no courses in any of the three areas.

(*a*) Draw a Venn diagram that will show the results of the survey.

(*b*) Determine the number of students who had taken classes in exactly

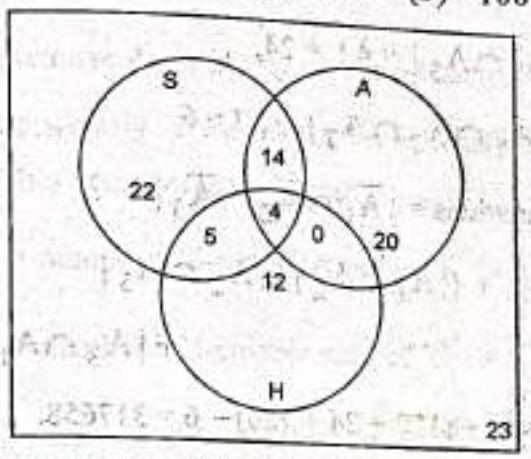
(*i*) one of the areas (*ii*) two of the areas.

27. Among integers 1 to 300, how many of them are divisible neither by 3, nor by 5, nor by 7? How many of them are divisible by 3 but not by 5, nor by 7 ?

28. How many integers between 1 and 2000 are divisible by 2, 3, 5 or 7 ?

ANSWERS

1. 10 **2.** 2 **3.** 125 **4.** 75 **5.** 80 **6.** 75
6. 75 **7.** 4; 38 **8.** 30; 15 **9.** 4; 13 **10.** 4; 41 **11.** 3
12. (*a*) 5 (*b*) 325 **13.** 5000 **14.** 100 **15.** (*i*) 17 (*ii*) 19
16. (*a*) 10 (*b*) 40 **17.** 7% **18.** (*i*) 27 (*ii*) 25
19. (*i*) 12 (*ii*) 54 (*iii*) 7 **20.** 11 **21.** 80 ; 64, 80, 108
22. (*i*) 3300 (*ii*) 1400 (*iii*) 4000 **23.** (*i*) 52 (*ii*) 30
24. (*i*) 20 (*ii*) 30 **25.** (*a*) 155 (*b*) 100 **26.** (*a*)



(*b*) (*i*) 54 (*ii*) 19

27. 162; 68 **28.** 1542

ADDITIONAL MATTER

Example 1. Find the number of permutations of the letters M, A, T, H, I, S , F, U, N such that none of the words MATH, IS and FUN occur as consecutive letters (*e.g.* the permutations MATHISFUN, INUMATHSF and ISMATHFUN and not allowed).

Sol. Let S′ be the set of all permutations of 9 letters given so that

$|S'| = 9! = 362880.$

Let A_1, A_2 and A_3 the sets which contains permutations in S′ with MATH as consecutive letters, IS as consecutive letters and FUN as consecutive letters respectively.

Then $|A_1|$ is equal to the number of permutations of six symbols

MATH, I, S, F, U, N

so that $|A_1| = 6! = 720.$

Similarly $|A_2| = 8! = 40320$ and $|A_3| = 7! = 5040.$

Again $|A_1 \cap A_2|$ is equal to the number of permutation of five symbols

MATH, IS, F, U, N ;

$|A_1 \cap A_3|$ is equal to the number of permutation of six symbols

MATH, I, S, FUN ;

$|A_2 \cap A_3|$ is equal to the number of permutation of six symbols

M, A, T, H, IS, FUN

and $|A_1 \cap A_2 \cap A_3|$ is equal to the number of permutations of 3 symbols

MATH, IS, FUN

so that $|A_1 \cap A_2| = 5! = 120$, $|A_1 \cap A_3| = 4! = 24$,

$|A_2 \cap A_3| = 6! = 720$ and $|A_1 \cap A_2 \cap A_3| = 3! = 6$.

Hence the required number of permutations $= |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3|$

$$= |S'| - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_2 \cap A_3| + |A_3 \cap A_1|) - |A_1 \cap A_2 \cap A_3|$$

$$= 362880 - (720 + 40320 + 5040) + (120 + 24 + 720) - 6 = 317658.$$

Example 2. Thirty cars were assembled in a factory. The options available with the car were a radio, an air conditioner and white-wall types. 15 cars have radios, 8 have air conditioners and 6 have white-wall tyres. Moreover 3 of them have all three options. Find at least how many cars do not have any option at all.

Sol. Let A_1, A_2 and A_3 be the sets of cars having option of radio, air conditioner and white wall tyres respectively.

Then $|A_1| = 15$, $|A_2| = 8$, $|A_3| = 6$ and $|A_1 \cap A_2 \cap A_3| = 3$.

Now $|A_1 \cap A_2| \geq |A_1 \cap A_2 \cap A_3| = 6$.

Similarly $|A_1 \cap A_3| \geq 6$ and $|A_2 \cap A_3| \geq 6$.

$$\therefore \quad |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

$$\leq 15 + 8 + 6 - 3 - 3 - 3 + 3 = 23.$$

$\therefore$ Not more than 23 cars have at least one option.

Hence minimum number of cars which do not have any option

$$= |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = 30 - |A_1 \cup A_2 \cup A_3| = 30 - 23 = 7.$$

3.3. Combinations with Repetition

Example 1. Find the number of 10-combinations of the multiset $T = \{3 \cdot a, 4 \cdot b, 5 \cdot c\}$.

Sol. Let S be the set of all 10-combination of the multiset

$T^* = \{\infty \cdot a, \infty \cdot b, \infty \cdot c\}$ so that

$|S| = {}^{10+3-1}C_{10} = {}^{12}C_{10} = 66.$

Let A_1 be the set of all 10-combination of T^* which contains more than 3 a's, A_2 be the set of all 10-combination of T^* which contains more than 4 b's and A_3 be the set of all 10-combinations of T^* which contains more than 5 c's.

To find $|A_1|$, if we remove 4 a's in any of the 10-combinations in A_1 then we are left with a 6-combination of T^* and conversely if we take a 6-combination of T^* add 4 a's to it, we get a 10-combination of T^* in which a occurs at least 4 times.

$\therefore$ $|A_1|$ = number of 6-combinations of $T^* = {}^{6+3-1}C_6 = {}^{8}C_6 = 28.$

Similarly $|A_2|$ = number of 5-combination of $T^* = {}^{5+3-1}C_5 = {}^{7}C_5 = 21$

and $|A_3|$ = number of 4-combination of $T^* = {}^{4+3-1}C_5 = {}^{6}C_4 = 15.$

Now the set $A_1 \cap A_2$ contains all 10-combinations of T^* in which a occurs at least 4 times and b occurs at least 5 times. If we remove 4 a's and 5 b's from any of these 10-combinations then we are left with 1-combination of T^* and conversely if to a 1-combination of T^*, we add 4 a's and 5 b's, we get a 10-combination in which a occurs at least 4 times and b occurs at least 5 times.

$\therefore$ $|A_1 \cap A_2|$ = number of 1-combinations of $T^* = {}^{1+3-1}C_1 = {}^{3}C_1 = 3.$

Similarly $|A_1 \cap A_3|$ = number of 0-combination of $T^* = {}^{0+3-1}C_0 = {}^{2}C_0 = 1$

and $|A_2 \cap A_3| = 0$ because there are no 10-combination in $A_2 \cap A_3$.

Also $|A_1 \cap A_2 \cap A_3| = 0.$

Hence by principle of inclusion-exclusion, the number of 10-combinations of multiset T

$$= |\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3| = |S| - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) - |A_1 \cap A_2 \cap A_3|$$

$$= 66 - (28 + 21 + 15) + (3 + 1 + 0) - 0 = 6.$$

Example 2. Find the number of integral solutions of $x_1 + x_2 + x_3 = 24$ subject to the conditions $1 \le x_1 \le 6$, $12 \le x_2 \le 18, -1 \le x_3 \le 12$.

Sol. Let $y_1 = x_1 - 1$, $y_2 = x_2 - 12$, $y_3 = x_3 + 1$.

Then given equation transforms to

$$y_1 + 1 + y_2 + 12 + y_3 - 1 = 24$$

or $y_1 + y_2 + y_3 = 12$. ...(1)

Let S be the set of all non-negative integral solutions of (1).

Then $|S| = {}^{12+3-1}C_{12} = {}^{14}C_{12} = 91$.

Let A_1, A_2, A_3 be the sets representing solutions (y_1, y_2, y_3) such that $y_1 \ge 5, y_2 \ge 7$ and $y_3 \ge 14$ respectively.

To find $|A_1|$, we again change the variables

$$z_1 = y_1 - 5,\ z_2 = y_2,\ z_3 = y_3$$

so that $|A_1|$ is same as the number of non-negative integral solutions of $z_1 + z_2 + z_3 = 7$.

$\therefore \quad |A_1| = {}^{7+3-1}C_7 = {}^{9}C_7 = 36.$

Similarly $|A_2| = {}^{5+3-1}C_4 = {}^{7}C_4 = 21$

and $|A_3| = 0$ because $y_3 \le 13$.

Now the set $A_1 \cap A_2$ contains all those solutions in S for which $y_1 \ge 5$ and $y_2 \ge 7$.

Let $u_1 = y_1 - 5,\ u_2 = y_2 - 7,\ u_3 = y_3$

so that $|A_1 \cap A_2|$ is same as the number of non-negative integral solutions of $u_1 + u_2 + u_3 = 0$.

$\therefore \quad |A_1 \cap A_2| = {}^{0+3-1}C_0 = 1.$

Similarly $|A_1 \cap A_3| = 0 = |A_2 \cap A_3|$.

To find $|A_1 \cap A_2 \cap A_3|$, let $v_1 = y_1 - 5, v_2 = y_2 - 7,$

$v_3 = z_3 - 14$ so that $|A_1 \cap A_2 \cap A_3|$ is same as the number of non-negative integral solution of $v_1 + v_2 + v_3 = -14$ and clearly no solution exists so that $|A_1 \cap A_2 \cap A_3| = 0$.

$\therefore$ Required number of solutions

$$= |\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3| = 91 - (36 + 21 + 0) + (1 + 0 + 0) - 0 = 35.$$

Example 3. Find the number of integral solutions of equation $x_1+x_2+x_3+x_4 = 18$ which satisfy $1 \le x_1 \le 5, -2 \le x_2 \le 4, 0 \le x_3 \le 5, 3 \le x_4 \le 9$.

Sol. Let $y_1 = x_1 - 1,\ y_2 = x_2 + 2, y_3 = x_3, y_4 = x_4 - 3$

so that given equation transforms to

$$y_1 + y_2 + y_3 + y_4 = 16. \qquad ...(1)$$

Let S be the set of all non-negative integral solutions of (1).

Then $|S| = {}^{16+4-1}C_{16} = {}^{19}C_{16} = 969.$

Let A_1 be the set containing solutions (y_1, y_2, y_3) such that $y_1 \ge 5$, A_2 be the set containing solution (y_1, y_2, y_3) such that $y_2 \ge 7$, A_3 be the set containing solutions (y_1, y_2, y_3) such that $y_3 \ge 6$ and A_4 be the set containing solutions (y_1, y_2, y_3) such that $y_4 \ge 7$.

To find $|A_1|$, we change the variables as

$$z_1 = y_1 - 5, \quad z_2 = y_2, \quad z_3 = y_3, \quad z_4 = y_4$$

so that $|A_1|$ is same as the number of non-negative integral solutions of $z_1 + z_2 + z_3 + z_4 = 11$.

$$\therefore \quad |A_1| = {}^{14}C_{11} = 364.$$

Similarly $|A_2| = {}^{12}C_9 = 220,$

$$|A_3| = {}^{13}C_{10} = 286 \quad \text{and} \quad |A_4| = {}^{12}C_9 = 220.$$

Now the set $A_1 \cap A_2$ contains all those solutions in S for which $y_1 \ge 5$ and $y_2 \ge 7$.

Let $u_1 = y_1 - 5, \ u_2 = y_2 - 7, \ u_3 = y_3, \ u_4 = y_4$

so that $|A_1 \cap A_2|$ is same as the number of non-negative integral solutions of $u_1 + u_2 + u_3 + u_4 = 4$.

$$\therefore \quad |A_1 \cap A_2| = {}^{7}C_4 = 35.$$

Similarly $|A_1 \cap A_3| = {}^{8}C_5 = 56, \ |A_1 \cap A_4| = {}^{7}C_4 = 35, \ |A_2 \cap A_3| = {}^{6}C_3 = 20,$

$$|A_2 \cap A_4| = {}^{5}C_2 = 10 \quad \text{and} \quad |A_3 \cap A_4| = {}^{6}C_3 = 20.$$

The intersection of any three of sets A_1, A_2, A_3, A_4 is empty.

$\therefore$ Required number of solutions $= |\overline{A}_1 \cap \overline{A}_2 \cap \overline{A}_3 \cap \overline{A}_4|$

$$= 969 - (364 + 220 + 286 + 220) + (35 + 56 + 35 + 20 + 10 + 20) = 55.$$

3.4. Derangements

A **derangement** of set $\{1, 2, ..., n\}$ of n elements is a permutation $i_1, i_2, ..., i_n$ of $\{1, 2, ..., n\}$ such that $i_1 \neq 1, i_2 \neq 2, ..., i_n \neq n$. Thus a derangement of $\{1, 2, ..., n\}$ is a permutation $i_1, i_2, ..., i_n$ of $\{1, 2, ..., n\}$ in which no integer is in its natural position.

We denote the number of derangements of $\{1, 2, ..., n\}$ by D_n.

3.5. For $n \geq 1$, prove that $\boxed{D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - ..... + (-1)^n \frac{1}{n!}\right)}$.

Proof : Let S denotes the set of all permutations of $\{1, 2, ..., n\}$ so that $|S| = n!$.

Let set A_i $(1 \leq i \leq n)$ contains those permutations of S in which i is in its natural position, for example, permutations in A_1 are of the form $1\ i_2\ i_3 .....i_n$ where $i_2, i_3, ..., i_n$ is a permutation of $\{2, 3, ..., n\}$.

$$\therefore \quad |A_i| = (n-1)! \quad \forall\ 1 \leq i \leq n.$$

The set $A_i \cap A_j$ $(1 \leq i < j \leq n)$ contains those permutations of S in which i and j are in their natural positions so that

$$|A_i \cap A_j| = (n-2)! \quad \forall\ 1 \leq i < j \leq n.$$

Continuing so on, in general for $1 \leq k \leq n$, we have

$$|A_{i1} \cap A_{i2} \cap ..... \cap A_{ik}| = (n-k)!$$

for any k-combination $\{i_1, i_2, ..., i_k\}$ of $\{1, 2, ..., n\}$.

Since there are ${}^nC_k$ k-combinations of $\{1, 2, ..., n\}$, therefore, by the principal of inclusion-exclusion, we have

$$D_n = n! - {}^nC_1 (n-1)! + {}^nC_2 (n-2)! - ..... + (-1)^n\ {}^nC_n\ 0!$$

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

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

Remark : We have $e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + ...$

$$\therefore \quad e^{-1} = \frac{D_n}{n!} + (-1)^{n+1}\frac{1}{(n+1)!} + (-1)^{n+2}\frac{1}{(n+2)!} + \dots,$$

$$\text{or} \quad e^{-1} - \frac{D_n}{n!} = (-1)^{n+1}\frac{1}{(n+1)!} + (-1)^{n+2}\frac{1}{(n+2)!} + \dots\dots$$

Since the series on R.H.S. is alternating series, therefore, the difference between e^{-1} and $\frac{D_n}{n!}$ is less than $\frac{1}{(n+1)!}$. It has been seen that e^{-1} and $\frac{D_n}{n!}$ agree to at least three decimal places for $n \geq 7$.

3.6. Prove that for $n \geq 3$, $D_n = nD_{n-1} + (-1)^{n-2}$.

Proof : The set D_n of derangements of $\{1, 2, ..., n\}$ can be partitioned into $n-1$ parts according to which of the integers 2, 3,...., n is in the first position of the permutation. Clearly, each such part will contain the same number of derangements.

$$\therefore \quad D_n = (n-1)d_n \qquad \dots(1)$$

where d_n is the number of derangement in which 2 is in the first position of the permutation.

Such derangements are of the form

$2\, i_2 i_3 \dots i_n$ where $i_2 \neq 2,\ i_3 \neq 3, ..., i_n \neq n$.

These d_n derangments can further be partitioned into two parts according as $i_2 = 1$ or $i_2 \neq 1$.

Let d_n' be the number of derangement of the form

$2\,1\, i_3\, i_4 \dots i_n$ where $i_3 \neq 3, ..., i_n \neq n$

and d_n'' be the number of derangements of form

$2\, i_2\, i_3\, i_4 \dots . i_n$ where $i_2 \neq 1,\ i_3 \neq 3, ..., i_n \neq n$.

$$\therefore \quad d_n = d_n' + d_n''. \qquad \dots(2)$$

From (1) and (2), we get

$$D_n = (n-1)(d_n' + d_n''). \qquad \dots(3)$$

Note that d_n' is same as the number of permutations $i_3\, i_4 \dots i_n$ of $\{3, 4, ..., n\}$ in which $i_3 \neq 3$, $i_4 \neq 4, ..., i_n \neq n$ *i.e.* d_n' is the number of derangements of $\{3, 4, ..., n\}$.

$\therefore \quad d_n' = D_{n-2}$.

Similarly d_n'' is equal to the number of derangements of $\{1, 3, ..., n\}$ so that

$$d_n'' = D_{n-1}.$$

From (3), (4) and (5), we have

$$D_n = (n-1)(D_{n-2} + D_{n-1})$$

$$\Rightarrow \quad D_n - nD_{n-1} = -[D_{n-1} - (n-1)D_{n-2}]. \quad \text{(6)}$$

The expression in the bracket on R.H.S. is same as the expression on L.H.S. with n replaced by $n-1$.

Thus we can apply (6) over and over again to get

$$D_n - nD_{n-1} = -[D_{n-1} - (n-1)D_{n-2}] = (-1)^2[D_{n-2} - (n-2)D_{n-3}]$$

$$= (-1)^3[D_{n-3} - (n-3)D_{n-4}]$$

.....

.....

$$= (-1)^{n-2}(D_2 - 2D_1)$$

$$= (-1)^{n-2}(1-0) \qquad [\because D_2 = 1, D_1 = 0]$$

$$= (-1)^{n-2}.$$

Hence $\boxed{D_n = nD_{n-1} + (-1)^n.}$

Example 1. Let n books be distributed into n students. Suppose that the books are returned and distributed to the students again later on. In how many ways can the books be distributed so that no student will get the some book twice ?

Solution. First time the books are distributed in $\lfloor n$ ways ; Since no student gets the some book that he got first time.

$\therefore$ second times the books are distributed in D_n ways

$\therefore$ Total number of ways $= \lfloor n \; D_n$

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

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

Example 2. A party is attended by 7 persons wearing hats which they left at counter. In how many ways can the hats be given back so that nobody receives his own hat ?

Sol. The numbers of ways in which 7 persons receive hats such that no one gets his own hat is equal to the number of derangements of $\{1, 2, 3, ..., 7\}$ *i.e.* D_7.

Now we find D_7.

We have, $$D_n = n!\left(1-\frac{1}{1!}+\frac{1}{2!}-....+(-1)^n\frac{1}{n!}\right)$$

$$\therefore \quad D_5 = 5!\left(1-1+\frac{1}{2}-\frac{1}{6}+\frac{1}{24}-\frac{1}{120}\right) = 44.$$

Also $D_n = n\,D_{n-1} + (-1)^n$

$$\therefore \quad D_6 = 6\,D_5 + (-1)^6 = 6 \times 44 + 1 = 265.$$

Thus $$D_7 = 7\,D_6 + (-1)^7 = 7 \times 265 - 1 = 1854.$$

Hence the number of ways in which 7 persons receive hats such that no one gets his own hat is 1854.

Example 3. There are n men and n women at a party. Find the number of ways in which n women can choose male partners for the first dance. How many ways are there for the second dance if everyone has to change partners ?

Sol. There are n ! possibilities for the first dance. For the second dance, each women has to choose a man partner other that the one with whom she danced first. The number of such possibilities is equal to number of derangements of $\{1, 2, ..., n\}$ *i.e.* D_n.

Example 4. A party is attended by n men and n women and every party-goers leaves his or her hat at the counter. In how many ways the hats be given back so that nobody receives his or her own hat but a man gets a male hat and a woman gets a female hat.

Sol. The number of ways in which n male hats can be given to n men such that nobody receives his own hat is D_n.

Similarly the number of ways in which n female hats can be given to n women such that nobody receives her own hat is D_n.

Hence by product rule, the required number of ways in $D_n \times D_n$.

Example 5. Obtain the Euler function $\phi(n)$ and the number of integers x such that $1 \le x < n$ and relatively prime to n.

Sol. Let $S = \{1, 2, 3, \ldots\ldots, n\}$. Let $p_1, p_2, \ldots\ldots, p_k$ be distinct prime divisors of n.

Write $A_i = \{x \in S : x \text{ is divisible by } p_i\}\ ; 1 \le i \le k$

The integers in S relatively prime to n are those in none of the subsets $A_1, A_2, \ldots\ldots, A_k$.

$$\therefore \quad \phi(n) = |\overline{A}_1 \cap \overline{A}_2 \cap \ldots\ldots \cap \overline{A}_k| = |S| - |A_1 \cup A_2 \cup \ldots\ldots \cup A_k|$$

If $d \mid n$ = then there are $\frac{n}{d}$ multiples of d in S

$$\therefore \quad |A_1| = \frac{n}{p_1}, |A_i \cap A_j| = \frac{n}{p_i p_j}, \ldots\ldots, |A_1 \cap A_2 \cap \ldots\ldots \cap A_k| = \frac{n}{p_1 p_2 \ldots\ldots p_k}$$

$\therefore$ By the principle of inclusion and exclusion

$$\phi(n) = n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{1 \le i\, j \le k} \frac{n}{p_i p_j} + \ldots\ldots + (-1)^k \frac{n}{p_1 p_2 \ldots\ldots p_k}$$

$$= n - \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots\ldots\ldots \left(1 - \frac{1}{p_k}\right)$$

MODULE-3

MODULE-3

1

LOGIC & PROPOSITIONAL CALCULUS

1.1. Introduction

Logic is the science of reasoning. It plays a vital role in any study involving reasoning. In fact it is a process by which we arrive at a conclusion from known statements with the use of laws of logic. The axiomatic approach to logic was first propounded by George Boole an Englishman. That is why logic relevant to mathematics *i.e.*, mathematical logic is called Boolean logic.

1.2. Definitions

Syntax : It is all about expressions : words and sentences.

Semantics : It is all about meanings of expressions.

Sentence : It is sensible combination of words.

Example : Number of positive integers is infinite.

Statement or proposition : A statement is a sentence in the grammatical sense conveying a situation which is neither imperative, interrogative nor exclamatory. It is a declarative sentence which is either true or false but not both. The truth or falseness of a statement is called its truth value.

The difference between an ordinary sentence and a logical statement is that whereas it is not possible to say about truth or otherwise of an ordinary sentence, it is an essential requirement for a logical statement. Now we consider some sentences and see whether they are logical statements, true or false.

(*i*) "3 + 3 = 8." This is a statement, but is a false statement. Its false value will denoted by the letter F or 0.

(*ii*) "Sun is a heavenly body." This is a statement and is a true statement. Its truth value is denoted by the letter T or 1.

(*iii*) "Why are you going to Bombay ?" This is not a statement as the sentence is not declarative.

(*iv*) "May God bless you with happiness !" This is not a statement because of the exclamation mark.

(*v*) "$(x-1)^2 = x^2 - 2x + 1$." This is a statement and its truth value is T or 1.

It should be noted that mathematical identity is always a statement.

(*vi*) Consider the sentence : $x + 5 = 10$. The truth of the sentence is open till we are told what x stands for. Such a sentence is called an open sentence. An open sentence is, thus, not a statement.

Note 1. Some authors define statement as : A statement is any meaningful, unambiguous, declarative sentence which is either true or false but not both.

Note 2. A statement cannot be true and false at the same time. This fact is known as the law of the **excluded middle**.

1.3. Logical Connectives and Compound Statements

Any statement whose truth or otherwise does not explicitly depend on another statement is said to be simple. For instance,

8 is an even number.

The set of real numbers is infinite are simple statements.

A compound statement is a combination of two or more simple statements.

The pharases or words which connect two simple statements are called *sentential connectives, logical connectives, logical operators or simply connectives*. Some of the connectives are "and", "or", "not", "if then", "if and only if".

When simple statements are combined to make compound statements, then simple statements are called **components**. Our problem is to determine the truth value of a compound statement from the truth values of their components.

Note. Simple statements are generally denoted by small letters $p, q, r, s, t, \ldots$

1.4. Truth Tables

It is a table giving the truth values of a compound statement. It has a number of columns (vertical lines), and rows (horizontal lines). The number of columns depends upon the number of simple statements and how involved are their relationships. The number of rows in a truth table depends only upon the number of simple statements. *In case of n statements there are* 2^n *rows.* The truth tables are very helpful in finding out the validity of a report.

1.5. Basic Logical Operations

There are three basic logical operations :

1. Conjunction
2. Disjunction
3. Negation

which correspond respectively to "and", "or" and "not".

Conjunction

Any two statements can be combined by the connective "and" to form compound statement called the "conjuction" of the original statements.

For example, consider the two statements :

He is practical. He is sensitive.

The conjuction is "He is practical and sensitive."

The conjuction will be true when both the statements will be true and false even if one of the components is false.

In symbols, two statements are denoted by p, q and their conjuction by $p \wedge q$. This is read is "p and q".

Rule. *$p \wedge q$ is true when both p and q are true.*

Truth Table

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

Examples

1. Let $p : 5 + 7 = 12$
   q : 2 is a prime number.
   $\therefore$ $p \wedge q$: $5 + 7 = 12$ and 2 is prime number.
   Now p is true and q is true
   $\therefore$ $p \wedge q$ is true.

2. Let p : Every even number is divisible by 2
   q : 12 is an odd number.
   $\therefore$ $p \wedge q$: Every even number is divisible by 2 and 12 is an odd number.
   Now p is true and q is false.
   $\therefore$ $p \wedge q$ is false.

Disjunction

Any two statements can be combined by the connective "or" to form a compound statement called the "disjunction" of the original statements.

For example, consider the two statements :

p : There is something wrong with the teacher

q : There is something wrong with the student.

Then $p \vee q$: There is something wrong with the teacher or with the student.

This 'or' is inclusive or, that is, there may be something wrong with the teacher or with the student or with both.

The disjunction will be false when both the components are false.

In symbols, the disjunction of two statements p and q is denoted by $p \vee q$. This is read as "p or q".

Rule : *$p \vee q$ is false when both p and q are false.*

Consider another two statements :

p : I shall watch the game on television

q : I shall go to college

$p \vee q$: I shall watch the game on television or go to college.

This is exclusive 'or', both p and q cannot happen together.

Exclusive OR or X-OR has the symbol $\overline{\vee}$.

Rule : $p \bar{\vee} q$ is true when either p or q is true, but not both.

Truth Table for $\vee$

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

Truth Table for $\bar{\vee}$

p	q	$p \bar{\vee} q$
T	T	F
T	F	T
F	T	T
F	F	F

Examples

1. Let $p : 5 < 12$

   $q : 8 + 3 = 12$

   $\therefore \quad p \vee q : 5 < 12$ or $8 + 3 = 12$

   Here p is true and q is false.

   $\therefore \quad p \vee q$ is true.

2. Let p : Every even integer is prime

   $q : 5 < 3$

   $\therefore \quad p \vee q$: Every even integer is prime or $5 < 3$.

   Now p is false and q is also false.

   $\therefore \quad p \vee q$ is false.

3. Let $p : 3 + 5 = 8$

   $q : 1 + 6 = 9$

   $\therefore \quad p \vee q = (3 + 5 = 8) \vee (1 + 6 = 9)$

   Now p is true and q is false.

   $\therefore \quad p \vee q$ is true.

Negation or Denial

To every statement, there corresponds a statement which is its negation. Negation refers to contradiction and not to a contrary statement. We should be very careful while writing the negation of the given statement. The best way is to put in the word "not" at the proper place or to put the phrase. "It is not the case that" in the beginning.

For example, if p stands for "He is a good student." Negation of p, denoted by $\sim p$ or $\neg p$ is either "He is not a good student" or "It is not the case that he is a good student." We cannot say that "He is a bad student" is the negation of p.

Rule. *If p is true, then $\sim p$ is false.*

and if p is false, then $\sim p$ is true.

Truth Table

p	$\sim p$
T	F
F	T

Note : Translating from English to Symbols

We should have the following points in mind while translating from English to Symbols.

1. In logic, the words "but" and "and" mean the same thing. Generally, "but" is used in place of and when the part of the sentence that follows is in some way unexpected.
2. The phrase neither p nor q means the same as not p and not q.

Example : You are given the following statements :

p : It is hot

q : It is sunny

Write each of the following sentences symbolically :

(*a*) It is not hot but it is sunny

(*b*) It is neither hot nor sunny

Sol. (*a*) The given sentence is equivalent to "It is not hot and it is sunny" which can be written symbolically as $\sim p \wedge q$.

(*b*) "It is neither hot nor sunny" means that it is not hot and it is not sunny. Therefore, the given sentence can be written symbolically as $\sim p \wedge \sim q$.

Note : Statement Variables

A "Statement form" or "Propositional form" is an expression made up of **statement variables** $\sim$, $\wedge$, $\vee$ that becomes a statement when actual statements are substituted for the component statement variable.

1.6. Tautologies and Contradictions (or Fallacies)

A tautology is a proposition which is true for all the truth values of its components. In a truth table of tautology there will be only T's in the last column.

(*a*) Truth Table

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

(*b*) Truth Table

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

Example : Consider the proposition $p \vee \sim p$. Its truth table is (*a*).

$\therefore$ the proposition is always true whatever be the truth value of its components.

$\therefore$ it is a tautology.

A contradiction (or fallacy) is proposition which is false for all truth values of its components.

Consider the proposition $p \wedge \sim p$. Its truth table is (*b*).

$\therefore$ $p \wedge \sim p$ is a contradiction.

Note : A compound proposition which can be either true or false depending on the truth values of its component propositions is called a **Contingency**.

Logically Equivalent

Two different compound propositions (or statement forms) are said to be **logically equivalent** if they have identical truth tables.

The symbol $\equiv$ is used for logical equivalence.

Example. Negation of the negation of a statement is equal to the statement.

Symbolically, $\sim(\sim p) \equiv p$.

Sol. **Truth Table**

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

Now truth values for p and $\sim(\sim p)$ are same and hence p and $\sim(\sim p)$ are logically equivalent. The logical equivalence $\sim(\sim p) \equiv p$ is called **involution law**.

Example : The sentences $p \to q$ and $\sim q \to \sim p$ are logically equivalent

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

$p \to q$

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

$\sim q \to \sim p$

$p \to q \equiv \sim q \to \sim p$.

1.7. Prove that

(*i*) $\sim(\sim p) = p$

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

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

...[De-Morgan's Laws]

Proof.

(*i*) Truth Table

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

A comparison of the first and third column shows that they are identical.

$\therefore \quad \sim(\sim p) = p$.

(*ii*) Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

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

(iii) Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

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

1.8. Prove that $(p \wedge q) \wedge r = p \wedge (q \wedge r)$ ...[Associative Law]

Proof.

Truth Table

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

A comparison of the last two columns show that they are identical.

Hence $(p \wedge q) \wedge r = p \wedge (q \wedge r)$.

1.9. Conditional Statement

Any statement of the form "if p then q", where p, q are statements, is called a conditional statement. Here p is sufficient for q but not essential. There can be q even without p.

Let p : you work hard

q : you will pass.

Now it is possible that a student may pass who has not worked hard. Although p is not necessary for q, q is necessary for p. It will not happen that one who works hard will not pass.

The conditional statement "if p then q" is denoted by $p \to q$ (to be read as p conditional q) or (p implies q).

The conditional $p \to q$ is also read as " if p then q" p implies q, p only if q, p is sufficient for q, q is necessary for p, q if p.

Rule. $p \to q$ is true in all cases except when p is true and q is false.

Truth Table

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

1.10. Prove that :

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

Proof.

(*i*) Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

$\therefore \quad p \to q = (\sim p) \vee q$

(*ii*) Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

$\therefore \quad \sim (p \to q) = p \wedge \sim q.$

1.11. Biconditional statement or equivalence

The statement "p if an only if q" is called a biconditional statement and is denoted by $p \leftrightarrow q$.

The biconditional is also read as

(*i*) q if and only if p

(*ii*) p implies q and q implies p

(*iii*) p is necessary and sufficient for q

(*iv*) q is necessary and sufficient for p

(*v*) p iff q

(*vi*) q iff p

Rule. $p \leftrightarrow q$

(*i*) . *true if both p and q have the same truth value i.e., either both are true or both are false.*

(ii) *false if p and q have opposite truth values.*

Truth Table

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

1.12. Prove that $(p \leftrightarrow q) \leftrightarrow r = p \leftrightarrow (q \leftrightarrow r)$

Proof.

Truth Table

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

The comparison of the last two columns shows that they are identical.

$\therefore \quad (p \leftrightarrow q) \leftrightarrow r = p \leftrightarrow (q \leftrightarrow r)$.

1.13. Precedence to Logical Operators

We formed formulas are fully paranthesised, so there is no ambiguity in their interpretition. Often, however, it is more convenient to omit some of the paranthesis for the sake of readability. *e.g.* we would prefer to write

$P \rightarrow Q \wedge R$ rather than

$(P \rightarrow ((\sim Q) \wedge R))$.

The syntax rules given below define what an expression means when some of the paranthesis are omitted. These conventions are analogous to those of elementary algebra, as well as most programming languages, where there is a precedure value that says

$a + b \times c$ means $a + (b \times c)$ rather than $(a + b) \times c$.

The syntax values for propositional logic are straightforward.

1. The most tightly binding operator is $\sim$. *e.g.* $\sim P \wedge Q$ means $(\sim P) \wedge Q$. Furthermore, $\sim P$ means $\sim (\sim P)$.

2. The second highest precedence is than $\wedge$ operator. In expressions combining $\wedge$ and $\vee$, the $\wedge$ operations comes first.

   e.g. $P \vee Q \wedge R$ means $P \vee (Q \wedge R)$.

   If there are several $\wedge$ operations in a sequence, they are performed left to right.

   e.g. $P \wedge Q \wedge R \wedge S$ means $(((P \wedge Q) \wedge R) \wedge S)$

3. The $\vee$ operator has the next level of precedence and it associates to the left.

4. The $\rightarrow$ operator has the next lower level of precedence.

   e.g. $P \wedge Q \rightarrow P \vee Q$ means $(P \wedge Q) \rightarrow (P \vee Q)$.

   The $\rightarrow$ operator associates to the right :

   thus $P \rightarrow Q \rightarrow R \rightarrow S$ means $(P \rightarrow (Q \rightarrow (R \rightarrow S)))$.

5. The $\leftrightarrow$ operator has the lowest level of precedence, and it associates to the right.

EXAMPLES

1. Let $p : 12 + 5 = 17$

   $q : 5 + 2 = 7$

   $\therefore$ $p \leftrightarrow q$: $12 + 5 = 17$ iff $5 + 2 = 7$

   Now p is true and q is true

   $\therefore$ $p \leftrightarrow q$ is true.

2. Let $p : 5 = 4$

   $q : 6 = 5$

   $\therefore$ $p \leftrightarrow q : 5 = 4$ iff $6 = 5$

   Now p is false and q is false

   $\therefore$ $p \leftrightarrow q$ is true.

3. Let p : Only one even integer is prime

   q : All odd integers are divisible by 5

   $\therefore$ $p \leftrightarrow q$: Only one even integer is prime iff all odd integers are divisible by 5.

   Now p is true and q is false.

   $\therefore$ $p \leftrightarrow q$ is false.

1.14. Laws of the Algebra of Propositions

Here 0 stands for contradiction, 1 for tautology.

Commutative Laws	
$p \vee q \leftrightarrow q \vee p$	$p \wedge q \leftrightarrow q \wedge p$
Associative Laws	
$(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$	$(p \wedge q) \wedge r \leftrightarrow p \wedge (q \wedge r)$

Distributive Laws

$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ $\quad p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

Identity Laws

$p \vee 0 \leftrightarrow p$ $\quad p \wedge 1 \leftrightarrow p$

Negation Laws

$p \wedge \sim p \leftrightarrow 0$ $\quad p \vee \sim p \leftrightarrow 1$

Idempotent Laws

$p \vee p \leftrightarrow p$ $\quad p \wedge p \leftrightarrow p$

Null Laws

$p \wedge 0 \leftrightarrow 0$ $\quad p \vee 1 \leftrightarrow 1$

Absorbtion Laws

$p \wedge (p \vee q) \leftrightarrow p$ $\quad p \vee (p \wedge q) \leftrightarrow p$

DeMorgan's Laws

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

Involution Laws

$\sim(\sim p) \leftrightarrow p$

1.15. Converse, Inverse and Contrapositive

If $p \to q$ is a direct statement, then

(*i*) $q \to p$ is called its converse (*ii*) $\sim p \to \sim q$ is called its inverse

and (*iii*) $\sim q \to \sim p$ is called its contrapositive.

Note Since $p \to q = \sim q \to \sim p$ and $q \to p = \sim p \to \sim q$

$\therefore$ contrapositive $\equiv$ direct statement and converse $\equiv$ inverse.

Note. If the direct statement is true, then its converse and inverse may or may not be true.

1.16. Duality

We know that *dual relationship* between 'line' and 'point' exists through the interchange of the words 'meet' and 'join'. For example :

'A line is the join of two points'

'A point is the meet of two lines'

Similarly there exists dual relationship in logic. We first interchange $\wedge$ and $\vee$.

For example :

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

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

EQUIVALENCE

Let S be a set of propositions and p, q be propositions generated by S. p and q are equivalent if $p \leftrightarrow q$ is a tautology. The equivalence of p and q is denoted by $p \leftrightarrow q$.

IMPLICATION

Let S be a set of propositions and p, q be propositions generated by S. p implies q if $p \rightarrow q$ is a tautology. $p \rightarrow q$ is written to indicate the implication.

1.17. Statement Patterns or Well-formed Formulas

If $p, q, r, \ldots$ are statements, which can be treated as variables, then any statement involving these statement and logical connectives $\wedge, \vee, \rightarrow, \leftrightarrow, \sim$ is called a statement pattern or a well formed formula.

Note. Brackets can be removed or introduced in statement patterns, but with care.

(i) $p \wedge (q \wedge r) = p \wedge q \wedge r$ (ii) $\sim(p \vee q) \neq \sim p \vee q$

ILLUSTRATIVE EXAMPLES

Example 1. For each of the following sentences, state whether it is a statement and indicate its truth value if it is a statement.

(i) $3 \times 5 + 4 = 19$.
(ii) Moon is not a heavenly body.
(iii) Today is Sunday.
(iv) Why are you smoking ?
(v) Do you like reading ?
(vi) Logic is a very interesting subject.
(vii) There are only 100 positive integers.
(viii) The sum of three angles of triangle is two right angles.
(ix) May God bless you with success !

Sol. (i) This is a true statement.

(ii) This is a false statement.

(iii) This is a statement which is true on Sunday but false on other days.

(iv) This is not a statement as the sentence is declarative.

(v) This is not a statement.

(vi) This is not a statement as it is an open sentence.

(vii) This is a false statement as the number of positive integers is infinite.

(viii) This is a true statement.

(ix) This is not a statement.

Example 2. You are given the following statements :

p : $5 \times 7 = 35$.

q : Moon is a heavenly body.

r : Jammu is the most populated city in India.

s : Food is necessary for life.

State the truth values of the followings :

(i) $p \wedge q, p \wedge r, p \wedge s, q \wedge r, q \wedge s, r \wedge s$. (ii) $p \vee q, p \vee r, p \vee s, q \vee r, q \vee s, r \vee s$.

Sol. Here p, q, s are true statements and r is false.

$\therefore$ (*i*) $p \wedge q, p \wedge s, q \wedge s$ are true and others are false.

(*ii*) All statements are true as there is only one false statement.

Example 3. Let p be the statement "the south-west monsoon is very good this year" and q be the statement "the rivers are rising". Give the verbal translation for (*i*) $p \vee \sim q$ (*ii*) $\sim (\sim p \vee \sim q)$.

Sol. (*i*) The south-west monsoon is very good this year but the rivers are not rising.

(*ii*) It is not true that the south -west monsoon is not very good or the rivers are not rising.

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

$\therefore$ the above verbal translation can also be written as : The south-west monsoon is very good this year and rivers are rising.

Example 4. Write the following statements in symbolic form and give their negations :

(*i*) If you work hard, you will get the first division. (*ii*) If it rains, he will not go to Kathua.

(*iii*) If Mahatma Gandhi was a saint then Sardar Patel was as iron man.

Sol. (*i*) Let the symbols for the statements be :

p : you work hard

q : first division

$\therefore$ the statements is $p \to q$

Its negation is $\sim(p \to q) = \sim(\sim p \vee q) = \sim(\sim p) \wedge \sim q = p \wedge \sim q$.

In words : Even if you work hard, you will not get first division.

(*ii*) Let p : It rains.

q : He will go to Kathua.

$\therefore$ symbolic expression is $p \to \sim q$

Its negation is $\sim(p \to \sim q) = \sim(p \to \sim q) = \sim(\sim p \vee \sim q)$

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

In words : Even if it rains , he will go to Kathua.

(*iii*) Let the symbols for the statements be :

p : Mahatma Gandhi was a saint

q : Sardar Patel was an iron man

$\therefore$ the statement is $p \to q$

Its negation is $\sim(p \to q) = \sim(\sim p \vee q) = \sim(\sim p) \wedge (\sim q)$

$= p \wedge \sim q$

In words : Even if Mahatma Gandhi was a saint man, Sardar Patel was not an iron man.

Example 5. Write the following statements in symbolic form :

"You can not ride the roller coaster if you are under 4 feet tall unless you are older than 16."

Sol p = "you can ride the roller coaster."

q = "you are under 4 feet tall."

r = "you are older than 16."

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

Example 6. Write the following statements in symbolic form

"Every student in this class has studied calculus."

Sol. $S(x) : x$ is in this class, $C(x) : x$ studied calculus

$\forall x(S(x) \rightarrow C(x))$

$\forall x\,(S(x) \wedge C(x))$ means "Every student is in this class and has studied calculus."

Example 7. Write the following statements in symbolic form

"Some student in this class has studied programming."

Sol. $S(x) : x$ is in this class, $P(x) : x$ studied programming.

$\exists\ x\,(S(x) \wedge P(x))$

Example 8. (*i*) Find the truth values of $\sim(\sim p \vee q)$ if p is true and q is false.

(*ii*) If p is true and q is false, find the truth values of $\sim(p \wedge \sim q)$.

Sol. (*i*) $\sim(\sim p \vee q) = \sim(\sim p) \wedge \sim q = p \wedge \sim q$

Now p is true and q is false

$\therefore$ p is true and $\sim q$ is true

$\therefore$ $p \wedge \sim q$ is true.

$\therefore$ truth values of $\sim(\sim p \vee q)$ is T.

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

Now p is true and q is false

$\therefore$ $\sim p$ is false and q is false.

$\therefore$ $\sim p \vee q$ is false.

Example 9. Determine which of the following statements are true or false :

(*i*) $[(6 < 8) \wedge (8 < 6)] \leftrightarrow 6 = 8$ (*ii*) $[(R \subseteq Q) \rightarrow (Q \subseteq R)] \rightarrow Q = R$

(*iii*) $[(\sqrt{2}$ is rational $) \vee (2$ is irrational$)] \rightarrow (1 = 0)$

Sol. (*i*) Let the symbols for the statements be

$p : 6 < 8$

$q : 8 < 6$

$r : 6 = 8$

$\therefore$ given statement is $(p \wedge q) \leftrightarrow r$

Now p is true and q is false

$\therefore$ $p \wedge q$ is false

Also r is false.

Now $p \wedge q$ is false and r is false.

$\therefore$ $(p \wedge q) \leftrightarrow r$ is true.

$\therefore$ $[(6 < 8) \wedge (8 < 6)] \leftrightarrow 6 = 8$ is true.

(ii) Let the symbols for the statements be

$p : \mathbf{R} \subseteq \mathbf{Q}$, $q : \mathbf{Q} \subseteq \mathbf{R}$

$r : \mathbf{Q} = \mathbf{R}$

$\therefore$ given statement is $(p \to q) \to r$

Now p is false, q is true and r is false.

$\therefore$ $p \to q$ is true.

$\therefore$ $(p \to q) \to r$ is false

$\therefore$ $[(R \subseteq Q) \to (Q \subseteq R)] \to Q = R$ is false.

(iii) Let the symbols for the statements be :

$p : \sqrt{2}$ is rational

$q : 2$ is irrational

$r : 1 = 0$

$\therefore$ given statement is $(p \vee q) \to r$

Now p is false, q is false and r is false.

$\therefore$ $p \vee q$ is false

$\therefore$ $(p \vee q) \to r$ is true.

$\therefore$ $[(\sqrt{2}$ is rational) $\vee$ (2 is irrational)$] \to (1 = 0)$ is true.

Example 10. Write down the truth table of the following statement :

$$[p \to (q \vee r)] \vee [p \leftrightarrow \sim r]$$

Sol.

Truth Table

p	q	r	$q \vee r$	$\sim r$	$p \to (q \vee r)$	$p \leftrightarrow \sim r$	$[p \to (q \vee r)] \wedge [p \leftrightarrow \sim r]$
T	T	T	T	F	T	F	F
T	F	T	T	F	T	F	F
F	T	T	T	F	T	T	T
F	F	T	T	F	T	T	T
T	T	F	T	T	T	T	T
T	F	F	F	T	F	T	F
F	T	F	T	T	T	F	F
F	F	F	F	T	T	F	F

Example 11. Prove that $p \leftrightarrow q = (p \wedge q) \vee (\sim p \wedge \sim q)$.

Sol.

Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

$\therefore \quad p \leftrightarrow q = (p \wedge q) \vee (\sim p \wedge \sim q)$.

Example 12. Prove that $(p \to r) \to (q \to s) = (p \wedge q) \to (r \vee s)$.

Sol.

Truth Table

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

A comparison of the last two columns in the truth table shows that they are identical.

$\therefore \quad (p \to r) \to (q \to s) = (p \wedge q) \to (r \vee s)$

Example 13. Prove that $p \to (q \wedge r) = (p \to q) \wedge (p \to r)$.

Sol.

Truth Table

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

A comparison of the fifth and eighth columns shows that they are identical.

$\therefore \quad p \to (q \wedge r) = (p \to q) \wedge (p \to r)$.

Example 14. Prove by means of a truth table that $p \leftrightarrow q = (p \to q) \wedge (q \to p)$.

Sol.

Truth Table

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

The like truth values of the last two columns prove the validity of the statement.

Example 15. Prove that $(p \wedge q) \to (p \vee q)$ is a tautology but $(p \vee q) \to (p \wedge q)$ is not.

Sol.

Truth Table

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

From the above table, it is clear that $(p \wedge q) \to (p \vee q)$ is a tautology while $(p \vee q) \to (p \wedge q)$ is not.

Example 16. Prove that $\{[(p \to q) \vee p] \wedge q\} \to q$ is a tautology.

Sol.

Truth Table

p	q	$p \to q$	$(p \to q) \vee p$	$[(p \to q) \vee p] \wedge q$	$\{[(p \to q) \vee p] \wedge q\} \to q$
T	T	T	T	T	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	T	F	T

From the above table, it is clear that $\{[(p \to q) \vee p] \wedge q\} \to q$ is a tautology.

Example 17. Prove that if $p \to q$ and $q \to r$ then $p \to r$.

Sol. Here we are given that $p \to q$, $q \to r$ and we have to prove that $p \to r$. The result will be established if we show that

$$[(p \to q) \wedge (q \to r)] \to (p \to r) \text{ is a tautology.}$$

Truth Table

p	q	r	$p \to q$	$q \to r$	$p \to r$	$(p \to q) \wedge (q \to r)$	$[(p \to q) \wedge q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	F	T	F	T	T	F	T
F	T	T	T	T	T	T	T
F	F	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	F	F	T	F	F	T
F	T	F	T	F	T	F	T
F	F	F	T	T	T	T	T

$\therefore$ if $p \to q$ and $q \to r$ then $p \to r$ $[\because [(p \to q) \wedge (q \to r)] \to (p \to r)$ is a tautology]

Example 18. Write down

(i) Contrapositive of $p \to \sim q$ (ii) Contrapositive of converse of $p \to \sim q$

(iii) Inverse of converse of $p \to q$.

Sol. (i) Contrapositive of $p \to \sim q$ is

$\sim(\sim q) \to \sim p = q \to \sim p$

(ii) Converse of $p \to \sim q$ is $\sim q \to p$

$\therefore$ contrapositive of $\sim q \to p$ is

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

$= \sim p \to q$

(iii) Converse of $p \to q$ is $q \to p$

Inverse of $q \to p$ is $\sim q \to \sim p$

Example 19. State the Converse and Contrapositive of the implication "If it snows tonight, then I will stay at home".

Sol. Let p : It snows tonight

q : I will stay at home.

Given statement is $p \to q$

Converse of statement is $q \to p$

i.e. "If I stay at home then it Snows tonight".

Contrapositive of statement is $\sim q \to \sim p$

i.e. "If I do not stay at home then It will not Snow tonight".

EXERCISE 1.1

1. Which of the following is a statement (or proposition) ? Justify your answer :
   (*i*) Listen to me, Krishna !
   (*ii*) 17 is a prime number.
   (*iii*) $x^2 + 5x + 6 = 0$.
   (*iv*) 6 has three prime factors.
   (*v*) Two non-empty sets have always a non-empty intersection.
   (*vi*) The real number x is less than 1.
   (*vii*) Two individuals are always related.
2. State the truth values of the following :
   (*i*) There are only finite number of rational numbers.
   (*ii*) $\sqrt{2}$ is a rational number.
   (*iii*) There is only one triangle apart from the triangles (congruent to it) with prescribed lengths for sides a, b, c with $a < b + c$.
   (*iv*) The quadratic equation $ax^2 + bx + c = 0, a \neq 0$, has always two real roots.
   (*v*) A triangle one of whose vertices lies on a circle and whose side opposite to this vertex is a diameter of the circle is a right angled triangle.
   (*vi*) There is always a real root for any quadratic equation.
   (*vii*) The number of ways of selecting 2 persons in two chairs out of n persons is ${}^nP_2$.
   (*viii*) $(\vec{a} + \vec{b})^2 = \vec{a}^2 + \vec{b}^2 + 2\vec{a}.\vec{b}$.
3. (*i*) Give the truth table for the statement $\sim p \vee q$
   (*ii*) Write down the truth table for $\sim p \wedge \sim q$
   (*iii*) Write down the truth table for the statement $(\sim p \vee q) \wedge (\sim p \wedge \sim q)$
   (*iv*) Give the truth table for the statement $(p \to q) \leftrightarrow (\sim p \vee q)$.
   (*v*) Write down the truth table for the statement $(p \wedge q) \to \sim p$.
   (*vi*) Give the truth table for the statement $(p \wedge q) \to (p \vee q)$.
   (*vii*) Give the truth table for $l \leftrightarrow m$ where $l = (p \to q) \wedge (q \to p)$ and $m = p \leftrightarrow q$.

4. (*i*) If p : lines l and m are perpendicular to each other

q : A is a point on m,

write down in symbols the statement r = A is a point on the line m which is perpendicular to l.

What is the negation of this statement ?

(*ii*) If p : I study

q : I fail,

What is the symbolism for the statement

r : I study or I fail.

What is the negation of this statement ?

(*iii*) 'Ram is smart and healthy'

'Ram is neither smart nor healthy'

Are these statements negations of each other ?

(*iv*) Are the following statements negation of each other ?

'x is not a rational number'

'x is not an irrational number.'

(*v*) Write down the statement. 'Two congruent triangles are precisely those which have corresponding sides equal' as an equivalence and write its negation also.

(*vi*) Write down the negation of the statement : 'All the sides of an equiangular triangle are of the same length'.

5. (*i*) If p stands for the statement, 'I do not like chocolates' and q for the statement. 'I like ice-cream', then what does $\sim p \wedge q$ stand for ?

(*ii*) If s stands for the statement, 'I will not go to school' and t for the statement, 'I will watch a movie', then what does $\sim s \vee t$ stand for ?

(*iii*) If p stands for the statement, 'I like tennis' and q stands for the statement, 'I like football' then what does $\sim p \wedge \sim q$ stand for ?

6. Prove that

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

(*iii*) $p \vee (q \vee r) = (p \vee q) \vee r$ (*iv*) $\sim(p \vee \sim q) = \sim p \wedge q$

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

7. Write down the truth table for

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

(*iii*) $(p \wedge q) \to (p \vee q)$ (*iv*) $p \wedge (q \to p)$

(*v*) $\sim(p \wedge q) \vee \sim(q \leftrightarrow p)$ (*vi*) $(p \to q) \vee \sim(p \leftrightarrow q)$

(*vii*) $\sim(p \to q) \leftrightarrow (p \wedge \sim q)$ (*viii*) $p \vee \sim q$

(*ix*) $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$

8. Prove the following distributive laws :
   (i) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ (ii) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
   (iii) $(p \vee q) \wedge r = (p \wedge r) \vee (q \wedge r)$ (iv) $(p \wedge q) \vee r = (p \vee r) \wedge (q \vee r)$

9. (i) Show that $(\sim p \wedge \sim q) \rightarrow (p \rightarrow q)$ is a tautology
   (ii) Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.
   (iii) Show that $(p \wedge q) \rightarrow (\sim p \vee q)$ is a tautology.
   (iv) $(p \wedge q) \rightarrow (p \leftrightarrow q)$ is a tautology.
   (v) $(p \wedge q) \rightarrow p$ is a tautology.
   (vi) $(p \wedge q) \wedge (\sim p \vee \sim q)$ is a contradiction.
   (vii) Show that $(p \vee q) \vee r \leftrightarrow p \vee (q \vee r)$ is a tautology.
   (viii) Show that $p \rightarrow (p \vee q)$ is a tautology.
   (ix) Show that $(p \vee q) \wedge (\sim p \wedge \sim q)$ is a contradiction.

10. Construct truth table of $\sim (p \wedge q) \rightarrow \sim p \vee \sim q$. Is it Contradiction or Tautology.

11. (i) Write down the truth table for $l \wedge m$ where $l = \sim q \rightarrow \sim r$, $m = \sim r \rightarrow \sim q$.
    (ii) Write down the truth table for $l \leftrightarrow m$ where $l = \sim (p \vee q)$, $m = \sim p \wedge \sim q$.

12. Construct the Truth table for the proposition
    $(p \rightarrow q) \rightarrow (q \rightarrow p)$

13. Write down the truth table for the following statement patterns :
    (i) $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$ (ii) $(p \rightarrow q) \rightarrow [(q \rightarrow r) \rightarrow (p \rightarrow q)]$

14. Prove that :
    $p \rightarrow (\sim q \vee r) \equiv (p \wedge q) \rightarrow r$.

15. Simplify
    (i) $\sim(\sim p \rightarrow \sim q)$ (ii) $\sim(\sim p \leftrightarrow q)$ (iii) $\sim(\sim p \vee \sim q)$

16. Find the converse, inverse and contrapositive of the following statement :
    "If $4x - 2 = 10$, then $x = 3$".

17. State Converse and Contrapositive of the implication "if today is Thursday, then I have a rest today".

ANSWERS

1. (i) Not a statement (ii) Statement (iii) Not a statement (iv) Statement
   (v) Statement (vi) Not a Statement (vii) Statement.

2. (i) F (ii) F (iii) T (iv) F (v) T (vi) F (vii) T (viii) T

3. (*i*)

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

(*ii*)

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

(*iii*)

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

(*iv*)

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

(*v*)

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

(*vi*)

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

(vii)

p	q	$p \to q$	$q \to p$	l	m	$l \leftrightarrow m$
T	T	T	T	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

4. (i) r is $p \wedge q$; 'l is not perpendicular to m or A is not a point on m'

(ii) r is $p \vee q$; 'I do not study and I do not fail'.

(iii) No (iv) Yes (v) $p \leftrightarrow q$;

'Two triangles are not congruent and have corresponding sides equal or two triangles are congruent and have a pair of corresponding sides equal.'

(vi) 'No all the sides of an equiangular triangle are of the same length'.

5. (i) I like chocolates and ice-cream. (ii) Either I will go to school or I will watch a movie.

(iii) I like neither tennis nor football.

7. (i)

Truth Tables

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

(ii)

Truth Table

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

(iii)

Truth Tables

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

(iv)

Truth Table

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

(v)

Truth Table

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

(vi)

Truth Table

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

(vii)

Truth Table

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

(viii)

Truth Table

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

Truth Table

(ix)

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

10.

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

Given statement is a Tautology as result is always true.

11. (i)

q	r	l	m	$l \wedge m$
T	T	T	T	T
T	F	T	F	F
F	T	F	T	F
F	F	T	T	T

(ii)

p	q	$p \vee q$	$\sim(p \vee q)$	$\sim p$	$\sim q$	$\sim p \wedge \sim q$	$l \leftrightarrow m$
T	T	T	F	F	F	F	T
T	F	T	F	F	T	F	T
F	T	T	F	T	F	F	T
F	F	F	T	T	T	T	T

12.

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

13. (*i*)

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

(*ii*)

p	q	r	$p \to q$	$q \to r$	$(q \to r) \to (p \to q)$	$(p \to q) \to [(q \to r) \to (p \to q)]$
T	T	T	T	T	T	T
T	T	F	T	F	T	T
T	F	T	F	T	F	T
T	F	F	F	T	F	T
F	T	T	T	T	T	T
F	T	F	T	F	T	T
F	F	T	T	T	T	T
F	F	F	T	T	T	T

15. (*i*) $\sim p \wedge q$ (*ii*) $p \leftrightarrow q$ (*iii*) $p \wedge q$

16. (*i*) Converse : If $x = 3$, then $4x - 2 = 10$ (*ii*) Inverse : If $4x - 2 \neq 10$, then $x \neq 3$

(*iii*) Contrapositive : If $x \neq 3$, then $4x - 2 \neq 10$

17. Converse : If I have a rest today, then Today is Thursday.

Contrapositive : If I do not have a rest today, then today is not Thursday.

1.18. Arguments

Def. of argument : An argument is a statement which asserts that given set of propositions $p_1, p_2, p_3, \ldots, p_n$ taken together gives another proposition P.

These are expressed as $p_1, p_2, p_3, \ldots\ldots, p_n \vdash$ P. The sign "$\vdash$" is spoken at turnstile. The propositions $p_1, p_2, p_3, \ldots\ldots\ldots, p_n$ are called "premises" or "assumptions" and P is called the "conclusion".

Valid argument : An argument $p_1, p_2, p_3, \ldots\ldots p_n \vdash$ P is true if P is true whenever all the premises $p_1, p_2, p_3, \ldots\ldots, p_n$ are true, otherwise the argument is false. A true argument is called valid argument, and a false argument is called a fallacy.

Note. If is important to realise that the truth or the conclusion is irrelevant as far as the validity of argument is concerned. A true conclusion is neither necessary nor sufficient for the validity of argument.

The validity can also be judged by the relationship $p_1 \wedge p_2 \wedge p_3 \ldots\ldots \wedge p_n \to$ P provided it is a tautology.

ILLUSTRATIVE EXAMPLES

Example 1. Test the validity of : If he works hard then he will be successful. If he is successful then he will be happy. Therefore, hard work leads to happiness.

Sol. Let the symbols for the statements be :

p : he works hard.

q : he is successful

r : he is happy.

The argument is :

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

Truth Table

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
T	T	T	T	T	T	T	T
T	F	T	F	T	F	T	T
F	T	T	T	T	T	T	T
F	F	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	F	F	T	F	F	T
F	T	F	T	F	F	T	T
F	F	F	T	T	T	T	T

From the table, it is clear that $[(p \to q) \wedge (q \to r)] \to (p \to r)$ is tautology.

$\therefore$ given argument is valid.

Note. Another method for testing the validity of argument.

In the last three examples, there were only two or there statements and consequently 4 to 8 rows in the truth table. But if there are four or more statements then the truth table will have 16 or more rows and the chance of the making a mistake will be more. To over come this difficulty *i.e.*, to reduce the size of the table we have another method, infact above method stated in another way, which follows as :

"Assume that the conclusion is false. Now if $p_1 \wedge p_2 \wedge \ldots\ldots \wedge p_n$ is a fallacy, then the argument is valid, otherwise the argument is invalid.

Example 2. Test the validity of :

"If my brother stands first in the class, I will give him a watch. Either he stood first or I was out of station. I did not give my brother a watch this time. Therefore I was out of station."

Sol. Let the symbols for the statements be :

p : my brother stands first in the class.

q : I give him a watch.

r : I was out of station.

The argument is $p \to q, p \vee r, \sim q / \therefore r$.

Assume that r is false.

Now there will be only four rows as there are only two variables p, q

Truth Table

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

Since $(p \to q) \wedge (p \vee r) \wedge (\sim q)$ is a fallacy.

$\therefore$ the argument is valid.

Example 3. Prove the validity of following arguments :

If man is a bachelor, he is unhappy.

If a man is unhappy, he dies young.

Therefore, bachelors die young.

Sol. Let p : man is a bachelor

q : man is unhappy

r : man dies young.

The given statement is $[(p \to q) \wedge (q \to r)] \to (p \to r)$

Truth Table

			I		II		
p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	I $\to$ II
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Since given statement is a tautology, so argument is valid.

Example 4. Check the validity of argument :

If I work, I cannot study. Either I work or pass mathematics.

I passed mathematics. Therefore, I study.

Sol. Let p : I work

q : I study

r : I pass mathematics

The given statement is

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

Truth Table

						I	II
p	q	r	$\sim q$	$p \to \sim q$	$p \vee r$	$(p \to \sim q) \wedge (p \vee r) \wedge (r)$	$I \to q$
T	T	T	F	F	T	F	T
T	T	F	F	F	T	F	T
T	F	T	T	T	T	T	F
T	F	F	T	T	T	F	T
F	T	T	F	T	T	T	T
F	T	F	F	T	F	F	T
F	F	T	T	T	T	T	F
F	F	F	T	T	F	F	T

The given statement is not a tautology.

So argument is not valid.

EXERCISE 1.2

1. Test the validity of :

   If it rains then crop will be good.

   It did not rain, therefore the crop will not be good.

2. Test the validity of :

   Unless we control population, all advances resulting from planning will be nullified. But this must not be allowed to happen. Therefore we must somehow control population.

3. Are the following arguments valid ? If valid, construct a formal proof ; if not valid, explain why.

   (*a*) If wages increase, then there will be inflation. The cost of living will not increase if there is no inflation. Wages will increase. Therefore, the cost of living will increase.

   (*b*) If the races are fixed or the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed.

ANSWERS

1. Not valid
2. Valid
3. (*a*) Not valid (*b*) Valid

1.19. Proposition Generated by a Set

Let S be any set of propositions. A proposition generated by S is any valid combination of propositions in S with conjunction, disjunction and negation.

Note. The conditional and biconditional operators are not included as they can be obtained from conjunction, disjunction and negation.

Equivalence

Let S be a set of propositions and p, q be propositions generated by S. p and q are equivalent if $p \leftrightarrow q$ is a tautology. The equivalence of p and q is denoted by $p \Leftrightarrow q$.

Implication

Let S be a set of propositions and p, q be propositions generated by S. p implies q if $p \rightarrow q$ is a tautology. $p \Rightarrow q$ is written to indicate the implication.

1. 20. Laws of Logic

Here 0 stands for contradiction, 1 for tautology.

Commutative Laws

$p \vee q \Leftrightarrow q \vee p$ $\qquad$ $p \wedge q \Leftrightarrow q \wedge p$

Associative Laws

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

Distributive Laws

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

Identity Laws

$p \wedge 0 \Leftrightarrow p$ $\qquad$ $p \vee 1 \Leftrightarrow p$

Negation Laws

$p \wedge \sim p \Leftrightarrow 0$ $\qquad$ $p \vee \sim p \Leftrightarrow 1$

Idempotent Laws

$p \vee p \Leftrightarrow p$ $\qquad$ $p \wedge p \Leftrightarrow p$

Null Laws

$p \wedge 0 \Leftrightarrow 0$ $\qquad$ $p \vee 1 \Leftrightarrow 1$

Absorbtion Laws

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

DeMorgan's Laws

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

Involution Laws

$\sim(\sim p) \Leftrightarrow p$

1.21. Common Implication and Equivalence

Detachment

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

Contrapositive

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

Disjunctive Addition

$$p \Rightarrow (p \vee q)$$

Conjunctive Simplification

$$(p \wedge q) \Rightarrow p \text{ and } (p \wedge q) \Rightarrow q$$

Disjunctive Simplification

$$(p \vee q) \wedge \sim p \Rightarrow q \text{ and } (p \vee q) \wedge \sim q \Rightarrow p$$

Chain Rule

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

CONDITIONAL EQUIVALENCES

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

Biconditional Equivalences

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

1.22. Chain Rule

Prove that $(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$

Proof.

Truth Table

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

Since $(p \to q) \wedge (q \to r) \to (p \to r)$ is a tautology

$\therefore \quad (p \to q) \wedge (q \to r) \Rightarrow (p \to r)$

1.23. Detachment Law

Prove that $(p \to q) \wedge p \Rightarrow q$

Proof.

Truth Table

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

Since $(p \to q) \wedge p \Rightarrow q$ is a tautology

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

1.24. Mathematical System

A mathematical system consists of

1. A set or universe, U.

2. **Definitions :** sentences that explain the meaning of concepts that relate to the universe. Any term used in describing the universe itself is said to be undefined. All definitions are given in terms of these undefined concepts of objects.

3. **Axions :** assertions about the properties of the universe and rules for creating and justifying more assertions. These rules always include the system of logic that we have developed to this point.

4. **Theorems** – the additional assertions mentioned above.

Example 1. In Euclidean geometry the universe consists of points and lines (two undefined terms). Among the definitions is a definition of parallel lines and among the axioms is the axiom that two distinct parallel lines never meet.

Example 2. In Propositional calculus, the universe consists of propositions. The axioms are the truth tables for the logical operators and the key definitions are those of implication and equivalence.

Theorem : A true proposition derived from axioms of mathematical system is called a theorem.

All theorems can be expressed in terms of a finite number of propositions $p_1, p_2, \ldots, p_n$, called the **premises** and the proposition C, called the **conclusion**. These theorems take the form $p_1 \wedge p_2 \wedge p_3 \wedge \ldots\ldots \wedge p_n \Rightarrow C$.

Proof : A proof of a theorem is a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply the conclusion.

There are two important types of proofs namely direct and indirect.

Direct Proof : It is a proof in which the truth of the premises of a theorem are shown to directly imply the truth of the theorem's conclusion.

Rules for Direct Proof

1. It must terminate in a finite number of steps.
2. Each step must be either a premise or a proposition that is implied from previous steps using any valid equivalence or implication.
3. The last step must be the conclusion of the theorem.

Indirect Poof

Negate the conclusion of the theorem and add this negation to the premises. If this set of propositions implies a contradiction, then the proof is complete.

Rules for Indirect Proof

1. The first step is the negated conclusions.
2. The last step must be a contradiction

ILLUSTRATIVE EXAMPLES

Example 1. Prove that the following are equivalences :

(i) $p \vee q \Leftrightarrow q \vee p$ (ii) $p \to q \Leftrightarrow \sim q \to p$ (iii) $(p \wedge q) \vee (\sim p \wedge q) \Leftrightarrow q$

Sol. (i)

Truth Table

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

Since $(p \vee q) \to (q \vee p)$ is a tautology

$\therefore$ $p \vee q$ and $q \vee p$ are equivalent

$\therefore$ $(p \vee q) \Leftrightarrow (q \vee p)$.

(ii)

Truth Table

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

Since $(p \to q) \to (\sim q \to \sim p)$ is a tautology

$\therefore$ $(p \to q)$ and $(\sim q \to \sim p)$ are equivalent

$\therefore$ $(p \to q) \Leftrightarrow (\sim q \to \sim p)$

(iii)

Truth Table

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

Since $(p \wedge q) \wedge (\sim p \wedge q) \to q$ is a tantology

$\therefore$ $(p \wedge q) \vee (\sim p \wedge q)$ and q are equivalent

$\therefore$ $(p \wedge q) \vee (\sim p \wedge q) \Leftrightarrow q$.

Example 2. Give direct proof of

$\sim p \vee q, s \vee p, \sim q \Rightarrow s$

Sol.

Step	Proposition	Justification
(1)	$\sim p \vee q$	Premise
(2)	$\sim q$	Premise
(3)	$\sim p$	Disjunctive simplification (1), (2).
(4)	$s \vee p$	Premise
(5)	s	Disjunctive simplification (3), (4). #

Note. Conditional Conclusion

The conclusion of a theorem is often a conditional proposition. The condition of the conclusion can be included as a premise in the proof of the theorem. Then we are to prove the consequence of the conclusion.

Example 3. Give indirect proof of

$$p \to r, q \to s, p \vee q \Rightarrow s \vee r$$

Sol.

Step	Proposition	Justification
(1)	$\sim(s \vee r)$	Negated conclusion
(2)	$\sim s \wedge \sim r$	De Morgan's Law, (1)
(3)	$\sim s$	Conjunctive simplification, (2)
(4)	$q \to s$	Premise
(5)	$\sim q$	Contrapositive (3), (4)
(6)	$\sim r$	Conjunctive simplification, (2)
(7)	$p \to r$	Premise
(8)	$\sim p$	Contrapositive, (6), (7)
(9)	$(\sim p) \wedge (\sim q)$	Conductive, (5), (8)
(10)	$\sim(p \vee q)$	De Morgan's Law, (9)
(11)	$P \vee q$	Premise
(12)	0	(10), (11) #

EXERCISE 1.3

1. *Show that*

(*i*) $p \wedge q$ logically implies $p \leftrightarrow q$

(*ii*) $p \leftrightarrow \sim q$ does not logically implies $p \to q$

2. Give direct proof of the theorem $p \to r, q \to s, p \vee q \Rightarrow s \vee r$.
3. Give direct proof of $p \to (q \to s), \sim r \vee p, q \Rightarrow r \to s$.
4. Give indirect proof of $a \to b, \sim (b \vee c) \Rightarrow \sim a$
5. Give direct and indirect proof of $p \to q, q \to r, \sim (p \wedge r), p \vee r \Rightarrow r$
6. Give direct and indirect proof of
$(p \to q) \wedge (r \to s), (q \to t) \wedge (s \to u), \sim (t \wedge u), p \to r \Rightarrow \sim p$

1.25. Proposition over a Universe

Let U be a non-empty set. A proposition over U is a sentence that contains a variable that can take on any value in U and which has a definite truth value as a result of any such substitution.

Examples : Consider

(*i*) $7x^2 - 6x = 0 \quad \Rightarrow \quad x(7x - 6) = 0$

$\Rightarrow \quad x = 0, \frac{7}{6}$

If we take **Q** as universe, then truth set (*i.e.*, solution set) of $7x^2 - 6x = 0$ is $\left\{0, \frac{7}{6}\right\}$.

If we take **Z** as universe, then truth set of $7x^2 - 6x = 0$ is $\{0\}$.

If we take **N** as universe, then truth set of $7x^2 - 6x = 0$ is ϕ.

(*ii*) $z^2 = 5$

If we take **Q** as universe, then truth set of $z^2 = 5$ is ϕ.

$\therefore \quad z^2 = 5$ is a contradiction over the rationals.

(*iii*) $(x + 3)(x - 3) = x^2 - 9$

If we take **Q** as universe, then truth set is **Q** as $(x + 3)(x - 3) = x^2 - 9$ is true for all rational numbers

$\therefore \quad (x + 3)(x - 3) = x^2 - 9$ is a tautology over the rationals.

Truth Set If $p(n)$ is a proposition over U, then the truth set of $p(n)$ is

$T_{p(n)} = \{a \in U / p(a) \text{ is true}\}$

Example Consider the set $\{1, 2, 3, 4\}$

Its power set is $\{\phi, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$

Let proposition be $\{1, 2\} \cap A = \phi$

$\therefore$ truth set of proposition taken over the power se of $\{1, 2, 3, 4\}$ is

$\{\phi, \{3\}, \{4\}, \{3, 4\}\}$.

Tautology and contradiction : A proposition over U is a tautology if its truth set is U. It is a contradiction if its truth set is empty.

Equivalence : Two propositions are equivalent if $p \leftrightarrow q$ is a tautology. In other words p and q are equivalent if $T_p = T_q$.

Example : $x + 7 = 12$ and $x = 5$ are equivalent propositions over the integers.

Implication : If p and q are propositions over U, then p implies q if $p \rightarrow q$ is a tautology. In other words $p \Rightarrow q$ when $T_p \subseteq T_q$.

Example : Over the natural numbers,

$n \leq 3 \Rightarrow n \leq 8$ as $\{0, 1, 2, 3\} \subseteq \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

Truth Set of compound Propositions

The truth sets of compound propositions can be expressed in terms of the truth sets of simple propositions. The following list gives the connection between compound and simple truth sets :

1. $T_{p \wedge q} = T_p \cap T_q$
2. $T_{p \vee q} = T_p \cup T_q$
3. $T_{\sim p} = T_p{}^c$
4. $T_{p \leftrightarrow q} = (T_p \cap T_q) \cup (T_p{}^c \cap T_q{}^c)$
5. $T_{p \rightarrow q} = T_p{}^c \cup T_q$.

ILLUSTRATIVE EXAMPLES

Example 1. If $U = P\{1, 2, 3, 4\}$, what are the truth sets of the following propositions ?

(*i*) $A \cap \{2, 4\} = \phi$ (*ii*) $3 \in A$ and $1 \notin A$ (*iii*) $A \cup \{1\} = A$

(*iv*) A is a proper subset of $\{2, 3, 4\}$ (*v*) $\# A^c = \# A$

Sol. (*i*) Truth set is $\{\phi, \{1\}, \{3\}, \{1, 3\}\}$

(*ii*) Truth set is $\{\{3\}, \{3, 2\}, \{3, 4\}, \{2, 3, 4\}\}$

(*iii*) Truth set is $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$

(*iv*) Truth set is $\{\{2\}, \{3\}, \{4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

(*v*) Truth set is $\{A \subseteq U, \# A = 2\}$

Example 2. Given the propositions over the natural numbers

$p : n < 4$

$q : 2n > 17$

and $r : n$ is a divisor of 18

What are the truth sets of

(*a*) q (*b*) $p \wedge q$ (*c*) r (*d*) $q \rightarrow r$

Sol. We have

$T_p = \{1, 2, 3\}$, $T_q = \{9, 10, 11, 12, \ldots\ldots\}$, $T_r = \{1, 2, 3, 6, 9, 18\}$

(*a*) $T_q = \{9, 10, 11, 12, \ldots\ldots\}$

(*b*) $T_{p \wedge q} = T_p \cap T_q = \{1, 2, 3\} \cap \{9, 10, 11, 12, \ldots\} = \phi$

(*c*) $T_r = \{1, 2, 3, 6, 9, 18\}$

(*d*) $T_{q \rightarrow r} = T_q{}^c \cup T_r = \{1, 2, 3, 4, 5, 6, 7, 8\} \cup \{1, 2, 3, 6, 9, 18\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 18\}$

Example 3. Let the universe be $\mathbf{Z}$, the set of integers. Which of the following propositions are equivalent over $\mathbf{Z}$?

(*a*) $0 < n^2 \leq 4$ (*b*) $0 < n^3 \leq 8$ (*c*) $0 < n \leq 2$

Sol. (*a*) Truth set is $\{-2, -1, 1, 2\}$ (*b*) Truth set is $\{1, 2\}$ (*c*) Truth set is $\{1, 2\}$

We know that two propositions are equivalent if their truth sets are equal

$\therefore$ (*b*) and (*c*) are equivalent.

EXERCISE 1.4

1. Over the universe of positive integers

   $p(n)$: $4n^2 - 3n = 0$

   $q(n)$: n is a perfect square and $n < 90$

   $r(n)$: n is a divisor of 36

   What are the truth sets of these propositions ?

2. Over the universe of positive integers :

   $p(n)$: n is prime and $n < 32$

   $q(n)$: n is a power of 3

   $r(n)$: n is a divisor of 27

   (*a*) What are the truth sets of these propositions ?

   (*b*) Which of the three propositions implies one of the others ?

3. If U = {0, 1, 2}, how many propositions over U could you list without listing two that are equivalent ?

4. (*a*) Determine the truth sets of the following propositions over the positive integers :

   $p(n)$: n is a perfect square and $n < 100$

   $q(n)$: $n = \#\,P(A)$ for some set A.

   (*b*) Determine $T_p \wedge q$ for p and q above.

ANSWERS

1. {1, 4, 9, 16, 25, 26, 49, 64, 81}, {1, 2, 3, 4, 6, 9, 12, 18, 36}
2. (*a*) T_p = {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31}

   T_q = {1, 3, 6, 9, 12, 15, 18, 21,.....}

   T_r = {1, 3, 9, 27} (*b*) r implies q 3. 256
4. T_p = {1, 4, 9, 16, 25, 36, 49, 64, 81}; T_q = {1, 2, 4, 8, 16, 32,...}, {1, 4, 16, 64}

1.26. Predicates

The predicate is the part of a sentence that gives information about the subject. For example, in the sentence "Ramesh is a resident of Amritsar", the word Ramesh is the subject and the phrase "is a resident of Amritsar" is the predicate. So, predicate is the part of the sentence from which the subject has been removed.

In logic, predicates can be obtained by removing any nouns from a statement. For example, if P stands for "is a resident of Amritsar" and Q stands for "is a resident of", then both P and Q are predicate symbols. The sentences "x is a resident of Amritsar" and "x is a resident of y" are denoted as $P(x)$ and $Q(x, y)$ respectively, where x and y are predicate variables that take values in appropriate sets.

The statement "x is greater than 5" has two parts. The first part, the variable x, is the subject of the statement. The second part—the predicate, "is greater than 5"—refers to a property that the subject of the statement can have. We can denote the statement "x is greater than 5" by $P(x)$, where P denotes the predicate "is greater than 5" and x is the variable. The statement $P(x)$ is also said to be the value of the **propositional function** P at x. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value.

Predicate. *A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables.*

The domain of a predicate variable is the set of all values which may be substituted in place of the variables. The predicates are also known as "**propositional function or open sentences**".

Truth Set : Let $P(x)$ be a predicate and x has domain D. Then the set $\{x \in D : P(x) \text{ is true}\}$ is called the **truth set** of $P(x)$.

Example : Let $P(x)$ be "x is an integer less than 6" and suppose the domain of x is the set of all positive integers. Then the truth set of $P(x)$ is $\{1, 2, 3, 4, 5\}$,

Let $P(x)$ and $Q(x)$ be predicates with common domain D of x. The notation $P(x) \Rightarrow Q(x)$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$.

Also, $P(x) \Leftrightarrow Q(x)$ means that $P(x)$ and $Q(x)$ have Identical truth sets.

For example, let the domain of x be the set of positive integers and let

$P(x)$: "x is an integer less than 6",

$Q(x)$: "x is a factor of 4".

$\therefore$ Truth set of $P(x)$ is $\{1, 2, 3, 4, 5, 6, 7\}$

and Truth set of $Q(x)$ is $\{1, 2, 4\}$.

Now every element in the truth set of $Q(x)$ is in the truth set of $P(x)$, so $Q(x) \Rightarrow P(x)$.

A statement involving the n variables $x_1, x_2, \ldots x_n$ can be denoted by $P(x_1, x_2, \ldots, x_n)$. A statement of the form $P(x_1, x_2, \ldots x_n)$ is the value of the **propositional function** P at the n-tuple $(x_1, x_2, \ldots x_n)$, and P is also called an **n-place predicate** or a **n-ary predicate.**

The symbolic analysis of predicates and quantified statements is called the **predicate calculus** whereas the symbolic analysis of ordinary compound statements is called the **statement calculus** or **propositional calculus.**

Example. *Let $P(x)$ denote the statement "$x > 3$". What are the truth values of $P(4)$ and $P(2)$?*

Sol. *Here $P(x)$ denotes the statement "$x > 3$".*

For obtaining the statement P(4), we replace x by 4 in the statement "$x > 3$". Therefore P (4), which is the statement "$4 > 3$", is true. Similarly P(2), which is the statement "$2 > 3$", is false.

Example. Let $Q(x, y)$ denote the statement "$x = y + 3$". What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Sol. Here $Q(x, y)$ denotes the statement "$x = y + 3$"

For obtaining the statement $Q(1, 2)$, we replace x by 1 and y by 2 in the statement "$x = y + 3$". Therefore $Q(1, 2)$, which is the statement "$1 = 2 + 3$", is false. Similarly $Q(3, 0)$, which is the statement "$3 = 0 + 3$", is true.

Example. Let $R(x, y, z)$ denote the statement "$x + y = z$". What are the truth values of the propositions $R(1, 2, 3)$ and $R(0, 0, 1)$?

Sol. Here $R(x, y, z)$ denotes the statement "$x + y = z$"

For obtaining the statement $R(1, 2, 3)$, we replace x by 1, y by 2 and z by 3 in the statement "$x + y = z$". Therefore $R(1, 2, 3)$, which is the statement "$1 + 2 = 3$", is true. Similarly $R(0, 0, 1)$, which is the statement "$0 + 0 = 1$", is false.

1.27. Quantifiers

If $p(n)$ is a propositions over U with $T_{p(n)} \neq \phi$, then we say "There exists an n in U such that $p(n)$ is true." We abbreviate this sentence as $(\exists n)_U (p(n))$. $\exists$ is known as **existential quantifier.**

It is clear that if $p(n)$ is a propositions over a universe U, its truth set $T_{p(n)}$ is a subset of U.

Examples

(1) $(\exists k)_Z, (5k = 100)$ means that there is an integer k such that 100 is a multiple of 5. This is true.

(2) $(\exists x)_Q (x^2 - 3 = 0)$ means that there is a rational number x such that $x^2 = 3$. This is false as the solution set of the equation $x^2 - 3 = 0$ over **Q** is empty. We write it as $((\exists x)_Q, (x^2 - 3 = 0)$

If $p(n)$ is a propositions over U, with $T_{p(n)} = U$. Them we say "for all n in U, $p(n)$ is true." We abbreviate this as $(\forall n)_U, (p(n))$. $\forall$ is known as **universal quantifier.**

$\exists x : P(x)$ means, "There exists an x such that $P(x)$ holds."

$\forall x : P(x)$ means, "For all x, it is the case that $P(x)$ holds."

So for example, if x denotes a real number, then

$\exists x : x^2 = 9$ is true, since 3 is an x for which $x^2 = 9$.

On the other hand, $\forall x : x^2 = 9$ is clearly false; not all numbers, when squared, are equal to 3.

$\forall x : x^2 + 1 > 0$ is true, but $\forall x : x^2 > 2$ is false, since for example $x = 1$ does not satisfy the predicate.

On the other hand, $\exists x : x^2 > 2$ is true, since $x = 2$ is an example that satisfies it.

Negation of Quantified Proposition

When we negate a quantified proposition, then the universal and existential quantifiers become complement of one another. In simple words negation of an existentially quantified proposition is a universally quantified proposition and negation of a universally quantified proposition is an existentially quantified proposition. In symbols,

$$\sim (\forall n)_U (p(n)) \Leftrightarrow (\exists n)_U (\sim p(n)) \text{ and } \sim (\exists n)_U (p(n)) \Leftrightarrow (\forall n)_U (\sim p(n))$$

Nested Quantifiers

Two quantifiers are nested if one is within the scope of the other.

e.g. "For every real number, there is a real number larger than it."

This can be written as $\forall x \exists y : y > x$.

Example : $\forall x \exists y (x + y = 0)$

Example : $\forall x\, Q(x)$, where $Q(x)$ is $\exists y\, P(x, y)$, where $P(x, y) : x + y = 0$.

Example : $\forall x \forall y (x + y = y + x)$ Commutative law for addition

Example : $\forall x \exists y (x + y = 0)$ Additive inverse property

Example : $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$ Associative law for addition

Example : $\forall x \forall y ((x > 0) \wedge (y < 0) \rightarrow (xy < 0))$ where the domain of both variables is real number.

"For every real number x and every real number y, if x is positive and y is negative, then xy is negative."

"The product of a negative real number and a positive real number is always negative."

Example : "The sum of two positive integers is always positive".

"For every two integers, if they are both positive then their sum is positive."

"For all positive integers x and y, $x + y$ is positive."

$\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow (x + y > 0)$, where domain is all integers.

$\forall x \forall y (x + y > 0)$, where domain is all positive integers.

Order of Quantifiers

The order of the quantifiers is important, unless all quantifiers are universal or all quantifiers are existential.

Example : $\forall x \forall y\, P(x, y) \equiv \forall y \forall x\, P(x, y)$

Example : $\exists x \exists y\, P(x, y) \equiv \exists y \exists x\, P(x, y)$

Example : $\forall x \exists y\, P(x, y)$ is NOT equivalent to $\exists y \forall x\, P(x, y)$

Example : $P(x, y) : x + y = 0$, where the domain of both x and y consists of all real numbers. Find the truth values of $\forall x \exists y\, P(x, y)$ and $\exists y \forall x\, P(x, y)$.

$\exists y \forall x\, P(x, y)$ denotes

"There is a real number y such that for every real number x, $x + y = 0$"

This statement is False.

$\forall x \exists y\, P(x, y)$ denotes

"For every real number x, there is a real number y such that $x + y = 0$."

This statement is true.

Binding Variables : When a quantifier is used on the variable x, Then this occurrence of the variable is **bound**. An occurrence of a variable that is not bound by a quantifier or set equal to a particular value is said to be **free**. All the variables that occur in a propositional function must be bound or set equal to a particular value to turn it into a proposition.

Example. In the statement $\exists x\,(x + y = 1)$, the variable x is bound by the existential quantification $\exists x$, but the variable y is free because it is not bound by a quantifier and no value is assigned to this variable. So the statement $\exists x\,(x + y = 1)$, x is bound, but y is free.

ILLUSTRATIVE EXAMPLES

Example 1. Translate into your own words and indicate whether it is true or false that $(\exists u)_{\mathbb{Z}}\,(4u^2 - 9 = 0)$.

Sol. Consider $4u^2 - 9 = 0$

$\therefore \quad 4u^2 = 9 \Rightarrow u^2 = \frac{9}{4} \Rightarrow u = \pm\frac{3}{2}$, which are not integers.

$\therefore$ the equation $4u^2 - 9 = 0$ has a solution in integers is false.

Example 2. Use quantifier to say that $\sqrt{3}$ is not a rational number.

Sol. $\sim(\exists x)_{\mathbb{Q}}\,(x^2 = 3)$.

Example 3. Over the universe of Books, define the propositions $B(x)$: x has a blue cover, $M(x)$: x is a mathematics book, $U(x)$: x is published in the United States and $R(x, y)$: The bibliography of x includes y.

Translate into words.

(a) $(\exists x)\,(M(x) \wedge \sim B(x))$, (b) $(\forall x)\,(M(x) \wedge U(x) \to B(x))$

(c) $(\exists x)\,(\sim B(x))$, (d) $(\exists y)\,((\forall x)\,(M(x) \to R(x, y))$

Express using quantifiers :

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States

(g) Not all books have bibliographies.

Sol. We have

$B(x)$: x has a blue cover

$M(x)$: x is a mathematics book

$U(x)$: x is published in the United States

$R(x, y)$: The bibliography of x includes y.

(a) There exists a mathematics book which has not a blue cover.

(b) Every mathematics book that is published in the United States has a blue cover.

(c) There exists a book whose cover is not blue.

(d) There exist a book that appears in the bibliograph of every mathematics book.

(e) $(\forall x)\,(B(x) \to M(x))$ (f) $(\exists x)\,(M(x) \wedge \sim U(x))$ (g) $(\exists x)\,(\forall y)\,(\sim R(x, y))$

Example 4. Let M (x) be "x is a mammal." Let A (x) be "x is an animal" and let W (x) be, "x is warm blooded."

(a) Translate into formula : Every mammal is warm blooded.

(b) Translate into English $(\exists x)$ (A $(x) \wedge (\sim M(x))$.

Sol. We have

M (x) : x is a mammal

A (x) : x is an animal

W (x) : x is warm blooded

(a) $(\forall x)$ (M $(x) \wedge$ W (x))

(b) There is an animal which is not mammal.

EXERCISE 1.5

1. Translate in your own words and indicate whether it is true or false that :

   $(\exists x)_Q\ (3x^2 - 12 = 0)$

2. Use quantifier to say that $\sqrt{5}$ is not a rational number.

3. Use universal quantifiers to state that the sum of two rational numbers is rational.

4. Use universal quantifiers to state that the sum of any two real numbers is real.

5. Over the universe of real numbers, use quantifiers to say that the equation $a + 2x = b$, has a solution for all values of a and b.

6. Let C (x) be "x is cold blooded." Let F (x) be "x is a fish and let S (x) be "x lives in the sea."

   (a) Translate into a formula : Every fish is cold blooded.

   (b) Translate into English : $(\exists x)$ (S $(x) \wedge \sim$ F (x)) and $(\forall x)$ (F $(x) \rightarrow$ S (x)).

ANSWERS

1. False
2. $\sim (\exists x)_Q\ (x^2 = 5)$
3. $(\forall a)_Q\ (\forall b)_Q$ ($a + b$ is a rational number)
4. $(\forall a)_R\ (\forall b)_R$ ($a + b$ is a real number)
5. $(\forall a)_R\ (\forall b)_R\ (\exists x)_R\ (a + 2x = b)$
6. (a) $(\forall x)$ (F $(x) \wedge$ C (x))

   (b) There exist animals that live in the sea that are not fish.

   Every fish lives in the sea.

1.28. The Theory of Inference for Statement Calculus

We study logic to give us rules of inference, or principles of reasoning. The theory associated with such rules in known as inference theory as 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 reasoning, then such a process of derivation is called a deduction or a formal proof. In 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.

In any argument, a conclusion is admitted to be true provided that the premises *i.e.* assumptions, axioms, hypotheses are accepted as true and the reasoning used in deriving the conclusion from the premises follows certain accepted rules of logical inference. Such an argument is called sound. In any argument, we are always concerned with its soundness. In logic, we concentrate our attention on the study of the rules of inference by which conclusions are derived from premises. Any conclusion which is arrived at by following these rules is called a valid conclusion, and the argument is called a valid argument. The actual truth values of the premises do not play any part in the determination of the validity of the argument. In short, in logic we are concerned with the validity but not necessarily with the soundness 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 $A \to B$ is a tautology, that is, $A \Rightarrow B$.

Similarly a set of premises $\{H_1, H_2, \ldots\ldots, H_m\}$ a conclusion C follows logically iff $H_1 \wedge H_2 \wedge \ldots\ldots \wedge H_m \Rightarrow C$.

RULES OF INFERENCE

Here are two rules of inference which are called rules P and T.

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

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

Example. Demonstrate that R is a valid inference from the premises $P \to Q$, $Q \to R$ and P.

Sol.

{1}	(1)	$P \to Q$	Rule **P**
{2}	(2)	P	Rule **P**
{1, 2}	(3)	Q	Rule **T**, (1), (2)
{4}	(4)	$Q \to R$	Rule **P**
{1, 2, 4}	(5)	R	Rule **T**, (3), (4)

The second column of numbers designates the formula as well as the line of derivation in which it occurs. The set of numbers in braces (the first column) for each line shows the premises on which the formula in the line depends. On the right, **P** or **T** represents the rule of inference, followed by a comment showing from which formulas and tautology that particular formula has been obtained For example, if we follow this notation, the third line shows that the formula in this line is numbered (3) and has been obtained

from premises in (1) and (2). The comment on the right says that the formula Q has been introduced using rule T and also indicates the details of the application of rule **T**.

Table of Implications

I_1 $P \wedge Q \Rightarrow P$	I_2 $P \wedge Q \Rightarrow Q$
I_3 $P \Rightarrow P \vee Q$	I_4 $Q \Rightarrow P \vee Q$
I_5 $\neg P \Rightarrow P \rightarrow Q$	I_6 $Q \Rightarrow P \rightarrow Q$
I_7 $\neg (P \rightarrow Q) \Rightarrow P$	I_8 $\neg (P \rightarrow Q) \Rightarrow \neg Q$
I_9 $P, Q \Rightarrow P \wedge Q$	I_{10} $\neg P, P \vee Q \Rightarrow Q$
I_{11} $P, P \rightarrow Q \Rightarrow Q$	I_{12} $\neg Q, P \rightarrow Q \Rightarrow \neg P$
I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$	I_{14} $P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$

Table of Equivalences

E_1 $\neg \neg P \Leftrightarrow P$	E_2 $P \wedge Q \Leftrightarrow Q \wedge P$
E_3 $P \vee Q \Leftrightarrow Q \vee P$	E_4 $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$
E_5 $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	E_6 $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$
E_7 $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	E_8 $\neg (P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
E_9 $\neg (P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	E_{10} $P \vee P \Leftrightarrow P$
E_{11} $P \wedge P \Leftrightarrow P$	E_{12} $R \vee (P \wedge \neg P) \Leftrightarrow R$
E_{13} $R \wedge (P \vee \neg P) \Leftrightarrow R$	E_{14} $R \vee (P \vee \neg P) \Leftrightarrow T$
E_{15} $R \wedge (P \wedge \neg P) \Leftrightarrow F$	E_{16} $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
E_{17} $\neg (P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$	E_{18} $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
E_{19} $P \rightarrow (Q \rightarrow R) \Leftrightarrow (P \wedge Q) \rightarrow R$	E_{20} $\neg (P \Leftrightarrow Q) \Leftrightarrow P \Leftrightarrow \neg Q$
E_{21} $P \Leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$	E_{22} $(P \Leftrightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$

1.29. Theory of Inference for the Predicate Calculus

The method of derivation involving predicate formulas follows the rules of inference given for the statement calculus and also certain additional rules which are required to deal with the formulas involving quantifiers. The rule **P**, regarding the introduction of a premise at any stage of derivation and **T**, the introduction of any formula which follows logically from the formulas already introduced, remain the same. If the conclusion is given in the form of a conditional, we use the rule of conditional proof called **CP**. Sometimes, we use the indirect method of proof in introducing the negation of the conclusion as an additional premise in order to arrive at a contradiction.

In order to use the equivalences and implications, we need some rules on how to eliminate quantifiers during the course of derivation. This 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.

The rules of generalization and specification follow. Here A (x) is used to denote a formula with a free occurrence of x. A (y) denotes a formula obtained by the substitution of y for x in A (x). For such a substitution A (x) must be free for y.

Rule **US** (Universal Specification) From (x) A (x) one can conclude A (y).

Rule **ES** (Existential Specification) From $(\exists\, x)$ A (x) one can conclude A (y) provided that y is not free in any given premise and also not free in any prior step of the derivation. These requirements can easily be met by choosing a new variable each time ES is used.

Rule **EG** (Existential Generalization) From A (x) one can conclude $(\exists\, y)$ A (y).

Rule **UG** (Universal Generalization) From A (x) one can conclude (y) A (y) provided that x is not free in any of the given premises and provided that if x is free in a prior step which resulted from use of **ES**, then no variables introduced by that use of ES appear free in A (x).

An invalid conclusion can be arrived at if the second restriction on rule **UG** was not imposed. We illustrate this by as example.

Let D (u, v) : u is divisible by v. Assume that the universe of discourse is {5, 7, 10, 11}, so that the statement $(\exists\, u)$ D $(u, 5)$ is true because both D (5, 5) and D (10, 5) are true. On the other hand, (y) D $(y, 5)$ is false because D (7, 5) and D (11, 5) are false. Consider now the following derivation.

{1}	(1)	$(\exists\, u)$ D $(u, 5)$	P
{1}	(2)	D $(x, 5)$	**ES**, (1)
{1}	(3)	(y) D $(y, 5)$	UG, (2) (neglecting second restriction)

In step 3 we have obtained from D $(x, 5)$ the conclusion (y) D $(y, 5)$. Obviously x is not free in the premise, and so the first restriction is satisfied. But x is free in step 2 which resulted by use of **ES**, and that x has been introduced by use of **ES** and appears free in D $(x, 5)$; hence it cannot be generalized. This is the reason why we obtained a false conclusion from a true premise.

Following examples explain the method of derivation.

ILLUSTRATIVE EXAMPLES

Example 1. Show that $(x)(H(x) \to M(x)) \wedge H(s) \Rightarrow M(s)$.

Sol.

{1}	(1)	$(x)(H(x) \to M(x))$	P
{1}	(2)	$H(s) \to M(s)$	US, (1)
{3}	(3)	$H(s)$	P
{1, 3}	(4)	$M(s)$	T, (2), (3), I_{11}

Note : In step 2 first we remove the universal quantifier.

Example 2. Show that $(\exists x) M(x)$ follows logically from the premises

$(x)(H(x) \to M(x))$ and $(\exists x) H(x)$

Sol.

{1}	(1)	$(\exists x) H(x)$	P
{1}	(2)	$H(y)$	ES, (1)
{3}	(3)	$(x)(H)(x) \to M(x))$	P
{3}	(4)	$H(y) \to M(y)$	US, (3)
{1, 3}	(5)	$M(y)$	T, (2), (4) I_{11}
{1, 3}	(6)	$(\exists x) M(x)$	EG, (5)

Note : In step 2 the variable y is introduced by ES. So a conclusion such as $(x) M(x)$ could not follow from step 5 as it would violate the rules given for UG.

EXERCISE 1.6

1. Show that : $(x)(P(x) \to Q(x)) \wedge (x)((Q(x) \to R(x) \Rightarrow (P(x) \to R(x))$.
2. Prove that : $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x) P(x) \wedge (\exists x) Q(x)$.

1.30. Introduction to Proofs

Now we introduce the notion of a proof and describe methods for constructing proofs. *A proof is a valid argument that establishes the truth of a mathematical statement.* A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems. Using these points and rules of inference, the final step of the proof establishes the truth of the statement being proved.

Some Terminology

1. **Theorem :** A theorem is a statement that can be shown to be true.
2. **Proof :** A proof is a valid argument that establishes the truth of a mathematical statement.
3. **Conjecture :** A conjecture is a statement that is being proposed to be a true statement but that has not been proved. When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.
4. **Axiom (Postulate) :** A statement that is assumed to be true and can be used as a basis for proving theorems.
5. **Lemma :** A theorem used to prove other theorems.
6. **Corollary :** A corollary is a theorem that can be established directly from a theorem that has been proved.

Steps for Proofs :

The first step of the proof usually involves selecting a general element of the domain. Subsequent steps show that this element has the property in question. Finally, universal generalization implies that the theorem holds for all members of the domain.

1.31. Methods of Proving Theorems

We will discuss the following methods of proofs.

Direct Proofs

A direct proof of a conditional statement $p \to q$ is constructed when the first step is the assumption that is p is true ; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true. A direct proof shows that a conditional statement $p \to q$ is true by showing that if p is true, then q must also be true and so that the combination p true and q false never occurs. In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together, with rules of inference, to show that q must also be true.

Example. Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd".

Sol. Note that this theorem state $\forall\, n\,(P(n) \to Q(n))$, where $P(n)$ is "n is an odd integer" and $Q(n)$ is "n^2 is odd". As we have said, we will follow the usual convention in mathematical proofs by showing that $P(ni)$ implies $Q(n)$, and not explicitly using universal instantiation. To begin a direct proof of Extra this theorem, we assume that the hypothesis of this conditional statement is true, namely, we

Assume that n is odd. So $n = 2k + 1$, where k is some integer.

$\therefore \quad n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \Rightarrow n^2$ is odd

$\therefore$ if n is an odd integer, then n^2 is an odd integer.

Proof by Contraposition

Direct proofs lead from the hypothesis of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion. Proofs of theorems of the type that are not direct proofs, that is, they do not start with the hypothesis and end with the conclusion, are called indirect proofs.

An extremely useful type of indirect proof is known as **proof by contraposition**. Proofs by contraposition make use of the fact that the conditional statement $p \to q$ is equivalent to its contrapositive, $\sim q \to \sim p$. This means that the conditional statement $p \to q$ can be proved by showing that its contrapositive, $\sim q \to \sim p$, is true. In a proof by contraposition of $p \to q$, we take $\sim q$ as a hypothesis, and using axioms, definition, and previously proven theorems, together with rules of inference, we show that $\sim p$ must follow.

Example. Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

Sol. Assume that "If $3n + 2$ is odd, then n is odd" is false ; *i.e.* n is even. So $n = 2k$ for some integer k.

$\therefore \quad 3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1) \Rightarrow 3n + 2$ is even i.e. not odd

This is the negation of the hypothesis of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true.

$\therefore$ by contraposition, we have proved the result that "If $3n + 2$ is odd, then n is odd".

Vacuous Proof : A proof that $p \to q$ is true based on the fact that p is false.

Trivial proof : A proof that $p \to q$ is true based on the fact that q is false.

Proof by Contradiction

Suppose we want to prove that a statement p is true. Also, suppose that we can find a contradiction q such that $\sim p \to q$ is true. Because q is false, but $\sim p \to q$ is true, we can conclude that $\sim p$ is false, which show that p is true. How can we find a contradiction q that might help us prove that p is true in this way ?

Since the statement $r \wedge \sim r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\sim p \to (r \wedge \sim r)$ is true for some proposition r. Proofs of this type are called **proofs by contradiction.**

In simple words, a proof that p is true based on the truth on the conditional statement $\sim p \to q$, where q is a contradiction.

Example. Prove that : $\sqrt{2}$ is irrational by giving a proof by contradiction.

Sol. Let p be the proposition "$\sqrt{2}$ is irrational. We suppose that $\sim p$ is true.

If $\sqrt{2}$ is rational, there exist integers a and b with $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors.

$$\therefore \quad 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow a^2 \text{ is even} \Rightarrow a \text{ is even}$$

Let $a = 2c$, for some integer c

$$\therefore \quad a^2 = 4c^2 \Rightarrow 2b^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow b^2 \text{ is even} \Rightarrow b \text{ is even}$$

$\therefore$ 2 divides a and b, which contradicts the fact that a and b have no common factors

Hence the result.

We will introduce several other important proof methods, including proofs where we consider different cases separately and proofs where we prove the existence of objects with desired properties.

Strategy behind constructing proofs. Includes selecting a proof method and then successfully constructing an argument step by step, based on this method.

Exhaustive Proof

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each use involves checking a single example.

Example. Prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Sol. For $n = 1$, $(n+1)^2 = 2^2 = 4$ and $3^n = 3^1 = 3$; for $n = 2$, we have $(n+1)^2 = 3^2 = 9$ and $3^n = 3^2 = 9$; for $n = 3$, we have $(n+1)^3 = 4^3 = 64$ and $3^n = 3^3 - 27$; and for $n = 4$, we have $(n+1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$. In each of these four cases, we see that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Proof by Cases

A proof cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Example. Prove that if n is an integer, then $n^2 \geq n$.

Sol. We can prove that $n^2 \geq n$ for every integer by considering three cases, when $n = 0$, when $n \geq 1$, and when $n \leq -1$. We split the proof into three cases because it is straight forward to prove the result by considering zero, positive integers, and negative integers separately :

(*i*) When $n = 0$, because $0^2 = 0$. It follows that $n^2 \geq n$ is true in this case.

(*ii*) When $n \geq 1$, when we multiply both sides of the inequality $n \geq 1$ by the positive integer n, we obtain $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

(*iii*) In this case $n \leq -1$. However, $n^2 \geq 0$. It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that iff n is an integer, then $n \geq n$.

Forward Proof

We may choose any method, we need a starting point for our proof. To begin a direct proof of a conditional statement, we start with the premises. Using these premises, together with axioms and known theorems, we can construct a proof using a sequence of steps that leads to the conclusion. This type of proof, called forward proof. Similarly, with indirect reasoning we can start with the negation of the conclusion and using a sequence of steps, obtain the negation of the premises.

Proof of Necessity and Sufficiency

In logic and mathematics, necessity and sufficiency are terms used to describe a conditional or implicational relationship between two statements. For example, in the conditional statement : "If p then q",

q is necessary for p, because the truth of p guarantees the truth of q. Similarly, p is sufficient for q, because p being true always implies that q is true, but p not being true does not always imply that q is not true.

In general, a necessary condition is one which must be present in order for another condition to occur, while a sufficient condition is one which produces the said condition. The assertion that a statement is a "necessary any sufficient" condition of another means that the former statement is true if and only if the latter is true. That is, the two statements must be either simultaneously true, or simultaneously false.

EXERCISE 1.7

1. Give a direct proof that if m and n are both perfect squares, then $n\,m$ is also a perfect square.
2. Prove that : If $n = a\,b$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
3. Show that at least four of any 22 days must fall on the same day of the week.
4. Give a proof by contradiction of the theorem "If $3\,n + 2$ is odd, then n is odd."
5. Use a proof by cases to show that $|x\,y| = |x|\,|y|$, where x and y are real numbers.
   (Recall that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.

MODULE-4

MODULE-4

1

ALGEBRAIC STRUCTURES AND MORPHISM

ALGEBRAIC STRUCTURES WITH ONE BINARY OPERATION, SEMI GROUPS, MONOIDS, GROUPS

1.0. Introduction

In the lower classes we have studied the concepts of binary compositions, relations and mappings. In this chapter we shall study an algebraic system with a binary operation defined on its elements and satisfying some postulates (or axioms). This algebraic system which occurs naturally in various mathematical situations is called a **Group.** The structure of a group is one of the simplest mathematical structure. Group is considered as the starting point of the study of various algebraic structures. The study of groups is the study of single algebraic operation in its purest form.

Definition. Binary Composition (operation)

Let A be a non-empty set. A mapping $f: A \times A \to A$ is called a **binary composition (or internal composition)** or simply (a composition) on A.

The mapping f corresponds to each ordered pair $(x, y) \in A$, a unique element $f(x, y)$, where $x, y \in A$.

Note 1. We may use any convenient notation for a composition but the most commonly used are $0, \oplus, \odot, +, .$, etc. Let $*$ be a composition on a non-empty set A. Then $*(x, y)$ or $x * y$, $x, y \in A$. denotes the image of (x, y) under $*$.

2. If $*$ is a composition on a set A, then we write it as $(A, *)$. Here A is a set with operation $*$. If $\oplus, \odot$, are two compositions on A, then we write it as $(A, \oplus, \odot)$. Here A is a set with two operations $\oplus$ and $\odot$.

Example (*i*) Let R be the set of reals, and $f: R \times R \to R$ be defined as

$f((x, y)) = xy$ for all $(x, y) \in R \times R$ where $x, y \in R$

Then f is a binary composition on R.

(*ii*) Let N be the set of naturals and $*: N \times N \to N$ be defined as

$x * y = x + y,\ x, y \in N.$

We know for all $x, y \in N \Rightarrow x + y \in N \Rightarrow x * y \in N$

$\therefore$ addition is a binary operation on N.

(*iii*) If we define $*: N \times N \to N$ as

$x * y = x - y,\ x, y \in N.$

And if we take $x = 3,\ y = 5$

Then $3 * 5 = 3 - 5 = -2 \notin N$

$\therefore x * y \notin N$ for all $x, y \in N$

$\therefore$ subtraction is not a binary operation on N.

Definition. (ALGEBRAIC STRUCTURE)

A set having one or more binary composition is called **Algebraic Structure.**

Types of Compositions.

We shall now discuss some important types of binary compositions which will be used i defining algebraic structures such as Group, Rings, Fields, Vector spaces.

(*a*) Commutative Composition. A binary composition * on a set A is called commutative composition

iff $x * y = y * x \ \forall \ x, y \in A$.

Example. The addition composition in the set of real numbers is commutative, *i.e.*, $x + y = y + x$, for a $x, y \in R$.

(*b*) Associative Composition. A binary composition * on a set A is called associative compositi iff $(x * y) * z = x * (y * z)$ for all $x, y, z \in A$.

Example (*i*). The addition composition in the set of real numbers is associative

i.e., $(x + y) + z = x + (y + z) \ \forall \ x, y, z \in \mathbf{R}$.

(*ii*) The composition * defined on R (set of reals) as $* : R \times R \to R$

by $x * y = x + 2y, x, y, \in \mathbf{R}$ is not associative.

Since $(x * y) * z = (x + 2y) * z = (x + 2y) + 2z = x + 2y + 2z$,

and $x * (y * z) = x * (y + 2z) = x + 2(y + 2z) = x + 2y + 4z$

Thus $(x * y) * z \neq x * (y * z)$.

(*c*) Composition with identity element. A binary composition * on a set A is called a compositi with identity element iff $\exists \ e \in A$, such that $e * x = x = x * e$ for all $x \in \mathbf{A}$.

Then the element e is called identity element of A, which is always unique.

Example (*i*). In the set of reals, 0 is the identity element under addition composition since $x + 0 = x = 0 +$ for all $x \in \mathbf{A}$.

(*ii*) The set N, of natural numbers, does not possess the identity element under addition compositi since there is no natural number e such that

$a + e = a$ for all $a \in \mathbf{N}$. [$\because 0 \notin$

(*d*) Invertible Elements. Let e be the identity element of set A under the composition '*' on the A. Let $\alpha \in A$, then $\beta \in A$ is called an inverse element of α iff $\alpha * \beta = e = \beta * \alpha$

Then the composition * is **a composition with inverse element,** which is always unique.

Example (*i*). In the set I of integers, 0 is the identity element under addition composition and each elem $a \in \mathbf{I}$ has its additive inverse $(-a) \in I$, since $a + (-a) = 0 = (-a) + a$. Thus every element of integers invertible.

(*ii*) In the set N of naturals, '1' is the identity element under multiplication composition but there is element other than '1' which is invertible.

(e) Distributive Operations. Let $*$ and $\square$ be two binary operations on a set A, Then we say that operation $*$ is distributive with $\square$ if

$x * (y \square z) = (x * y) \square (x * z) \ \forall \ x, y, z \in A$ (Left distributive Law)

and $(y \square z) * x = (y * x) \square (z * x) \ \forall \ x, y, z \in A$ (Right distributive Law)

Note. If the composition $*$ is commutative, Then

Left distributive law $\Leftrightarrow$ Right distributive law.

Example (i). In the set of naturals multiplication composition is distributive over addition composition since $x . (y + z) = x . y + x . z \ \forall \ x, y, z \in N$.

1.1. Definition (Group)

Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $<G, *>$ is called a **group** if it satisfies the following axioms

(i) $a * b \in G, \forall \ a, b \in G$ **(Closure Property)**

(ii) $(a * b) * c = a * (b * c), \forall \ a, b, c \in G$ **(Associative Property)**

(iii) $\exists$ an element $e \in G$ such that $e * a = a = a * e, \forall \ a \in G$. Then e is called the **identity element** of G w.r.t. the operation $*$. **(Existence of identity)**

(iv) For all $a \in G$, $\exists \ b \in G$ such that $a * b = e = b * a$ then b is called the **inverse of a** and is denoted by a^{-1}. **(Existence of inverse)**

Note 1. If the operation '$*$' is denoted by '+', the group is denoted by $<G, +>$.

2. If the operation $*$ is denoted by '$\cdot$', the group is denoted by $<G, \cdot>$.56.

1.1.0. Finite and Infinite Groups

If the set G in the group $<G, *>$ is a finite set, then it is called a **finite group** otherwise it is called an **infinite group**.

1.1.1. Order of a Group

The **order of a finite group** $<G, *>$ is defined as the number of distinct elements in G. It is denoted by $o(G)$ or $|G|$. If a group G has n elements, then $o(G) = n$.

Remark : The order of an infinite group is not defined or we say that the order is infinite.

1.1.2. Abelian and Non-abelian Groups

A group $<G, *>$ is called an **abelian group** or **commutative group**

iff $a * b = b * a, \ \forall \ a, b \in G$.

If $a * b \neq b * a, \forall \ a, b \in G$, then the group $<G, *>$ is called a non-abelian group.

1.1.3. Groupoid, Semi-Group and Monoid

Groupoid : A non empty set G together with a binary operation $*$ defined on it is called a **Groupoid** if it satisfies the followimg axiom

$a * b \in G \ \forall \ a, b \in G$.

Semi-Group : A non empty set G together with a binary operation $*$ defined on it is called a **Semi-group** if it satisfies the following axioms :

(*i*) $a * b \in G \quad \forall\ a, b \in G$ (*ii*) $(a * b) * c = a * (b * c) \forall\ a, b, c \in G$.

Monoid : A non empty set G together with a binary operation $*$ defined on it is called a **Monoid** if it satisfies the following axioms

(*i*) $a * b \in G \quad \forall\ a, b \in G$. (*ii*) $(a * b) * c = a * (b * c) \forall\ a, b, c \in G$

(*iii*) $\exists$ an element $e \in G$ such that $a * e = a = e * a \quad \forall\ a \in G$.

Here e is called the identity element of G w.r.t. the binary operation $*$.

ILLUSTRATIVE EXAMPLES

Example 1. Show that the set of all natural numbers form a semi-group under the composition of addition.

Sol. Let $N = \{1, 2, 3, 4, ...\}$ be the set of natural numbers.

(*i*) **Closure Property :** Since $n + m \in N, \quad \forall\ n, m \in N$

$\therefore$ N is closed under addition.

(*ii*) **Associative Property :** Since

$$(n + m) + p = n + (m + p), \quad \forall\ n, m\, p \in N.$$

$\therefore$ Associative property hold in N under addition.

Hence N is a semi-group under addition.

Note : (N, +) is not a monoid, as (N, +) do not have identity (zero) element.

Example 2. Show that the set $G = \left\{\begin{bmatrix} x & y \\ x & y \end{bmatrix} : x, y \in R, \text{ s.t. } x + y \neq 0\right\}$ form a semi-group under the operation of matrix multiplication.

Sol. The G satisfies the following under multiplication of matrices.

(*i*) **Closure Property :** Let $A = \begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix}, B = \begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix}$ be any two elements of G, where $x_1 + y_1 \neq 0$ and $x_2 + y_2 \neq 0$.

$$\Rightarrow \quad (x_1 + y_1)(x_2 + y_2) = x_1 x_2 + y_1 x_2 + x_1 y_2 + y_1 y_2 \neq 0$$

$$\therefore \quad AB = \begin{bmatrix} x_1 & y_1 \\ x_1 & y_1 \end{bmatrix} \begin{bmatrix} x_2 & y_2 \\ x_2 & y_2 \end{bmatrix} = \begin{bmatrix} x_1 x_2 + y_1 x_2 & x_1 y_2 + y_1 y_2 \\ x_1 x_2 + y_1 x_2 & x_1 y_2 + y_1 y_2 \end{bmatrix} \in G$$

for $x_1 x_2 + y_1 x_2 + x_1 y_2 + y_1 y_2 \neq 0$.

$\therefore$ G is closed under multiplication.

(*ii*) **Associative Property :** Since matrix multiplication is associative.

$\therefore$ Associative property hold in G also.

Hence G form a semi-group under multiplication.

Note : The above set do not form a monoid under multiplication. Since it has no identity element.

Proof. Let $E = \begin{bmatrix} a & b \\ a & b \end{bmatrix}$ be the element of G such that

$$AE = A = EA, \ \forall\ A = \begin{bmatrix} x & y \\ x & y \end{bmatrix} \in G, \text{ where } x + y \neq 0.$$

i.e. $$\begin{bmatrix} x & y \\ x & y \end{bmatrix}\begin{bmatrix} a & b \\ a & b \end{bmatrix} = \begin{bmatrix} x & y \\ x & y \end{bmatrix} = \begin{bmatrix} a & b \\ a & b \end{bmatrix}\begin{bmatrix} x & y \\ x & y \end{bmatrix}$$

i.e. $$\begin{bmatrix} xa + ya & xb + yb \\ xa + ya & xb + yb \end{bmatrix} = \begin{bmatrix} x & y \\ x & y \end{bmatrix} = \begin{bmatrix} ax + bx & ay + by \\ ax + bx & ay + by \end{bmatrix}$$

Taking first two, we get

$$(x+y)\,a = x \quad \Rightarrow \quad a = \frac{x}{x+y}$$

$$(x+y)\,b = y \quad \Rightarrow \quad b = \frac{y}{x+y}$$

Also, taking , last two, we get

$$(a+b)\,x = x \quad \Rightarrow \quad (a+b-1)\,x = 0$$

$$(a+b)\,y = y \quad \Rightarrow \quad (a+b-1)\,y = 0, \text{ on adding we get}$$

$$(a+b-1)\,(x+y) = 0, \quad \text{but } x+y \neq 0$$

$\Rightarrow$ $$a + b - 1 = 0$$

$\Rightarrow$ $$a + b = 1$$

Thus, the element E in G is not unique.

Hence the identity element in G do not exist.

Example 3. Let M(X) be the set of all mapping of a non-empty set X into itself, then show that M(X) form a monoid under the composition of composite of mapping.

Sol. Let $M(X) = \{f \mid f : X \to X \text{ is a mapping}\}$

(*i*) **Closure Property :** Let $f, g \in M(X)$ be any two elements, then.

$f \circ g : X \to X$ is also mapping.

$\therefore$ $f \circ g \in M(X)\ \forall f, g \in M(X)$.

$\therefore$ M(X) is closed under the composite of mapping.

(*ii*) **Associative Property :** Let $x \in X$ be arbitrary element and let $f, g, h \in M(X)$ be any elements. Then

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) \text{ and}$$

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

$$\therefore \quad ((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x) \; \forall \, n \in X$$

$$\Rightarrow \quad (f \circ g) \circ h = f \circ (g \circ h) \; \forall f, g, h \in M(X)$$

$\therefore$ Associative law hold in M(X).

(*iii*) **Existence of identity :** There exist an element $i : X \to X$ defined by $i(x) = x, \; \forall x \in X$ such that

$$f \circ i = f = i \circ f \; \forall f \in M(X)$$

i is called the identity element of M(X) under composite of mapping.

Hence M(X) form a moniod.

Example 4. Show that the set S = {0}, under the operation of usual addition of integers, is an abelian group of order one.

Sol. Closure Property : For all $a, b \in S$,

$a = 0, \; b = 0, \; a + b \in S$ as $0 + 0 = 0 \in S$.

Thus closure property holds in S.

Associativity : We know addition of integers is associative

i.e. $(a + b) + c = a + (b + c) \quad \forall \; a, b, c \in S.$

Here $a = 0, \; b = 0, \; c = 0$ and $(0 + 0) + 0 = 0 + (0 + 0)$

Thus associative property holds in S.

Existence of identity : $\forall \; a \in S$, there exists $0 \in S$ such that

$$a + 0 = a = 0 + a.$$

Here $a = 0$ and $0 + 0 = 0 = 0 + 0$.

Thus $0 \in S$ works for the identity element of S.

Existence of inverse : $\forall \; a \in S$, there exists $-a \in S$ such that

$$a + (-a) = 0 = (-a) + a$$

Here $a = 0$ and $-a = -0 = 0$.

Thus every element of S has inverse.

Since all the axioms of a group are satisfied. Hence <S, +> is a group.

Also addition of integers is commutative

i.e. $a + b = b + a \quad \forall \; a, b \in S.$

Here $0 + 0 = 0 + 0$. S contains only one element.

Therefore, $< S, + >$ is an abelian group of order one.

Example 5. (*a*) Show that the set natural numbers or the set of positive integers does not form a group under addition and multiplication.

(*b*) Show that the set **Z** of integers forms an infinite abelian group w.r.t. usual addition of integers.

(*c*) Show that $(\mathbf{Z}, -)$ is not group where **Z** is the set of integers

Solution. (*a*) Let $\mathbf{N} = \{1, 2, 3.....\}$ be the set of natural numbers of the set of positive integers.

First we consider the operation of addition :

(i) **Closure property.** Since $n + m \in \mathbf{N} \quad \forall\, n, m \in \mathbf{N}$, so **N** is closed under +.

(ii) **Associative property.** Since $(n+m)+p = n+(m+p)\ \forall\, m, n, \quad p \in \mathbf{N}$, so the associativity holds under + in **N**.

(iii) **Existence of identity.** $e \in \mathbf{N}$ will be identity of **N** under + if

$e + n = n \quad \forall\, n \in \mathbf{N}$

But $e + n = n$ is possible if $e = 0$

But $0 \notin \mathbf{N}$

So identity under + does not exist in **N**

Hence $(\mathbf{N}, +)$ does not form a group.

Now we consider the operation of multiplication :

(i) **Closure property.** Since $n\, m \in \mathbf{N} \quad \forall\, n, m \in \mathbf{N}$, so **N** is closed under multiplication.

(ii) **Associativity.** Since $(a\, b)\, c = a\, (b\, c) \quad \forall\, a, b, c \in \mathbf{N}$, so associativity holds in **N**.

(iii) **Existence of identity.** Since $1 \in \mathbf{N}$ and $1.\, n = n = n.\, 1\ \forall\, n \in \mathbf{N}$, so 1 is the identity element.

(iv) **Existence of inverse.** Take $4 \in \mathbf{N}, 4 \in \mathbf{N}$. But there does not exist any $n \in \mathbf{N}$ such that $4.\, n = 1 = n\, .\, 4.$

So inverse of 4 does not exist in **N**.

$\therefore$ **N** is not a group under multiplication.

(*b*) **Closure Property :** We know that the sum of two integers is also an integer

i.e. $\quad a + b \in \mathbf{Z} \quad \forall\, a, b \in \mathbf{Z}.$

Thus Closure Property holds in **Z**.

Associativity : We know that addition of integers is an associative operation

i.e. $\quad (a + b) + c = a + (b + c), \quad \forall\, a, b, c \in \mathbf{Z}$

Thus Associative Property holds in **Z**.

Existence of identity : There exist $0 \in \mathbf{Z}$ such that

$$a + 0 = a = 0 + a \quad \forall\, a \in \mathbf{Z}$$

Thus, the element $0 \in \mathbf{Z}$ works for the identity element in **Z**.

Existence of inverse : For all $a \in \mathbf{Z}\ \exists\, -a \in \mathbf{Z}$ such that

$$a + (-a) = 0 = (-a) + a$$

Thus, the element $-a$ is the inverse of the element a in $\mathbf{Z}$.

Since all the axioms of a group are satisfied. Hence $<\mathbf{Z}, +>$ is a group. Moreover, the addition of integers is commutative

i.e. $\quad a+b=b+a \quad \forall\, a, b \in \mathbf{Z}$

$\therefore \quad <\mathbf{Z}, +>$ is an abelian group.

Also, $\mathbf{Z}$ contains an infinite number of elements.

Therefore, $<\mathbf{Z}, +>$ is an infinite abelian group.

Remark : A group is always a semi-group (or groupoid, monoid), where as the converse is not true in general.

(c) **(*i*) Closure property.** Since $n-m \in \mathbf{Z} \quad \forall\, n, m \in \mathbf{Z}$, so closure property holds.

(*ii*) Associativity. Take $a=1, b=2, c=3$

Then $a, b, c \in \mathbf{Z}$

$(a-b)-c=(1-2)-3=-1-3=-4$

$a-(b-c)=1-(2-3)=1-(-1)=2$

$\therefore \quad (a-b)-c \neq a-(b-c)$ in this case.

$\therefore$ associative law does not hold in $\mathbf{Z}$ under subtraction.

$\therefore \quad (\mathbf{Z}, -)$ is not a group.

Example 6. **(*a*)** Show that the set $\mathbf{Q}$ of rationals form an infinite abelian group w.r.t. usual addition of rationals.

(b) Show that the set $\mathbf{R}^*$ of all non zero real numbers forms an infinite abelian group under the operation of multiplication of real numbers

(*c*) The set $\mathbf{C}^*$ of all non-zero complex numbers forms an infinite abelian group under the operation of multiplication of complex numbers.

Solution. **(*a*)** Let $\mathbf{Q}$ be the set of rational numbers. Then

(i) Closure property. Let $a, b \in \mathbf{Q}$ so that $\quad a=\dfrac{p_1}{q_1}$ and $b=\dfrac{p_2}{q_2}$ for some $p_1, p_2, q_1, q_2 \in \mathbf{Z}$ and $q_1 \neq 0, q_2 \neq 0$.

Then $\quad a+b=\dfrac{p_1}{q_1}+\dfrac{p_2}{q_2}=\dfrac{p_1 q_2+p_2 q_1}{q_1 q_2} \in \mathbf{Q}$, since $\mathbf{Z}$ is closed under $+$ and $q_1 \neq 0, q_2 \neq 0$, implies that $q_1 q_2 \neq 0$.

(ii) Associativity. Let $a, b, c \in \mathbf{Q}$.

$\therefore \quad a=\dfrac{p_1}{q_1}, b=\dfrac{p_2}{q_2}, c=\dfrac{p_3}{q_3}$ for some $q's$ and $q's \in \mathbf{Z}$ and $q_1 \neq 0, q_2 \neq 0, q_3 \neq 0$.

Then $(a+b)+c = \left(\frac{p_1}{q_1}+\frac{p_2}{q_2}\right)+\frac{p_3}{q_3} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} + \frac{p_3}{q_3}$

$$= \frac{(p_1 q_2 + p_2 q_1) q_3 + p_3 q_1 q_2}{(q_1 q_2) q_3}$$

$$= \frac{p_1 q_2 q_3 + p_2 q_1 q_3 + q_1 q_2 p_3}{q_1 q_2 q_3}$$

since commutativly and associativity holds in **Z**.

$$a + (b+c) = \frac{p_1}{q_1}+\left(\frac{p_2}{q_2}+\frac{p_3}{q_3}\right) = \frac{p_1}{q_1} + \frac{p_2 q_3 + p_3 q_2}{q_2 q_3}$$

$$= \frac{p_1 (q_2 q_3) + (p_2 q_3 + p_3 q_2) q_1}{q_1 (q_2 q_3)}$$

$$= \frac{p_1 q_2 q_3 + p_2 q_3 q_1 + p_3 q_2 q_1}{q_1 q_2 q_3}$$

$$= \frac{p_1 q_2 q_3 + p_2 q_1 q_3 + q_2 q_1 p_3}{q_1 q_2 q_3}$$

$\therefore \quad (a+b)+c = a+(b+c) \ \forall \ a, b, c \in \mathbf{Q}$.

So, the associative law holds.

(iii) Existence of identity. The number $0 \in \mathbf{Q}$ and $a+0 = a = 0+a \ \forall \ a \in \mathbf{Q}$

$\therefore$ 0 is the identity element.

(iv) Existence of inverse. Let $a \in \mathbf{Q}$ so that $a = \frac{p}{q}$ for some $p, q \in \mathbf{Z}$ and $q \neq 0$,

Then $b = \frac{-p}{q} \in \mathbf{Q}$

$$a + b = \frac{p}{q} + \frac{-p}{q} = \frac{pq - pq}{pq} = \frac{0}{pq} = 0$$

Similarly $b + a = 0$

$\therefore \quad a + b = 0 = b + a$

$\therefore \quad b$ is the inverse of a

$\therefore \quad (\mathbf{Q}, +)$ is a group.

Moreover the addition of rationals is commutative

as $a + b = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_2}{q_1 q_2} = \frac{p_2 q_1 + p_1 q_2}{q_1 q_2} = \frac{p_2}{q_2} + \frac{p_1}{q_1}$

$= b + a \ \forall \ a, b \in Q$

And Q contains an infinite number of elements.

Therefore (Q, +) is an infinite abelian group.

(b) Closure Property : We know that product of two reals is also a real number

i.e., $a.b \in \mathbf{R}^* \quad \forall \quad a, b \in \mathbf{R}^*$

Associativity : We know that multiplication of reals is an associative operation as

$(a.b).c = a.(b.c) \quad \forall \quad a, b, c \in \mathbf{R}^*$

Existence of inverse : For all $a \in \mathbf{R}^*, \exists \frac{1}{a} \in \mathbf{R}^*$ such that $a \cdot \left(\frac{1}{a}\right) = 1 = \left(\frac{1}{a}\right) \cdot a$.

Thus, the element $\frac{1}{a}$ is the inverse of the element $a \in \mathbf{R}^*$.

Since all the axioms of a group are satisfied. Hence $<\mathbf{R}^*, \cdot>$ is a group. Moreover, the multiplication of reals is commutative

i.e. $a \cdot b = b \cdot a, \ \forall \ a, b \in \mathbf{R}^*$.

$\therefore$ $<\mathbf{R}^*, \cdot>$ is an abelian group.

Also, $\mathbf{R}^*$ contains an infinite number of elements.

Therefore, $<\mathbf{R}^*, \cdot>$ is an infinite abelian group.

(*c*) Let C_1 be set of all non-zero complex nos.

i.e., $C_1 = \{x + iy \mid x, y$ are not both zero and $x, y \in R\}+$

(*i*) Let $z_1 = a + ib, \ z_2 = c + id \in C_1$

Then $z_1 z_2 = (ac - bd) + i(ad + bc)$

And $z_1 z_2 = 0$

if $ac - bd = 0$ and $ad + bc = 0$

which is possible when either $a = 0 = b$

or $c = 0 = d$

$\Rightarrow$ either $a + ib$ or $c + id$ is a zero complex number.

But $a + ib$ and $c + id$ both are non-zero complex numbers.

Thus $z_2 z_2$ is a non-zero complex number

$\therefore$ $z_1 z_2 \in C_1$

Thus C_1 is closed under multiplication.

(*ii*) Let $z_1 = a + ib, \ z_2 = c + id, \ z_3 = e + if \in C_1$

Then $(z_1 z_2) z_3 = [(a + ib)(c + id)](e + if)$

$= [(ac - bd) + i(ad + bc)](e + if)$

$= [(ac - bd)e - (ad + bc)f] + i[(ac - bd)f + (ad + bc)e]$

And $z_1 (z_2 z_3) = (a + ib)[(c + id)(e + if)]$

$= (a + ib)[(ce - df) + i(cf + de)]$

$$= [a(ce-df)-b(cf+de)]+i[b(ce-df)+a(cf+de)]$$
$$= [ace-adf-bcf-bde]+i[bce-bdf+acf+ade]$$
$$= [ace-bde-adf-bcf]+i[acf-bdf+ade+bce]$$
$$= [(ac-bd)e-(ad+bc)f]+i[(ac-bd)f+(ad+bc)e]$$

$\therefore \quad (z_1 z_2) z_3 = z_1 (z_2 z_3)$.

Thus multiplication in C_1 is associative $1 + i0 \in C_1$ such that

(iii) $(a + ib) = (1 + i0) = a + ib = (a + ib)(1 + i0)$

$\therefore$ $1 + i0$ is the identity element.

(iv) Let $z = a + ib \in C_1 \Rightarrow$ a, b are reals and are not both zero.

Now $$\frac{1}{z} = \frac{1}{a+ib} = \frac{a-ib}{(a+ib)(a-ib)} = \frac{a-ib}{a^2+b^2}$$

$$= \frac{a}{a^2+b^2} + i\left(\frac{-b}{a^2+b^2}\right)$$

Since a and b are not both zero $\Rightarrow$ $a^2 + b^2 \neq 0$.

Thus $\frac{1}{z} \in C_1$

Check that $z \cdot \frac{1}{z} = 1 + i0 = \frac{1}{z} \cdot z$

$\therefore \frac{1}{z} = \left(\frac{a}{a^2+b^2}\right) + i\left(\frac{-b}{a^2+b^2}\right)$ is multiplicative inverse of $z \in C_1$

Hence C_1 is a group under multiplication.

Example 7. Let $\mathbf{Q}^*$ denote the set of all rational numbers except -1. Show that $\mathbf{Q}^*$ forms an infinite abelian group under the operation $*$ defined by

$$a * b = a + b + ab, \text{ for } a, b \in \mathbf{Q}^*.$$

Sol. Here $\mathbf{Q}^*$ = The set of all rational numbers other than -1.

For $a, b, c \in \mathbf{Q}^*$

$\Rightarrow$ a, b, c are rational numbers other than -1.

(i) **Closure property :** Since a and b are rational numbers so $a + b + ab$ is also a rational number

If $a + b + ab = -1$ then $a + b + ab + 1 = 0$

$\Rightarrow$ $a + ab + b + 1 = 0$

$\Rightarrow$ $a(1 + b) + (1 + b) = 0$

$\Rightarrow$ $(a + 1)(b + 1) = 0$

$\Rightarrow$ $a = -1$ or $b = -1$, which is not true

$\therefore$ $a + b + ab \neq -1 \Rightarrow a + b + ab \in \mathbf{Q}^*$.

$\therefore$ closure property holds in $\mathbf{Q}^*$.

(*ii*) **Associative property :**

$$(a * b) * c = (a + b + ab) * c$$

$$= a + b + ab + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc$$

$$a * (b * c) = a * (b + c + bc)$$

$$= a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc$$

$\therefore \quad (a * b) * c = a * (b * c)$

$\therefore$ associative law holds in $\mathbf{Q}^*$.

(*iii*) **Existence of identity :** Let $e \in \mathbf{Q}^*$ be the identity element of $\mathbf{Q}^*$. Then

$$a * e = a = e * a$$

$$\Rightarrow \quad a + e + ae = a$$

$$\Rightarrow \quad (1 + a)e = 0$$

$$\Rightarrow \quad e = 0 \qquad (\because a \neq -1 \Rightarrow 1 + a \neq 0)$$

(*iv*) **Existence of inverse :** For any $a \in \mathbf{Q}^*$, let

$$a * b = 0$$

$$\Rightarrow \quad a + b + ab = 0$$

$$\Rightarrow \quad a + (1 + a)b = 0$$

$$\Rightarrow \quad (1 + a)b = -a$$

$$\Rightarrow \quad b = -\frac{a}{1+a} \in \mathbf{Q}^*.$$

as $\quad b = -\dfrac{a}{1+a} \neq -1$

$$\left[\because \quad \text{if } -\frac{a}{1+a} = -1 \Rightarrow -a = -1 - a \Rightarrow 0 = -1 \text{ which is not true}\right]$$

$\therefore \quad -\dfrac{a}{1+a}$ is the inverse of a.

(*v*) **Commutative property :**

$$a * b = a + b + ab$$

$$= b + a + ba$$

$$= b * a.$$

Hence $\mathbf{Q}^*$ forms an abelian group under the composition $*$.

Remark : We can check closed property, commutative property, existence of identity element and existence of inverse from the composition table, which we define as :

Composition Table or Operation Table

A composition table is a type of square array which indicates all the possible 'products' in the system. (The system must be finite). The elements to the left of the operation are arranged on the left of the table and the elements on the right of the operation are arranged on the top of the table. Of course the order of the elements on the top should be kept the same as the order of the elements on the left.

The composition table can be constructed by the rule

(i, j)th entry in the table

= (ith entry on the left) $\cdot$ (jth entry on the top).

Further Let S be finite set and * be a binary operation on S. From composition table, we can draw the following conclusions :

(*i*) If all the elements in the composition table are the elements of S then S is closed under * operation.

(*ii*) If any row is same as the first row in the composition table then the exteme left element in the 2^{nd} row is the left identity of S. Similarly, if any column is some as the first column. Then the element at the top of 2^{nd} column is the right identity of S.

(*iii*) If every row contains only one identity element, then the elemen headed by that row works as the left inverse of the element headed by that column, in which the identity element lies. Also then the element headed by the column is the right inverse of the element headed by that row.

(*iv*) If all the entries in a row are different, then the left concellation law holds. Similarly if all the entries in a column are different, then right cancellation law holds.

(*v*) If the entries in the composition table are symmetrical above the principal diagonal, then S is commutative w.r.t. the operation *.

Example 8. Show that the set $G = \{1, \omega, \omega^2\}$ of cube roots of unity forms a finite abelian group of order 3 under multiplication of complex numbers.

Sol. Here $G = \{1, \omega, \omega^2\}$.

To prove that $\langle G, \cdot \rangle$ is an abelian group. We form the composition table using $\omega^3 = 1$ as given below :

•	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(*i*) **Closure Property** : Since all the elements in composition table are elements of G, so G is closed under multiplication.

(*ii*) **Associativity** : Since the elements of G are complex numbers and multiplication of complex numbers is associative, so multiplication is associative in G also.

(*iii*) **Existence of identity** : Since 2^{nd} row is same as the first row

$\therefore$ 1 is the left identity. Also 2^{nd} column is same as the first column

$\therefore$ 1 is the right identity. So 1 is the identity of G.

i.e., $1 \cdot a = a = a \cdot 1 \quad \forall\, a \in G$.

(*iv*) **Existence of inverse :** Here each row (column) of the composition table contains identity element 1 once and only once. So the element left to 1 is the left inverse of the element above 1. Similarly the element above 1 is the right inverse of element left to 1.

Thus we see that

$1 \cdot 1 = 1 = 1 \cdot 1$ so $1^{-1} = 1$.

Also $\omega \cdot \omega^2 = 1 = \omega^2 \cdot \omega$, so $\omega^{-1} = \omega^2$ and $(\omega^2)^{-1} = \omega$.

(*v*) *Abelian* : Since the entries in the composition table are symmetrical about the principal diagonal.

Hence G is an abelian group under mulitplication.

Example 9. Show that the set G of all n-nth roots of unity forms an abelian group of order n, under the usual multiplication of complex numbers, where n is a fixed positive integer.

Sol. Let G = The set of all n-nth roots of unity

$$= \left\{ e^{\frac{i2k\pi}{n}} : 0 \le k < n \right\} = \left\{ 1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots\ldots, e^{\frac{2\pi i(n-1)}{n}} \right\}$$

The operation is multiplication of complex numbers.

Closure property :

$$\forall\ e^{\frac{2ik_1\pi}{n}}, e^{\frac{2ik_2\pi}{n}} \in G,\ 0 \le k_1, k_2 < n.$$

Now $e^{\frac{2ik_1\pi}{n}} \cdot e^{\frac{2ik_2\pi}{n}} = e^{\frac{2i(k_1+k_2)\pi}{n}} \in G$ if $k_1 + k_2 < n$

and the closure property is satisfied.

If $k_1 + k_2 \ge n$, then by division algorithm,

$$k_1 + k_2 = nq + r, \text{ where } 0 \le r < n \text{ and } q \in Z.$$

Here $e^{\frac{2ik_1\pi}{n}} \cdot e^{\frac{2ik_2\pi}{n}} = e^{\frac{2i(k_1+k_2)\pi}{n}} = e^{\frac{2i(nq+r)\pi}{n}}$

$$= e^{2iq\pi} \cdot e^{\frac{2ir\pi}{n}} = \left(e^{2i\pi}\right)^q \cdot e^{\frac{2ir\pi}{n}}$$

$$= (1)^q \cdot e^{\frac{2ir\pi}{n}} \qquad [\text{But } e^{2i\pi} = \cos 2\pi + i \sin 2\pi = 1 + i0 = 1]$$

$$= e^{\frac{2ir\pi}{n}} \in G \text{ as } 0 \le r < n.$$

$\therefore$ the closure property is satisfied.

Associativity and Commutativity : Since the elements of G are complex numbers and multiplication of complex numbers is associative and commutative.

$\therefore$ multiplication is associative and commutative in G.

Existence of identity : When $k = 0$, then $e^{\frac{i2(0)\pi}{n}} = e^0 = 1$.

Here 1 works as the identity element in G.

Existence of inverse : The inverse of 1 is 1 itself.

$\forall\ e^{\frac{2ik\pi}{n}} \in G,\ k = 1, 2, 3, \ldots\ldots n-1$, then $e^{\frac{2i(n-k)\pi}{n}} \in G$

such that $e^{\frac{2ik\pi}{n}} \cdot e^{\frac{2i(n-k)\pi}{n}} = e^{\frac{2in\pi}{n}} = e^{2i\pi} = 1.$

$\therefore$ inverse of $e^{\frac{2ik\pi}{n}}$ is $e^{\frac{2i(n-k)\pi}{n}}$ [$\because$ the operation is commutative]

Hence $\langle G, \cdot \rangle$ forms a finite abelian group.

Example 10. Let $G = \left\{ \pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$.

Prove that G forms a finite non-abelian group of order 8 under the composition of matrix multiplication.

Sol. Given $G = \{\pm 1, \pm i, \pm j, \pm k\}$

The operation denoted by multiplicatively is defined as

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k = -ji, jk = i = -kj, ki = j = -ik$$

Clearly the system is closed under the given operations and associative law holds.

i.e. $\forall\ a, b \in G \Rightarrow a \cdot b \in G$ and $\forall\ a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$

The element $1 \in G$ works as the identity element as

$\forall\ a \in G,\ a \cdot 1 = a = 1 \cdot a.$ [$\because$ $1 \cdot 1 = 1$ and $(-1)(-1) = 1$]

Inverse of 1 is 1 and inverse of -1 is -1 [$\because$ $i(-i) = 1$]

Inverse of i is $-i$ and inverse of $-i$ is i [$\because$ $j(-j) = 1$]

Inverse of j is $-j$ and inverse of $-j$ is j [$\because$ $k(-k) = 1$]

Inverse of k is $-k$ and inverse of $-k$ is k [$\because$ $ij = k$ and $ji = -k$]

Further since $ij \neq ji$

i.e. $\forall\ a, b \in G,\ ab \neq ba$ (in general).

Thus G is a finite non abelian group of order 8.

QUARTERNION GROUP

If we let

$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, $j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$ then, we have the identities $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j; ji = -k, kj = -i, ik = -j$

then, the set $G = \{\pm 1, \pm i, \pm j, \pm k\}$ form a finite non-abelian group. This group is called **Quarternion Group** and is generally denoted by Q_8.

Example 11. (*a*) Show that the set of all matrices of the form $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, where α is a real number forms an abelian group under the operation of matrix multiplication.

(*b*) Show that the set G of all $m \times n$ matrices over **Z** (or **Q**, **R** or **C**) forms an infinite abelian group under the operation of addition of matrices.

Sol. (*a*) Let $G = \{A_\alpha : A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, where $\alpha \in \mathbf{R}\}$.

The binary operation defined on G is multiplication of matrices.

(*i*) **Closure Property :** Let $A_\alpha, A_\beta \in G$ be any two elements

where $A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$, $A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$, $\alpha, \beta \in \mathbf{R}$

Now $A_\alpha A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

$$= \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & -\cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta + \cos\alpha\sin\beta & -\sin\alpha\sin\beta + \cos\alpha\cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$$

$= A_{\alpha+\beta} \in G$, for $\alpha\beta \in \mathbf{R} \Rightarrow \alpha + \beta \in \mathbf{R}$.

$\therefore$ Closure property hold in G.

(*ii*) **Associative Property :** For all $A_\alpha, A_\beta, A_\gamma \in G$,

$$(A_\alpha A_\beta).A_\gamma = (A_{\alpha+\beta})\,A_\gamma = A_{(\alpha+\beta)+\gamma} = A_{\alpha+(\beta+\gamma)} \quad [\because (\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)]$$

$$= A_\alpha \cdot A_{\beta+\gamma} = A_\alpha \cdot (A_\beta \cdot A_\gamma)$$

$\therefore$ Associative property holds in G.

(*iii*) **Existence of identity :** $\exists$ an element

$A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in G such that

$$A_\alpha . A_0 = A_{\alpha+0} = A_\alpha = A_0 \cdot A_\alpha, \forall\, A_\alpha \in G$$

$\therefore$ A_0 works for the identity element for G.

(*b*) Let G = The set of all $m \times n$ matrices over integers **Z**.

(*i*) **Closure property.** Let A, B, $\in$ G

$\therefore$ $A = \left(a_{ij}\right)_{m\times n}$ and $B = \left(b_{ij}\right)_{m\times n}$ where $a_{ij}, b_{ij} \in \mathbf{Z}$ $\forall$ i, j

Then $A + B = \left(a_{ij} + b_{ij}\right)_{m\times n}$

Since $a_{ij}, b_{ij} \in \mathbf{Z}$

$\therefore$ $A + B \in G$ $\forall$ $A, B \in G$.

$\therefore$ closure property holds in G.

(*ii*) **Associative property.** Since the set of all matrices is associative under addition, so **G** is associative under +.

(*iii*) **Existence of identity.** Take $O = [0]_{m\times n}$ where 0 is zero integer

Let $A = \left(a_{ij}\right)_{m\times n} \in G$ so that $a_{ij} \in \mathbf{Z}$.

Then $O + A = (0)_{m\times n} + \left(a_{ij}\right)_{m\times n} = \left(0 + a_{ij}\right)_{m\times n}$

$= \left(a_{ij}\right)_{m\times n} = A = A + O$ similarly.

O is identity of G.

(*iv*) **Existence of inverse.**

Let $A = \left(a_{ij}\right)_{m\times n} \in G$, so that $a_{ij} \in \mathbf{Z}$

$a_{ij} \in \mathbf{Z} \Rightarrow -a_{ij} \in \mathbf{Z} \Rightarrow B = \left(-a_{ij}\right)_{m\times n} \in G$

$A + B = \left(a_{ij}\right)_{m\times n} + \left(-a_{ij}\right)_{m\times n}$

$= \left(a_{ij} + \left(-a_{ij}\right)\right)_{m\times n} = (0)_{m\times n} = O = B + A$, similarly.

$\therefore$ B is inverse of A and $B \in G$.

Also G contains an infinite number of elements

(*v*) Let A, B $\in$ G as in (*i*)

Then $A + B = \left(a_{ij} + b_{ij}\right)_{m\times n}$ as in (*i*)

$= \left(b_{ij} + a_{ij}\right)_{m\times n}$, since + is commutative in **Z**

$= \left(b_{ij}\right)_{m\times n} + \left(a_{ij}\right)_{m\times n}$

$= B + A$.

$\therefore$ G is commutative under +.

Hence G is an infinite commutative group under +

ADDITION MODULO n

Now we define another type of addition known as '**Addition modulo n**' and written as '$a +_n b$' where a and b are any integers and n is a fixed positive integer.

We define $a +_n b = r, 0 \le r < n$ where r is least non-negative remainder when $a + b$ (usual addition) is divided by n. Also it is written as $a + b \equiv r \pmod n$, *e.g.*,

(*i*) $18 +_5 9 = 2$ as $18 + 9 = 27 = 5\,(5) + 2$, *i.e.*, 2 is least non-negative remainder when $18 + 9$ is divided by 5.

(*ii*) $-37 +_4 2 = 1$ as $-37 + 2 = -35 = -9\,(4) + 1$, *i.e.*, 1 is least non-negative remainder when $-37 + 2$ is divided by 4.

Note : When a and b are integers such that $a - b$ is divisible by n (a fixed positive integer) then we write $a \equiv b \pmod n$ and read it as a **is congruent to** b **modulo** n.

e.g., $21 \equiv 1 \pmod 5$, $33 \equiv 1 \pmod 4$

MULTIPLICATION MODULO n

Further we define another type of multiplication known as '**Multiplication modulo n**' and written as $a \times_n b$ where a and b are any integers and n is a fixed positive integer.

We define $a \times_n b = r,\ 0 \le r < n$ where r is least non-negative remainder when ab (usual multiplication) is divided by n. Also it is written as $ab \equiv r \pmod n$, *e.g.*,

(*i*) $8 \times_7 3 = 3$ as $8 \times 3 = 24 = 3(7) + 3$, *i.e.*, 3 is least non-negative remainder when $8 \times 3 = 24$ is divided by 7.

(*ii*) $3 \times_6 5 = 3$ as $3 \times 5 = 15 = 2(6) + 3$ as 6 divides $3 \times 5 - 3$, *i.e.*, $3.5 \equiv 3 \pmod 6$.

ADDITIVE GROUP OF INTEGERS MODULO n

Example 12. Show that the set Z_n or $J_n = \{0, 1, 2, 3, \ldots\ldots, n-1\}$, $n > 1$, $n \in Z$ forms a finite abelian group under the composition of addition (congruence) modulo n.

Sol. Given Z_n or $J_n = \{0, 1, 2, 3, \ldots, n-1\}$, $n > 1$, $n \in \mathbf{Z}$.

The composition defined is addition modulo n.

$\therefore$ $\forall\ a, b \in J_n$, $a * b$ or $a +_n b$ = least non negative remainder r when $a + b$ is divided by n

i.e. $a * b$ or $a +_n b = r \Rightarrow a + b - r$ is divisible by n.

i.e. $a + b \equiv r \pmod n$.

Closure property : $\forall\ a, b \in J_n$, $0 \le a, b < n$

$a + b \equiv r \pmod n$, where $0 \le r < n$.

Now $r \in J_n$.

$\therefore$ the closure property is satisfied.

Associativity : $\forall\ a, b, c \in J_n$

The least non-negative remainder remains the same if

$(a+b)+c$ or $a+(b+c)$ are divided by n.

$\therefore \quad (a * b) * c = a * (b * c)$

Thus associative property holds in J_n.

Commutativity : $\forall\ a, b \in J_n$

The least non-negative remainder remains the same if $a+b$ or $b+a$ is divided by n.

i.e. $a+b \equiv r \pmod n$ and $b+a \equiv r \pmod n$

$\therefore \quad a * b = b * a.$

Thus commutative property holds in J_n.

Existence of identity : $\forall\ a \in J_n,\ 0 \le a < n.$

Here a is the least non-negative remainder when $a+0$ or $0+a$ are divided by n

$\therefore \quad a * 0 = a = 0 * a$

Thus $0 \in J_n$ is the identity element.

Existence of inverse : Inverse of $0 \in J_n$ is 0 itself.

Also for all $a \in J_n,\ a \neq 0,\ n-a \in J_n$ such that

$a+(n-a) \equiv 0 \pmod n$

and $(n-a)+a \equiv 0 \pmod n$

i.e. $a * (n-a) = 0 = (n-a) * a$

Thus $n-a$ is the inverse of a.

Hence $< J_n, * >$ is an abelian group of order n.

Note : J_n under addition modulo n is called **additive group of integers modulo n.**

Example 13. Show that the set $J_p = \{1, 2, 3, ..., p-1\}$, where p is a prime number forms a finite abelian group of order p, under the composition of multiplication (congruence) modulo p.

Sol. Given $J_p = \{1, 2, 3, ..., p-1\}$, p is a prime number, $p > 1$. The composition defined is multiplication modulo p.

$\therefore \quad \forall\ a, b \in J_p,\ a * b$ or $a \times_p b$ = least non negative remainder r when $a\,b$ is divided by p.

i.e. $a * b$ or $a \times_p b = r \Rightarrow a\,b - r$ is divisible by p

i.e. $a\,b \equiv r \pmod p$.

Closure property : $\forall\ a, b \in J_p,\ 1 \le a, b < p$

$a\,b \equiv r \pmod p$ where $0 \le r < p$

If possible let $r = 0$, then $a\,b \equiv 0 \pmod p$

$\Rightarrow \quad p \mid a\,b - 0 \quad \Rightarrow \quad p \mid a\,b$

But p is prime.

$\therefore$ either $p \mid a$ or $p \mid b$, where $1 \le a, b < p$.

$\therefore$ we get an absurd result.

Thus $r \neq 0$ *i.e.* $r \in J_p \Rightarrow J_p$ is closed under $*$.

Commutativity : $\forall\ a, b \in J_p$

The least non-negative remainder remains the same if ab or ba is divided by p.

i.e. $a\,b \equiv r \pmod p$ and $b\,a \equiv r \pmod p$

$\therefore$ $a * b = b * a$

Thus commutative property holds in J_p.

Associativity : $\forall\ a, b, c \in J_p$

The least non-negative remainder remains the same if $(a\,b)\,c$ or $a\,(b\,c)$ is divided by p.

$\therefore$ $(a * b) * c = a * (b * c)$

Thus associative property holds in J_p.

Existence of identity : $\forall\ a \in J_p$

$a * 1 = a = 1 * a$ as $a \,.\, 1$ and $1 \,.\, a$ leave the same remainder a when divided by p.

$\therefore$ $1 \in J_p$ works as an identity element for the set J_p.

Existence of inverse : $\forall\ a \in J_p$, $1 \le a < p$

Consider a set $S = \{1 * a, 2 * a, 3 * a, \ldots\ldots, (p-1) * a\}$

As J_p is closed, therefore $S \subseteq J_p$

Further all the elements of S are different.

If possible

let $i * a = j * a$, $1 \le i, j < p$; $i \neq j$ and let $i > j \Rightarrow 0 < i - j < p$

$\Rightarrow$ $i\,a \equiv j\,a \pmod p$

$\Rightarrow$ $p \mid i\,a - j\,a \Rightarrow p \mid (i-j)\,a$, where p is prime

$\Rightarrow$ either $p \mid i-j$ or $p \mid a$

But $1 \le a < p$ and $0 < i - j < p$ which are absurd.

$\therefore$ all the elements of S are different.

$\Rightarrow$ $0(S) = p - 1 = 0(J_p) \Rightarrow S = J_p$

Now $1 \in J_p \Rightarrow 1 \in S$

let $k * a = 1$ *i.e.* $k\,a \equiv 1 \pmod p$

where $k \in J_p$ is an inverse of a *i.e.* inverse of every element of J_p exists.

Hence $< J_p, * >$ is an abelian group of order $p - 1$.

Note 1. If p is not prime, then J_p is not a group.

e.g. $G = \{1, 2, 3, 4, 5\}$ under multiplication (congruence) modulo 6 is not a group.

Here we find $2, 3 \in G$, but $2 * 3 = 0$

i.e. $2 \cdot 3 \equiv 0 \pmod 6$, where $0 \notin G$.

Thus G is not closed under the given operation.

Note 2. The group J_p is known as **Multiplication group of integers modulo p.**

Remark : The set $G = \{[0], [1], [2], \ldots\ldots, [n-1]\}$ of residue classes modulo n forms a finite abelian group under the operation defined by

$[i] + [j] = [i + j]$, where $[i]$ denotes the residue class of i modulo n.

Here in fact the operation is

$$[i] + [j] = \begin{cases} [i+j] & \text{if} \quad i+j<n \\ [r] & \text{if} \quad i+j \geq n, \end{cases}$$

where $i + j = nq + r$ *i.e.* $i + j \equiv r \pmod n$.

+	[0]	[1]	[2]	.....	$[n-1]$
[0]	[0]	[1]	[2]	.....	$[n-1]$
[1]	[1]	[2]	[3]	.....	[0]
[2]	[2]	[3]	[4]	.....	[1]
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
$[n-1]$	$[n-]$	[0]	[1]	.....	$[n-2]$

Closure Property : Since all the elements in the composition table are the elements of G, so G is closed under the composition +.

Associativity : Since the elements of G are residue classes over integers and addition of integers is associative. So addition of residue classes in G is also associative.

Existence of identity : Since the second row is same as the first row and also the second column is same as the first column.

$\therefore$ [0] works as the identity element of G.

i.e. $[0] + [i] = [i] = [i] + [0]$, $\forall\, [i] \in G$.

Existence of inverse : Here each row (column) of the composition table contains identity element [0] once and only once. So the element left of [0] is the left inverse of the element above [0]. Similarly, the element above [0] is the right inverse of the element left to [0]. Thus we see that inverse of $[i]$ is $[n-i]$, where $1 \leq i \leq n-1$ and inverse of [0] is [0].

Commutativity : Since the entries in the composition table are symmetrical about the principal diagonal.

$\therefore$ Commutative law hold in G.

Moreover, as the set G is finite set. Hence (G, +) form a finite abelian group.

Note : The above group is known as **additive group of residue classes modulo *n*** and is generally denoted by $I/<n>$, the quotient group.

Remark : The set $G = \{[1], [2], \ldots\ldots, [p-1]\}$ of residue classes modulo p forms a finite abelian group under the operation defined by

$[i] \cdot [j] = [ij]$, where $[i]$ denotes the residue class of i modulo p and p is a prime number.

Here in fact the operation is

$$[i] \cdot [j] = \begin{cases} [ij] & \text{if} \quad ij < p \\ [r] & \text{if} \quad ij > p, \end{cases}$$

where $ij = np + r$ *i.e.* $ij \equiv r \pmod{p}$ and $1 \le r \le p-1$

·	[1]	[2]	[3]	.....	[p–1]
[1]	[1]	[2]	[3]	.....	[p–1]
[2]	[2]	[4]	[6]	.....	[p–2]
[3]	[3]	[6]	[9]	.....	[p–3]
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
.....	.....	.....	.....	.....	.....
[p–2]	[p–2]	[p–4]	[p–6]	.....	[2]
[p–1]	[p–1]	[p–2]	[p–3]		[1]

Closure Property : Since all the elements in the composition table are the elements of G, so G is closed under the composition.

Associativity : Since the elements of G are residue classes over integers and multiplication of integers is associative, so multiplication of residue classes in G is also associative.

Existence of identity : Since the second row is same as the first row and also the second column is same as the first column.

$\therefore$ [1] works as the identity element of G.

i.e. $[1] \cdot [j] = [j] = [j] \cdot [1], \forall [j] \in G.$

Existence of inverse : Here each row (column) of the composition table contain identity element [1] once and only once. So the element left of [1] is the left inverse of the element above [1]. Similarly, the element above [1] is the right inverse of the element left to [1]. Thus we see that the inverse of $[p-r]$ is $[r']$ where $1 \le r, r' < p$ such that $[r][r'] = [1]$.

Commutativity : Since the entries in the composition table are symmetrical about the principal diagonal.

$\therefore$ commutative law hold in G.

Moreover, as the set G is finite set. Hence $(G, \cdot)$ form a finite abelian group.

Note : The above group is known as **multiplicative group of residue classes modulo p** and is generally denoted by $I/<p>$, the quotient group.

1.1.5. Some Special Groups

1. General linear group of degree n

Example 14. Show that the set of all $n \times n$ matrices having non-zero determinant over the set of real numbers under the operation of matrix multiplication is a non-abelian group. This group is known as **General linear group of degree n** and is denoted by **GL (n, R)**.

OR

Show that the set of all $n \times n$ non-singular matrices over the set of reals under matrix multiplication is a non-abelian group.

Sol. Let G be the set of all $n \times n$ non-singular matrices over the reals.

Closure Property : Let A, B be any two numbers of G.

$\therefore$ A B is also a $n \times n$ real matrix.

Since $|AB| = |A||B| \neq 0$ (Since $|A| \neq 0, |B| \neq 0$)

$\therefore$ A B is non-singular $n \times n$ matrix over the reals.

$\therefore$ $AB \in G, \forall A, B \in G$.

Thus G is closed under matrix multiplication.

Associativity : Since the set of all matrices is associative under multiplication, so G is also associative under multiplication.

Existence of Identity : Let I be the identity matrix of order $n \times n$, where $|I| = 1 \neq 0$.

Also $AI = A = IA, \quad \forall \ A \in G$.

$\therefore$ I is the identity element of G.

Existence of Inverse : Let $A \in G$ so that A is a $n \times n$ non-singular matrix over the reals.

Let $B = \frac{1}{|A|} \text{adj } A$, then B is an $n \times n$ matrix over the reals.

$$|B| = \frac{1}{|A|}|\text{adj } A| = \frac{|A|^{n-1}}{|A|} = |A|^{n-2} \neq 0,$$

$\therefore$ $B \in G$.

Now $AB = A\frac{1}{|A|} \text{adj } A$ [$\because A \text{ adj } A = |A| I$]

$= \frac{1}{|A|}|A| \cdot I = I.$

Similarly $BA = I$

$\therefore \quad AB = I = BA$

$\therefore \quad A^{-1} = B \in G$

$\therefore$ G is a group under matrix multiplication.

Since G has an infinite number of elements, therefore G is an infinite group.

Also since, in general matrix multiplication is non-commutative, *i.e.* $AB \neq BA$, therefore G is a infinite non abelian group.

Note : The set **GL(n, F)** of all $n \times n$ matrices having non-zero determinant over the field F under th operation of matrix multiplication is a non-abelian group.

II. SPECIAL LINEAR GROUP OF DEGREE n

Example 15. The set of all $n \times n$ matrices having unit determinant over the set of real numbers under th operation of matrix multiplication is a non-abelian group. This group is known as **Special linear group o degree n** and is denoted by **SL(n, R).**

Sol. Let G = SL(n, **R**) = set of all $n \times n$ matrices having unit determinant over the set of real numbers

To show that G forms a non-abelian group under the composition of multiplication of matrices.

Closure Property : Let A, B be any two members of G.

$\therefore \quad |A| = 1, \quad |B| = 1$

Now $|AB| = |A||B| = 1 \cdot 1 = 1$

$\Rightarrow \quad AB \in G, \quad \forall A, B \in G.$

Thus closure property holds in G.

Associativity : Since the multiplication of matrices is an associative operation. Thus the associative property holds in G also.

Existence of Identity : $\exists$ a unit matrix $I = I_n \in G$ such that

$$A \cdot I = A = I \cdot A, \ \forall A \in G$$

$\therefore \quad I \in G$ works for the identity element for G.

Existence of inverse : Let $A \in G$ be any element, then $\exists$

$$B = \frac{1}{|A|} \text{adj } (A) \in G \text{ such that}$$

$AB = I = BA$

For $$|B| = \left| \frac{1}{|A|} \text{adj. } (A) \right| = \frac{|\text{adj. } (A)|}{|A|^n} = \frac{|A|^{n-1}}{|A|^n}$$

$$= \frac{1}{|A|} = \frac{1}{1} = 1.$$

Also $$AB = A \cdot \frac{1}{|A|} \text{adj } (A) = \frac{A \cdot \text{adj } (A)}{|A|} = \frac{|A| I}{|A|} = I.$$

Similarly, $BA = I$

$\therefore$ $AB = I = BA$

$\therefore$ $B = A^{-1}$ is the inverse of the element A in G.

Non-commutativity : Since in general matrix multiplication is non-commutative. In particular matrix multiplication in G is also non-commutative.

Hence $G = SL(n, \mathbf{R})$ forms a non-abelian group under multiplication of matrices.

Note : The set $\mathbf{SL}(n, \mathbf{F})$ of all $n \times n$ matrices having determinant 1 over the field F under the operation of matrix multiplication is a non-abelian group.

III. GROUP OF PERMUTATIONS

Definition : Permutation

Let S be a non-empty set. A permutation on S is defined as a map from S to S which is both one-one and onto.

Example 16. Let A(S) denotes the set of all permutations on a non-empty set S. Then A(S) forms a group under the operation of composition of maps. Moreover if S contains n elements, then the group A(S) contains $n!$ elements. This group **A(S)** is called **Permutation Group.**

Sol. Here, A(S) = The set of all the permutations on S.

$\therefore$ $A(S) = \{f : S \to S$ is a one-one onto map.$\}$

Let $f, g, h \in A(S)$.

$\therefore$ f, g, h are one-one onto maps from S to S.

Closure property : Since f, g are maps from S to S, so $f \circ g$ is also a map from S to S.

$f \circ g : S \to S$ is defined by $(f \circ g)(x) = f(g(x)), \ \forall x \in S$.

We prove that $f \circ g$ is one-one as well as onto.

For one-one :

Let $x_1, x_2 \in S$ such that $(f \circ g)(x_1) = (f \circ g)(x_2)$

$\Rightarrow$ $f(g(x_1)) = f(g(x_2))$

$\Rightarrow$ $g(x_1) = g(x_2)$, since f is one-one

$\Rightarrow$ $x_1 = x_2$, since g is also one-one

$\therefore$ $f \circ g$ is one-one

For onto

Let $z \in S$.

Since $f : S \to S$ is onto and $z \in S$, so $\exists\, y \in S$ such that $f(y) = z$.

Since $g : S \to S$ is onto and $y \in S$, so $\exists\, x \in S$ such that $g(x) = y$.

Consider $(f \circ g)(x) = f(g(x)) = f(y) = z$.

$\therefore$ $f \circ g$ is onto.

So, $f \circ g$ is a one-one map of S onto S.

$\therefore$ $f \circ g$ is a permutation on S.

$\Rightarrow$ $f \circ g \in A(S)$, $\forall f, g \in A(S)$.

Thus A(S) is closed under composition of maps.

Associativity : Let $x \in S$ be an arbitrary element.

For all $f, g, h \in A(S)$,

$\therefore$ $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$

$\therefore$ $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$, $\forall x \in S$.

$\Rightarrow$ $(f \circ g) \circ h = f \circ (g \circ h)$

Thus associativity property holds in A(S).

Existence of identity : Define a map $i : S \to S$ by

$$i(x) = x, \quad \forall x \in S$$

Let $x_1, x_2 \in S$. Then $i(x_1) = i(x_2) \Rightarrow x_1 = x_2$.

$\therefore$ i is one-one.

If $x \in S$, then $i(x) = x$

$\therefore$ i is onto

$\therefore$ i is a one-one map of S onto itself.

$\therefore$ i is a permutation on S.

So, $i \in A(S)$.

Also $(f \circ i)(x) = f(i(x)) = f(x)$, $\forall x \in S$.

$\therefore$ $f \circ i = f$. Similarly $i \circ f = f$, $\forall f \in A(S)$

$\therefore$ i is identity element of A(S).

Existence of inverse : For all $f \in A(S)$, f is one- one and onto map of S to S.

$\therefore$ f is invertible map and f^{-1} is also one - one and onto.

$\therefore$ f^{-1} is a also a permutation on S.

$\therefore$ $f^{-1} \in A(S)$

Also $f^{-1} : S \to S$ is defined by $f^{-1}(y) = x$ iff $f(x) = y$

Let $x \in S$.

$\therefore$ $f(x) \in S$. Let $f(x) = y$ $\therefore$ $y \in S$.

Also $f(x) = y \Rightarrow f^{-1}(y) = x$.

Now $(f^{-1} o f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = i(x)$

$\therefore (f^{-1} o f)(x) = i(x), \forall x \in S.$

$\Rightarrow f^{-1} o f = i$, similarly, $f o f^{-1} = i$

$\therefore f^{-1}$ is inverse of f

$\therefore$ A (S) forms a group under the operation of composition of maps.

Further if S contains n elements, then

The number of elements in A(S)

= The number of permutations of S.

= The number of arrangements of n elements

$= \lfloor n$.

Definition : Symmetric group.

If a set S has n elements, then the group A(S) of permutations on S having $\lfloor n$ elements is called a **symmetric group** of degree n. It is also denoted by S_n.

$\therefore$ Symmetric group S_n = The group of permutations of a set of n elements.

For example. Let f be a permutation on S = { 1, 2, 3, 4 } such that $f(1) = 3$, $f(2) = 4$, $f(3) = 2$, $f(4) = 1$.

We write the above permutation in a better way as $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$. Here in the first line write the elements of S and in the second line we write the images of the elements of S such that the image of each element in first row occurs below it.

Multiplication of the two permutations.

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

Then $f(1) = 2, f(2) = 3, f(3) = 4, f(4) = 1$.

$g(1) = 3, g(2) = 2, g(3) = 1, g(4) = 4$.

Since f takes 1 to 2 and g takes 2 to 2, so fg takes 1 to 2.

f takes 2 to 3 and g takes 3 to 1, so fg takes 2 to 1.

f takes 3 to 4 and g takes 4 to 4, so fg takes 3 to 4.

Finally, f takes 4 to 1 and g takes 1 to 3, so fg takes 4 to 3.

Here, to find fg, we first applied f and then g.

$\therefore fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

Cyclic permutation.

A permutation f on a set S is called a **cyclic permutation of length l** if $\exists\ x_1, x_2, \ldots\ldots, x_\ell \in S$ such that $f(x_1) = x_2,\ f(x_2) = x_3, \ldots\ldots,\ f(x_{\ell-1}) = x_\ell,\ \ f(x_\ell) = x_1$ and $f(x) = x\ \forall\ x \in S$ if $x \neq x_1, x_2, \ldots\ldots, x_\ell$.

We write it as $(x_1\, x_2 \ldots\ldots x_{\ell-1}\, x_\ell)$.

Here the image of each element in the row is the next element and the image of the last element is the first element.

For example, if $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix}$ be a permutation of degree 6.

Then $f(1) = 3,\ f(3) = 4, f(4) = 1, f(2) = 2, f(5) = 5, f(6) = 6$.

Thus $f = (134)$ is a cyclic permutation of length 3.

Here the element whose image is the element itself is called an **invariant element**. In the above example 2, 5, 6 are invariant elements.

Remark : (*i*) The length of a cyclic permutation is the number of objects permuted by the cycle.

(*ii*) A cyclic permutation of length ℓ is also called **ℓ-cycle.**

(*iii*) A cycle of length 1 is the **identity permutation.**

(*iv*) A cycle of length 2 is called **transposition** or **bi-cycle** or **2-cycle.**

Example 17. Write down all the elements of the permutation group (or symmetric group) S_3 on three elements 1, 2 and 3.

Sol. Let $S = \{1, 2, 3\}$.

Then there are $\lfloor 3 = 6$ elements in S_3

$$\therefore\quad S_3 = \left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$$

This can be written as

$S_3 = \{i, (12), (13), (23), (123), (132)\}$.

EXERCISE 1.1

1. Show that the set of natural numbers form a monoid under the composition of multiplication.
2. Let X be any non-empty set, let P(X) denote the power set of X. Then show that
   (*a*) P(X) form a monoid under the operation $\cap$, intersection of sets.
   (*b*) P(X) form a monoid under the operation $\cup$, union of sets.
3. Let $M_2(I)$ be the set of all 2×2 matrices over the set of integers. Show that the set $M_2(I)$ form a monoid under the composition of multiplication of matrices.
4. Show that the set $S = \{-1, 1\}$ under the operation of usual multiplication of integers, is an abelian group of order two.
5. Show that the set **Z** of integers does not form a group under multiplication.

6. Show that the set of rational numbers does not form a group under multiplication.
7. Show that the set of all non-zero rational numbers forms a group under multiplication.
8. Show that the set R of reals form an infinite abelian group w.r.t. usual addition of reals.
9. Show that the set of reals **R** does not form a group under multiplication.
10. Show that the set **C** of all complex nu8mbers forms an infinite abelian group under the operation of addition of complex numbers.
11. Check whether the set E of all even integers forms a group under the binary operation $a * b = 2a + 2b$
12. Does the set **E** of all even integers form a group under usual addition ?
13. Check whether the set **O** of all odd integers forms a group under addition.
14. Prove that the set of complex numbers z, such that $|z| = 1$ forms a group under multiplication of complex numbers.
15. Show that the set of $\mathbf{Q}^+$ of all positive rational numbers forms an abelian group under the operation defined by

$$a * b = \frac{ab}{2} \quad \forall \ a, b \in \mathbf{Q}^+.$$

16. Show that the set of all positive rational numbers under the composition defined by $a * b = \frac{ab}{3}$ forms an infinite abelian group.
17. Let m be an arbitrary but a fixed non-zero integer. Then show that the set $G = \{ma : a \in \mathbf{Z}\}$ of all integral multiple of m, is an infinite abelian group w.r.t. ordinary addition of integers.
18. Let $\mathbf{Q}^*$ denotes the set of all rational numbers except 1, then show that $\mathbf{Q}^*$ forms an infinite abelian group under the operation o defined by $a \, o \, b = a + b - ab$ for all $a, b \in \mathbf{Q}^*$.
19. (*a*) Does the set of all integers form group under the operation $a * b = a + b + 1$.

    (*b*) Examine if **Z**, the set of integers, is a group under the binary operation o given $a \circ b = a + b - 1$.

    (*c*) Examine if **Z**, the set of integers, is a group under the binary operation o given by $a \circ b = a + b + 2 \ \forall \ a, b \in \mathbf{Z}$.
20. Let a set $G = \{e, a, b, c\}$ under a composition defined as below by given composition table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

    Is G a group ? If it is, whether abelian ?
21. Show that the set $G = \{ 2^n : n$ is an integer $\}$ forms an infinite abelian group under multiplication.
22. Let a be an arbitrary but a fixed non-zero integer. Show that the set $G = \{ a^n ; n \in \mathbf{Z}\}$ of all integral powers of a, form an infinite abelian group w.r.t. multiplication.

23. Let $G = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$. Show that G is an infinite abelian group w.r.t. addition composition defined by, for all $a + b\sqrt{2}$, $c + d\sqrt{2} \in G, (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$, where $a, b, c, d \in \mathbf{Q}$.

24. Show that the set $G = \{x : x$ is a rational number, $0 < x \leq 1\}$ does not form a group w.r.t. ordinary multiplication of rational numbers.

25. Let X be any non-empty set, let P(X) denotes the power set of X. Show that

(*i*) P(X) does not form a group under the operation $\cap$, intersection of sets.

(*ii*) P(X) does not form a group under the operation $\cup$, union of sets.

26. Show that the set of all 2×2 non-singular matrices over the set of real numbers **R**, forms an infinite non-abelian group under the composition of matrix multiplication.

27. Show that the set $G = \left\{\begin{bmatrix} x & y \\ x & y \end{bmatrix}, x, y \in \mathbf{R}, \text{s.t.} x + y \neq 0\right\}$ does not form a group under the operation of matrix multiplication.

28. Show that the set $G = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a, b, c, d \in \mathbf{R}$ s.t. $a d - b c = 1\right\}$ forms a non-abelian group.

29. Show that the set of all 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where a, b are real numbers, not both zero simultaneously, forms an infinite abelian group.

30. Prove that all matrices of the form $\begin{bmatrix} x & x \\ x & x \end{bmatrix}$, where x is a non-zero real, is a group with respect to matrix multiplication.

31. Show that the following set with the given binary operation is a group. Find the identity element and the inverse of each element and check whether it is abelian group or not.

(*a*) Let $S = \{(a, b) : a, b \in \mathbf{R}$, s.t. $a \neq 0\}$, the binary operation $\times$ on S is defined as $(a, b) \times (c, d) = (a c, b c + d)$.

(*b*) Let $S = \{(a, b) : a, b \in \mathbf{I}$ s.t. either $a \neq 0$ or $b \neq 0\}$, the binary operation $\times$ on S is defined as $(a, b) \times (c, d) = (a c - b d, a d + b c)$

(*c*) Let $G = \{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ where $a \neq 0$, be a real number$\}$, the binary operation defined as usual multiplication of matrices.

(*d*) Let $G = \{\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, where a, b, c are real numbers$\}$, the binary operation on G as the usual multiplication of matrices.

32. Show that the set $G = \{0, 1, 2, 3, 4, 5\}$ is a finite abelian group of order 6 under addition modulo 6.
33. Show that the set $G = \{1, 2, 3, 4, 5, 6\}$ is a finite abelian group of order 6 under the composition 'multiplication modulo 6'.
34. Prove that the set of positive integers which are less than n and co-prime to n forms an abelian group under the operation of multiplication modulo n.

Or

Show that the set $U(n) = \{x : x \in \mathbf{Z} \text{ s.t. } 1 \leq x < n \text{ and } (x, n) = 1\}$ forms a finite abelian group under the operation of multiplication modulo n.

35. Show that the set $G = \{0, 1, 2, 3\}$ forms a group under addition modulo 4.
36. Show that the set of all one-one onto maps from set A to A forms a group.
37. Let S be a non-empty set and P (S) denote the power set of S. Then $(P(X), \Delta)$ is an abelion group under the binary operation of symmetric difference Δ, given by $A \Delta B = (A \setminus B) \cup (B \setminus A) \forall A, B \in P(S)$
38. Show that the set of all rational numbers of the form $\frac{p}{2^q}$ is a group under addition, where p and q are integers.
39. Show that the set $S = \{2^a 3^b : \text{where } a, b \text{ are integers}\}$ under the binary operation defined as usual multiplication of rational is an abelian group.
40. Write down all the elements of the permutation group (or symmetric group) S_4 on four elements 1, 2, 3 and 4.

ANSWERS

11. Not a group 12. Group 13. Not a group 19. (a) group (b) group (c) group
20. Abelian group

31. (a) $(1, 0), \left(\frac{1}{a}, -\frac{b}{a}\right)$, not abelian group (b) $(1, 0), \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$, abelian group

(c) $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{bmatrix}$, abelian group (d) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$, not abelian

1.2. Elementary Properties of a Group

Let $< G, * >$ be a group under the operation $*$. Then G has the following elementary properties.

I. Uniqueness of identity element

The identity element of a group is unique.

Proof : If possible, suppose that e_1, e_2 are two identity elements of a group.

$\therefore$ $e_1 * e_2 = e_2$ (Since e_1 is identity element) ...(1)

also $e_1 * e_2 = e_1$ (Since e_2 is identity element) ...(2)

Thus $e_1 = e_2$ [From (1) and (2)]

$\therefore$ the identity element of a group is unique.

II. Uniqueness of inverse element

The inverse of each element of a group is unique.

Proof. Let e be the identity element of the group $(G, *)$ and $a \in G$ be an arbitrary element.

If possible, let $b_1, b_2 \in G$, be two inverses of a

$\therefore \quad a * b_1 = e = b_1 * a \qquad (\because\ b_1 \text{ is inverse of } a)$ ...(1)

and $a * b_2 = e = b_2 * a \qquad (\because\ b_2 \text{ is inverse of } a)$ ...(2)

Now $b_1 = b_1 * e$ (Since e is identity of G)

$= b_1 * (a * b_2)$ [$\because$ of (2)]

$= (b_1 * a) * b_2$ (By associativity in G)

$= e * b_2$ [$\because$ of (1)]

$= b_2$

$\therefore \quad b_1 = b_2$

Hence each element of a group has unique inverse.

III. Cancellation laws hold in a group

For $a, b, c \in G$, we have

$a * b = a * c \Rightarrow b = c$ (Left cancellation law)

$b * a = c * a \Rightarrow b = c$ (Right cancellation law)

Proof : Let $a, b, c \in G$. Since $a \in G$ so $a^{-1} \in G$ such that

$a^{-1} * a = e = a * a^{-1}$ ...(1)

Now suppose that $a * b = a * c$

$\Rightarrow \quad a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow \quad (a^{-1} * a) * b = (a^{-1} * a) * c,$ (By associative law in G)

$\Rightarrow \quad e * b = e * c$

$\Rightarrow \quad b = c.$

$\therefore \quad a * b = a * c \Rightarrow b = c$

Similarly, we can prove that

$b * a = c * a \Rightarrow b = c.$

IV. For every $a \in G$, $(a^{-1})^{-1} = a$.

Proof : $\forall\ a \in G \Rightarrow a^{-1} \in G,$

then $a\,a^{-1} = e = a^{-1}a$

$\Rightarrow$ inverse of a is a^{-1}

Again $a^{-1}a = e = a\,a^{-1}$

$\Rightarrow$ inverse of a^{-1} is a

i.e. $(a^{-1})^{-1} = a.$

V. Reversal law for inverse of the product

$(a * b)^{-1} = b^{-1} * a^{-1} \quad \forall\, a, b \in G.$

Proof. Since $a, b \in G \quad \therefore\ a * b \in G$

$\Rightarrow\ c \in G$ where $c = a * b$ ...(1)

Also $b, a \in G \quad \Rightarrow\ b^{-1}, a^{-1} \in G \Rightarrow b^{-1} * a^{-1} \in G$

$\Rightarrow\ d \in G$ where $d = b^{-1} * a^{-1}$ ...(2)

Consider $c * d = (a * b) * d$ [$\because$ of (1)]

$= a * (b * d)$ (Associative law in G)

$= a * \left(b * \left(b^{-1} * a^{-1}\right)\right)$ [$\because$ of (2)]

$= a * \left(\left(b * b^{-1}\right) * a^{-1}\right),$ (By associativity in G)

$= a * (e * a^{-1}) = a * a^{-1} = e.$

$\therefore\quad c * d = e.$ [$\because$ of (2)]

Now consider $d * c = (b^{-1} * a^{-1}) * c$ (Associative law in G)

$= b^{-1} * (a^{-1} * c)$ [$\because$ of (2)]

$= b^{-1} * \left(a^{-1} * (a * b)\right)$ (Associative law in G)

$= b^{-1} * \left((a^{-1} * a) * b\right)$

$= b^{-1} * (e * b) = b^{-1} * b = e$

$\therefore\quad d * c = e$

$\therefore\quad c * d = e = d * c$

$\Rightarrow\quad c^{-1} = d$

$\Rightarrow\quad (a * b)^{-1} = b^{-1} * a^{-1}.$

VI. If $a, b \in G$ be any elements. Then the equations $a * x = b$ and $y * a = b$ have unique solution in G.

Proof. We first prove that the equation $a * x = b$ has a solution in G.

Since $a \in G$, so $\exists\ a^{-1} \in G$ such that ...(1)

$a * a^{-1} = e = a^{-1} * a$

Since $a^{-1}, b \in G$ so $a^{-1} * b \in G.$

Take $x = a^{-1} * b \quad \therefore\ x \in G$

Now $a * x = a * (a^{-1} * b)$

$= (a * a^{-1}) * b$ (Associative law in G)

$= e * b$

$= b$

$\therefore$ the equation $a * x = b$ has a solution in G.

Uniqueness. Let x_1, x_2 be two solutions of the equation $a * x = b$ in G.

$\therefore$ $a * x_1 = b$ and $a * x_2 = b$

$\Rightarrow$ $a * x_1 = a * x_2 \Rightarrow x_1 = x_2$ (By left cancellation law in a group)

Hence the equation $a * x = b$ has a unique solution in G.

Similarly, we can prove that the equation $y * a = b$ has a unique solution in G.

(Solution is $b * a^{-1}$)

VII. Left identity and right identity are the same in a group

Let e and e' be the left identity and right identity in the group (G, *). Then

$e * e' = e'$ (Here e is the left identity)

also $e * e' = e$ (Here e' is the right identity)

Thus $e' = e$.

Hence left identity and right identity in a group are same.

VIII. Left inverse and right inverse of every element in a group is same

Let e be the identity of the group (G, *) and let b and c be the left and right inverse of the element $a \in G$ respectively. Then

$b * a = e$ and $a * c = e$

Now $b = b * e$

$= b * (a * c) = (b * a) * c$

$= e * c$

$= c$.

Hence the left inverse and the right inverse of every element in a group is same.

1.2.1. Theorem : Let G be a non-empty set together with a binary operation * such that closure property and associative law hold in G. Then the existence of left identity and left inverse in G implies the existence of same right identity and same right inverse in G.

1.2.2. Definition of a Group based on Left axioms

Let G be a non-empty set together with a binary operation * defined on it, then the algebraic structure <G, *> is a group if it satisfies the following axioms

(*i*) $a * b \in G, \forall a, b \in G$ (Closure Property)

(*ii*) $(a * b) * c = a * (b * c), \forall a, b, c \in G$ (Associative Property)

(iii) $\exists$ an element $e \in G$ such that

$$e * a = a \ , \forall a \in G$$ (Existence of left identity)

(iv) For all $a \in G$, $\exists$ an element $b \in G$ such that

$$b * a = e.$$ (Existence of left inverse)

1.2.3. Definition of a Group based on Right axioms

Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $<G, *>$ is a group if it satisfies the following axioms

(i) $a * b \in G, \ \forall \ a, b \in G$ (Closure Property)

(ii) $(a * b) * c = a * (b * c), \ \forall a, b, c \in G$ (Associative property)

(iii) $\exists$ an element $e \in G$ such that

$$a * e = a, \ \forall a \in G$$ (Existence of right identity)

(iv) For all $a \in G$, $\exists$ an element $b \in G$ such that

$$a * b = e$$ (Existence of right inverse)

Note : If $< G, * >$ be an algebraic system in which closure property, associative property holds. Then G need not be a group if left identity and right inverse exist in G (or right identity and left inverse exist in G).

For example : Let G be any set containing atleast two elements.

Define a binary operation $*$ on G by $a * b = b, \forall a, b \in G$.

Clearly, closure property, associative law holds in G.

Also the element $e \in G$ be the left identity in G for $e * a = a, \ \forall a \in G$.

Moreover, $a * e = e \ \Rightarrow \ e$ is the right inverse of a.

But $<G, *>$ is not a group, for if a, b be two distinct elements of G then $a * b = b$ also $b * b = b$ so $a * b = b * b \ \Rightarrow \ a = b$ (by right cancellation law), a contradiction.

1.2.4. Theorem. A semi-group in which both the equations $a x = b$ and $y a = b$ have a unique solution, is a group. Prove it.

(It is also called a definition of a group)

Or

Let G be a set with binary operation which is associative. Assume that for all elements a and b in G, the equations $a x = b$ and $y a = b$ have unique solution in G, then prove that G is a group

Note : If in a semi-group G only one of the equation has a solution. Then G may not be a group.

For example. Consider the algebraic system $<G, \cdot>$ defined by $a \cdot b = b, \forall a, b \in G$.

Here $<G, \cdot>$ is a semi-group in which only $a x = b$ has a solution in G. But G is not a group.

(Already proved)

1.2.5. Theorem. Prove that any finite semi-group is a group iff both the cancellation laws hold.

(It is also called a definition of a group, but for finite sets)

Note : If one cancellation law holds, then the system may not be a group.

For example : Let G be any set containing at least two elements. Define a binary operation $*$ on G by $a * b = b$, $\forall\ a, b \in G$.

Clearly closed property and associative law holds.

i.e. G is a semi group.

Here $\forall\ a, b, c \in G$, $a * b = b$ and $a * c = c$.

$\therefore\ a * b = a * c \Rightarrow b = c$ *i.e.* left cancellation law holds.

But G is not a group under $*$.

Here right cancellation law does not hold. (as in 1.2.3)

Remark 1. In a semi-group, the cancellation laws may not hold.

For example : Let S = Set of 2×2 matrices over integers.

Now S is a semi-group under multiplication.

Here $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ are (any) three elements of S.

$$AB = AC \qquad \left(\text{each} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}\right)$$

But $B \neq C$.

$\therefore$ Left cancellation law does not hold.

Similarly we can check right cancellation law does not hold.

Remark 2. There are semi-groups which are not groups but they satisfy cancellation laws.

For example : Consider **N** = Set of all natural numbers.

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

Under the operation of ordinary multiplication, N is closed and associative law holds.

i.e. **N** is a semi-group.

Also both the cancellation laws hold

i.e. $\forall\ a, b, c \in \mathbf{N}$

$$ab = ac \Rightarrow b = c$$

and

$$ba = ca \Rightarrow b = c.$$

But this system is not a group. (Here inverse of its elements do not exist)

Note : $\langle \mathbf{N}, \cdot \rangle$ is an infinite semi-group with cancellation laws hold.

$\therefore$ $\langle \mathbf{N}, \cdot \rangle$ is not a group.

Thus the above theorem cannot be generalized to infinite semi-groups.

1.2.6. Power of an element of a group.

Notation : Let G be a group under the composition multiplication.

If $a \in G$ be any element, then by closure property $a \cdot a \in G$.

Similarly, $(a \cdot a) \cdot a \in G$ and so on.

We denote (or write) $a \cdot a$ as a^2 and $(a \cdot a) \cdot a$ as a^3 and so on.

Similarly, $a^{-1} \cdot a^{-1}$ is denoted as a^{-2} and $(a^{-1} \cdot a^{-1}) \cdot a^{-1}$ by a^{-3} and so on.

Since $a \cdot a^{-1} = e$, therefore we denote $a^0 = e$.

Thus $$a^n = \underbrace{a\, a\, a \ldots\ldots a}_{n \text{ times}}$$

$$a^{-n} = (a^{-1})^n = \underbrace{(a^{-1})(a^{-1})\ldots\ldots(a^{-1})}_{n \text{ times}}, \forall\, n \in \mathbf{N}$$

Thus $a^{-n} = (a^{-1})^n \ \forall\ n \in \mathbf{N}$. Here $a^n \in G\ \forall n \in I$.

If $<G, +>$ is a group, then

$$a + a = 2a \quad \textit{i.e.}\ a \text{ is operated two times.}$$

$$n\,a = a + a + \ldots\ldots + a \ (n \text{ times})$$

$$0\,a = O$$

(On left side 0 is zero integer. On right side O is zero element of the group)

$$(-1)\,a = -a \qquad \text{(additive inverse of } a\text{)}$$

$$(-n)\,a = n(-a) \ \ \forall\ n \in I$$

Here $n\,a \in G\ \forall\, n \in I$.

Remark : If $<G, \cdot>$ is a group.

$\forall\ a \in G,\ \forall\ m, n \in I$, we can prove by the method of mathematical induction

(*i*) $a^m \cdot a^n = a^{m+n}$

(*ii*) $(a^m)^n = a^{mn}$

(*iii*) $a^{-n} = (a^{-1})^n = (a^n)^{-1}$.

Here (*i*) and (*ii*) are also called **Laws of indices in a group.**

1.3. Order of an Element

Definition : Let a be an element of a group G. If there exists a positive integer n such that $a^n = e$, then a is said to have finite order, and the smallest such positive integer n with this property such that $a^n = e$ is called the **order of** a and is denoted by $O(a)$.

If there does not exist a positive integer n such that $a^n = e$, then a is said to have **infinite order** or the **order does not exist** or the **order is zero.**

Note : (*i*) In a group G, order of identity element is always 1.

i.e. $O(e) = 1$.

(*ii*) In case of additive notation the above terminology is stated as :

Let a be an element of a group G. If there exists a positive integer n such that $n\,a = 0$, then a is said to have finite order, and the smallest such positive integer n with this property such that $na = 0$ is called the **order of** a, and is denoted by $O(a)$.

If there does not exist a positive integer n such that $n\,a = 0$, then a is said to have **infinite order**, or the **order does not exist** or the **order is zero.**

Examples : 1. In a group $\langle \mathbf{Q} - \{0\}, \cdot \rangle$, we have $O(1) = 1$ (as $1^1 = 1$), and $O(-1) = 2$ (as $(-1)^2 = 1$). But the order of any other element does not exist.

2. In the group $(\{0, 1, 2, 3, 4, 5\}, +_6)$ the order of every element exists.

e.g. $O(0) = 1, O(1) = 6, O(2) = 3, O(3) = 2, O(4) = 3, O(5) = 6$.

Note : The order of an element in an infinite group may or may not exist. But there do exist **infinite groups** in which order of every element exists.

Example : Give an example of an infinite group each element of which has a finite order.

Sol. Let $G = \{z ; z \in C \text{ and } z^n = 1 \text{ for some positive integer } n\}$

$\therefore$ G = Union of all n, nth roots of unity, where $n \in \mathbf{N}$.

Under the composition of multiplication of complex numbers, G is an infinite group with identity element $z = 1$.

The order of each element is n which is finite, where $n \in \mathbf{N}$.

Then G is an infinite group in which order of every element exists.

1.3.1. Theorem (*i*) In a finite group the order of every element exists.

Theorem (*ii*) If G is a finite group of order n then show that for any $a \in G$, $\exists$ some positive integer r, $1 \le r \le n$, such that $a^r = e$.

1.3.2. Theorem. Let G be a group and $a \in G$ be of order m. Prove that

(*i*) $a^0 = e, a, a^2, \ldots\ldots, a^{m-1}$ are all different.

(*ii*) $\forall\ n \in I$, a^n is equal to some one from the above list.

1.3.3. Theorem. Let G be a finite group and let $a \in G$ be an element of order n. Then $a^m = e$ iff n is a divisor of m.

Proof. Firstly, let n be a divisor of m *i.e.* $n \mid m$, where $O(a) = n$.

$\therefore$ there exists a positive integer q such that

$$m = nq$$

Now $$a^m = a^{nq} = (a^n)^q = e^q = e.$$ $\left[\because O(a) = n \;\; \therefore a^n = e\right]$

Conversely let $a^m = e$, where $O(a) = n$.

By division algorithm theorem

$m = nq + r$, where $q, r \in I$ and $0 \le r < n$

$\therefore \quad e = a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$

$\Rightarrow \quad a^r = e$, where $0 \le r < n$

which is not possible, because $O(a) = n$ and n is the least positive integer such that $a^n = e$.

$\therefore$ Above result holds only if $r = 0$

i.e. when $m = nq + 0 = nq$

i.e. when n is a divisor of m.

1.3.4. Theorem. Let G be a group and let $a \in G$ be order m. Then $\boxed{O(a^k) = \frac{m}{(m,k)}}$, where $k \in N$.

Cor. 1. If $O(a) = m$, then $O(a^k) = m$ iff $(m, k) = 1$.

By above theorem,

$$O(a^k) = \frac{m}{(m,k)}$$

$\therefore \quad O(a^k) = m$ iff $\frac{m}{(m,k)} = 1$ *i.e.* iff $(m, k) = 1$.

2. If $O(a) = p$, where p is a prime number, then $(\because (p, k) = 1)$

$O(a^k) = p$, for all $k = 1, 2, \ldots, p-1$.

1.3.5. Theorem. Let a, b and x be any elements of a group G. Then prove that

(*i*) $O(a^{-1}) = O(a)$

(*ii*) $(x^{-1} a x)^k = x^{-1} a^k x$, for all $k \in I$

(*iii*) $O(a) = O(x^{-1} a x)$

(*iv*) $O(ab) = O(ba)$

Proof. (*i*) Let $O(a) = m$ and $O(a^{-1}) = n$

$\Rightarrow$ m, n are the least +ve integers such that

$a^m = e$ and $(a^{-1})^n = e$

Now $(a^{-1})^m = a^{-m} = (a^m)^{-1} = e^{-1} = e$, but $O(a^{-1}) = n$ ...(1)

$\therefore \quad n \mid m$

Again, $a^n = (a^{-1})^{-n} = [(a^{-1})^n]^{-1} = e^{-1} = e$, but $O(a) = m$ ...(2)

$\therefore \quad m \mid n$

From (1) and (2), we get

$$m = n$$

$\therefore \quad O(a^{-1}) = O(a).$

(*ii*) We shall prove by induction that

$$(x^{-1} a x)^k = x^{-1} a^k x, \text{ for all } k \in \mathbf{I}$$

when $k = 1$, L.H.S. $= (x^{-1} a x)^1 = x^{-1} a^1 x =$ R.H.S.

$\therefore$ the result is true for $n = 1$.

Let the result holds for $k = m$, where m is a positive integer.

$\therefore \quad (x^{-1} a x)^m = x^{-1} a^m x$ is true.

Now $(x^{-1} a x)^{m+1} = (x^{-1} a x)^m (x^{-1} a x) = (x^{-1} a^m x)(x^{-1} a x) = x^{-1} a^m (x x^{-1}) a x$

$= x^{-1} a^m e a x = x^{-1} a^{m+1} x.$

$\therefore$ The result is true for $k = m + 1$ also.

Hence the result is true for all positive integers.

Also when $k = 0$, then

L.H.S. $= (x^{-1} a x)^0 = e = x^{-1} e x = x^{-1} a^0 x$

$=$ R.H.S.

Now, let $k = -m$, where m is a positive integer.

$\therefore \quad (x^{-1} a x)^k = (x^{-1} a x)^{-m} = \{(x^{-1} a x)^m\}^{-1} = \{x^{-1} a^m x\}^{-1}$

$= x^{-1} a^{-m} (x^{-1})^{-1}$

[By Reversal law $(a b)^{-1} = b^{-1} a^{-1}$]

$= x^{-1} a^k x.$ $[\because (x^{-1})^{-1} = x]$

$\therefore$ The result is true for zero and negative integers also. Hence the result is proved for all integers.

(*iii*) Let $O(x^{-1} a x) = m$ and $O(a) = n$

Now $(x^{-1} a x)^n = x^{-1} a^n x = x^{-1} e x = x^{-1} x = e$

But $O(x^{-1} a x) = m$

$\therefore \quad m \mid n$ ...(1)

Again $\because \quad O(x^{-1} a x) = m$

$\Rightarrow \quad (x^{-1} a x)^m = e$

$$\Rightarrow \quad x^{-1} a^m x = e = x^{-1} x$$

$$\Rightarrow \quad x^{-1} a^m x = x^{-1} e x$$

$$\Rightarrow \quad a^m = e \qquad \text{[Using left and right cancellation laws]}$$

$$\Rightarrow \quad O(a) = n$$

But $\quad n \mid m \qquad \ldots(2)$

From (1) and (2), we get

$$m = n.$$

i.e. $\quad O(x^{-1} a x) = O(a).$

(*iv*) From (*iii*) we have

$$O(a) = O(x^{-1} a x), \quad \forall\ a, x \in G$$

Replacing a by $a\,b$ and x by a, we get

$$O(a\,b) = O(a^{-1}(a\,b)\,a) = O(a^{-1} a\,b\,a)$$
$$= O(e\,b\,a) = O(b\,a)$$

Aliter : Since $a\,b = e\,a\,b = (b^{-1} b) a\,b = b^{-1}(b\,a)\,b$

$$\therefore \quad O(a\,b) = O(b^{-1}(b\,a)\,b) \qquad \text{[Using (iii)]}$$

$$\Rightarrow \quad O(a\,b) = O(b\,a).$$

Remark : If $a, b \in G$ be elements of finite order of a group G, then $O(ab)$ may not be finite and if it is finite even then it need not be equal to $O(a)\,O(b)$.

Example (*i*). Let $G = \{f ;\ f : \mathbf{R} \to \mathbf{R}$ is one-one and onto function$\}$ be a group under the operation of composition of functions.

Let $f_1, f_2 \in G$ be two elements such that $f_1(x) = -x$ and $f_2(x) = 1-x$. Then $O(f_1) = 2 = O(f_2)$, but $O(f_1 f_2)$ does not exist.

Sol. For $\quad f_1^{\,2}(x) = f_1(f_1(x)) = f_1(-x) = -(-x) = x \Rightarrow O(f_1) = 2$

and $\quad f_2^{\,2}(x) = f_2(f_2(x)) = f_2(1-x) = 1-(1-x) = x$

$$\Rightarrow \quad O(f_2) = 2$$

But $\quad f_1 f_2(x) = f_1(f_2(x)) = f_1(1-x) = -(1-x) = -1+x$

Also, $(f_1 f_2)^n(x) \neq x, \ \forall\ n \in \mathbf{N}.$

$\therefore \quad O(f_1 f_2)$ does not exist.

Example (*ii*). Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R$ such that $a\,d - b\,c \neq 0 \right\}$

i.e. G is a group of all non-singular 2×2 matrices under the operation of multiplication of matrices.

Let $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ be two elements of G.

Prove that $O(A) = O(B) = 2$ but $O(AB)$ does not exist.

Sol. Here $A^2 = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \Rightarrow O(A) = 2$

$B^2 = \begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \Rightarrow O(B) = 2$

and $AB = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} = \begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$

.....

.....

$$(AB)^n = \begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}, \forall n \in \mathbf{N}$$

$\therefore$ O (AB) does not exist.

Example (*iii*). Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of Quaternions under multiplication. Then

$O(i) = 4 = O(j)$, but $O(ij) = O(k) = 4$.

$[\because i^4 = j^4 = k^4 = 1$ and $ij = k]$

Thus $O(ij) \neq O(i)\,O(j)$.

Example (*iv*). Let $G = \{(0, 1, 2, 3, 4, 5), +_6\}$ be a group under the composition of multiplication modulo 6.

Here $O(2) = 3$ and $O(4) = 3$, but $O(2 +_6 4) = O(0) = 1$

Therefore, $O(2 +_6 4) \neq O(2)\,O(4)$.

Example (*v*). Let $S_3 = \{i, (12), (13), (23), (123), (132)\}$ be the symmetric group on three elements 1, 2 and 3.

Let $a = (12)$ and $b = (123)$. Then

$O(a) = 2$, $O(b) = 3$. $[\because a^2 = i$ and $b^3 = i]$

Now $ab = (12)(123) = (13)$ and $ba = (123)(12) = (23)$

But $O(ab) = O((13)) = 2 \neq O(a) \cdot O(b)$.

1.3.6. Theorem. If a, b be any two elements of a group G such that $ab = ba$ and $(O(a), O(b)) = 1$. Then prove that $O(ab) = O(a)\,O(b)$.

Proof. Let $O(a) = m$ and $O(b) = n$, where $(m, n) = 1$.

Let $O(ab) = k$. To show that $k = mn$, where $ab = ba$.

Now $e = (ab)^{nk} = a^{nk}\,b^{nk} = a^{nk}.(b^n)^k$

$= a^{nk}.e^k = a^{nk}\,e = a^{nk}$

i.e. $a^{nk} = e$, but $O(a) = m$

$\Rightarrow m \mid nk$, but $(m, n) = 1$

$\therefore m \mid k$. ...(1)

Similarly, $e = (a\,b)^{m\,k} = a^{m\,k}\,b^{m\,k} = (a^m)^k\,b^{m\,r}$

$= e^k\,b^{m\,r} = e\,b^{m\,k} = b^{m\,k}$

i.e. $b^{m\,k} = e$, but $O(b) = n$

$\Rightarrow n \mid m\,k$, but $(m, n) = 1$

$\therefore n \mid k.$ ...(2)

From (1) and (2), we get

$m \mid k$ and $n \mid k \Rightarrow [m, n] \mid k$ ...(3)

But $[m, n] \cdot (m, n) = m\,n$

$\Rightarrow [m, n] \cdot 1 = m\,n$

$\therefore$ From (3), we have

$m\,n \mid k.$ ...(4)

Again $(a\,b)^{m\,n} = a^{m\,n}\,b^{m\,n} = (a^m)^n\,(b^n)^m = e^n\,e^m = e\,e = e$

but $O(a\,b) = k$ ...(5)

$\therefore k \mid m\,n$

$\therefore$ from (4) and (5), we get

$k = m\,n$

i.e. $O(a\,b) = O(a) \cdot O(b)$.

1.3.7. Definition : Idempotent element.

In a semi-group G, an element a is called an **idempotent element** if $a^2 = a$.

ILLUSTRATIVE EXAMPLES

Example 1. Show that if G is a group then $a \in G$ is an idempotent if and only if $a = e$, the identity of G.

Sol. Given G is a group.

Let $a \in G$ is an idempotent element

$\Rightarrow a^2 = a$

$\Rightarrow a\,a = a\,e$ [Using left cancellation law]

$\Rightarrow a = e.$

Conversely let $a = e$, the identity of G [$\because a = e$]

$\therefore a\,a = a\,e$

$= e\,e = e = a$

$\Rightarrow a^2 = a$

$\Rightarrow a$ is an idempotent element.

Example 2. Let G be a group such that $a^2 = e$, for all $a \in G$. Show that G is abelian.

Or

Show that a group in which every element is its own inverse is an abelian group.

Or

If each element of a group, except the identity element, is of order 2, show that the group is abelian.

Sol. Let $a, b \in G$ be any two elements, where $a \neq e$, $b \neq e \Rightarrow ab \neq e$.

$\therefore \quad a^2 = e \quad$ and $\quad b^2 = e \quad$ (or $O(a) = 2$, $O(b) = 2$)

$\Rightarrow \quad a^{-1} = a \quad$ and $\quad b^{-1} = b \quad$ (*i.e.* every element is its own inverse)

Also $a, b \in G \Rightarrow ab \in G$ (By Closure Property)

$\therefore \quad (ab)^2 = e \quad$ (or $O(ab) = 2$)

$\Rightarrow \quad (ab)^{-1} = ab$

But $\quad (ab)^{-1} = b^{-1} a^{-1}$

$\therefore \quad b^{-1} a^{-1} = ab$

$\Rightarrow \quad ba = ab \quad [\because b^{-1} = b \text{ and } a^{-1} = a]$

$\therefore$ G is abelian group.

Example 3. If in a group G, $a^5 = e$ and $aba^{-1} = b^2$ for all $a, b \in G$. Prove that if $b \neq e$, then $O(b) = 31$.

Sol. Now $\quad b^2 = aba^{-1} \quad ...(1)$

$\therefore \quad b^4 = (aba^{-1})^2$

$= ab^2 a^{-1} \quad [\because (x^{-1} ax)^n = x^{-1} a^n x]$

$= a(aba^{-1}) a^{-1} \quad$ [Using (1)]

$= a^2 ba^{-2}$

$\therefore \quad b^8 = (a^2 ba^{-2})^2$

$= a^2 b^2 a^{-2} = a^2 (aba^{-1}) a^{-2} \quad$ [Using (1)]

$= a^3 ba^{-3}$

$\therefore \quad b^{16} = (a^3 ba^{-3})^2 = a^3 b^2 a^{-3}$

$= a^3 (aba^{-1}) a^{-3} \quad$ [Using (1)]

$= a^4 ba^{-4}$

Similarly, $b^{32} = a^5 b a^{-5}$

$b^{32} = e b e^{-1} = b$ $[\because a^5 = e]$

$\Rightarrow$ $b . b^{31} = b e$

$\Rightarrow$ $b^{31} = e.$ [By left cancellation law]

$\therefore$ $O(b)$ must divide 31. But 31 is a prime number.

$\therefore$ $O(b) = 31$.

Example 4. If G is an abelian group, then $(a b)^n = a^n b^n$, holds for all $a, b \in G$ and for all $n \in I$.

Sol. Given G is an abelian group.

Let $a, b \in G$. We shall prove the result $(a b)^n = a^n b^n$ by Mathematical Induction.

If $n = 0$, then $(a b)^0 = e = e e = a^0 b^0$

$\therefore$ the result is true for $n = 0$.

If $n = 1$, then $(a b)^1 = a b = a^1 b^1$

$\therefore$ the result is true for $n = 1$.

Suppose that the result is true for $n = k \geq 1$.

$\therefore$ $(a b)^k = a^k b^k$

Consider $(a b)^{k+1} = (a b)^k (a b) = (a^k b^k)(a b)$

$\Rightarrow$ $= \big((a^k b^k) a\big) b$, by associativity in G

$= \big(a^k (b^k a)\big) b$, by associativity in G

$= \big(a^k (a b^k)\big) b$, since G is abelian

$= \big((a^k a) b^k\big) b$, by associativity

$= (a^{k+1} b^k) b$

$= a^{k+1} (b^k b)$ by associativity

$= a^{k+1} b^{k+1}$.

$\therefore$ the result is true for $n = k + 1$, if it is true for $n = k$.

But we have already proved the result for $n = 1$.

$\therefore$ the result is true for every positive integer n.

When n is a negative integer

Let $n = -m$ for some positive integer m.

Then $(ab)^n = (ab)^{-m}$

$= ((ab)^m)^{-1}$

$= (a^m b^m)^{-1}$, since m is a positive integer

$= (b^m a^m)^{-1}$, since G is abelian

$= (a^m)^{-1} (b^m)^{-1} = a^{-m} b^{-m}$

$= a^n b^n$

Hence $(ab)^n = a^n b^n, \forall \ n \in \mathbf{I}$.

Example 5. Show that the equation $y^2 a y = a^{-1}$ is solvable for y in a group G if and only if a is the cube of some element in G.

Sol. Firstly, let equation $y^2 a y = a^{-1}$ is solvable in G

$\Rightarrow$ $\exists\ b \in$ G such that $b^2 a b = a^{-1}$

$\Rightarrow$ $bbaba = a^{-1}a = e \Rightarrow baba = b^{-1}e = b^{-1} \Rightarrow babab = e$

$\Rightarrow$ $bababa = ea = a$

$\Rightarrow$ $(ba)^3 = a$, where e is identity element of G

$\therefore$ a is cube of some element in G.

Conversely : Let $a = m^3$ for some element $m \in$ G

Now $y^2 a y = (m^{-2})^2 a\ m^{-2}$ for $y = m^{-2}$

$= m^{-4} m^3 m^{-2} = m^{-3} = a^{-1}$

$\Rightarrow$ $y^2 a y = a^{-1}$ is satisfied for $y = m^{-2} \in$ G

$\therefore$ equation $y^2 a y = a^{-1}$ is solvable for y in a group G.

Example 6. If in a group G, $xy^2 = y^3 x$ and $yx^2 = x^3 y$, then show that $x = y = e$ where is the identity of G

Sol. $xy^2 = y^3 x \Rightarrow x = y^3 x y^{-2}$

$x^2 = xy^3 xy^{-2} = xy^2 yxy^{-2} = y^3 xyxy^{-2}$ [$\because xy^2 = y^3 x$]

$x^2 y = y^3 xyxy^{-1}$ ...(1)

Now $yx^2 = x^3 y \Rightarrow yx^2 = xy^3 xyxy^{-1}$ [use (1)]

$\Rightarrow$ $x^2 = y^{-1} xy^3 xyxy^{-1}$

$\Rightarrow$ $x^2 y = y^{-1} xy^3 xyx$ ...(2)

By (1) and (2), we obtain,

$y^3 xyxy^{-1} = y^{-1} xy^3 xyx \Rightarrow y^4 xyx = xy^3 xyxy$

$\Rightarrow$ $y^4 xyx = xy^2 yxyx = y^3 xyxyxy$ [$\because xy^2 = y^3 x$]

$\Rightarrow$ $(yx)^2 = (xy)^3$ ...(3)

Interchanging x and y in (3), we get,

$(xy)^2 = (yx)^3$ ...(4)

Now (3) and (4) imply

$(xy)^2 = (yx)^2 = (yx)^2(yx) = (xy)^3(yx)$

$\Rightarrow \quad e = xy^2x \Rightarrow x^{-2} = y^2$

Further $xy^2 = y^3x \Rightarrow xx^{-2} = yx^{-2}x$

$\Rightarrow \quad x^{-1} = yx^{-1} \Rightarrow y = e$

Lastly $yx^2 = x^3y \Rightarrow ex^2 = x^3e \Rightarrow x = e$

Hence the result.

Example 7. If G is an abelian group then show that for $a, b \in G$

(*i*) a^{-1} and b^{-1} commute (*ii*) a^{-1} and b commute (*iii*) a and b^{-1} commute

Sol. $\because$ G is abelian group

So $ab = ba \ \forall \ a, b \in G$

(*i*) Here $ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1}$

$\Rightarrow \quad b^{-1}a^{-1} = a^{-1}b^{-1} \Rightarrow a^{-1}$ and b^{-1} commute

(*ii*) Here $ab = ba \Rightarrow a^{-1}(ab) = a^{-1}(ba)$

$\Rightarrow \quad (a^{-1}a)b = (a^{-1}b)a \Rightarrow eb = (a^{-1}b)a$

$\Rightarrow \quad b = (a^{-1}b)a \Rightarrow b(a^{-1}a) = (a^{-1}b)a$

$\Rightarrow \quad (ba^{-1})a = (a^{-1}b)a \Rightarrow ba^{-1} = a^{-1}b$ (by right cancellation law)

$\Rightarrow \quad a^{-1}$ and b commute

(*iii*) Here $ab = ba \Rightarrow (ab)b^{-1} = (ba)b^{-1}$

$\Rightarrow \quad a(bb^{-1}) = b(ab^{-1}) \Rightarrow ae = b(ab^{-1})$

$\Rightarrow \quad a = b(ab^{-1}) \Rightarrow (bb^{-1})a = b(ab^{-1}) \Rightarrow b(b^{-1}a) = b(ab^{-1})$

$\Rightarrow \quad b^{-1}a = ab^{-1}$ (by left cancellation law)

$\therefore \quad a$ and b^{-1} commute.

Example 8. Find order of each element of group $\{(0, 1, 2, 3, 4, 5), +_6\}$, i.e. composition is addition modulo 6.

Sol. Let $(G, +_6)$ be a group where $G = \{0, 1, 2, 3, 4, 5\}$ with composition as addition modulo 6

Here $e = 0$

We know $m\,a = e$, m is least positive integer

$\Rightarrow \quad O(a) = m$

Now order of identity element of each group is 1

$\therefore \quad O(e) = O(0) = 1$

To find O(1)

$2(1) = 1 +_6 1 = 2, \ 3(1) = 1 +_6 2(1) = 1 +_6 2 = 3$

$4(1) = 1 +_6 3(1) = 1 +_6 3 = 4, \ 5(1) = 1 +_6 4(1) = 1 +_6 4 = 5$

$6(1) = 1 +_6 5(1) = 1 +_6 5 = 0 = e$

$\therefore$ $6(1) = e$ and $m(1) \neq e$ for $m < 6$

$\Rightarrow$ $O(1) = 6$

To find O(2)

$2(2) = 2 +_6 2 = 4$, $3(2) = 2 +_6 2(2) = 2 +_6 4 = 0$

$\therefore$ $3(2) = e$ and $m(2) \neq e$ for $m < 3$

$\Rightarrow$ $O(2) = 3$

To find O(3)

$2(3) = 3 +_6 3 = 0 = e \Rightarrow O(3) = 2$

To find O(4)

$1(4) = 4, 2(4) = 4 +_6 4 = 2, \; 3(4) = 4 +_6 2(4) = 4 +_6 2 = 0 = e$

$\therefore$ $3(4) = e$ and $m(4) \neq e$ for $m < 3$

$\Rightarrow$ $O(4) = 3$

To find O(5)

$1(5) = 5, 2(5) = 5 +_6 5 = 4, 3(5) = 5 +_6 2(5) = 5 +_6 4 = 3$

$4(5) = 5 +_6 3(5) = 5 +_6 3 = 2, 5(5) = 5 +_6 4(5) = 5 +_6 2 = 1$

$6(5) = 5 +_6 5(5) = 5 +_6 1 = 0 = e$

$\therefore$ $6(5) = e$ and $m(5) \neq e$ for $m < 6$

$\Rightarrow$ $O(5) = 6$

EXERCISE 1.2

1. Show that a group of even order has an element of order 2.
2. Show that in a group of even order the number of elements whose order is 2 are odd.
3. Give an example of a group G and elements $a, b \in G$ such that $O(a)$ and $O(b)$ are finite, but $O(ab)$ is not finite.
4. Let G be a group such that $(ab)^n = a^n b^n$, for three consecutive integers n and for all $a, b \in G$. Show that G is abelian.
5. If $(ab)^2 = a^2 b^2, \forall\ a, b \in G$, a group. Then show that G must be an abelian group.
6. Find the order of each element of the group $\{(0, 1, 2, 3, 4), +_5\}$.
7. Find the order of each element of the group of four 4th roots of unity.
8. Find the order of each element of the following group

$$G = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$$

under matrix multiplication.

9. Consider the element $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ in G, the group of 2×2 non-singular matrices having unit determinant over R. What is the order of A ?

10. Show that in a group of non-zero rational numbers under multiplication, only 1 and -1 are elements of finite order and all other elements are of infinite order.

11. If the elements a, b and ab of a group are each of order 2, prove that $ab = ba$.

12. In S_3, give an example of two elements a, b such that $(ab)^2 \neq a^2 b^2$.

13. If $(G, +)$ is a group such that $2a = 0$ for all $a \in G$, then show G is an abelian group.

14. Prove that every group of order 4 and less is commutative.

15. Show that if G is a group of even order then it has at least one element different from identity element which is its own inverse.

16. A non-empty set G with a binary composition denoted multiplicatively is a group if and only if
   (i) $(ab)c = a(bc)$ $\forall$ $a, b, c \in G$
   (ii) $\exists$ an element $e \in G$ such that $ae = G$
   (iii) For each $a \in G$, $\exists$ and element $b \in G$ such that $ab = e$

17. A non-empty set G with a binary composition denoted multiplicatively is a group if and only if
   (i) $(ab)c = a(bc)$ $\forall$ $a, b, c \in G$.
   (ii) $\exists$ an element $e \in G$ such that $ea = a$ $\forall$ $a \in G$.
   (iii) For each $a \in G$, $\exists$ $b \in G$ such that $ba = e$

18. Prove that the equations $ax = b$ and $ya = b$ have unique solutions in a group G $\forall$ $a, b \in G$.

19. If for a group G, $a^m b^n = ba$ for $a, b \in G$. show that $a^m b^{n-2}, a^{m-2} b^n, ab^{-1}$ have same order.

20. If $a^2 b = ba^2 = b$ for all $a, b \in G$ (a semi group), then prove that G is abelian.

21. A non-empty set G is a group under multiplication if and only if
   (i) $(ab)c = a(bc)$ $\forall$ $a, b, c \in G$.
   (ii) The equations $ax = b$ and $ya = b$ have solutions in G for any $a, b \in G$.

22. Given G be a finite semi group. Prove that $\exists$ $x \in G$ such that $x^2 = x$.

Or

Prove a finite semi gorup has an idempotent element.

ANSWERS

6. 1, 5, 5, 5, 5
7. $0(1) = 1, 0(-1) = 2, 0(i) = 4, 0(-i) = 4$
8. $0(1) = 1, (-1) = 2, 0(\pm i) = 4, 9(\pm j) = 4$ and $0(\pm k) = 4$
9. 0(A) does not exist
12. $S_3 = \{i, (12), (13), (23), (123), (132)\}$

CONGRUENCE RELATIONS AND QUOTIENT STRUCTURES

1.4. Congruence Relation on Integers

Definition :

For a fixed positive integer n in $\mathbf{Z}$. Define a relation (say) $\equiv_n$ on $\mathbf{Z}$ as follows :

For all $a, b \in \mathbf{Z}$, $a \equiv_n b$ if and only if $n \mid (a-b)$

i.e. $a - b = nk$ for some $k \in \mathbf{Z}$.

Remark : (1) This relation on $\mathbf{Z}$ is called **congruence modulo n** and $a \equiv_n b$ **is also denoted by** $a \equiv b \pmod{n}$. However, if $a-b$ is not divisible by n, then we write it as $a \not\equiv b \pmod{n}$.

(2) We read $a \equiv b \pmod{n}$ as **'a is congruent to b modulo n'.**

(3) Two integers a and b are congruent modulo a positive integer n, if and only if a and b leave the same remainder when divided by n.

Proof. Let r_1, r_2 be the remainders when a and b are respectively divided by n, then

$$a = np + r_1 \text{ and } b = nq + r_2, \text{ for some } p, q \in \mathbf{Z}.$$

$$\Rightarrow \quad a - b = (np + r_1) - (nq + r_2)$$

$$a - b = n(p-q) + (r_1 - r_2)$$

$(r_1 - r_2)$ is the remainder when $a-b$ is divided by n.

Now given $a \equiv b \pmod{n}$ iff $n \mid a-b$

i.e. iff $r_1 - r_2 = 0$

i.e. iff $r_1 = r_2$

Hence the result.

Theorem : Congruence relation $\equiv_n$ on integers is an equivalence relation.

Proof. Since for all $a \in \mathbf{Z}$, we have $a - a = 0 = n0 \Rightarrow a \equiv_n a$ for all $a \in \mathbf{Z}$.

$\therefore$ $\equiv_n$ is reflexive.

Now, let $a, b \in \mathbf{Z}$ such that $a \equiv_n b$. Then $\exists\, k \in \mathbf{Z}$ such that

$$a - b = nk \quad \Rightarrow \quad b - a = (-k)n$$

$$\Rightarrow \quad n \mid (b-a)$$

So $b \equiv_n a$ $\therefore$ $\equiv_n$ is symmetric.

Finally, let $a, b, c \in \mathbf{Z}$ such that $a \equiv_n b$ and $b \equiv_n c$. Then $\exists$ integers p and q such that

$$a - b = np \quad \text{and} \quad b - c = nq.$$

On adding, we get $a - c = np + nq = n(p+q)$ where $p + q \in \mathbf{Z}$

$$\Rightarrow \quad n \mid (a-c)$$

so $a \equiv_n c$ $\therefore$ $\equiv_n$ is transitive.

Hence $\equiv_n$ *i.e.* congruence modulo n is an equivalence relation on $\mathbf{Z}$.

Properties of Congruence Relation :

Let $a, b, c, d \in \mathbf{Z}$ and n a fixed positive integer.

If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then

(i) $(a+c) \equiv (b+d) \pmod n$ (ii) $ac \equiv bd \pmod n$.

Proof. (i) Since $a \equiv b \pmod n$ and $c \equiv d \pmod n$

$\Rightarrow \quad n \mid (a-b)$ and $n \mid c-d$

$\Rightarrow \quad n \mid (a-b)+(c-d) \Rightarrow n \mid (a+c)-(b+d) \Rightarrow (a+c) \equiv (b+d) \pmod n$.

(ii) Also $a \equiv b \pmod n \Rightarrow n \mid a-b$

and $c \equiv d \pmod n \Rightarrow n \mid c-d$

$\therefore \quad n \mid a-b \Rightarrow n \mid c(a-b) \Rightarrow n \mid ca-cb$

Also $n \mid c-d \Rightarrow n \mid b(c-d) \Rightarrow n \mid bc-bd$.

Thus $n \mid ca-cb$ and $n \mid bc-bd$

$\Rightarrow \quad n \mid (ca-cb)+(bc-bd) \Rightarrow n \mid ca-bd \Rightarrow n \mid ac-bd \Rightarrow ac \equiv bd \pmod n$.

Cor. If $a \equiv b \pmod n$ then for any integer c, we have

(i) $(a+c) \equiv (b+c) \pmod n$ (ii) $ac \equiv bc \pmod n$.

Remark. From above, we find that addition, subtraction or multiplication to both sides of a congruence by an integer does not change the congruence. But this may not be true if we divide both sides of a congruence by an integer.

For example : Consider the congruencies

$24 \equiv 12 \pmod 4$ *i.e.* $6.4 \equiv 6.2 \pmod 4$

If we divide both sides of this congruence by 6, then we obtain $4 \equiv 2 \pmod 4$ which is not true as $4 \nmid (4-2)$. Hence $4 \equiv 2 \pmod 4$.

The next theorem will throw some light in this regard.

Theorem : Let a, b, c be integers and n be a positive integer n.

(i) $ab \equiv ac \pmod n$ if and only if $b \equiv c \left(\mod \frac{n}{(a,n)}\right)$

(ii) If $ab \equiv ac \pmod n$ and $(a, n) = 1$, then $b \equiv c \pmod n$.

Proof. (i) Let $d = (a, n)$. Since $n > 0$, $d \neq 0$.

$\therefore \quad \exists$ integers r and t such that $(r, t) = 1$ and $a = dr$, $n = dt$.

Now $ab \equiv ac \pmod n$

$\Rightarrow \quad n \mid ab-ac \Rightarrow dt \mid dr\,b - dr\,c$

$\Rightarrow \quad t \mid rb-rc$ *i.e.* $t \mid r(b-c)$

But t and r are relatively prime $\because (r, t) = 1$

$\therefore \quad t \mid b-c \quad i.e. \quad b \equiv c \pmod{t}$

i.e. $\quad b \equiv c \left(\mod \frac{n}{d}\right) \quad (\because n = dt)$

i.e. $\quad b \equiv c \left(\mod \frac{n}{(a,n)}\right).$

(*ii*) The proof of this follows from (*i*) as $(a, n) = 1$.

ILLUSTRATIVE EXAMPLES

Example 1. $26 \equiv 2 \pmod{12}$

Sol. As $\quad 12 \mid 26-2$ *i.e.* $12 \mid 24$

$\therefore \quad 26 \equiv 2 \pmod{12}$

Example 2. Show that n is odd iff $n \equiv 1 \pmod 2$

Sol. Firstly let n is odd

$\therefore \quad n = 2k+1 \; ; k \in \mathbf{Z} \quad \Rightarrow \quad n-1 = 2k$

$\Rightarrow \quad 2 \mid n-1$

$\Rightarrow \quad n \equiv 1 \pmod 2$

Conversely let $n \equiv 1 \pmod 2$

$\therefore \quad 2 \mid n-1 \quad \Rightarrow \quad \exists \; k \in \mathbf{Z}$ s.t.

$n-1 = 2k$

i.e. $\quad n = 2k+1 \quad \Rightarrow \quad n$ is odd.

Example 3. Show that for every prime $p > 5$ either $p^2 - 1$ or

$p^2 + 1$ is divisible by 10

Sol. Since $p > 5$ and p is a prime, so p is odd

$\therefore \quad 2 \mid p^2 - 1$ and $2 \mid p^2 + 1$ ...(1)

As $\quad 5 \nmid p$, we have

$p \equiv 1, 2, 3,$ or $4 \pmod 5$

$\Rightarrow \quad p^2 \equiv 1$ or $4 \pmod 5$

$\Rightarrow \quad p^2 \equiv \pm 1 \pmod 5$

$\Rightarrow \quad 5 \mid p^2 - 1$ or $5 \mid p^2 + 1$ ...(2)

From (1) and (2),

$10 \mid p^2 - 1$ or $10 \mid p^2 + 1$.

Example 4. Prove that if n is composite, then $(n-1)! \equiv 0 \pmod{n}$ except for $n = 4$.

Sol. Since n is composite

$\therefore \quad n = a\,b, \quad 1 < a \le b < n$

For $a = b = 2$,

$(n-1)! = 3! = 6 \neq 0 \pmod 4$

Let $a = b \neq 2$

Then $n = a\,b = a.\,a > 2\,a$

$\Rightarrow \qquad (n-1) \ge 2\,a$

$\Rightarrow$ both a and $2\,a$ occurs in $(n-1)!$

$\Rightarrow \qquad a\,.\,2\,a \mid (n-1)!$

$\Rightarrow \qquad a^2 \mid (n-1)!$

$\Rightarrow \qquad n \mid (n-1)!$

$\Rightarrow \qquad (n-1)! \equiv 0 \pmod n.$

Lastly let $\qquad a \neq b$

Then $\qquad 1 < a < b < n$

$\Rightarrow \qquad 1 < a < b \le n-1$

$\Rightarrow$ both a and b occur in $(n-1)!$

$\Rightarrow \quad ab \mid (n-1)!$

$\Rightarrow \qquad (n-1)! \equiv 0 \pmod n$

Example 5. Prove that an integer is divisible by 3 iff its num of digits is divisible by 3

Sol. Let $N = a_m 10^m + a_{m-1}\,10^{m-1} + \ldots\ldots + 10^2 a_2 + 10\,a_1 + a_0$ be decimal expansion of an integer N

Consider integer polynomial

$$f(x) = \sum_{k=0}^{m} a_k\, x^k$$

Then $\qquad N = f(10)$

Now $\qquad 10 \equiv 1 \pmod 3$

$\Rightarrow \qquad f(10) \equiv f(1) \pmod 3$

$\Rightarrow \qquad N \equiv \sum_{k=0}^{m} a_k \pmod 3$

Thus $\quad 3 \mid N$

iff $\quad 3 \mid \sum_{k=0}^{m} a_k$.

Example 6. For any prime p, prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$

Sol. We have

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{b-2}b^2 + \ldots\ldots + \binom{p}{p-1}ab^{p-1} + b^p$$

Since $p \left| \binom{p}{r} \right.$, for $1 \le r \le p-1$

so $\binom{p}{r} \equiv 0 \pmod{p}$ for $1 \le r \le p-1$

Thus $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Example 7. If $a^h \equiv 1 \pmod{m}$ for some positive integer h then $(a, m) = 1$

Sol. Let $a^h \equiv 1 \pmod{m}$

Then $a^h = 1 + mk,\ k \in \mathbf{Z}$

$\Rightarrow \quad a^h - mk = 1$

$\Rightarrow \quad a\,a^{h-1} + m(-k) = 1$

$\Rightarrow \quad (a, m) = 1$

Example 8. For $n \ge 1$, using congruence, show that $43 \mid 6^{n+2} + 7^{2n+1}$.

Sol. We have

$$\begin{aligned} 6^{n+2} + 7^{2n+1} &= 6^n \cdot 6^2 + 7^{2n} \cdot 7 \\ &\equiv 6^n \cdot 36 + 49^n \cdot 7 \\ &\equiv 6^n \cdot 36 + 6^n \cdot 7 \pmod{43} \\ &\equiv 6^n \cdot 43 \\ &\equiv 0 \pmod{43} \end{aligned}$$

$\Rightarrow \quad 43 \mid 6^{n+2} + 7^{2n+1}$

Example 9. Show that $2^{15} \cdot 14^{40} + 1$ is divisible by 11

Sol. We have

$$2^4 \equiv 5 \pmod{11}$$

$$\therefore \quad (2^4)^2 \equiv 5^2 \equiv 3 \pmod{11}$$

i.e. $\quad 2^8 \equiv 3 \pmod{11}$

Multiply (1) and (2)

$$2^{12} \equiv 15 \equiv 4 \pmod{11}$$

$$2^{12} \cdot 2^3 \equiv 4 \cdot 2^3 \pmod{11}$$

$$2^{15} \equiv 32 \equiv -1 \pmod{11} \quad \ldots(3)$$

Since $14 \equiv 3 \pmod{11}$

$\therefore$ $14^{40} \equiv 3^{40} \pmod{11}$

and $3^2 \equiv -2 \pmod{11}$

$\Rightarrow$ $3^4 \equiv -18 \equiv 4 \pmod{11}$

$\Rightarrow$ $3^8 \equiv 16 \equiv 5 \pmod{11}$

$\Rightarrow$ $3^{10} \equiv 45 \equiv 1 \pmod{11}$

Thus $14^{40} \equiv 3^{40} \equiv 1 \pmod{11}$ ...(4)

Multiply (3) and (4)

$$2^{15} \cdot 14^{40} \equiv -1 \pmod{11}$$

i.e. $2^{15} \cdot 14^{40} + 1 \equiv 0 \pmod{11}$

$\Rightarrow$ $2^{15} \cdot 14^{40} + 1$ is divisible by 11.

Example 10. Find the remainder when $1! + 2! + 3! + \ldots\ldots\ldots + 100!$ is divided by 12.

Sol. For $n \geq 4$, we have

$$n! \equiv 0 \pmod{12}$$

$\therefore$ $1! + 2! + 3! + 4! + \ldots\ldots\ldots + 100! \equiv 1! + 2! + 3! \pmod{12}$

$$\equiv 9 \pmod{12}$$

The remainder = 9.

Example 11. Find the remainder when 4444^{4444} is divided by 9.

Sol. We have $4444 = 9 \cdot 493 + 7$

$$\equiv 7 \pmod{9}$$

$$\equiv -2 \pmod{9}$$

$\therefore$ $4444^{4444} \equiv (-2)^{4444} \pmod{9}$

As $-8 \equiv 1 \pmod{9}$

$\therefore$ $4444^{4444} \equiv (-2)^{3 \cdot 1481 + 1} \pmod{9}$

$$\equiv (-8)^{1481} \cdot (-2) \pmod{9}$$

$$\equiv 1 \cdot (-2) \pmod{9}$$

$$\equiv 7 \pmod{9}$$

7 is the remainder.

Example 12. Verify that $2^{2^5}+1$ is divisible by 641.

Sol. We have $2^{2^5}+1 = 2^{32}+1$

Now $2^{11} = 2048 \equiv 125 \pmod{641}$

$\Rightarrow$ $2^{22} \equiv (125)^2 \equiv 241 \pmod{641}$

$\therefore$ $2^{11}.2^{22} \equiv 125 \times 241 \pmod{641}$

$\Rightarrow$ $2^{33} \equiv 30125 \equiv -2 \pmod{641}$

Since $(2,641) = 1$

$\therefore$ $2^{32} \equiv -1 \pmod{641}$

$\Rightarrow$ $2^{2^5}+1 \equiv 0 \pmod{641}$

i.e. $641 \mid 2^{2^5}+1$

Example 13. Find the remainder when

(*a*) 2^{50} is divided by 7 (*b*) $53^{103}+103^{53}$ is divided by 39.

Sol. We have

$$2^{50} = 2^{3\cdot16+2}$$
$$= 8^{16}.2^2$$
$$= 8^{16}.4$$

Since $8 \equiv 1 \pmod 7$

$\therefore$ $8^{16} \equiv 1 \pmod 7$

Thus $2^{50} \equiv 4 \pmod 7$

$\Rightarrow$ 4 is the remainder when 2^{50} is divided by 7.

(*b*) We have

$53 \equiv 14 \pmod{39}$ and $103 \equiv -14 \pmod{39}$

$\therefore$ $53^{103}+103^{53} \equiv 14^{103}+(-14)^{53} \pmod{39}$

$$\equiv 14^{53}(14^{50}-1) \pmod{39}$$
$$\equiv 14^{53}(196^{25}-1) \pmod{39}$$

Since $196 \equiv 1 \pmod{39}$

$\therefore$ $196^{25} \equiv 1 \pmod{39}$

Thus $53^{103}+103^{53} \equiv 14^{53}(1-1) \pmod{39}$

$$\equiv 0 \pmod{39}$$

$\Rightarrow$ 39 divides $53^{103}+103^{53}$.

EXERCISE 1.3

1. Prove that if $c > 0$ and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$
2. Give an example to show that
   (*i*) If $ab \equiv 0 \pmod{m}$, then $a \not\equiv 0 \pmod{m}$ and $b \not\equiv 0 \pmod{m}$
   (*ii*) $a^2 \equiv b^2 \pmod{m}$ does not imply $a \equiv b \pmod{m}$
3. If $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ then $a \equiv b \pmod{g}$
   where $g = (m, n)$.
4. Find the remainder when
   (*i*) 3^{40} is divided by 23 (*ii*) 48^{49} and $111^{33} + 333^{111}$ are divided by 7.
5. Show that $2^{37} - 1$ is divisible by 233.
6. Using congruences, prove the following, for $n \geq 1$,
   (*i*) $7 \mid 3^{2n+1} + 2^{n+2}$ (*ii*) $13 \mid 3^{n+2} + 4^{2n+1}$ (*iii*) $27 \mid 2^{5n+1} + 5^{n+2}$

ANSWERS

2. (*i*) $a = 2, b = 3$ and $m = 6$ (*ii*) $a = 3, b = 2$ and $m = 5$
4. (*i*) 2 (*ii*) 6, 0

1.5. Quotient Structures

Definition : (Quotient set)

A Quotient set is a set derived from another by an equivalence relation.

Definition : (Quotient Structure)

Let S be a structure, R, an equivalence relation. If the equivalence classes form a structure of the same species as S under relations derived from passing to quotients, R is said to be compatible with the structure on S, and this structure on the equivalence classes of S is called the quotient structure, or the derived structure, of S/R.

Definition : (Free Monoid)

In abstract algebra, the **free monoid** on a set is the monoid whose elements are all the finite sequence (or strings) of zero or more elements from that set, with string concatenation as the monoid operation and with the unique sequence of zero elements, often called the empty string and denoted by ε or λ, as the identity element. The free monoid on a set A is usually denoted A^*. The free semigroup on A is the subsemigroup of A^* containing all elements except the empty string. It is usually denoted A^+.

More generally, an abstract monoid (or semigroup) S is described as free if it is isomorphic to the free monoid (or semigroup) on some set.

Definition : (Cyclic Group)

Definition :

A group G is called a **cyclic group** if $\exists\ a \in G$ such that each element of G can be written as an integral power of a *i.e.*, if $b \in G$, then $\exists\ a \in G$ such that $b = a^n$ for some integer n.

a is then called a **generator of G.**

Note. (*i*) If G is a cyclic group generated by a, we write it as $G = < a >$.

(*ii*) If G is a group under addition, then G is called a **cyclic group** if each element of G is an integral multiple of a *i.e.*, if $b \in G$, then $b = n\,a$ for some integer n.

(*iii*) A cyclic group is also called a **Monic group.**

(*iv*) If $G = < a >$ be a cyclic group of order n, then

$G = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$ *i.e.*, $O(G) = O(a) = n$.

(*v*) If a is a generator of a cyclic group G, then a^{-1} is also a generator of G, for any $x \in G$, we have $x = a^n$, also $x = (a^{-1})^{-n}$, where $n, -n \in \mathbf{Z}$.

Examples of Cyclic groups

Example 1. Show that the multiplicative group $\{1, w, w^2\}$ formed by the cube roots of unity is a cyclic group.

Sol. Let G be the group of cube roots of unity under multiplication.

$\therefore \quad G = \{1, \omega, \omega^2\}$.

Here, $1 = \omega^3$, therefore each element of G is an integral power of ω.

$\therefore$ G is cyclic group generated by ω *i.e.* $G = < \omega >$.

Example 2. Show that the multiplicative group $\{1, -1, i, -i\}$ formed by the fourth roots of unity is a cyclic group.

Sol. $G = \{1, -1, i, -i\}$ is a group under multiplication.

Since $1 = (i)^4$, $-1 = i^2$, $-i = i^3$.

Therefore each element of G is an integral power of i.

$\therefore$ G is a cyclic group generated by i *i.e.* $G = < i >$.

Example 3. Show that the group **Z** of integers under addition is an infinite cyclic group generated by 1.

Sol. Since each $n \in \mathbf{Z}$ can be written as $n = n \cdot 1$

$\therefore \quad \mathbf{Z} = < 1 >$.

Also each $n \in \mathbf{Z}$ can be written as $n = (-n)(-1)$ where $-n \in \mathbf{Z}$

$\therefore \quad \mathbf{Z} = < -1 >$ *i.e.* **Z** has two generators 1 and -1.

Example 4. Show that the group $G = \{(0, 1, 2, 3, 4, 5\}, +_6\}$ is a cyclic group under the operation addition congruence modulo 6.

Sol. Since $1 = 1\ (1)$

$2 = 1 +_6 1 = 2\ (1)$

$3 = 1 +_6 1 +_6 1 = 3\,(1)$

$4 = 1 +_6 1 +_6 1 +_6 1 = 4\,(1)$

$5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5\,(1)$

$0 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 6\,(1)$.

$\therefore$ every element n of G can be written as $n = n\,(1)$.

$\therefore$ $G = <1>$ *i.e.* G is a cyclic group.

Note : Here G is also generated by 5 *i.e.* $G = <5>$. (Can be easily proved)

$\therefore$ A group may have more than one generators.

Example 5. Prove that the five roots of unity form a cyclic group under multiplication.

Sol. We know that the n –nth roots of unity

$$G = \left\{ e^{\frac{2r\pi i}{n}} : 0 \le r \le n-1 \right\}$$

from an abelian group under multiplication

Let $G_1 = \left\{ e^{\frac{2r\pi i}{5}} : 0 \le r \le 4 \right\} = \{1, e^x, e^{2x}, e^{3x}, e^{4x}\}$ where $x = \frac{2\pi i}{5}$

form an abelian group

Clearly $G_1 = <e^x>$ is a cyclic group generated by e^x

As $e^{2x} = (e^x)^2$, $e^{3x} = (e^x)^3$, $e^{4x} = (e^x)^4$

$$e^{5x} = e^{5\left(\frac{2\pi i}{5}\right)} = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1 + i \cdot 0 = 1$$

Theorem. Let G be a finite group of order n. If G contains an element of order n, then G must be cyclic.

Proof. Let $a \in G$ such that $O(a) = n$.

Let $H = \{a^r : r \in I\}$ be a subgroup of G.

But $O(a) = n \Rightarrow H = \{e, a, a^2, \ldots, a^{n-1}\} = <a>$

i.e., H is a cyclic subgroup of G generated by a.

Also $O(H) = O(G)$

$\Rightarrow$ $G = H = <a>$.

i.e., G is a cyclic group.

Note : In order to show that a finite group is cyclic or not. Find the order of every element of G. If G contains an element whose order is equal to the order of the group, then the group must be cyclic and that element will be the generator of the cyclic group, otherwise the group is not cyclic.

Theorem : Every cyclic group is abelian.

Proof. Consider a cyclic group G generated by a. *i.e.* $G = <a>$.

Let $x, y \in G$ be arbitrary elements.

$\therefore \quad x = a^n$ and $y = a^m$ for some integers n and m.

Then $xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx.$

$\therefore$ G is an abelian group.

Remark : The converse of above theorem need not be true *i.e.* An abelian group need not be cyclic.

Example 6. Give two examples of abelian groups which are not cyclic.

Sol. (*i*) Let $\langle \mathbf{Q}, + \rangle$ be the group of rational numbers under addition.

It is an abelian group which is not cyclic.

For, suppose that $\frac{m}{n} \in \mathbf{Q}$ is a generator of $\mathbf{Q}$.

Then every element of $\mathbf{Q}$ should be an integral multiple of $\frac{m}{n}$.

Let $\frac{1}{3n} \in \mathbf{Q}$ be any element.

Let $\frac{1}{3n} = k \cdot \frac{m}{n}$ for some integer k.

$\Rightarrow \qquad \frac{1}{3} = km,$

which is not possible as k, m are integers, where as $\frac{1}{3}$ is not.

Hence no element can act as generator of $\mathbf{Q}$.

(*ii*) Let $G = \left\{ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$

The composition defined on G is usual multiplication of matrices.

The composition table is given below :

·	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Since all the elements in the composition table are the elements of G. Therefore G is closed under multiplication. Also the multiplication of 2×2 matrices is associative.

Also I is the identity element of G and

$A^2 = B^2 = C^2 = I$ implies that $A^{-1} = A, \quad B^{-1} = B, \quad C^{-1} = C.$

$\therefore$ inverse of each element exists in G.

Also the entries on both sides of the diagonal are identical.

$\therefore$ G is an abelian group of order 4.

Since $A^2 = B^2 = C^2 = I \quad \therefore \quad O(A) = O(B) = O(C) = 2$

Also $O(I) = 1$.

$\therefore$ G has no element whose order is equal to the order of G *i.e.*, 4.

Hence G is not a cyclic group.

Theorem : Prove that the order of a cyclic group is equal to order of its generator.

ILLUSTRATIVE EXAMPLES

Example 1. Show that the set of *n*-*n*th roots of unity forms a cyclic group under multiplication.

Sol. We know that the set of *n*-*n*th roots of unity *i.e.* $G = \left\{ e^{\frac{2r\pi i}{n}} : 0 \le r \le n-1 \right\}$ forms an abelian group under multiplication.

Let $x = e^{\frac{2\pi i}{n}}$.

$\therefore \quad G = \left\{1, e^x, e^{2x}, e^{3x}, e^{4x}, \ldots\ldots e^{(n-1)x}\right\}$.

Clearly $G = \langle e^x \rangle$ is a cyclic group of order *n*, generated by e^x,

since $e^{rx} = (e^x)^r$ for all $0 \le r \le n-1$.

Example 2. Show that the group $< G, X_7 >$ is cyclic where $G = \{1, 2, 3, 4, 5, 6\}$. How many generators are there ?

Sol. Firstly we are to show that there exists an element $x \in G$ such that $O(x) = O(G) = 6$, then G will be cyclic group and x will be generator.

Here identity element of G is $e = 1$

Further $3^1 = 3, \; 3^2 = 3 X_7 3 = 2$

$3^3 = 3^2 X_7 3 = 2 X_7 3 = 6, \; 3^4 = 3^3 X_7 3 = 6 X_7 3 = 4$

$3^5 = 3^4 X_7 3 = 4 X_7 3 = 5, \; 3^6 = 3^5 X_7 3 = 5 X_7 3 = 1$

so that $3^6 = 1 = e$ and $3^a \neq 1$ for $a < 6$

$\therefore$ $O(3) = 6$ $O(G)$ so that 3 is a generator

We have $3^6 = 1, \; 3^5 = 5, \; 3^4 = 4, \; 3^3 = 6, \; 3^2 = 2, \; 3^1 = 3$

$\therefore$ G can be expressed as $\{3^6, 3^2, 3^1, 3^4, 3^5, 3^3\}$

i.e. $\{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\}$

$\Rightarrow$ G is cyclic.

II[nd] Part : To determine number of generators ?

An element $3^n \in G$ will be generator of G if g.c.d. of n and 6 is one

and we have $(1, 6) = (5, 6) = 1$

so there are two generators 3^1, 3^5.

Example 3. How many generators are there of cyclic group of order 10 ?

Sol. Let G be a cyclic group of order 10 generated by 'a'

$\therefore \quad O(a) = O(G) = 10$

So $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10} = e\}$

An element $a^n \in G$ will be generator of G if g. c. d of n and 10 is one

and we have $(1, 10) = (3, 10) = (7, 10) = (9, 10) = 1$

So there are four generators of G namely a^1, a^3, a^7 and a^9.

EXERCISE 1.4

1. Show that $G = \{1, 2, 3, 4\}$ forms a cyclic group under multiplication modulo 5.
2. If an abelian group of order 6 contains an element of order 3, then show that it must be cyclic group.
3. Let G be a cyclic group of order 8. Find how many generators are there.
4. Define cyclic group. Determine which of the following are cyclic groups and find their generator.

   (*i*) $\{1, -1, i, -i\}$ (*ii*) $(Z, +)$ (*iii*) $(R, +)$
5. Evaluate $1^6, 1^{-5}$ where $1 \in Q$, the additive group of rational numbers.
6. Show that group $\{1, 5, 7, 11\}$ of intergers under multiplication moduls 12 is not a cyclic group.

ANSWERS

3. 4 generators **4.** (*i*) Cyclic (*ii*) Cyclic (*iii*) Not Cyclic **5.** $1^6 = 6$, $1^{-5} = -5$

1.6. Substructures

Definition : In mathematical logic, an (induced) substructure or (induced) subalgebra is a structure whose domain is a subset of that of a bigger structure, and whose functions and relations are the traces of the functions and relations of the bigger structure. Some examples of **subalgebras** are **subgroups**, **submonoids**, **subrings**, **subfileds**, **subalgebras of algebras** over a field, or **induced subgraphs**. Shifting the point of view, the larger structure is called an **extension** or a **superstructure** of its substructure.

Definition : (Submonoids)

Let $(G, *)$ be a monoid and $H \subseteq G$

Then $(H, *)$ **is called a submonoid of** $(G, *)$ **Iff** (*i*) **H is closed under the operation** $*$.

(*ii*) There exists an identity element $e \in H$.

For example : Let Z = set of all integers with * as binary operation, which is monoid, Then

$Z_1 = \{a^k \mid 0 \le k \le n,$ 'a' positive integer $\in Z\}$ with binary operation * is a submonoid of (Z, *).

Definition : (Subgroups)

A non-empty subset H of a group <G, *> is said to be a subgroup of G if <H, *> is itself a group.

Here H is a group in itself under the same (or induced) operation of G.

Notice that every group G has atleast two subgroups, viz., $\{e\}$ and G itself. These two are called **trivial or improper** subgroups. If H is a subgroup of a group G such that $H \neq \{e\}$ and $H \neq G$, then H is called a **non-trivial** or **Proper** subgroup of G.

For example

(*i*) We know $< \mathbf{R}, + >$, the set of all reals under addition is a group. Also <Q, + >, the set of rationals is also a group and $\mathbf{Q} \subset \mathbf{R}$

$\therefore$ $< \mathbf{Q}, + >$ is a subgroup of $< \mathbf{R}, + >$.

(*ii*) $< \mathbf{Q}^+, \cdot >$ is a group and $\mathbf{Q}^+$ (the set of positive rationals) is a subset of **R** (the set of real numbers). Also $< \mathbf{R}, + >$ is a group.

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

But $< \mathbf{Q}^+, \cdot >$ is not a subgroup of $< \mathbf{R}, + >$.

(*iii*) $< \mathbf{Q} - \{0\}, \cdot >$ is a group.

$\therefore$ $< \mathbf{Q}^+, \cdot >$ is a subgroup of $< \mathbf{Q} - \{0\}, \cdot >$

(*iv*) Let $G = \{1, -1, i, -i\}$ and $H = \{1, -1\}$, where $i^2 = -1$.

Here G is a group under usual multiplication of complex numbers and H is a subgroup of G.

(*v*) Let G be the set of all 2×2 non-singular matrices over complex numbers, then G is a group under matrix multiplication.

Let $H = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$.

Clearly $H \subset G$. Also H is a group in itself under the same operation of matrix multiplication.

Hence H is a subgroup of G.

Some Observations

1. If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.
2. If H and K are subgroups of a group G and $H \subseteq K$, then H is a subgroup of K.

Notation : If H is a subgroup of G. Then we write it as $H \le G$ (or $H < G$).

Again H is a proper subgroup of G is denoted as

$H < G$ (or $H < G, H \neq G$).

PROPERTIES OF SUBGROUPS

I. The identity element of a subgroup is same as the identity element of the group.

Proof. Let H be a subgroup of a group G.

Let e and e' be the identity elements of G and H respectively

Let $a \in H$ be any element [$\because$ e' is the identity of H]

$\therefore$ $a e' = a$

Also $\because\ a \in H$ and $H \subseteq G \Rightarrow a \in G$

$\therefore \quad a\,e = a$ [$\because$ e is the identity of G]

$\therefore$ we have $a\,e = a\,e'$

$\Rightarrow \quad e = e'.$ [by left cancellation law]

Hence the identity of a group and that of a subgroup is the same.

II. The inverse of any element of a subgroup is the same as the inverse of the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ be any element.

Since $H \subseteq G \quad \therefore\ a \in G.$

Let b be the inverse of a in H and c be the inverse of a in G.

$\therefore \quad b\,a = e$ and $c\,a = e$

$\Rightarrow \quad b\,a = c\,a$

$\Rightarrow \quad b = c.$ [by right cancellation law]

Hence the inverse of any element of a subgroup is same as the inverse of the same element regarded as an element of the group.

III. The order of any element in a subgroup is the same as the order of the element regarded as the element of the group.

Proof. Let e be the identity element of G and H.

Let $a \in H$ such that $o(a) = n$

$\Rightarrow \quad a^n = e$ and $a^m \neq e$ for every $m < n$.

Also $a \in H \Rightarrow a \in G$ and so $a^n = e \in G \Rightarrow o(a) = n$ in G.

Hence order of any element in a subgroup is same as the order of the element regarded as the element of the group.

IV. Subgroup of an abelian group is abelian.

Proof. Let H be a subgroup of an abelian group G

$\therefore \quad H \subseteq G.$

Let $a, b \in H$ be any two elements

$\therefore \quad a, b \in G \Rightarrow a\,b = b\,a$ [$\because$ G is abelian]

$\therefore \quad \forall\ a, b \in H$ we have $a\,b = b\,a$

Hence H is an abelien subgroup of G.

The converse of above result is false

i.e., A subgroup may be abelian even if G is not abelian.

Remark : (I) A non-abelian group may also have abelian subgroups.

For example : (*i*) The sets $\{1, -1\}$ and $\{1, -1, i, -i\}$ are abelian subgroups of the non-abelian group of Quaternion Q_8 under multiplication.

(*ii*) The sets $H = \{I, (12)\}$ and $K = \{I, (123), (132)\}$ are abelian subgroups of the non-abelian group S_3, the symmetric group on three numbers 1, 2, 3.

(II) A non-abelian group may also have a non-abelian subgroup.

For example : (*i*) SL (2, R) is a non-abelian subgroup of the non-abelian group GL (2, R) under the composition of multiplication of matrices.

(*ii*) S_3 and A_4 are non-abelian subgroups of non-abelian group S_4 under the composition of composite of mappings. [See Chapter on Permutation groups]

CRITERION FOR A SUBSET TO BE A SUBGROUP OF A GROUP

Lemma I. A non-empty subset H of a group G is a subgroup iff

(*i*) $a\,b \in H, \forall\ a, b \in H$ (*ii*) $a^{-1} \in H, \ \forall\ a \in H$.

Proof. Necessary part. Suppose that a non-empty subset H of a group G is its subgroup.

Therefore H itself forms a group.

$\therefore$ The conditions (*i*) and (*ii*) hold in H, by the definition of a group

Sufficient Part. Suppose that H is a non- empty subset of a group G such that the conditions (*i*) and (*ii*) hold in H.

$\therefore$ The closure property and the existence of inverse holds in H.

Now, let $a, b, c \in H$ [$\because H \subseteq G$]

$\therefore$ $a, b, c \in G$

$\therefore$ $(a\,b)\,c = a\,(b\,c)$ since G is group.

So, the associative law holds in H.

Since H is a non-empty subset of G, so $\exists\ a \in H$.

$\therefore$ By (*ii*), $a^{-1} \in H$ $a, a^{-1} \in H$

So,

$\therefore$ $a\,a^{-1} \in H$, from (*i*)

$\Rightarrow$ $e \in H$, where e is identity element of G.

$\Rightarrow$ The identity element exists in H.

Therefore, H itself is a group

Thus H is a subgroup of G.

Note : The above two conditions can be combined to *a* single condition $a\,b^{-1} \in H\ \forall\ a, b \in H$

Lemma II. A non empty subset H of a group G is a subgroup iff $a\,b^{-1} \in H\ \forall\ a, b \in H$.

Proof : Necessary Part : Suppose that a non empty subset H of a group G is its subgroup.

$\therefore$ H itself forms a group.

$\Rightarrow$ $\forall\ b \in H \Rightarrow b^{-1} \in H$.

Also $\forall\ a, b \in H \Rightarrow a, b^{-1} \in H$ ($\because$ H is a group)

$\Rightarrow$ $a\,b^{-1} \in H$.

Sufficient part : Suppose that H is a non-empty subset of a group G such that $\forall\, a, b \in H \Rightarrow a b^{-1} \in H$.

To prove H is a subgroup of G.

Clearly associative law holds in H, as it holds in G and elements of H are also elements of G. Further

$$\forall\, a \in H \Rightarrow a, a \in H \Rightarrow a a^{-1} \in H \Rightarrow e \in H$$

i.e. identity element exists in H.

Now $e, a \in H \Rightarrow e a^{-1} \in H \Rightarrow a^{-1} \in H$

$\therefore\ \forall\, a \in H \Rightarrow a^{-1} \in H$ *i.e.* inverses are there in H.

Also $\forall\ a, b \in H \Rightarrow a, b^{-1} \in H$ ($\because$ inverses are there in H)

$\Rightarrow\quad a(b^{-1})^{-1} \in H$

$\Rightarrow\quad a b \in H.$

$\therefore$ closure property holds in H.

$\therefore$ H is a group in itself under the operation of G.

Hence H is a subgroup of G.

Remark : In case of additive notation, the above two lemmas can be stated as :

A non-empty subset H of a group G is a subgroup iff

(*i*) $a + b \in H,\ \forall\, a, b \in H$

(*ii*) $-a \in H,\ \forall\, a \in H.$

The above two conditions can be combined to a single condition $a - b \in H,\ \forall\, a, b \in H.$

CRITERION FOR A FINITE SUBSET TO BE A SUBGROUP OF A GROUP

Lemma : A non-empty finite subset H of a group is a subgroup of G iff $a b \in H, \forall\, a, b \in H.$

Proof : Necessary Part. Let a non-empty finite subset H of a group G be its subgroup.

$\therefore$ H itself is a group

$\therefore\ a b \in H,\quad \forall\, a, b \in H.$ (By closure property)

Sufficient Part. Suppose that H is a non-empty finite subset of a group G such that $a b \in H, \forall\, a, b \in H.$

$\therefore$ The operation of multiplication is a binary operation on H.

Let $a, b, c \in H \Rightarrow a, b, c \in G,$ since $H \subseteq G.$

$\Rightarrow\ (a b) c = a (b c),$ since G is a group.

$\therefore$ The associative law holds in H under multiplication.

Firstly we prove that cancellation laws hold in H.

Let $a, b, c \in H$ such that $a b = a c.$

Since $a \in H,$ so $a \in G.$

$\therefore\ a^{-1} \in G$ such that $a a^{-1} = e = a^{-1} a$

Now $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$

$\Rightarrow eb = ec \Rightarrow b = c$

$\therefore ab = ac \Rightarrow b = c.$

Similarly $ba = ca \Rightarrow b = c.$

$\therefore$ The cancellation laws hold in H.

$\therefore$ H is a non-empty finite set with an associative binary operation in H and the cancellation laws hold in H.

$\therefore$ H itself is a group. (already proved)

Thus H is a subgroup of G.

Notice that the above theorem holds for only finite subsets of a group.

Remark : In case of additive notation, the above lemma can be stated as

A non-empty finite subset H of a group G is a subgroup iff

$a - b \in H, \quad \forall a, b \in H.$

Theorem : (*i*) Prove that the intersection of two subgroups of a group is again a subgroup of the group.

Proof. Let H and K be two sub groups of a group G.

$\therefore$ H and K are subsets of G.

$\Rightarrow H \cap K \subseteq G.$

Now let $x, y \in H \cap K$

$\therefore x, y \in H$ and $x, y \in K$

$\Rightarrow xy^{-1} \in H$ and $xy^{-1} \in K,$ since H, K are both subgroups of G.

$\Rightarrow xy^{-1} \in H \cap K$

$\therefore xy^{-1} \in H \cap K, \ \forall \ x, y \in H \cap K$

$\therefore$ $H \cap K$ is a subgroup of G.

Theorem : (*ii*) The intersection of an arbitrary collection of subgroups of a group is again a subgroup of the group.

Sol. Let G be the group and $\{H_\lambda \mid \lambda \in \wedge\}$ be a family of subgroups of G.

Take $H = \bigcap_{\lambda \in \wedge} H_\lambda$

Since H_λ is a subgroup of G, $\forall \lambda \in \wedge$

$\therefore e \in H_\lambda \ \forall \lambda \in \wedge$

$\Rightarrow e \in \bigcap_{\lambda \in \wedge} H_\lambda$

$\Rightarrow e \in H \Rightarrow H \neq \phi$

Also as $H_\lambda \subseteq G, \forall \lambda \in \wedge$

so $\bigcap_{\lambda \in \wedge} H_\lambda \subseteq G$

$\Rightarrow$ $H \subseteq G$

Now let $a, b \in H$

$\Rightarrow$ $a, b \in \bigcap_{\lambda \in \wedge} H_\lambda$

$\Rightarrow$ $a, b \in H_\lambda, \forall \lambda \in \wedge$

$\Rightarrow$ $ab^{-1} \in H_\lambda \ \forall \lambda \in \wedge$ ($\because$ for each $\lambda \in \wedge$, H_λ is a subgroup of G)

$\Rightarrow$ $ab^{-1} \in \bigcap_{\lambda \in \wedge} H_\lambda$

$\Rightarrow$ $ab^{-1} \in H$

$\Rightarrow$ H itself is a group and $H \subseteq G$

so H is a subgroup of G.

Remark. The union of any two subgroups of a group is not necessarily a subgroup of the group.

For example : (*i*) The sets $H = \{0, 3\}$ and $K = \{0, 2, 4\}$ are subgroups of the group $G = \{0, 1, 2, 3, 4, 5\}$ under the operation addition modulo 6. But the union $H \cup K = \{0, 2, 3, 4\}$ is not a subgroup of G, for $2, 3 \in H \cup K$, but $2 + 3 = 5 \notin H \cup K$.

(*ii*) The set $n\mathbf{Z} = \{\ldots\ldots, -3n, -2n, -n\, 0, 2n, 3n, \ldots\ldots\}$ of integral multiple of n, is a subgroup of the group of integers under addition.

$\therefore$ $2\mathbf{Z} = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}$

and $3\mathbf{Z} = \{\ldots\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ are subgroups of $\mathbf{Z}$, under addition.

But $2\mathbf{Z} \cup 3\mathbf{Z} = \{\ldots\ldots, -9, -6, -4, -3, -2, 0, 2, 3, 4, 6, 9, \ldots\ldots\}$ is not a subgroup of Z, for $4, 3 \in 2\mathbf{Z} \cup 3\mathbf{Z}$ but $4 + 3 = 7 \notin 2\mathbf{Z} \cup 3\mathbf{Z}$.

(*iii*) The set $H = \{1, -1, i - i\}$ and $K = \{1, -1, j - j\}$ are subgroups of the Quaternion group Q_8, but $H \cup K = \{1, -1, i - i, j, -j\}$ is not a subgroup of the Q_8 for, $i, j \in H \cup K$, but $i, j = k \notin H \cup K$.

(*iv*) The sets $H = \{I, (12)\}$ and $K = \{I, (13)\}$ are subgroups of S_3, the symmetric group on three numbers 1, 2, 3. But $H \cup K = \{I, (12), (13)\}$ is not a subgroup of S_3, for $(12), (13) \in H \cup K$, but $(12)(13) = (123) \notin H \cup K$.

Theorem : The union of two subgroups of a group is a subgroup iff one is contained in the other.

Proof. Necessary Part : Let H_1 and H_2 be two subgroups of a group G such that $H_1 \cup H_2$ is again a subgroup of G.

We shall prove that either $H_1 \subseteq H_2$, or $H_2 \subseteq H_1$.

If possible, suppose that $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$.

Since $H_1 \not\subseteq H_2$, so $\exists\ a \in G$ such that $a \in H_1$ but $a \notin H_2$.

Again since $H_2 \not\subseteq H_1$, so $\exists\ b \in G$ such that $b \in H_2$ but $b \notin H_1$.

Since $a \in H_1$ and $H_1 \subseteq H_1 \cup H_2$ so $a \in H_1 \cup H_2$.

Similarly $b \in H_2$ and $H_2 \subseteq H_1 \cup H_2 \Rightarrow b \in H_1 \cup H_2$

$\therefore\ a, b \in H_1 \cup H_2$

$\Rightarrow\ a b^{-1} \in H_1 \cup H_2$, since $H_1 \cup H_2$ is a subgroup

$\Rightarrow\ a b^{-1} \in H_1$ or $a b^{-1} \in H_2$.

First consider the case when $a b^{-1} \in H_1$.

Since $a \in H_1$ and H_1 is a subgroup $\therefore\ a^{-1} \in H_1$

$\therefore\ a^{-1}(a b^{-1}) \in H_1$

$\Rightarrow\ (a^{-1} a) b^{-1} \in H_1$

$\Rightarrow\ e b^{-1} \in H_1$

$\Rightarrow\ b^{-1} \in H_1$

$\Rightarrow\ (b^{-1})^{-1} \in H_1$

i.e., $b \in H_1$, which is not true.

$\therefore$ This case is not possible.

Now consider the case $a b^{-1} \in H_2$

Since $b \in H_2$.

$\therefore\ (a b^{-1}) b \in H_2 \quad \Rightarrow\ a(b^{-1} b) \in H_2$

i.e., $a e \in H_2 \quad \Rightarrow\ a \in H_2$, which is again false.

$\therefore$ This case is also not possible.

So both the cases are not possible. Therefore, our supposition is wrong.

$\therefore$ either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Sufficient Part : Suppose that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

$\Rightarrow\ H_1 \cup H_2 = H_2$ or $H_1 \cup H_2 = H_1$

$\Rightarrow\ H_1 \cup H_2$ is a subgroup of G, since both H_1 and H_2 are subgroups of G.

PRODUCT OF TWO SUBGROUPS

Let H and K be two subgroups of a group G, then the set HK defined by $HK = \{h k : \text{for all } h \in H, k \in K\}$ is called the product of the subgroups H and K.

Results : 1. A non-empty subset H of a group G is a subgroup, then $HH = H$.

2. A non-empty subset H of a group G is subgroup iff $HH^{-1} = H$.

3. If H and K are two subgroups of a group G, then HK is a subgroup of G iff $HK = KH$.

Definition. The **Centre of a group** G is denoted by Z (G) or C (G) or Z and is defined as

$$Z = C(G) = Z(G) = \{g \in G \mid gx = xg, \quad \forall x \in G\}.$$

Theorem. The centre Z (G) of a group G is a subgroup of G.

Proof. Let $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$ be the centre of a group G.

Clearly $Z(G) \subseteq G$.

Since $ex = xe, \quad \forall x \in G \quad \therefore \quad e \in Z(G)$.

Therefore, Z (G) is a non-empty subset of G.

Let $g_1, g_2 \in Z(G)$ be any two elements, then

$$g_1 x = x g_1 \quad \text{and} \quad g_2 x = x g_2, \quad \forall x \in G \quad \Rightarrow \quad x\, g_2^{-1} = g_2^{-1} x.$$

Now, $x(g_1 g_2^{-1}) = (x g_1)\, g_2^{-1} = (g_1 x)\, g_2^{-1} = g_1 (x\, g_2^{-1}) = g_1 (g_2^{-1} x) = (g_1\, g_2^{-1})\, x$

i.e., $x(g_1 g_2^{-1}) = (g_1\, g_2^{-1})\, x, \quad \forall x \in G.$

So, $g_1 g_2^{-1} \in Z(G), \quad \forall \ g_1, g_2 \in Z(G)$.

Hence, Z (G) is a subgroup of G.

Remark. G is an abelian group iff Z (G) = G.

Proof. Firstly, let Z (G) = G

i.e., $Z(G) = \{g \in G : gx = xg, \ \forall x \in G\} = G$

$\Rightarrow \quad xy = yx, \quad \forall x, y \in G \quad \Rightarrow$ G is an abelian group.

Conversely, let G be abelian $\quad \Rightarrow \quad xy = yx, \quad \forall x, y \in G.$

To show that Z (G) = G.

Since Z (G) is a subgroup of G $\quad \therefore \quad Z(G) \subseteq G$

Now, let $x \in G$ be any element

$\because$ G is abelian $\quad \therefore \quad xy = yx, \quad \forall y \in G.$

$\Rightarrow \quad x \in Z(G)$

$\therefore \quad G \subseteq Z(G)$

Hence $Z(G) = G$.

ILLUSTRATIVE EXAMPLES

Example 1. Show that the set $n\mathbf{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\ldots\}$ of all integral multiples of n, is a subgroup of the group **Z** of all integers under the operation of addition.

Sol. We know that **Z**, the set of integers forms a group under addition.

Now $n\mathbf{Z} = \{nm : m \in \mathbf{Z}\}$

Since $n, m \in \mathbf{Z} \quad \Rightarrow \quad nm \in \mathbf{Z}$

$\therefore \quad n\mathbf{Z} \subseteq \mathbf{Z}$.

We now show that $n\mathbf{Z}$ forms a group under addition.

Let $x, y \in n\mathbf{Z}$ so that $x = n m_1$ and $y = n m_2$ for some $m_1, m_2 \in \mathbf{Z}$.

$\therefore\ x - y = n m_1 - n m_2 = n(m_1 - m_2) \in n\mathbf{Z}$. [Since $m_1 - m_2 \in \mathbf{Z}$ for every $m_1, m_2 \in \mathbf{Z}$.]

$\therefore$ The closure property holds in $n\mathbf{Z}$.

The associative law holds in $n\mathbf{Z}$ since it holds in $\mathbf{Z}$ and $n\mathbf{Z} \subseteq \mathbf{Z}$.

Also $0 = n\,0 \in n\mathbf{Z}$ and $x + 0 = x = 0 + x,\ \forall x \in n\mathbf{Z}$.

$\therefore$ 0 is identity element of $n\mathbf{Z}$.

Now for $x = n m \in n\mathbf{Z}$ we have $y = n(-m) \in n\mathbf{Z}$.

And $x + y = n m + n(-m) = nm - nm = 0 = y + x$.

$\therefore$ y is the inverse of x in $n\mathbf{Z}$.

$\Rightarrow$ inverse of every element in $n\mathbf{Z}$ exists.

$\therefore$ $n\mathbf{Z}$ forms a group under addition.

Thus $n\mathbf{Z}$ is a subgroup of $\mathbf{Z}$.

Example 2. Let C^* denote the group of all non-zero complex numbers. Show that the set $S = \{z \in C^* \text{ s.t. } |z| = 1\}$ is a subgroup of C^*.

Sol. Since $|\in C^*$ and $|1| = 1$, $\therefore 1 \in S$

i.e., S is non-empty subset of C^*

Let $z_1, z_2 \in S$ be any two element $\Rightarrow |z_1| =$ and $|z_2| = 1$

Now $|z_1 z_2| = |z_1||z_2| = 1 \cdot 1 = 1$

$\Rightarrow$ $z_1 z_2 \in S$

$\therefore$ the closure property hold in S

The associative law holds in S since it holds in C^* and $S \subseteq C^*$

Since $1 \cdot z = z = z \cdot 1$ for all $z \in C^*$

In particular $1 \cdot z = z = z \cdot 1$ for all $z \in S$

$\therefore$ 1 is the identity element of S

Since for every $z \in S \Rightarrow z \in C^*$ $\therefore \exists\, z' \in C^*$ s.t.

$z z' = 1 = z' z$ [$\because$ C^* is a group]

But $|z z'| = |1| = |z' z|$

$\Rightarrow$ $|z||z'| = 1 = |z'||z|$

$\Rightarrow$ $1 \cdot |z'| = 1 \Rightarrow |z'| = 1 \Rightarrow z' \in S$

$\therefore$ for every $z \in S, \exists\, z' \in S$ *s.t.*

$z z' = 1 = z' z$

$\therefore$ inverse of every elements of S exists in S

$\Rightarrow$ S is a group under multiplication.

Hence S is a subgroup of C^*.

Example 3. Let G be group of 2×2 non singular matrices over R under multiplication. Show

$$W = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \Big/ a\,d \neq 0 \right\} \text{ is a subgroup of G.}$$

Sol. Clearly $W = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \Big/ \begin{matrix} a\,d \neq 0 \\ a, b\,d \in R \end{matrix} \right\}$ is non empty

subset of group $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big/ \begin{matrix} a, b, c, d \in R \\ \text{and } a\,d - b\,c \neq 0 \end{matrix} \right\}$ as $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in W$

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_b & b_2 \\ 0 & d_2 \end{bmatrix} \in W$ where $a_1\,d_1 \neq 0,\ a_2\,d_2 \neq 0$

Now $AB^{-1} = \begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} \begin{bmatrix} \frac{1}{a_2} & -\frac{b_2}{a_2\,d_2} \\ 0 & \frac{1}{d_2} \end{bmatrix}$ $\left(B^{-1} = \frac{1}{a_2\,d_2} \begin{bmatrix} d_2 & -b_2 \\ 0 & a_2 \end{bmatrix} \right)$

$$= \begin{bmatrix} \frac{a_1}{a_2} & -\frac{a_1\,b_2}{a_2\,d_2} + \frac{b_1}{d_2} \\ 0 & \frac{d_1}{d_2} \end{bmatrix} \in W \qquad \left(\because \frac{a_1}{a_2} \times \frac{d_1}{d_2} = \frac{a_1\,d_1}{a_2\,d_2} \neq 0 \right)$$

$\Rightarrow$ W is a subgroup of G.

Example 4. If e is an identity element of a group G, then $\{e\}$ is a subgroup of G.

Solution. Since e is the identity element of group G, therefore $e \in G$.

Let $H = \{e\}$, then $H \subseteq G$.

Since $e\,e = e \in H$, therefore closure property holds in H.

Also $(e\,e)\,e = e\,(e\,e) = e$.

$\therefore$ Associatively to holds is H

Since $e\,e = e = e\,e$

$\therefore$ e is identity element of H and

$e^{-1} = e \in H$.

$\therefore$ H itself is a group

$\therefore$ H is a subgroup of G

Remark. The subgroup G and $\{e\}$ are called **trivial** or **improper** subgroups of G. Any subgroup of group G other then G and $\{e\}$ is called **proper subgroup** of G.

Example 5. (*i*) Can an abelian group have non abelian subgroup ?

(*ii*) Can a non abelian group have an abelian subgroup ?

Sol. (*i*) No, Let G be an abelian group and H be its subgroup, then the operation on H is commutative. Since it is commutative in G and $H \subseteq G$. Hence an abelian group cannot have a non-abelian subgroup.

(*ii*) Yes. A non-abelian group can have an abelian subgroup.

For Example : The $\{1, -1, i, -i\}$ is a an abelian subgroup of the non-abelian group of quaternion $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ under the composition of multiplication.

Example 6. Let G be the group of all 2×2 non-singular matrices over the reals. Find the centre of G.

Sol. Here $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a,b,c,d \in \mathbf{R} \text{ s.t. } ad - bc \neq 0 \right\}$.

Now by definition of C (G),

$$C(G) = \{g \in G \mid gx = xg, \quad \forall x \in G\}.$$

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(G)$ be any element. Then it should commutate with all elements of G.

In particular it commutes with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in G$.

$$\Rightarrow \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow \begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$$

$$\Rightarrow \quad b = c, \quad a = d. \qquad ...(1)$$

$$\text{Also} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Rightarrow \begin{bmatrix} a+b & b \\ c+d & d \end{bmatrix} = \begin{bmatrix} a & b \\ a+c & b+d \end{bmatrix}$$

$$\Rightarrow \quad a + b = a, \qquad b = c = 0. \qquad \text{(using (1))}$$

Hence $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in C(G)$ is of the form $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$.

Hence $C(G) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \neq 0 \in \mathbf{R} \right\}$.

EXERCISE 1.5

1. Show that the set **Z** of all integers is a subgroup of the set of rational numbers under the operation of addition.
2. Verify the following statements for being true or false.
   (*a*) The multiplication group $\{1, -1\}$ is a sub group of the multiplicative group $\{1, -1, i, -i\}$
   (*b*) The additive group of even integers is a subgroup of the additive group of all integers.
   (*c*) The set of odd integers in not a subgroup of $< \mathbf{Z}, + >$.

3. If x is any element of group G, then show that $\{x^n \mid n \in Z\}$ is a subgroup of G.

4. Is Q_0, the set of non-zero rational numbers, a subgroup of

$G = \{a + \sqrt{2}\, b \mid a, b \in Q \text{ and } a^2 + b^2 \neq 0\}$ a group under multiplication ? Justify.

5. For positive integers m, n, show that $n\,Z$ is a subgroup of $m\,Z$ if $m \mid n$.

6. Show that SL(2, **R**) is a subgroup of the group GL(2, **R**) under the composition of multiplication of matrices.

7. Show that the set of cube roots of unity $H = \{1, w, w^2\}$ and the set of fourth roots of unity $K = \{1, -1, i, -i\}$ are subgroups of the group of twelfth roots of unity $G = \left\{\text{cis}\,\frac{2k\pi}{12} : k = 0, 1, 2, 3, \ldots, 11\right\}$ under multiplication of complex numbers.

8. Show that the sets $H = \{0, 3\}$ and $K = \{0, 2, 4\}$ are subgroups of the group $G = \{0, 1, 2, 3, 4, 5\}$ under the operation addition modulo 6.

1.7. COSETS

Definitions : Let H be a subgroup of a group G. If $a \in G$, then the set $Ha = \{h\,a : h \in H\}$ is called a **right coset of H in G** determined by a and the set $aH = \{a\,h : h \in H\}$ is called the **left coset of H in G** determined by a.

If the operation is addition, then the right coset becomes $H + a = \{h + a : h \in H\}$ and the left coset becomes $a + H = \{a + h : h \in H\}$.

Note : If e is the identity element of group G, then He and eH are right and left cosets of H in G.

Also $He = \{h\,e : h \in H\} = \{h : h \in H\} = H$.

$eH = \{e\,h : h \in H\} = \{h : h \in H\} = H$.

∴ If H is a subgroup of a group G, then H itself is a right coset as well as left coset of H in G determined by e.

Remark : When G is an abelian group then there is no distinction between a left coset and a right coset *i.e.* left coset = right coset *i.e.* $aH = Ha$.

Lagrange's Theorem : The order of each subgroup of a finite group is a divisor of the order of the group.

Proof : Let G be a group of finite order n.

Let H be a subgroup of G and let $O(H) = m$.

Suppose $h_1, h_2, \ldots h_m$ be m distinct members of H.

Let $a \in G$. Then Ha is a right coset of H in G and we have

$Ha = \{h_1 a, h_2 a, \ldots h_m a\}$

Ha has m distinct members, since $h_i a = h_j a$, $1 \leq i, j \leq m$; $i \neq j$

By right cancellation law $\Rightarrow h_i = h_j$, a contradiction.

Therefore each right coset of H in G has m distinct members.

Any two distinct right cosets of H in G are disjoint *i.e.*, they have no element in common. Since G is a finite group, the number of distinct right cosets of H in G will be finite, (say) equal to k.

The union of these k distinct right cosets of H in G is equal to G. Thus if

$H a_1, H a_2, \ldots H a_k$ are the k distinct right cosets of H in G, then $G = H a_1 \cup H a_2 \cup \ldots \cup H a_k$.

$\Rightarrow$ Number of elements in G = the number of elements in $H a_1$ + the number of elements in $H a_2 + \ldots +$ the number of elements in $H a_k$ [$\because$ two distinct right cosets are mutually disjoint]

$\Rightarrow O(G) = k m \quad \Rightarrow \quad n = k m$

$\Rightarrow k = \frac{n}{m} \Rightarrow m$ is a divisor of n

$\Rightarrow$ O(H) is a divisor of O(G).

Hence the proof of the theorem.

Note : In the proof, we should prove properties (above) III, IV and V.

Converse of Lagrange's Theorem. If G is a finite group and m divides O(G), then there exists a subgroup H of G such that $O(H) = m$.

The converse of Lagranges Theorem is not true.

Definition : The number of distinct left or right cosets of a subgroup H in group G is called the **index of H** in G and is denoted by i_G **(H)** or **[G : H]**.

Note. Here k is the index of H in G. We have $m = \frac{n}{k}$. Thus k a divisor of n. Therefore the index of every subgroup of a finite group is a divisor of the order of the group and $n = m k \Rightarrow O(G) = O(H)\,[G : H]$

Another Method of Theorem.

1.8. Normal Subgroups (or Invariant Subgroups or Self Conjugate subgroups)

In general, if H is a subgroup of a group G, then the left coset a H of H in G may not be equal to the corresponding right coset H a. In this section, our aim is to study a particular class of subgroups H for which each left coset of H in G is equal to the corresponding right coset of H in G. We call such subgroups as normal subgroups.

Definition : A subgroup H of a group G is called **a normal subgroup** of G if every left coset of H in G is equal to the corresponding right coset of H in G.

i.e. $a H = H a, \quad \forall a \in G.$

If the composition defined on G be addition, then H will be a **normal subgroup** of G iff.

$$a + H = H + a, \quad \forall a \in G.$$

Remark : (*i*) When G is an abelian group. Then every subgroup H of G is a normal subgroup, for $aH = H a$, $\forall a \in G$.

(*ii*) The subgroups $\{e\}$ and G of any group G are always normal subgroups of G. These are called trivial normal subgroups.

(*iii*) If H is a normal subgroup of G, then we write it as $H \Delta G$.

Theorem : A subgroup H of a group G is a normal subgroup of G iff $g h g^{-1} \in H$ for every $h \in H$, $g \in G$.

Proof : Firstly, let H be a normal subgroup of G.

$\therefore \quad gH = Hg, \ \forall g \in G$

Let $h \in H$ and $g \in G$ be any element. Then

$gh \in gH = Hg \Rightarrow gh \in Hg$

$\Rightarrow \quad gh = h_1 g$ for some $h_1 \in H$

$\Rightarrow \quad gh g^{-1} = h_1 \in H$

$\Rightarrow \quad gh g^{-1} \in H.$

Conversely. Let H be a subgroup of G such that

$gh g^{-1} \in H, \quad \forall \ h \in H, \ g \in G.$

We show that H is a normal subgroup *i.e.* $aH = Ha, \ \forall a \in G.$

Let $a \in G$ be any element. Then by given hypothesis

$ah a^{-1} \in H, \quad \forall \ h \in H.$

Let $ah \in aH$ be any element. Then $ah = (ah a^{-1}) a \in Ha$

$\Rightarrow \quad ah \in Ha$

$\therefore \quad aH \subseteq Ha.$ ...(1)

Again, Let $b = a^{-1}$ be any element of G.

Then by given hypothesis $bhb^{-1} \in H$.

But $bhb^{-1} = a^{-1} h (a^{-1})^{-1} = a^{-1} ha \in H.$

Let $ha \in Ha$ be any element. Then $ha = (aa^{-1}) ha = a(a^{-1} ha) \in aH$

$\Rightarrow \quad ha \in aH$

$\therefore \quad Ha \subseteq aH.$ ...(2)

From (1) and (2), we get

$aH = Ha, \quad \forall a \in G.$

Hence H is a normal subgroup of G.

Theorem : Let H be a subgroup of a group G. Then the following statements are equivalent

(*i*) $gh g^{-1} \in H, \quad \forall \ g \in G, h \in H$ (*ii*) $gHg^{-1} = H, \quad \forall \ g \in G.$

(*iii*) $gH = Hg \quad \forall \ g \in G.$

Proof. (*i*) $\Rightarrow$ (*ii*) Since $gh g^{-1} \in H, \quad \forall g \in G, h \in H.$

Let $gh g^{-1} = h_1$ for some $h_1 \in H$

$\Rightarrow \quad gHg^{-1} = H, \quad \forall g \in G.$

(*ii*) $\Rightarrow$ (*iii*) Let $gHg^{-1} = H, \quad \forall g \in G$

$\Rightarrow \quad (gHg^{-1}) g = Hg$

$\Rightarrow \quad g\,H\,(gg^{-1}) = H\,g$

$\Rightarrow \quad g\,H\,e = H\,g \qquad (\because H\,e = H)$

$\Rightarrow \quad g\,H = H\,g.$

(iii) $\Rightarrow$ *(i)* Let $\quad g\,H = H\,g, \quad \forall g \in G$

$\Rightarrow \quad g\,h = h_1\,g$ for some $h, h_1 \in H$

$\Rightarrow \quad g\,h\,g^{-1} = h_1 \in H$

$\Rightarrow \quad g\,h\,g^{-1} \in H, \quad \forall g \in G, h \in H.$

Hence *(i)* $\Rightarrow$ *(ii)* $\Rightarrow$ *(iii)* $\Rightarrow$ *(i)*.

Hence the given statements are equivalent.

Theorem : Let H am nd K be two subgroups of a group G. Then

(i) if H is a normal subgroup of G, then HK = KH is a subgroup of G.

(ii) if H and K both are normal subgroups, then HK = KH is a normal subgroup of G.

Proof. *(i)* Given H is a normal subgroup of G. To show that HK = KH is a subgroup of G.

Let $b \in K$ be any element. Then $H\,b = bH$ $\qquad [\because H \Delta G]$

$\Rightarrow \quad H\,b = bH \in KH, \quad \forall b \in K \qquad \ldots(1)$

$\Rightarrow \quad HK \subseteq KH.$

Similarly, $b\,H = H\,b \in HK \quad i.e., \quad bH \in HK, \quad \forall b \in K \qquad \ldots(2)$

$\Rightarrow \quad KH \subseteq HK.$

$\therefore$ from (1) and (2), we get $HK = KH$.

$\therefore$ By Theorem, HK (= KH) is a subgroup of G.

(ii) Let H and K be both normal subgroups of G.

$\therefore$ By *(i)* HK = KH is a subgroup of G. To show that H is a normal subgroup of G.

Let $g \in G$ be any element. Then

$g\,(HK)\,g^{-1} = g\,H\,(g^{-1}g)\,K\,g^{-1} = (g\,H\,g^{-1})\,(g\,K\,g^{-1}) \subseteq HK.$

$[\because$ H, K are normal subgroup $\therefore g\,H\,g^{-1} \subseteq H, g\,K\,g^{-1} \subseteq K]$

Hence HK is a normal subgroup of G.

ILLUSTRATIVE EXAMPLES

Example 1. Show that the set $H = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{R} \text{ s.t. } ad - bc = 1\right\}$ is a normal subgroup of the group $G = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{R} \text{ s.t. } ad - bc \neq 0\right\}$.

Sol. Since $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $|I| = 1 \Rightarrow I \in H$.

$\therefore$ H is a non-empty subset of G.

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \in H$ be any two elements,

where a_1, b_1, c_1, d_1 and $a_2, b_2, c_2, d_2 \in \mathbf{R}$ s.t. $|A| = a_1 d_1 - b_1 c_1 = 1$ and $|B| = a_2 d_2 - b_2 c_2 = 1$.

Now $|AB| = |A||B| = 1 \cdot 1 = 1 \Rightarrow AB \in H$.

Also $|A^{-1}| = \left|\frac{1}{|A|} \text{adj} A\right| = \frac{|\text{adj} A|}{|A|^2} = \frac{|A|}{|A|^2} = \frac{1}{|A|} = \frac{1}{1} = 1$.

[or $AA^{-1} = I \Rightarrow |AA^{-1}| = |I| \Rightarrow |A||A^{-1}| = 1$

$\Rightarrow 1|A^{-1}| = 1 \Rightarrow |A^{-1}| = 1$].

$\Rightarrow A^{-1} \in H$.

$\therefore$ H is a subgroup of G.

To show that H is a normal subgroup of G.

Let $A \in H$ and $B \in G$ be any elements, then $|A| = 1$.

Also $|B| \neq 0 \Rightarrow B^{-1}$ exists.

Now $|BAB^{-1}| = |B||A||B^{-1}| = |B| \cdot 1 \cdot \frac{1}{|B|} = 1$ $\left[\because |B^{-1}| = \frac{1}{|B|}\right]$

$\Rightarrow BAB^{-1} \in H, \forall A \in H$ and $B \in G$.

Hence H is a normal subgroup of G.

Example 2. The centre Z (G) of a group G is a normal subgroup of G.

Sol. We know $Z(G) = \{g \in G ; xg = gx \quad \forall x \in G\}$.

Clearly $Z(G) \subseteq G$.

Since $ex = xe, \quad \forall x \in G \Rightarrow e \in Z(G)$.

$\therefore$ Z (G) is a non-empty subset of G.

Let $a, b \in Z(G)$ be any two elements, then

$ax = xa, \quad \forall x \in G$ and $bx = xb, \quad \forall x \in G \Rightarrow xb^{-1} = b^{-1}x$.

Now $x(ab^{-1}) = (xa)b^{-1} = (ax)b^{-1} = a(xb)^{-1} = a(b^{-1}x) = (ab^{-1})x$

$\Rightarrow \quad x(ab^{-1}) = (ab^{-1})x \quad \forall x \in G$.

$\therefore \quad ab^{-1} \in Z(G) \quad \forall a, b \in Z(G)$.

So, Z (G) is a subgroup of G.

Now, we show that $Z(G)$ is a normal subgroup of G.

Let $h \in Z(G)$ and $g \in G$, then

$$g h g^{-1} = (gh) g^{-1} = (hg) g^{-1} = h(g g^{-1}) = he = h \in Z(G)$$

$\therefore$ $g h g^{-1} \in Z(G), \forall g \in G, h \in Z(G)$

Hence $Z(G)$ is a normal subgroup of G.

Example 3. If H is a subgroup of G of index 2 in G. Then H is normal subgroup of G.

Sol. Let H be a subgroup of G such that $[G : H] = 2$.

$\therefore$ The number of distinct left (or right) cosets of H in G is 2.

To show that H is a normal subgroup of G.

It is sufficient to prove that $xH = Hx, \quad \forall x \in G$.

Let $x \in G$ be arbitrary element of G.

Case I. When $x \in H$.

Since $x \in H$ So, $xH = H = Hx$

Hence $xH = Hx$.

Case II. When $x \notin H$.

$\therefore$ $xH \neq H$ and $Hx \neq H$.

Also $[G : H] = 2$.

$\therefore$ $H \cup xH = G = H \cup Hx$

$\Rightarrow$ $xH = Hx$.

Combining the two cases, we find that

$$xH = Hx \quad \forall x \in G.$$

$\therefore$ H is a normal subgroup of G.

Example 4. A subgroup H of a group G is a normal subgroup of G iff the product of two right cosets of H in G is again a right coset of H in G.

Or

Prove that a subgroup H of a group G is normal

iff $Ha\, Hb = H\, ab \; \forall\, a, b \in G$ (the composition is denoted multiplicatively).

Sol. Let H be a normal subgroup of G and

let Ha, Hb be two right cosets of H in G. Then

$$(Ha)(Hb) = H(a(Hb))$$
$$= H((aH)b)$$
$$= H(Ha)b, \text{ since H is a normal subgroup of G so } aH = Ha$$
$$= H(H(ab))$$
$$= (HH)ab$$
$$= Hab, \text{ since H is a subgroup of G so } HH = H$$

$\therefore \quad (H\,a)\,(H\,b) = H\,a\,b.$

$\because \quad a, b \in G \quad \Rightarrow \quad a\,b \in G$

$\therefore \quad H\,a\,b$ is a right coset of H in G.

Thus the product of two right cosets of H in G is again a right coset of H in G.

Conversely, suppose H is a subgroup of a group G such that the product of two right cosets of H in G is again a right coset of H in G.

To show that H is a normal subgroup of G.

Let $g \in G$ be any element.

$\therefore \quad g^{-1} \in G$, since G is a group.

$\therefore \quad H\,g, H\,g^{-1}$ be two right cosets of H in G.

$\therefore \quad (H\,g)\,(H\,g^{-1})$ is again a right coset of H in G.

Since H is a subgroup of G, therefore $e \in H$, where e is the identity element of G.

Since $e \in H$.

$\therefore \quad (e\,g)\,(e\,g^{-1}) \in (H\,g)\,(H\,g^{-1}).$

$\Rightarrow \quad g\,g^{-1} \in (H\,g)\,(H\,g^{-1})$

$\Rightarrow \quad e \in (H\,g)\,(H\,g^{-1}).$

Also H is a right coset of H in G and $e \in H$.

$\therefore \quad (H\,g)\,(H\,g^{-1})$ and H are two right cosets of H, each containing e.

$\therefore \quad (H\,g)\,(H\,g^{-1}) \cap H \neq \phi.$

Since the two right cosets of H in G are either disjoint or identical.

$\Rightarrow \quad (H\,g)\,(H\,g^{-1}) = H.$

Let $h \in H$ be any element.

$\therefore \quad (h\,g)\,(h\,g^{-1}) \in (H\,g)\,(H\,g^{-1})$

$\Rightarrow \quad (h\,g)\,(h\,g^{-1}) \in H$, since $(H\,g)\,(H\,g^{-1}) = H.$

$\Rightarrow \quad h\,(g\,h\,g^{-1}) \in H.$

$\Rightarrow \quad g\,h\,g^{-1} \in h^{-1}\,H.$

$\because \quad h \in H$ and H is a subgroup $\Rightarrow \quad h^{-1} \in H \quad \Rightarrow \quad h^{-1}\,H = H$

$\therefore \quad g\,h\,g^{-1} \in H.$

This is true $\forall\, g \in G$ and $h \in H$.

Hence H is a normal subgroup of G.

Example 5. Prove that the intersection of any collection of normal subgroups is itself a normal subgroup.

Sol. Let H_n be normal subgroups of group G for all $n \in N$

and consider $H = \bigcap_{n=1}^{\infty} H_n$

$\because$ H_n is normal subgroup of G for all $n \in N$

$\Rightarrow$ H_n is subgroup of G for all $n \in N$

$\Rightarrow$ $\bigcap_{n=1}^{\infty} H_n$ is a subgroup of G

$\Rightarrow$ H is a subgroup of G.

Further to show **H is normal in G**

Let $h \in \bigcap_{n=1}^{\infty} H_n$ be any element

$\Rightarrow$ $h \in$ each H_n for all $n \in N$

$\Rightarrow$ $g h g^{-1} \in H_n$ for all $g \in G$, $n \in N$

$\Rightarrow$ $g h g^{-1} \in \bigcap_{n=1}^{\infty} H_n = H$ ($\because$ H_n is normal subgroup for each $n \in N$)

$\because$ $h \in H \Rightarrow g h g^{-1} \in H$ for all $g \in G$

$\Rightarrow$ H is normal in G

Hence $H = \bigcap_{n=1}^{\infty} H_n$ is normal subgroup of G.

EXERCISE 1.6

1. Let G denotes the group of all non-singular upper triangular 2×2 matrices with real entries *i.e.*, the matrices of the form $\begin{bmatrix} a & b \\ o & d \end{bmatrix}$, where $a, b, d \in \mathbf{R}$ and $ac \neq 0$. Show that $H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbf{R} \right\}$ is a normal subgroup of G.
2. Let H be a subgroup of a group G. Let $g \in G$ be a fixed element of G. Then show that $g H g^{-1} = \{g h g^{-1} : h \in H\}$ is a subgroup of G and $W = \bigcap_{g \in G} g H g^{-1}$ is a normal subgroup of G.
3. Let H be a subgroup of a group G. If $x^2 \in H$, for all $x \in G$, then prove that H is a normal subgroup of G.
4. Prove that the intersection of two normal subgroups is a normal subgroup.
5. Let H and K be normal subgroups of a group G such that $H \cap K = \{e\}$. Prove that $h k = k h$, for all $h \in H$ and $k \in K$.
6. Give an example of a non-abelian group in which all the subgroups are normal.

7. If H is a normal subgroup of G and K is a subgroup of G such that $H \subseteq K \subseteq G$. Show that H is also a normal subgroup of K.

8. Give an example of two subgroups H, K which are not normal, but HK is a subgroup.

9. Show that a non empty subset H of a group G is normal subgroup of G iff $(g\,a)\ (g\,b)^{-1} \in H\ \forall\ b \in H, g \in G$.

10. Show that the set SL $(n, \mathbf{R})$ of all $n \times n$ matrices of determinant 1 over real numbers is a normal subgroup of GL $(n, \mathbf{R})$, the group of $n \times n$ invertible matrices over real numbers.

11. A cyclic subgroup T of a group G is normal in G. Prove that every subgroup of T is also normal in G.

12. Prove that a normal subgroup of G. commutes with every complex of G.

1.9. Quotient Groups

The idea of a normal subgroup is a very important concept in the group theory. Now we shall show that with the help of a normal subgroup of a group, we can construct a new group from the given group, known as **quotient group.**

Theorem : Let H be a normal subgroup of a group G. Then the set G/H of all the right cosets of H in G forms a group under the composition defined by $(H\,a)\,(H\,b) = H\,a\,b$.

Definition : Quotient group (or Factor group or Residue Class group).

If H is a normal subgroup of a group G, then the group G / H of all the right cosets of H in G under the composition $(H\,a)\,(H\,b) = H\,a\,b$ is called **a quotient group** or **a factor group.**

Note. If the composition in G/H is addition, then the composition in G/H is defined by

$$(H + a) + (H + b) = H + (a + b).$$

Remark : If H is a normal subgroup of a **finite** group G, then G / H form a group of order $\frac{O(G)}{O(H)}$.

Proof : By Theorem, G / H forms a group.

$$O(G / H) = \text{The number of distinct right cosets of H in G.}$$

$$= \frac{O(G)}{O(H)}.$$

Theorem : If H is a subgroup of an abelian group G, then the group G/H of all right cosets of H in G forms an abelian group under the composition defined by $H\,a \,.\, H\,b = H\,a\,b$.

Proof. If H is a subgroup of an abelian group G, then H is a normal subgroup of G.

$\therefore$ G/H forms a quotient group. (already done)

Let $H\,a, H\,b \in G/H$ so that $a, b \in G$.

$(H\,a)\,(H\,b) = H\,a\,b = H\ b\,a$, since G is abelian $\therefore\ ab = ba$

$= (H\,b)\,(H\,a)$.

Hence G / H is an abelian group.

Remark. The convese of the above result is not true that is, the quotient group may be abelian even if G may not be abelian.

For Example. Give an example of a non-abelian group G and a normal subgroup H of G such that quotient group G / H is abelian.

Sol. Ex. (*i*) Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the non-abelian group of unit Quaternion under multiplication defined by

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik.$$

Let $H = \{1, -1, i, -i\}$ be a subgroup of G.

Then $[G : H] = \dfrac{O(G)}{O(H)} = \dfrac{8}{4} = 2.$

$\therefore$ H is a normal subgroup of G.

$\therefore$ G/H is a group of all right (or left) cosets of H in G is of order 2, a prime. Hence G/H is an abelian group, but G is non-abelian.

Ex. (*ii*) Let $S_3 = \{i, (12), (13), (23), (123), (132)\}$ be the symmetric group on three numbers 1, 2 and 3 is a non-abelian group. Then

$H = \{i, (123), (132)\}$ be a normal subgroup of S_3 such that the quotient group $S_3 / H = \{H, (12)\ H\}$ is an abelian group. [$\because$ every group of order 2 is abelien]

Theorem : Let N be a normal subgroup of a group G. Show that G / N is abelian iff for all $x, y \in G, xyx^{-1}y^{-1} \in N$.

Proof. Firstly, let N be a normal subgroup of G such that G/N is abelian.

To show that $xyx^{-1}y^{-1} \in N, \quad \forall x, y \in G.$

Now, $Nxyx^{-1}y^{-1} = NxNyNx^{-1}Ny^{-1} = NxNy(Nx)^{-1}(Ny)^{-1}$ [Since G/N is abelian]

$= Nx(Nx)^{-1}Ny(Ny)^{-1}$

$= NN$

$= N$

Thus $Nxyx^{-1}y^{-1} = N \Rightarrow xyx^{-1}y^{-1} \in N, \quad \forall x, y \in G.$

Conversely. Let for all $x, y \in G$, $xyx^{-1}y^{-1} \in N$.

To show that G / N is abelian.

Since $xyx^{-1}y^{-1} \in N$

$\Rightarrow Nxyx^{-1}y^{-1} = N \Rightarrow NxNyNx^{-1}Ny^{-1} = N$

$\Rightarrow NxNy(Nx)^{-1}(Ny)^{-1} = N \Rightarrow NxNy(Nx)^{-1} = N(Ny) = Ny$

$\Rightarrow NxNy = NyNx, \quad \forall x, y \in G$

$\Rightarrow$ G / N is abelian.

Theorem : Every quotient group of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by a

$\therefore$ G is an abelian group

$\therefore$ Each subgroup of G is normal subgroup.

Let H be any subgroup of G.

$\therefore$ H is a normal subgroup of G. So G/H form a quotient group.

We prove that G / H is a cyclic group generated by H a.

Let $Hx \in G/H$ be arbitrary element, where $x \in G$.

$\therefore$ But $G = \langle a \rangle$

$\therefore$ $x = a^n$ for some integer n.

$\therefore$ $Hx = Ha^n = \underbrace{Ha.a..a}_{n \text{ times}}$

$= \underbrace{Ha.Ha....Ha}_{n \text{ times}}$

$= (Ha)^n$.

$\therefore$ $Hx = (Ha)^n$, $\forall$ $Hx \in G/H$.

$\therefore$ G / H is a cyclic group generated by H a.

So, each quotient group of a cyclic group is cyclic.

Remark. The converse of above result may not be true *i.e.* quotient group may be cyclic even if the group may not be cyclic.

Theorem : If G is a group such that G / Z(G) is cyclic, where Z(G) is the centre of G. Then G is abelian.

Proof. Let N = Z(G) and let $G/N = \langle gN \rangle$ be a cyclic group.

Let $a, b \in G$ be any two element.

$\Rightarrow$ $aN, bN \in G/N$.

$\therefore$ $aN = (gN)^m$ and $bN = (gN)^n$ for some $m, n \in I$

$\Rightarrow$ $aN = g^m N$ and $bN = g^n N \Rightarrow a^{-1} g^m \in N$ and $b^{-1} g^n \in N$

$\Rightarrow$ $g^{-m} a \in N$, $g^{-n} b \in N$. $(\because x \in N \Rightarrow x^{-1} \in N)$

Let $g^{-m} a = n_1$, $g^{-n} b = n_2$, for some $n_1, n_2 \in N$.

$\Rightarrow$ $a = g^m n_1$, and $b = g^n n_2$

$ab = g^m n_1 g^n n_2 = g^m (n_1 g^n) n_2 = g^m (g^n n_1) n_2$

$= g^m g^n n_1 n_2 = g^{m+n} n_1 n_2$.

Similarly, $ba = (g^n n_2)(g^m n_1) = g^n (n_2 g^m) n_1 = g^n (g^m n_2) n_1 = g^n g^m n_2 n_1$

$= g^{m+n} n_1 n_2$. $[\because n_1, n_2 \in N = Z(G) = n_1 n_2 = n_2 n_1]$

$\therefore$ $ab = ba$.

Hence G is abelian.

ILLUSTRATIVE EXAMPLES

Example 1. Let $\mathbf{Z}$ be the additive group of integers. Let $H = 3\mathbf{Z}$ be the additive group of integers multiple of 3, Prove that H is a normal subgroup of $\mathbf{Z}$. Also find the elements of $\mathbf{Z}/H$.

Sol. $H = 3\mathbf{Z}$ forms a subgroup of the additive group $\mathbf{Z}$ of all integers.

Let $g \in \mathbf{Z}$ and $h \in H$.

$\therefore$ $h = 3n$ for some $n \in \mathbf{Z}$.

Then $g + h + (-g) = g + (3n) + (-g) = 3n \in H$.

$\therefore$ H is a normal subgroup of $\mathbf{Z}$.

$\therefore$ $\mathbf{Z}/H$ forms a quotient group, where $\mathbf{Z}/H = \{H + a : a \in \mathbf{Z}\}$.

Let $a \in \mathbf{Z}$. By division algorithm, $\exists$ integers q and r such that

$a = 3q + r$, where $0 \le r \le 2$.

$\therefore$ $H + a = H + (3q + r) = (H + 3q) + r$.

$= H + r$, since $3q \in H$ and hence $H + 3q = H$.

$\therefore$ $H + a = H + r$ where $0 \le r \le 2$.

$\therefore$ $H + a$ is equal to one of $H + 0$, $H + 1$, $H + 2$.

$\therefore$ $\mathbf{Z}/H = \{H, H + 1, H + 2\}$.

Example 2. If H be a normal subgroup of a group G and $[G : H] = m$, then show that for any $x \in G$, $x^m \in H$.

Sol. Since H is a normal subgroup of group G such that $[G : H] = m$.

$\therefore$ $O(G/H) = m$.

$\therefore$ $\forall\ xH \in G/H$, where $x \in G$, we have

[$\because$ if $O(G) = n$ then $a^n = e, \forall\ a \in G$]

$(xH)^m = H$

$x^m H = H$

$\Rightarrow$ $x^m \in H$.

Thus $\forall x \in G$, we have $x^m \in H$.

Definition. A group G is called a **Simple Group** if it has no proper normal subgroups.

Example 3. Show that every cyclic group of prime order is a simple group.

Sol. Let $G = \langle a \rangle$ be a cyclic group of order p, where p is a prime number.

Since 1 and p are the only positive divisor of $O(G) = p$

$\therefore$ By Lagrange's theorem

G has no normal subgroup other than $\{e\}$ and G.

Hence G is a simple group.

Definition. Let H be a non-empty subset of a group G. Then the set $N(H) = \{a \in G : aH = Ha\}$, is called the **normalizer** of H in G.

Example 4. Let n be a positive integer and $N = n\mathbf{Z}$ be a subgroup of the additive group of integers $\mathbf{Z}$. Show that $O(\mathbf{Z}/N) = n$.

Sol. Let $\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and

$N = n\mathbf{Z} = \{\ldots -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$

$\therefore$ $\mathbf{Z}/N = \{N + a : a \in G\}$ be the quotient group under the composition defined by

$(N + a) + (N + b) = N + (a + b)$.

We show that $N, N + 1, N + 2, \ldots, N + (n - 1)$ are n district elements of $\mathbf{Z}/N$.

Let $a \in \mathbf{Z}$ be any element such that $a \neq 1, 2, 3, \ldots, (n - 1)$.

Then by Division Algorithm Theorem

$a = nq + r$, where $0 \leq r < n$.

Now $N + a = N + (nq + r) = (N + nq) + r = N + r$. [$\because nq \in N$ and $N + a = N$ for $a \in N$]

Therefore $O(\mathbf{Z}/N) = n$.

Example 5. If N is a normal subgroup of a finite group G such that $([G : N], O(N)) = 1$. Show that any element $x \in G$ satisfying $x^{O(N)} = e$ must be in N.

Sol. Let $O(N) = m$ and $[G : N] = l$. Then $(l, m) = 1$.

$\therefore$ $\exists\, a, b \in I$ s.t. $am + bl = 1$.

Since N is a normal subgroup of G.

$\therefore$ G/N is a group of order l.

$\Rightarrow$ $(Nx)^l = N$, for any $Nx \in G/N$.

Also $(Nx) = (Nx)^1 = (Nx)^{am+bl} = (Nx)^{am}(Nx)^{bl}$

$= \{(Nx)^m\}^a \{(Nx)^l\}^b = N^a N^b = N^{a+b} = N$.

$\therefore$ $Nx = N \Rightarrow x \in N$.

Example 6. Let $(\mathbb{Z}, +)$ be the group of integers and $H = \{4n \mid n \in \mathbb{Z}\}$. Then find the members of $\mathbb{Z}/H$.

Sol. Let $(\mathbb{Z}, +) = \{\ldots -2, -1, 0, 1, 2, \ldots\}$ be group of integers under addition

and $H = \{4n \mid n \in \mathbb{Z}\} = \{\ldots -8, -4, 0, 4, 8, \ldots\}$

For cosets of H in $\mathbb{Z}$

For $0 \in \mathbb{Z}$, $0 + H = \{\ldots -8, -4, 0, 4, 8, \ldots\}$

For $1 \in \mathbb{Z}$, $1 + H = \{\ldots -7, -3, 1, 5, 9, \ldots\}$

For $-1 \in \mathbb{Z}$, $-1 + H = \{\ldots -9, -5, -1, 3, 7, \ldots\}$

For $2 \in \mathbb{Z}$, $2 + H = \{\ldots -6, -2, 2, 6, 10, \ldots\}$

For $-2 \in \mathbb{Z}, -2 + H = \{\ldots -10, -6, -2, 2, 6, \ldots\} = 2 + H$

For $3 \in \mathbb{Z}, 3 + H = \{\ldots -5, -1, 3, 7, 11, \ldots\} = -1 + H$

For $-3 \in \mathbb{Z}, -3 + H = \{\ldots -11, -7, -3, 1, 5, \ldots\} = 1 + H$

$\therefore$ cosets of $\mathbb{Z}/H$ are $0 + H, 1 + H, 2 + H, 3 + H$.

Example 7. Give an example of a non-abelian group G and *a* normal subgroup H of G such that quotient group G/H is abelian.

Or

Show that if the quotient group G/H is abelian, then G may not be abelian.

(Jammu University 2013, 2014)

Sol. (*i*) Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the set of unit quaternion under multiplication defined by

$$i^2 = j^2 = k^2 = -1, \quad ij = k = -ji, \quad jk = i = -kj, \quad ki = j = -ik$$

form a non-abelian group. Then $H = \{1, -1, i, -i\}$ is a subgroup of G.

Also $[G : H] = \dfrac{O(G)}{O(H)} = \dfrac{8}{4} = 2$

$\therefore$ H is a normal subgroup of G.

$\therefore$ G/H is a group of all right (or left) cosets of H in G is of order 2, a prime. Hence G/H is abelian group. But G is non-abelian.

(*ii*) Let $G = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, c, d \in \mathbf{R} \text{ and } ad \neq 0\right\}$. Then G forms a group under matrix multiplication. Its identity elements is unit matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

if $A = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in G$, then $A^{-1} = \begin{bmatrix} \dfrac{1}{a} & \dfrac{-b}{ad} \\ 0 & \dfrac{1}{d} \end{bmatrix}$

$\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}$ and $\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \in G$

$$\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} = \begin{bmatrix} 2 & 13 \\ 0 & 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 11 \\ 0 & 12 \end{bmatrix}$$

$$\therefore \quad \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix} \neq \begin{bmatrix} 2 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix}$$

$\therefore$ G is not an abelian group

Let $H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in R \right\}$. Then $H \subseteq G$.

Let A, B, $\in H$

$\therefore \quad A = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix}, b, c \in \mathbf{R}.$

$$AB = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & c+b \\ 0 & 1 \end{bmatrix} \in H.$$

$$A^{-1} = \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix} \in H \quad \forall \ A \in H.$$

$\therefore$ H is a subgroup of G. We now prove that H is normal subgroup of G.

Let $X \in G$ and $A \in H$.

$\therefore \quad X = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ for some $a, b, d \in \mathbf{R}$ such that $a\,d \neq 0$

$$A = \begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix} \text{ for some } e \in \mathbf{R}$$

Then $X^{-1} = \begin{bmatrix} \frac{1}{a} & \frac{-b}{a\,d} \\ 0 & \frac{1}{d} \end{bmatrix}$

$$XAX^{-1} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & e \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & aed+bd\frac{-b}{d} \\ 0 & 1 \end{bmatrix}$$

$\therefore$ H is normal subgroup of G.

$\therefore$ G / H forms a quotient group.

Let $Hx, Hy \in G/H$ so that $x, y \in G$.

G / H will be abelian if $(Hx)(Hy) = (Hy)(Hx)$.

i.e., if $\quad Hxy = Hyx$.

i.e., if $\quad (xy)(yx)^{-1} \in H$

i.e., if $\quad (xy)(x^{-1}y^{-1}) \in H$

$\because \quad x, y \in G$

$\therefore \quad x = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ for some $a, b, d \in \mathbf{R}$ *s.t.* $b\,d \neq 0$ and $y = \begin{bmatrix} c & e \\ 0 & f \end{bmatrix}$ for some $c, e, f \in \mathbf{R}$ *s.t.c.f.* $\neq 0$

Then $x^{-1} = \begin{bmatrix} \frac{1}{a} & \frac{-b}{ad} \\ 0 & \frac{1}{d} \end{bmatrix}, y^{-1} = \begin{bmatrix} \frac{1}{c} & \frac{-e}{cf} \\ 0 & \frac{1}{f} \end{bmatrix}$

Then $(xy)(x^{-1}y^{-1})$

$$= \begin{bmatrix} ac & ae+bf \\ 0 & df \end{bmatrix} \begin{bmatrix} \frac{1}{ac} & \frac{-e}{acf} - \frac{b}{adf} \\ 0 & \frac{1}{fd} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & -\frac{nce}{acf} - \frac{acb}{adb} + \frac{bf}{fd} \\ 0 & 1 \end{bmatrix} \in H$$

$\therefore \quad (xy)(x^{-1}y^{-1}) \in H$

$\therefore$ G / H is abelian whereas G is non-abelian.

EXERCISE 1.7

1. Using Lagrange's theorem prove that if G is a finite group and N a normal subgroup of G, them for any $x \in G$, O (x) in G is divisible by O $(\bar{x})$ in G / N where $\bar{x} = Nx$.
2. Give the example of a group G and a normal subgroup H such that G/H is cyclic but G may not be cyclic.
3. If H is a subgroup of a group G, N(H) be the normalizer of H in G. then
   (*i*) N (H) is a subgroup of G.
   (*ii*) H is a normal subgroup of N(H).
   (*iii*) If H and K are subgroups of G and H is a normal subgroup of K, then $K \subseteq N(H)$ *i.e.*, N (H) is the largest subgroup of G in which H is normal.
   (*iv*) H is a normal subgroup of G iff $N(H) = G$.
4. If H, K are normal subgroups of a group G and $H \subset K$, then show that K / H is a normal subgroup of G / H.
5. Let N_1 and N_2 be two normal subgroups of a group G. Prove that $G/N_1 = G/N_2$ if and only if $N_1 = N_2$.

2

ALGEBRAIC STRUCTURES WITH TWO BINARY OPERATIONS, RINGS, INTEGRAL DOMAIN AND FIELDS

2.0 INTRODUCTION

Till now we have studied algebraic systems with one binary operation namely, group, semi group and monoid. But there are systems (sets) with more than one binary operations defined on them namely the set of integers, the set of rational numbers etc. with two binary operations addition and multiplication. Though these sets form groups under addition and not under multiplication, yet they do have certain specific properties satisfied w.r.t multiplication as well. These properties lead to the concept of a ring which we define as follow :–

2.1. RINGS

2.1.1. Definition. Ring :

A non-empty set R together with two binary operations denoted additively (+) and multiplicatively (·), is called a **ring** if for all $a, b, c \in R$, the following axioms are satisfied.

(i) $a + b \in R$ [closed under addition]

(ii) $(a + b) + c = a + (b + c)$ [addition is associative]

(iii) $\exists$ an element $0 \in R$ such that $0 + a = a = a + 0$ [existence of additive identity]

(iv) For every $a \in R$, $\exists$ an element $-a \in R$ such that $(-a) + a = 0 = a + (-a)$ [existence of additive inverse]

(v) $a + b = b + a$ [addition is commutative]

(vi) $a \,.\, b \in R$ [closed under multiplication]

(vii) $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ [multiplication is associative]

(viii) $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ and $(a + b) \,.\, c = a \,.\, c + b \,.\, c$ [distributive laws hold]

A ring R under the binary operations (+) and (·) is denoted by the algebraic system $\langle R, +, \cdot \rangle$

Remark : The algebraic system $\langle R, +, \cdot \rangle$ is called a ring if R forms an abelian group under addition and semi-group under multiplication along with distributive property.

2.1.2. Definition. Commutative ring. A ring $\langle R, +, \cdot \rangle$ in which

$a\,b = b\,a$ for all $a, b \in R$

holds, is called a **commutative ring.**

Otherwise R is called a **non-commutative ring.**

2.1.3. Definition. Ring with unity. A ring $<R, +, \cdot>$ is said to be a ring with unity if there exists an element $1 \in R$ s.t. $a \cdot 1 = a = 1 \cdot a$ for all $a \in R$.

Then 1 is called the **unity of the ring** R.

Otherwise R is called a **ring without unity.**

Remark : The unity of a ring is also called the **identity element of the ring.**

ILLUSTRATIVE EXAMPLES

Example 1. Prove that the set I of all integers is a ring with respect to usual addition and multiplication of integers.

Sol. (A) Properties of Addition

(*i*) $\forall\ a, b \in I \Rightarrow a + b \in I$ [$\because$ sum of two integers is an integer]

(*ii*) $\forall\ a, b, c \in I \Rightarrow (a + b) + c = a + (b + c)$ [$\because$ Associative Property holds in integers]

(*iii*) $\forall\ a \in I$, there exists $0 \in I$ such that $a + 0 = 0 + a = a$.

Here '0' is called additive identity.

(*iv*) $\forall\ a \in I$, there exists $-a \in I$ such that $a + (-a) = 0 = (-a) + a$

Here $-a$ is additive inverse of a.

(*v*) $\forall\ a, b \in I \Rightarrow a + b = b + a$ [$\because$ Commutative property holds in integers]

(B) Properties of Multiplication

(*i*) $\forall\ a, b \in I \Rightarrow a \cdot b \in I$ [$\because$ product of two integers is an integer]

(*ii*) $\forall\ a, b, c \in I \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$

[Associative property holds for integers with respect to multiplication]

(C) Distributive Laws

We know that $\forall\ a, b, c \in I$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

$\therefore$ $<I, +, \cdot>$ is a ring.

Since there exists an integer $1 \in I$ such that

$$a \cdot 1 = 1 \cdot a = a \ \forall\ a \in I$$

Thus I is a ring with unity.

Also we know $\forall\ a, b \in I \Rightarrow a \cdot b = b \cdot a$

$\therefore$ I is also a commutative ring.

Hence $<I, +, \cdot>$ is a commutative ring with unity.

RING OF GAUSSIAN INTEGERS

Example 2. A Gaussian integer is a complex number $a + i\,b$ where a and b are integers. Show that the s J $[i]$ of all Gaussian integers is a ring with usual addition and multiplication of complex numbers.

Sol. Given $J[i] = \{a + i\,b \mid a, b \in \text{integers}\}$

Since each element of $J[i]$ is a complex number, so properties of complex numbers are also true f the elements of $J[i]$

(A) Properties of Addition

(i) $\forall\ a + i\,b,\ c + i\,d \in J[i]$, where a, b, c, d are integers

$(a + i\,b) + (c + i\,d) = (a + c) + i\,(b + d)$

$\in J[i]$ $[\because\ a, b, c, d \in I \Rightarrow\ a + c, b + d \in$

$\therefore$ $J[i]$ is closed under addition.

(ii) $\forall\ a + i\,b, c + i\,d, e + i\,f \in J[i]$, where a, b, c, d, e, f are integers

$[(a + i\,b) + (c + i\,d)] + (e + i\,f)$

$= [(a + c) + i\,(b + d)] + (e + i\,f) = [(a + c) + e] + i\,[(b + d) + f]$

$= [a + (c + e)] + i\,[b + (d + f)]$ [$\because$ Associative Property for integers hol

$= (a + i\,b) + [(c + e) + i\,(d + f)] = (a + i\,b) + [(c + i\,d) + (e + i\,f)]$

$\therefore$ addition is associative in $J[i]$.

(iii) $\forall\ a + i\,b \in J[i]$, there exists $0 + i\,0 \in J[i]$

such that $(a + i\,b) + (0 + i\,0) = (a + 0) + i\,(b + 0) = a + i\,b$

and $(0 + i\,0) + (a + i\,b) = (0 + a) + i\,(0 + b)$

$= a + i\,b$

$\therefore$ $(a + i\,b) + (0 + i\,0) = a + i\,b = (0 + i\,0) + (a + i\,b)$

Thus $0 + i\,0$ is additive identity.

(iv) $\forall\ a + i\,b \in J[i]$, there exists $-a - i\,b \in J[i]$ $(\because\ a, b \in I \Rightarrow\ -a, -b, \in$

such that $(a + i\,b) + (-a - i\,b) = [a + (-a)] + [b + (-b)]\,i = 0 + 0\,i$

and $[-a + (-b)\,i] + [a + i\,b] = [(-a) + a] + i\,[(-b) + b] = 0 + i\,0$

$\therefore (a + i\,b) + [(-a) + (-b)\,i] = 0 + i\,0 = [(-a) + (-b)\,i] + [a + i\,b]$

Thus $(-a) + (-b)\,i$ is the additive inverse of $a + i\,b$.

(B) Properties of Multiplication :

(i) $\forall\ a + i\,b, c + i\,d \in J[i]$

$(a + i\,b)(c + i\,d) = (a\,c + i^2\,b\,d) + i\,(a\,d + b\,c) = (a\,c - b\,d) + i\,(a\,d + b\,c)$

$\in J[i]$ [$\because\ a, b, c, d \in I \Rightarrow\ a\,c - b\,d, a\,d + b\,c \in$

$\therefore$ $J[i]$ is closed under multiplication.

(ii) $\forall\ a+ib, c+id, e+if \in J[i]$

$[(a+ib)(c+id)](e+if) = (a+ib)[(c+id)(e+if)]$ [Verify it]

(C) Distributive Law.

Let $a+ib, c+id, e+if \in J[i]$

Then $(a+ib).[(c+id)+(e+if)] = (a+ib).[(c+e)+i(d+f)]$

$= [a.(c+e) - b(d+f)] + i[b(c+e) + a(d+f)]$

$= [ac + ae - bd - bf] + i[bc + be + ad + af]$

$= [(ac - bd) + (ae - bf)] + i[(ad + bc) + (af + be)]$

And $(a+ib).(c+id) + (a+ib)(e+if)$

$= [(ac - bd) + i(ad + bc)] + [(ae - bf) + i(af + be)]$

$= [(ac - bd) + (ae - bf)] + i[(ad + bc) + (af + be)]$

$\therefore$ Left Distributive Law holds

Similarly Right Distributive Law holds.

Hence J[i] is a ring.

RING OF MATRICES

Example 3. Prove that the set M of all $n \times n$ matrices over reals is a non-commutative ring with unity, with zero divisors under addition and multiplication of matrices.

Sol. Let A, B, C be any members of M.

$\therefore$ A, B, C are $n \times n$ matrices over reals.

$\Rightarrow A = [a_{ij}]_{n\times n}, B = [b_{ij}]_{n\times n}, C = [c_{ij}]_{n\times n}$

where $a_{ij}, b_{ij}, c_{ij} \in \mathbf{R}$ for $1 \le i \le n,\ 1 \le j \le n$.

(A) Properties of addition

(i) $\forall$ A, B $\in$ M, we have

$A + B = [a_{ij}]_{n\times n} + [b_{ij}]_{n\times n}$

$= [a_{ij} + b_{ij}]_{n\times n}$ [$\because a_{ij}, b_{ij}$ are reals $\Rightarrow$ $a_{ij} + b_{ij}$ is also real]

$\in$ M

$\therefore$ addition is closed.

(ii) $\forall$ A, B, C $\in$ M we have

$A + (B + C) = [a_{ij}] + ([b_{ij}] + [c_{ij}]) = [a_{ij}]_{n\times n} + [b_{ij} + c_{ij}]_{n\times n}$

$= [a_{ij} + (b_{ij} + c_{ij})]_{n\times n} = [(a_{ij} + b_{ij}) + (c_{ij})]_{n\times n}$

[$\because$ Associative Property holds in reals]

$= [a_{ij} + b_{ij}]_{n\times n} + [c_{ij}]_{n\times n}$

$= (A + B) + C.$

(*iii*) For $A \in M$, there exists $O = [0]_{n\times n} \in M$ such that

$$A + O = [a_{ij}] + [0]$$
$$= [a_{ij} + 0]$$
$$= [a_{ij}] = A.$$

Similarly $O + A = A$.

$\Rightarrow$ $A + O = A = O + A$

$\therefore$ O is the additive identity.

(*iv*) Since $A = [a_{ij}]_{n\times n}$

$\Rightarrow$ $-A = [-a_{ij}]_{n\times n}$ [$\because$ $a_{ij} \in R \Rightarrow -a_{ij} \in R$]

$\therefore$ $A + (-A) = [a_{ij}] + [-a_{ij}] = [a_{ij} + (-a_{ij})]$

$= [0]_{n\times n} = O$

and $(-A) + A = [-a_{ij}] + [a_{ij}] = [(-a_{ij}) + a_{ij}] = [0]_{n\times n} = O$

so that $A + (-A) = O = (-A) + A$.

$\therefore$ the additive $-A$ of $A \in M$ exits.

(*v*) For $A, B \in M$,

$$A + B = [a_{ij}]_{n\times n} + [b_{ij}]_{n\times n}$$
$$= [a_{ij} + b_{ij}]_{n\times n} = [b_{ij} + a_{ij}]_{n\times n}$$

[$\because$ $a_{ij} + b_{ij} = b_{ij} + a_{ij}$ as a_{ij} and b_{ij} are reals]

$$= [b_{ij}] + [a_{ij}] = B + A$$

$\therefore$ commutative Law for addition holds.

(B) Properties of Multiplication

(*i*) Let $A = [a_{ij}]_{n\times n}$ and $B = [b_{jk}]_{n\times n} \in M$

Then $AB = [c_{ik}]_{n\times n}$ where $c_{ik} = \sum_{j=1}^{n} a_{ij}\, b_{jk} \in R$

$\therefore$ $AB \in M$

$\therefore$ M is closed under multiplication.

(*ii*) Let $A = [a_{ij}]_{n\times n}$, $B = [b_{jk}]_{n\times n}$ and $C = [c_{kp}]_{n\times n}$ be three element of M.

Let $AB = [d_{ik}]_{n\times n}$ where $d_{ik} = \sum_{j=1}^{n} a_{ij}\, b_{jk}$

and $BC = [e_{jp}]_{n\times n}$ where $e_{jp} = \sum_{k=1}^{n} b_{jk}\, c_{kp}$

Now (i, p)th element of (AB) C = (ith row of AB) (pth column of C)

$$= \sum_{k=1}^{n} d_{ik}\, c_{kp} = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} a_{ij}\, b_{jk} \right) c_{kp} = \sum_{k=1}^{n} \sum_{j=1}^{n} a_{ij}\, b_{jk}\, c_{kp}$$

and (i, p)th element of A (BC) = (ith row of A) (pth column of BC)

$$= \sum_{j=1}^{n} a_{ij}\, e_{jp} = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} b_{jk}\, c_{kp} \right)$$

$$= \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij}\, b_{jk}\, c_{kp} = \sum_{k=1}^{n} \sum_{j=1}^{n} a_{ij}\, b_{jk}\, c_{kp}$$

$\therefore$ A (BC) = (AB) C.

Thus matrix multiplication is associative.

(C) Distributive Laws.

Let $A = [a_{ij}]_{n \times n}$, $B = [b_{jk}]_{n \times n}$ and $C = [c_{jk}]_{n \times n}$ be three element of M.

Then $B + C = [b_{jk} + c_{jk}]_{n \times n}$

$\therefore$ (i, k) element of A (B + C) $= \sum_{k=1}^{n} a_{ij} (b_{jk} + c_{jk}) = \sum_{k=1}^{n} (a_{ij}\, b_{jk} + a_{ij}\, c_{jk})$

$$= \sum_{k=1}^{n} a_{ij}\, b_{jk} + \sum_{k=1}^{n} a_{ij}\, c_{jk}$$

= (i, k)th element of AB + (i, k)th element of AC

= (i, k)th element of (AB + AC)

Also A (B + C) and AB + AC are of type $n \times n$.

$\therefore$ M is a ring.

(a) Since the matrix multiplication is not commutative, in general, so M is non-commutative ring.

(b) Also, we know, there is identity matrix $I_{n \times n} \in M$ such that $AI = IA = A \ \forall \ A \in M$.

$\therefore$ I is the multiplicative identity.

(c) Also, we know there exists matrices $A \neq O, B \neq O$ but $AB = O$

For example, $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix} \neq O$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 3 \end{bmatrix} \neq O \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$.

Hence M is non-commutative ring, with unity and with zero divisors.

Example 4. Prove that the set $R = \{(a, b) \mid a, b \in \mathbf{R}\}$ is a commutative ring under the addition and multiplication of ordered pairs defined as

$(a, b) + (c, d) = (a + c, b + d)$

$(a, b)\,(c, d) = (a\,c, b\,d) \ \forall \ (a, b), (c, d) \in R$

Sol. Given $R = \{(a, b) \mid a, b \in \mathbf{R}\}$

(A) Properties of Addition.

(*i*) Let $x, y \in \mathbf{R}$ Then $x = (a, b)$ and $y = (c, d)$

where a, b, c, d are reals.

$\therefore \quad x + y = (a, b) + (c, d) = (a + c, b + d)$

$\in \mathbf{R}$ [$\because a, b, c, d \in \mathbf{R} \Rightarrow a + c, b + d \in \mathbf{R}$]

$\therefore$ R is closed under addition.

(*ii*) Let $x, y, z \in \mathbf{R}$, then $x = (a, b)$, $y = (c, d)$ and $z = (e, f)$

where a, b, c, d, e, f are reals.

Then $(x + y) + z = [(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f) = [(a + c) + e, (b + d) + f]$

and $x + (y + z) = (a, b) + [(c, d) + (e, f)] = (a, b) + (c + e, d + f) = [a + (c + e), b + (d + f)]$

$= [(a + c) + e, (b + d) + f]$

[$\because a, b, c, d, e, f$ are reals and Associative Property holds for reals]

$\therefore \quad (x + y) + z = x + (y + z) \quad \forall\ x, y, z \in \mathbf{R}$.

(*iii*) For each $x = (a, b) \in \mathbf{R}$, there is $O = (0, 0) \in R$ such that

$x + O = (a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = x$

similarly $0 + x = x$

$\therefore \quad x + 0 = x = 0 + x$.

so that (0, 0)is the additive identity.

(*iv*) For each $x = (a, b) \in \mathbf{R}$ there is $y = (-a, -b) \in \mathbf{R}$ such that

$x + y = (a, b) + (-a, -b)$ ($\because a, b \in \mathbf{R} \Rightarrow -a, -b$ are reals)

$= [(a + (-a)),\ b + (-b)] = [0, 0] = O$

similarly $y + x = 0$

$\therefore \quad x + y = 0 = y + x$

$\therefore \quad y = (-a, -b) \in R$ is the additive inverse of $x \in \mathbf{R}$.

(*v*) $\forall\ x, y \in \mathbf{R}$, where $x = (a, b)$ and $y = (c, d)$

$x + y = (a, b) + (c, d) = (a + c, b + d) = (c + a, d + b)$

[$\because$ For a, b, c, d reals commutative law holds]

$= (c, d) + (a, b) = y + x$

$\therefore \quad x + y = y + x \quad \forall\ x, y \in \mathbf{R}$.

(B) Properties of multiplication

(*i*) Let $x, y \in \mathbf{R}$. Then $x = (a, b)$ and $y = (c, d) \in \mathbf{R}$

$\therefore \quad xy = (a, b)(c, d) = (ac, bd)$

$\in \mathbf{R}$

[$\because a, b, c, d \in \mathbf{R} \Rightarrow ac, bd$ are reals]

$\therefore$ R is closed under multiplication.

(ii) Let $x, y, z \in \mathbf{R}$. Then $x = (a, b)$, $y = (c, d)$, $z = (e, f)$

where a, b, c, d, e, f are reals

$\therefore \quad (x\,y)\,z = [(a, b)\,(c, d)]\,(e, f)$

$= (a\,c, b\,d)\,(e, f) = ((a\,c)\,e, (b\,d)\,f) = (a\,(c\,e), b\,(d\,f))$

$\in \mathbf{R}$ [$\because$ $(a\,c)\,e = a\,(c\,e)$, $(b\,d)\,f = b\,(d\,f)$ as Associative Property in reals under multiplication holds]

And $x\,(y\,z) = (a, b)\,[(c, d)\,(e, f)]$

$= (a, b)\,[(c\,e, d\,f)] = (a\,(c\,e), b\,(d\,f))$

Hence $(x\,y)\,z = x\,(y\,z) \quad \forall\ x, y, z \in \mathbf{R}$.

(C) Distributive Laws

Let $x, y, z \in \mathbf{R}$. Then $x = (a, b)$, $y = (c, d)$ and $z = (e, f)$

where a, b, c, d, e, f are reals.

$\therefore \quad x\,.\,(y + z) = (a, b)\,[(c, d) + (e, f)] = (a, b)\,(c + e, d + f)$

$= [a\,(c + e), b\,(d + f)] = (a\,c + a\,e, b\,d + b\,f)$

and $x\,.\,y + x\,.\,z = (a, b)\,(c, d) + (a, b)\,(e, f)$

$= (a\,c, b\,d) + (a\,e, b\,f) = (a\,c + a\,e, b\,d + b\,f)$

$\therefore \quad x\,.\,(y + z) = x\,.\,y + x\,.\,z \quad \forall\ x, y, z \in \mathbf{R}$

Similarly $(y + z)\,.\,x = y\,.\,x + z\,.\,x \quad \forall\ x, y, z \in \mathbf{R}$

Hence R is a ring with respect to given operations.

Also $\forall\ x, y \in \mathbf{R}$, $x = (a, b)$ and $y = (c, d) \in \mathbf{R}$

$x\,y = (a, b)\,(c, d) = (a\,c, b\,d)$

$= (c\,a, d\,b)$ [$\because$ $a\,c = c\,a$ and $b\,d = d\,b$]

$= (c, d)\,(a, b) = y\,x$

$\therefore$ **R is a commutative ring under given operations.**

Example 5. **RING OF INTEGERS MODULO *n***

Show the set Z_n or $J_n = \{0, 1, 2, \ldots\ldots, n-1\}$ form a finite commutative ring with unity 1, under addition modulo and multiplication modulo n. (n is prime > 1).

Sol. Given Z_n or $J_n = \{0, 1, 2, 3, \ldots, n-1\}$, $n > 1$, $n \in Z$.

The composition defined is addition modulo n.

$\therefore \quad \forall\ a, b \in J_n$, $a * b$ or $a +_n b$ = least non negative remainder r when $a + b$ is divided by n

i.e. $a * b$ or $a +_n b = r \Rightarrow a + b - r$ is divisible by n.

i.e. $a + b \equiv r \pmod{n}$.

Closure property : $\forall\ a, b \in J_n\ \ 0 \le a, b < n$

$$a + b \equiv r \pmod{n}, \text{ where } 0 \le r < n.$$

Now $r \in J_n$.

$\therefore$ the closure property is satisfied.

Associativity : $\forall\ a, b, c \in J_n$

The least non-negative remainder remains the same if

$(a + b) + c$ or $a + (b + c)$ are divided by n.

$\therefore \quad (a * b) * c = a * (b * c)$

Thus associative property holds in J_n.

Commutativity : $\forall\ a, b \in J_n$

The least non-negative remainder remains the same if $a + b$ or $b + a$ is divided by n.

i.e. $\quad a + b \equiv r \pmod{n}$ and $b + a \equiv r \pmod{n}$

$\therefore \quad a * b = b * a.$

Thus commutative property holds in J_n.

Existence of identity : $\forall\ a \in J_n\ \ 0 \le a < n.$

Here a is the least non-negative remainder when $a + 0$ or $0 + a$ are divided by n

$\therefore \quad a * 0 = a = 0 * a$

Thus $0 \in J_n$ is the identity element.

Existence of inverse : Inverse of $0 \in J_n$ is 0 itself.

Also for all $a \in J_n,\ a \neq 0,\ n - a \in J_n$ such that

$$a + (n - a) \equiv 0 \pmod{n}$$

and $\quad (n - a) + a \equiv 0 \pmod{n}$

i.e. $\quad a * (n - a) = 0 = (n - a) * a$

Thus $n - a$ is the inverse of a.

Hence $< J_n, * >$ is an abelian group of order n.

Closure property under multiplication : The composition multiplication is defined as :

$\forall\ a, b \in J_n$, $a * b$ or $a\ X_n\ b$ = least non negative remainder r when $a\,b$ is divided by n is devise by n

i.e. $a * b$ or $a\ X_n\ b = r \Rightarrow a\,b - r$ or $a\,b \equiv r \pmod{n}$

For all $a, b \in J_n\ \ 1 \le a, b < n$

$$a\,b \equiv r \pmod{n} \text{ where } 0 \le r < n$$

If possible, let $r = 0$ then $a\,b \equiv 0 \pmod{n}$

$\Rightarrow \quad n \mid a\,b - 0 \Rightarrow n \mid a\,b \mid$

But n is prime so either $n \mid a$ or $n \mid b$ where $1 \le a, b < n$

$\therefore \quad r \neq 0$ *i.e.* $r \in J_n \Rightarrow J_n$ is closed under

Commutativity : $\forall\ a, b \in J_n$, the least non-negative remainder remains the same if $a\,b$ or $b\,a$ is divided by n *i.e.* $a\,b \equiv r \pmod n$ and $b\,a \equiv r \pmod n$

$\therefore\ a * b = b * a$

$\Rightarrow$ commutative property holds in J_n or Z_n.

Associative : $\forall\ a, b, c \in J_n$

The least non-negative remainder remains the same if $(a\,b)\,c$ or $a\,(b\,c)$ is divided by n.

$\therefore\ (a * b) * c = a * (b * c)$

Thus associativity holds in J_n

Existence of identity $\forall\ a \in J_n$

$a * 1 = a = 1 * a$ as $a \cdot 1$ and $1 \cdot a$ leave the remainder a when divided by n

$\therefore\ 1 \in J_n$ works as an identity element for J_n

Distributive : $\forall\ a, b, c \in J_n$

$a \times_n (b +_n c) = a \times_n (b + c)$ $\quad (\because\ b +_n c \equiv b + c \pmod n)$

$= $ least non-negative remainder when $a\,(b + c) = a\,b + a\,c$ is divided by n

$= a\,b +_n a\,c$

$= (a \times_n b) +_n (a \times_n c)$ $\quad (\because\ a\,b \equiv a \times_n b \pmod n,\ a\,c \equiv a \times_n c \pmod n)$

Similarly $(a +_n b) \times_n c = (a \times_n c) +_n (b \times_n c)$

$\therefore$ distributive laws holds in J_n

Also number of elements in J_n are n *i.e.* finite

Hence J_n or Z_n a finite commutative ring with unity 1.

Example 6. Let R be a ring such that $x^2 = x\ \forall\ x \in R$. Prove

(*i*) R is a commutative ring (*ii*) $x + x = 0\ \forall\ x \in R$ (*iii*) $x + y = 0 \Rightarrow x = y$.

Sol. (*i*) Let $x, y \in R \Rightarrow x + y \in R$ [$\because$ R is closed under addition]

$\therefore\ (x + y)^2 = x + y \Rightarrow x^2 + x\,y + y\,x + y^2 = x + y$

$\Rightarrow (x^2 + y^2) + (y\,x + x\,y) = x + y$ [by commutative and associative]

$\Rightarrow (x + y) + (y\,x + x\,y) = (x + y) + 0$ [Property of addition in R]

$\Rightarrow y\,x + x\,y = 0$ [by left Cancellation Law for addition in R]

$\Rightarrow y\,x + x\,y = x\,y + x\,y$ [$\because$ By Part (*ii*), $x\,y + x\,y = 0$ for $x\,y \in R$]

$\Rightarrow y\,x = x\,y$ [By right Cancellation Law for addition in R]

$\Rightarrow$ R is a commutative ring.

(*ii*) Given $x \in R \Rightarrow x + x \in R$

$\therefore (x+x)^2 = x + x \Rightarrow (x+x)(x+x) = x + x \Rightarrow (x+x)x + (x+x)x = x + x$

$\Rightarrow (x^2 + x^2) + (x^2 + x^2) = x + x \Rightarrow (x+x) + (x+x) = x + x$ [$\because x^2 = x$]

$\Rightarrow (x+x) + (x+x) = (x+x) + 0$

$\Rightarrow x + x = 0$ [by left cancellation law]

Hence the result.

(*iii*) We have $x + y = 0$

$\Rightarrow x + y = x + x$ [$\because$ By Part (*ii*), $x + x = 0$]

$\Rightarrow y = x$ [by left cancellation law]

$\Rightarrow x = y$

Hence the result.

Example 7. Show that set of real numbers R is a ring under the composition $\oplus$ and $\odot$ defined as $a \oplus b = a + b + 1$ and $a \odot b = a + b + ab \ \forall \ a, b \in R$.

Sol. (A) Properties of Addition

(*i*) Let $a, b \in R$, then $a + b + 1 \in R \Rightarrow a \oplus b \in R$

$\therefore$ R is closed under the operation $\oplus$

(*ii*) Let $a, b, c, \in R$

Then $(a \oplus b) \oplus c = (a + b + 1) \oplus c$

$= (a + b + 1) + c + 1 = a + b + c + 2$

and $a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$

$\therefore (a \oplus b) \oplus c = a \oplus (b \oplus c) \ \forall \ a, b, c \in R$

$\therefore$ R satisfies associative property.

(*iii*) For each $a \in R$, we want to show there is $e \in R$ such that

$a \oplus e = e \oplus a = a$

i.e. $a + e + 1 = e + a + 1 = a \Rightarrow e = -1 \in R$

$\therefore \ \forall \ a \in R$, there is an identity $e = -1 \in R$

such that $a \oplus e = e \oplus a = a$

(*iv*) For each $a \in R$, we want to show there is an element $b \in R$ such that

$a \oplus b = e = b \oplus a$

$\Rightarrow a + b + 1 = -1 = b + a + 1$

$\Rightarrow b = -2 - a \in R$ ($\because a \in R$)

$\therefore \ \forall \ a \in R$, there is an inverse element $b = -2 - a \in R$ such that $a \oplus b = -1 = b \oplus a$

(v) Now $a \oplus b = a+b+1 = b+a+1$
$= b \oplus a$ $(\because a, b \in R \Rightarrow a+b = b+a)$

$\Rightarrow a \oplus b = b \oplus a \ \forall \ a, b \in R$

$\therefore$ R satisfies commutativity.

(B) **Properties of multiplication**

(i) $\forall \ a, b \in R \Rightarrow a+b+ab \in R$

$\Rightarrow a \oplus b \in R$ $(\because a, b \in R \text{ (reals)} \Rightarrow a+b, ab \in R)$

$\therefore$ R is closed under multiplication.

(ii) $(a \circledast b) \odot c = (a+b+ab) \odot c$
$= a+b+ab+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$
$= a+b+c+ab+ac+bc+abc$

$a \odot (b \odot c) = a \odot (b+c+bc)$
$= a+(b+c+bc)+a(b+c+bc) = a+b+c+bc+ab+ac+abc$
$= a+b+c+ab+ac+bc+abc$

$\therefore (a \odot b) \odot c = a \odot (b \odot c) \ \forall \ a, b, c \in R.$

$\Rightarrow$ R satisfies associativity under multiplication

(C) **Distributive Laws :** For each $a, b, c \in R$

$a \odot (b \oplus c) = a \odot (b+c+1)$
$= a+b+c+1+a(b+c+1) = 2a+b+c+ab+ac+1$

$(a \odot b) \oplus (a \odot c) = (a+b+ab) \oplus (a+c+ac) = (a+b+ab)+(a+c+ac)+1$
$= 2a+b+c+ab+ac+1$

$\therefore \ a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \ \forall \ a, b, c \in R$

Similarly $(b \oplus c) \odot a = (b \odot a) \oplus (c \odot a) \ \forall \ a, b, c \in R$

Hence $(R, \oplus, \odot)$ is a ring.

Example 8. Prove that set of all matrices of form $\begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix}$, $(x, y \in \text{reals})$ with matrix addition and matrix multiplication is a ring. Is it a commutative ring ?

Sol. Let $R = \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} : x, y \in \text{reals} \right\}$

(A) **Properties of Addition**

(i) Let $A = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}$

$\therefore \ A+B = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix} + \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix} = \begin{bmatrix} 0 & x_1+x_2 \\ 0 & y_1+y_2 \end{bmatrix} \in R$

$(\because x_1+x_2 \in \text{reals and } y_1+y_2 \in \text{reals})$

$\Rightarrow$ R is closed under addition

(*ii*) Let $A=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}, B=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}, C=\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}$ where $x_1, x_2, x_3, y_1, y_2, y_3$ are reals

$$\therefore \quad (A+B)+C=\begin{bmatrix}0 & x_1+x_2\\ 0 & y_1+y_2\end{bmatrix}+\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}=\begin{bmatrix}0 & (x_1+x_2)+x_3\\ 0 & (y_1+y_2)+y_3\end{bmatrix}$$

$$=\begin{bmatrix}0 & x_1+(x_2+x_3)\\ 0 & y_1+(y_2+y_3)\end{bmatrix}$$ (∵ Associative property holds for reals)

$$=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}+\begin{bmatrix}0 & x_2+x_3\\ 0 & y_2+y_3\end{bmatrix}$$

$$=A+(B+C)$$

⇒ Associative property holds in R under addition.

(*iii*) For each $A=\begin{bmatrix}0 & x\\ 0 & y\end{bmatrix}\in R$, there is $O=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in R$

such that $A+O=\begin{bmatrix}0 & x+0\\ 0 & y+0\end{bmatrix}=\begin{bmatrix}0 & x\\ 0 & y\end{bmatrix}=A$ and $O+A=\begin{bmatrix}0 & 0+x\\ 0 & 0+y\end{bmatrix}=\begin{bmatrix}0 & x\\ 0 & y\end{bmatrix}=A$

$\therefore \quad A+O=A=O+A$

⇒ $O=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ is an identity element of R.

(*iv*) For each $A=\begin{bmatrix}0 & x\\ 0 & y\end{bmatrix}\in R$, there is $B=\begin{bmatrix}0 & -x\\ 0 & -y\end{bmatrix}\in R$

such that $A+B=\begin{bmatrix}0 & x+(-x)\\ 0 & y+(-y)\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}=O$

and $B+A=\begin{bmatrix}0 & -x+x\\ 0 & -y+y\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}=O$

i.e. $A+B=B+A=O$

⇒ $B=-A$ is inverse element of R

(*v*) For each $A=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}$ and $B=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}$

$$A+B=\begin{bmatrix}0 & x_1+x_2\\ 0 & y_1+y_2\end{bmatrix}=\begin{bmatrix}0 & x_2+x_1\\ 0 & y_2+y_1\end{bmatrix}$$ (∵ commutativity holds in reals)

$$=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}+\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}=B+A$$

⇒ $A+B=B+A$

$\therefore$ matrix addition is commutative.

(B) Properties under Multiplication

(i) Let $A=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}$ and $B=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}\in R$ where x_1, x_2, y_1, y_2 are reals

$$\therefore\ AB=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}=\begin{bmatrix}0 & x_1y_2\\ 0 & y_1y_2\end{bmatrix}\in R \qquad (\because x_1y_2, y_1y_2 \text{ are reals})$$

⇒ R is closed under multiplication

(ii) Let $A=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}, B=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}$ and $C=\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}\in R$

$$\text{Now } (AB)C=\left(\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}\right)\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}=\begin{bmatrix}0 & x_1y_2\\ 0 & y_1y_2\end{bmatrix}\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}=\begin{bmatrix}0 & (x_1y_2)y_3\\ 0 & (y_1y_2)y_3\end{bmatrix}$$

$$A(BC)=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\left(\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}\right)=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_2y_3\\ 0 & y_2y_3\end{bmatrix}=\begin{bmatrix}0 & x_1(y_2y_3)\\ 0 & y_1(y_2y_3)\end{bmatrix}$$

$$=\begin{bmatrix}0 & (x_1y_2)y_3\\ 0 & (y_1y_2)y_3\end{bmatrix}$$

$\left(\begin{array}{l}\because\ x_1(y_2y_3)=(x_1y_2)y_3\\ y_1(y_2y_3)=(y_1y_2)y_3\\ \text{as associativity holds in reals}\end{array}\right)$

$\therefore\ A(BC)=(AB)C$

⇒ matrix multiplication is associative.

(C) Distributive Laws

Let $A=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}, B=\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}, C=\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}\in R$

Now $$A(B+C)=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\left(\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}+\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}\right)=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_2+x_3\\ 0 & y_2+y_3\end{bmatrix}$$

$$=\begin{bmatrix}0 & x_1(y_2+y_3)\\ 0 & y_1(y_2+y_3)\end{bmatrix}=\begin{bmatrix}0 & x_1y_2\\ 0 & y_1y_2\end{bmatrix}+\begin{bmatrix}0 & x_1y_3\\ 0 & y_1y_3\end{bmatrix}$$

$$=\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_2\\ 0 & y_2\end{bmatrix}+\begin{bmatrix}0 & x_1\\ 0 & y_1\end{bmatrix}\begin{bmatrix}0 & x_3\\ 0 & y_3\end{bmatrix}$$

$$=AB+AC$$

Similarly $(B + C)A = BA + CA$

$\therefore$ distributive laws holds in R

$\Rightarrow$ R is a ring under matrix addition and multiplication.

To Check Commutative Property

Let $A = \begin{bmatrix} 0 & x_1 \\ 0 & y_1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & x_2 \\ 0 & y_2 \end{bmatrix}$

$\therefore \quad AB = \begin{bmatrix} 0 & x_1 y_2 \\ 0 & y_1 y_2 \end{bmatrix}$ and $BA = \begin{bmatrix} 0 & x_2 y_1 \\ 0 & y_2 y_1 \end{bmatrix}$

Clearly $AB \neq BA$

so R is a non-commutative ring.

EXERCISE 2.1

1. (*a*) Prove that $< \mathbf{Q}, +, \cdot >$ where $\mathbf{Q}$ is the set of all rationals, is a commutative ring with unity.
   (*b*) Prove that $< R, +, \cdot >$ where R is the set of all reals, is a commutative ring with unity.
2. Prove that the set of matrices of order 2 forms a ring under addition and multiplication of matrices.
3. Prove that the set $G = \{a + \sqrt{2}\, b \mid a, b \in \mathbf{Q}\}$ where $\mathbf{Q}$ is the set of rationals, is a ring.
4. Prove that the set $R = \{(a, b) \mid a, b \in \text{Reals}\}$ is a ring under the addition and multiplication of ordered pairs defined as
   $(a, b) + (c, d) = (a + c, b + d)$
   $(a, b)(c, d) = (ac - bd, bc + ad) \quad \forall\ (a, b), (c, d) \in R.$
5. Show that the set of rational numbers $\mathbf{Q}$ is a ring under the compositions $\oplus$ and $\odot$ defined as $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab. \quad \forall\ a, b \in \mathbf{Q}$
6. Let $G = \{0, 1, 2, 3, 4, 5\}$. Define the compositions $\oplus$ and $\odot$ on G as $p \oplus q$ = The least non-negative remainder on dividing $p + q$ by 6 for all $p, q \in G$ and $p \odot q$ = The least non-negative remainder on dividing pq by 6 for all $p, q \in G$.
   Show that G is a commutative ring with unity under $\oplus$ and $\odot$.
7. Show that the set G of all real valued functions of x, defined on $[0, 1]$ is a ring, under the addition and multiplication defined as below :
   $(f + g)(x) = f(x) + g(x) \quad \forall\ x \in [0, 1]$
   $(fg)(x) = f(x)\, g(x) \quad \forall\ x \in [0, 1]$ where $f, g \in G$.
8. Let G be the set of all real valued functions on $(-\infty, \infty)$. We define addition and multiplication as below
   $(f + g)(x) = f(x) + g(x) \quad \forall\ f, g \in G,\ x \in (-\infty, \infty)$
   $(f \times g)(x) = f[g(x)] \quad \forall\ f, g \in G,\ x \in (-\infty, \infty).$
   Is G is a ring under these operations ?

9. Let $< R, +, \cdot >$ is a commutative ring. In R, define a binary operation $\times$ by, $a \times b = a \cdot b + b \cdot a \ \forall \ a, b \in R$. Show that $< R, +, \times >$ is a commutative ring.

10. Give an example of the following :

(*a*) A commutative ring without unity. (*b*) A non-commutative ring with unity.

(*c*) A ring with zero divisors (*d*) A non-commutative ring.

11. If R is a system satisfying all the conditions for a ring with unit element with the possible exception $x + y = y + x \ \forall \ x, y \in R$.

Prove that this axiom, that $x + y = y + x$ also hold in R and thus R is a ring.

12. Let $F = \{ f : \mathbf{R} \to \mathbf{R} : f$ is a continuous function$\}$ *i.e.*, F is the set of all real continuous functions. Then F forms an **infinite commutative ring with unity** under the operations of addition and multiplication defined by $(f + g)(x) = f(x) + g(x)$, for all $f, g \in F$ and $x \in \mathbf{R}$ $(f g)(x) = f(x) g(x)$, for all $f, g \in F$ and $x \in \mathbf{R}$.

13. Let X be a non-empty set. Let P(X) denotes the power set of X (*i.e.*, set of all subsets of X). Then P(X) forms a **commutative ring with unity X,** under the operation + and .defined by

$A + B = A \Delta B = (A \cup B) - (A \cap B)$ $A.B = A \cap B$.

Note : If the set X is a finite set, then $<P(X), +, \cdot>$ forms a finite commutative ring with unity.

14. Let R_1 and R_2 be two rings. Define $R = R_1 \times R_2$ *i.e.* $R = R_1 \times R_2 = \{(a, b) : a \in R_1$ and $b \in R_2\}$.

Then R forms a ring under the operations + and $\cdot$ defined by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (a c, b d)$ for all $(a, b), (c, d) \in R$.

The ring R is called the **direct product** of rings R_1 and R_2.

Note : (*i*) R is commutative ring iff both R_1 and R_2 are commutative rings.

(*ii*) R is with unity iff both R_1 and R_2 have unity.

15. Prove that the set $R = \left\{ x + y \cdot 3^{\frac{1}{3}} + z \cdot 9^{\frac{1}{3}} ; x, y, z \in Q \right\}$ is a ring w.r.t. addition and multiplication.

ANSWERS

8. Not a ring

10. (*a*) Ring of even integers (*b*) Ring of $n \times n$ matrices over reals

(c) Ring of 2×2 matrices (d) Ring of 2×2 matrices over reals

2.2. Properties of Rings

We now prove some basic properties of rings. Before that we point out following conventions which we shall follow henceforth :

Let $< R, +, \cdot >$ be a ring and $a, b, c, d \in R$.

1. We often drop the symbol for multiplication and write $a \cdot b$ simply as $a\ b$.

2. Multiplication is assumed to be performed before addition [accordingly, $a\ b + c\ d$ stands for $(a\ b) + (c\ d)$].

3. We write $a - b$ instead of $a + (-b)$.

4. We refer $<R, +, \cdot>$ as a ring R under the operations + and $\cdot$ or as a ring R together with the operations + and $\cdot$ or simply as a ring R.

Theorem : Let R be a ring and $a, b, c \in R$. Then

(*i*) $a \cdot 0 = 0 \cdot a = 0$ (*ii*) $a(-b) = (-a)b = -ab$ (*iii*) $(-a)(-b) = ab$

(*iv*) $a(b-c) = ab - ac$ (*v*) $(b-c)a = ba - ca$

Proof. (*i*) $a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0 = a \cdot 0 + 0$

$\Rightarrow a \cdot 0 = 0.$ [By left cancellation law in $<R, +>$]

Similarly $0 \cdot a = 0$.

(*ii*) $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$

$\Rightarrow a(-b) = -ab.$ [By definition of additive inverse in $<R, +>$]

The proof is similar for the other part.

(*iii*) $(-a)(-b) = -(-a)b = -(-ab))$, by using (*ii*).

This completes the proof of the theorem.

Now in the group $<R, +>$, $-(-x) = x$ for all $x \in R$,

where it follows that $-(-ab) = ab$.

(*iv*) We have $a(b-c) = a(b + (-c) = ab + a(-c) = ab - ac.$ [By Left Distributive law]

(*v*) We have $(b-c)a = (b + (-c))a = ba + (-c)a$

$= ba - ca.$ [By Right Distributive law]

In particular, we notice that $(-a)^2 = a^2$ for all $a \in R$ and if the ring R has an identity 1, then

$1 \cdot (-1) = (-1) \cdot 1 = -1$ and $(-1)(-1) = 1$.

Considering the property (*i*), the additive identity 0 is called the zero element of the ring R. Also we note that if $1 = 0$ in a ring R, then $a = a \cdot 1 = a \cdot 0 = 0$ for all $a \in R$. So in this case R becomes the **trivial ring** {0}.

The following identities are easy applications of distributive laws :

Theorem : Let R be a ring and $a, b, c, d \in R$. Then

(*i*) $(a+b)(c+d) = ac + bc + ad + bd$ (*ii*) $(a-b)(c-d) = ac - bc - ad + bd$

(*iii*) $(a+b)^2 = a^2 + ab + ba + b^2$ (*iv*) $(a-b)^2 = a^2 - ab - ba + b^2$

(*v*) $(a+b)(a-b) = a^2 - ab + ba - b^2$

Proof. Easy exercise.

(Using Distributive Laws)

Theorem : Identity element in a ring R is unique.

Proof. Suppose e_1 and e_2 to be two identities of ring R. Then, $xe_1 = e_1 x = x$ and $xe_2 = e_2 x = x \ \forall x \in R$.

Then from the first equation, replacing x by e_2 we get $e_1 e_2 = e_2$ and from the second equation, replacing x by e_1, we get $e_1 e_2 = e_1$. Thus $e_1 = e_2$. Hence identity of a ring is unique.

Theorem : Let R be a ring having a unique left identity e_l. Then e_l is also the right identity.

Proof : Let R be a ring with a unique left identity e_l *i.e.*, $e_l x = x, \forall x \in R$.

We show that e_l is also the right identity of R *i.e.*, $x e_l = x, \forall x \in R$.

Let $x \in R$ and $\forall y \in R$, we have $(x e_l - x + e_l) y = x e_l y - xy + e_l y = xy - xy + y = y$

$\Rightarrow$ $x e_l - x + e_l$ is also a left identity of R.

But left identity e_l is unique.

$\therefore$ $x e_l - x + e_l = e_l \Rightarrow x e_l = x \forall x \in R$

i.e., e_l is also the right identity of R.

Definition. An element x in a ring R is called **idempotent** if $x^2 = x$.

For example : In M_3 (**R**), the ring of real square matrices of order 3, the following matrices are idempotents.

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{bmatrix} \text{ for } A^2 = A, B^2 = B.$$

There are rings in which every element is idempotent.

Definition. A ring R is called a **Boolean ring** if every element of R is idempotent, *i.e.*, $x^2 = x$ for all $x \in R$.

We prove the following interesting properties of a Boolean ring :

Theorem. Let R be a Boolean ring. Then

(*i*) $2x = 0$ for all $x \in R$; (*ii*) $xy = yx$ for all $x, y \in R$.

Proof. (*i*) Let $x \in R \Rightarrow -x \in R$. [$\because$ R is Boolean Ring]

Now $x = x^2 = (-x)^2 = -x$

$\therefore$ $x = -x \Rightarrow 2x = 0$ for all $x \in R$.

(*ii*) Let $x, y \in$ **R**. Then

$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$ ...(1)

$\Rightarrow$ $0 = xy + yx$. (using cancellation under addition)

Also $xy \in R \Rightarrow 2xy = 0$ [$\because$ of (*i*)]

$\Rightarrow$ $xy + xy = 0 = xy + yx$ (using (1))

$\Rightarrow$ $xy = yx$. [By left cancellation law]

Note : From the above theorem we see that a Boolean ring is a commutative ring but the converse need not be true.

For example : The ring **Z** is a commutative ring which is not a Boolean ring.

We now define the invertible elements of a ring under multiplication.

Definition. Let R be a ring with identity $1 \neq 0$. Then an element $u \in R$ is called a **unit (or invertible)** if there exists $v \in R$ such that $uv = vu = 1$. Then v is called the **inverse of** u and is denoted by u^{-1}.

Remark : Unity must be a unit but every unit is not unity.

For example : In **Z**, the ring of integers, the unity is 1, where as units are 1 and -1.

Theorem. Let R be a ring with unity 1 ($\neq 0$). Then the set of units of R forms a group under multiplication in R.

Proof. Let $U = \{u \in R: uv = 1 = vu$ for some $v \in R\}$ *i.e.*, U be the set of units of R.

We will show that $<U, \cdot>$ is a subgroup of semigroup $<R, \cdot>$.

Clearly $U \neq \phi$, for $1 \in U$.

Let $u, v \in U$, then $\exists\ u^{-1}, v^{-1} \in R$ such that $uu^{-1} = 1 = u^{-1}u$ and $vv^{-1} = 1 = v^{-1}v$.

Consider $uv(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = u.1.u^{-1} = uu^{-1} = 1$.

Similarly $(v^{-1}u^{-1})(uv) = v^{-1}(u^{-1}u)v = v^{-1}.1.v = v^{-1}v = 1$.

$\therefore\quad uv(v^{-1}u^{-1}) = 1 = (v^{-1}u^{-1})uv \Rightarrow uv$ is a unit and $(uv)^{-1} = v^{-1}u^{-1}$ and so $uv \in U$.

Also $1 \in U$

$\therefore$ For each $u \in U, \exists\ u^{-1} \in U$ such that $uu^{-1} = 1 = u^{-1}u \Rightarrow u^{-1} \in U, \forall\ u \in U$.

Hence U forms a subgroup of Semi group $<R, \cdot>$ and so U forms a group under multiplication.

Definition. An element x in a ring R is called **nilpotent** if $x^n = 0$ for some positive integer n. The smallest positive integer (for x) with this property is called the **degree of nilpotency** of the element x.

Remark. The zero element in every ring satisfy the relation $0^1 = 0$.

But there are non-zero elements x in a ring also.

For example :

In the ring M_3 (R), if we consider the matrices $A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 3 \\ 5 & 2 & 6 \\ -2 & -1 & -3 \end{bmatrix}$, then we can easily verify that $A^2 = O$ and $B^2 = O$, though neither A nor B is the zero (null) matrix. Thus in a ring there may be some non zero elements whose integral power is zero for some positive integer greater than 1.

Theorem : The sum of two nilpotent elements of a commutative ring is also nilpotent.

Proof. Let R be a commutative ring and $a, b \in R$ be nilpotent elements such that $a^m = 0$ and $b^n = 0$ for some positive integers m and n. Now

$$(a+b)^{m+n} = a^{m+n} + {}^{m+n}c_1\ a^{m+n-1}b + \ldots + {}^{m+n}c_r\ a^{m+n-1}b^r + \ldots + b^{m+n}$$

$$= a^m\{a^n + {}^{m+n}c_1\ a^{n-1}b + \ldots\ldots + {}^{m+n}c_n\ b^n\} + \{{}^{m+n}c_{n+1}\ a^{m-1}b + \ldots\ldots + b^m\}b^n$$

$$= 0. \qquad (\because a^m = 0 \text{ and } b^n = 0)$$

$\Rightarrow$ $a + b$ is also nilpotent.

ILLUSTRATIVE EXAMPLES

Example 1. If a ring R has no non-zero nilpotent elements then prove that for any idempotent e of R, $ex = xe\ \forall\ x \in R$.

Solution : $\forall\ x \in R$,

Consider $(xe - exe)^2 = (xe - exe)(xe - exe)$

$= xexe - xeexe - exexe + exeexe$

$= xexe - xe^2xe - exexe + exe^2xe$ (But e is idempotent *i.e.* $e^2 = e$)

$= xexe - xexe - exexe + exexe$

$= 0.$

But R has no non-zero nilpotent

$$xe - exe = 0 \Rightarrow xe = exe. \quad \ldots(1)$$

$\Rightarrow$ Similarly $(ex - exe)^2 = 0 \Rightarrow ex - exe = 0$

$$\Rightarrow \quad ex = exe. \quad \ldots(2)$$

From (1) and (2), we get $ex = xe$.

Example 2. If R be an algebraic system satisfying all the axioms of a ring with the possible exception of $a + b = b + a \; \forall \; a, b \in R$. If there exists one element $c \in R$ such that $ac = bc \Rightarrow a = b \; \forall \; a, b \in R$, prove that R is a ring.

Sol. $\forall \; a, b \in R$ and given $c \in R$.

Consider $(a + b)(c + c) = a(c + c) + b(c + c) = ac + ac + bc + bc.$ ...(1)

Also $(a + b)(c + c) = (a + b)c + (a + b)c = ac + bc + ac + bc.$ ...(2)

From (1) and (2), we get

$$ac + ac + bc + bc = ac + bc + ac + bc.$$

Using cancellation laws under addition, we get

$$ac + bc = bc + ac$$

$\Rightarrow$ $$(a + b)c = (b + a)c.$$

By the given property of c, we get

$$a + b = b + a$$

$\Rightarrow$ R is a ring.

Example 3. If R is a ring with identity such that $(xy)^2 = x^2y^2$ for all $x, y \in R$, then show that R is commutative. Give an example to show that the above result may be false if R does not have an identity.

Sol. Let R be a ring with identity such that $(xy)^2 = x^2y^2$ for all $x, y \in R$.

Let $x, y \in R$ be any elements $\therefore \; y + 1 \in R$.

$\therefore$ $$[x(y + 1)]^2 = x^2(y + 1)^2$$

$$(xy + x)^2 = x^2(y^2 + 2y + 1)$$

$$(xy)^2 + x^2 + xyx + x^2y = x^2y^2 + 2x^2y + x^2$$

$$x^2y^2 + x^2 + xyx + x^2y = x^2y + 2x^2y + x^2 \quad \ldots(1)$$

$$xyx = x^2y.$$

Replacing x by $x + 1$ in (1), we get

$$(x + 1)y(x + 1) = (x + 1)^2y$$

$$(xy + y)(x + 1) = (x^2 + 1 + 2x)y$$

$$xyx + xy + yx + y = x^2y + y + 2xy \quad \text{[using (1)]}$$

$$x^2y + xy + yx + y = x^2y + y + 2xy$$

$$yx = xy.$$

$\therefore$ R is commutative.

Now for the required example :

Let $R = \left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} ; \forall\ a, b \in \mathbf{R}\right\} \subset M_2(\mathbf{R})$. It is easy to verify that R is a non commutative ring.

Indeed, $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

$$\therefore \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Let $A, B \in R$. Then,

$$A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \text{ for some } a, b, c, d \in \mathbf{R}.$$

Then it is easy to see that

$$(AB)^2 = A^2 B^2 = \begin{bmatrix} a^2 c^2 & a^2 cd \\ 0 & 0 \end{bmatrix}.$$

Note. Here we notice that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a left identity of R and R has no right identity.

Example 4. If in a ring R, $x^3 = x$ for all $x \in R$, then show that R is commutative.

Sol. Let $x, y \in R$ be real numbers, then

$$(x^2 y - x^2 y x^2)^2 = x^2 y x^2 y - x^2 y x^2 y x^2 - x^2 y x^2 x^2 y + x^2 y x^2 x^2 y x^2$$
$$= x^2 y x^2 y - x^2 y x^2 y x^2 - x^2 y x^2 y + x^2 y x^2 y x^2$$
$$= 0$$

$$\Rightarrow \quad x^2 y - x^2 y x^2 = 0 \qquad [\because x^4 = x^2]$$

$$\Rightarrow \quad x^2 y = x^2 y x^2. \qquad \ldots(1)$$

Similarly, $(y x^2 - x^2 y x^2)^2 = y x^2 y x^2 - y x^2 x^2 y x^2 - x^2 y x^2 y x^2 + x^2 y x^2 x^2 y x^2$
$$= y x^2 y x^2 - y x^2 y x^2 - x^2 y x^2 y x^2 + x^2 y x^2 y x^2$$
$$= 0$$

$$\Rightarrow \quad y x^2 - x^2 y x^2 = 0$$

$$\Rightarrow \quad y x^2 = x^2 y x^2. \qquad \ldots(2)$$

From (1) and (2), we get

$$x^2 y = y x^2. \qquad \ldots(3)$$

Further, $(x^2 - x)^3 = x^2 - x$ $[\because x^3 = x, \forall x \in R]$

$$\Rightarrow \quad 4x^2 - 4x = x^2 - x$$

$$\Rightarrow \quad 3x^2 = 3x.$$

$\therefore \quad (x^2-x)^2 = (x^2-x)(x^2-x) = 2x^2-2x = 3x^2-x^2-3x+x$

$= 3x-x^2-3x+x$

$= x-x^2.$

Thus $(x^2-x)^2 = x-x^2.$ ...(4)

$\therefore$ from (3), we get

$(x^2-x)^2 y = y(x^2-x)^2$

$\Rightarrow \quad (x-x^2)y = y(x-x)^2$ [using (4)]

$\Rightarrow \quad xy-x^2y = yx-yx^2.$

$\Rightarrow \quad xy-yx^2 = yx-yx^2$ [using (3)]

$\Rightarrow \quad xy = yx.$

Hence, R is commutative.

Example 5. Show that a ring R is commutative iff

$(a+b)^2 = a^2+b^2+2ab$ for all $a, b \in R$.

Sol. Firstly, let R be commutative ring

$\Rightarrow \quad ab = ba$, for all $a, b \in R$.

Now $(a+b)^2 = (a+b)(a+b) = a^2+ab+ba+b^2$ [$\because ba = ab$]

$= a^2+ab+ab+b^2$

$= a^2+2ab+b^2 = a^2+b^2+2ab.$

Conversely, Let $(a+b)^2 = a^2+2ab+b^2$, for all $a, b \in R$.

To show that R is commutative.

Since $(a+b)^2 = (a+b)(a+b) = a^2+ab+ba+b^2$

$\therefore \quad a^2+2ab+b^2 = a^2+ab+ba+b^2$

$\Rightarrow \quad ab+ab = ab+ba \Rightarrow ab = ba.$

Hence R is commutative ring.

Example 6. (*a*) Show that any ring of prime order is commutative.

(*b*) Show that a ring of order p^2 where p is prime, need not be commutative.

Sol. (*a*) Let R be a ring of prime order p

$\therefore \quad <R, +>$ is a cyclic group

Take $<R, +> = <a>$

so that $O(a) = O(R) = p$

Let $x_1, x_2 \in R$ be any elements

$\therefore \quad x_1 = la, \; x_2 = ma$ for $l, m \in Z$

Now $x_1x_2 = (l\ a)\ (m\ a) = l\ m\ a^2 = m\ l\ a^2 = (m\ a)\ (l\ a) = x_2x_1$

$\Rightarrow \quad x_1x_2 = x_2x_1$ for $x_1, x_2 \in R$

$\therefore$ R is commutative ring

(*b*) Let $R = \left\{\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}\right\}$

be set of 2×2 matrices with second row having zero entries

Here R is a ring under matrix addition and multiplication.

Also $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ and $\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$

i.e. R is not commutative and it is ring of order $4 = 2^2$ where 2 is prime

EXERCISE 2.2

1. Prove that a ring R has no non zero nilpotent elements if and only if 0 is the only solution of the equation $x^2 = 0$ in R.
2. Show that in a ring R, a non zero idempotent cannot be nilpotent.
3. Which of the following algebraic structures $<R, +, \cdot>$ forms a ring ?
   (*i*) Let X be any set and R = the power set of X. Define $A + B = A \cup B$ and $A \cdot B = A \cap B$ for all $A, B \in R$.
   (*ii*) Let R be the set of all real –valued continuous functions defined on **R**. Define
   $(f + g)(x) = f(x) + g(x)$ and $(f \circ g)(x) = f(g(x))$ for all $f, g \in R$ and for all $x \in \mathbf{R}$.
4. Let **R** be the set of all real numbers and F be the set of all real-valued continuous functions defined on **R**. Define $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)\ g(x)$ for all $f, g \in F$ and for all $x \in \mathbf{R}$. Show that $<F, +, \cdot>$ is a ring under the binary operations defined above.
5. Let Q be the set of all symbols $a_0 + a_1 i + a_2 j + a_3 k$, where $a_r \in \mathbf{R}$, $r = 0, 1, 2, 3$,. Two symbols $a_0 + a_1 i + a_2 j + a_3 k$ and $b_0 + b_1 i + b_2 j + b_3 k$ are considered to be equal if and only if $a_r = b_r$, $r = 0, 1, 2, 3$. Define addition and multiplication as a formal sum and product using the following relations ; $i^2 = j^2 = k^2 = -1$, $i\ j = -j\ i = k$, $j\ k = -k\ j = i$, $k\ i = -i\ k = j$.
   Prove that Q is non-commutative ring with identity (this ring, is called the **ring of real quaternions**).
6. Give an example of a ring which contains elements a, b such that
   (*i*) $(a + b)^2 \neq a^2 + 2\ a\ b + b^2$ (*ii*) $(a + b)(a - b) \neq a^2 - b^2$.
7. Show that if $1 - a\ b$ is invertible in a ring R with 1 then so is $1 - b\ a$ and that $(1 - b\ a)^{-1} = 1 + b\ (1 - a\ b)^{-1}\ a$.
8. Show that $[x] \in \mathbf{Z}_n$ is a unit if and only if gcd $(x, n) = 1$.

9. If a is nilpotent in the ring R, Show that $1 - a$ is a unit.

10. If x, y, z, t are any elements of ring R, prove that $(x-y)(z-t) = (xz + yt) - (xt + yz)$.

11. Let $\langle G, + \rangle$ be an abelian group and R be the set of all endomorphisms of G. Define $(f+g)(x) = f(x) + g(x)$ and $(f \circ g)(x) = f(g(x))$ for all $f, g \in R$ and for all $x \in G$. Then $\langle R, +, o \rangle$ is a ring (which is called the ring of endomorphisms of G).

ANSWERS

3. (*i*) Not a ring (*ii*) Not a ring

2.3. Integral Domains, Division Rings and Fields

In this section, we develope rings with certain special conditions. To begin with, let us consider the finite ring $\mathbf{Z}_6$, the ring of integers modulo 6. In this ring, if we take the product of two non zero elements, [2] and [3] (modulo 6),then we have $[2]\cdot[3] = [6] = [0]$. Thus this ring has some non zero elements whose product is zero (additive identity) of the ring. Also in $M_2(R)$, the ring of 2×2 matrices over the set of real numbers, we have $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, but none of the elements on the left hand side is zero (null matrix) of the ring. In general, we define the following :

Definitions :

Left zero divisor : Let $\langle R, +, \cdot \rangle$ is a ring. An element $a \in R$ is called a **left zero divisor if** $\exists\ b \neq 0 \in R$ s.t. $ab = 0$.

Right zero divisor : An element $a \in R$ is called a **right zero divisor if** $\exists\ b \neq 0 \in R$ s.t. $ba = 0$.

Zero divisor : An element $a \in R$ is called a **zero divisor if** $\exists\ b \neq 0 \in R$ s.t. $ab = 0 = ba$.

Note : $0 \in R$ is a zero divisor.

Proper zero divisor

An element $a \neq 0 \in R$ is called a **proper zero divisor if** $\exists\ b \neq 0 \in R$ s.t. $ab = 0 = ba$.

Note : If a is a proper zero divisor of R, then b is also a proper zero divisor of R.

Definition : A ring R is said to satisfy left [right] cancellation property if for all $a, b, c \in R$, $a \neq 0$ and $ab = ac$ [resp. $ba = ca$] implies that $b = c$.

The following theorem establishes a relation between cancellation property for multiplication and zero divisors in a ring R.

Theorem : Let R be a ring. Then the following conditions are equivalent :

(*i*) R has no zero divisors ; (*ii*) R satisfies left cancellation property ;

(*iii*) R satisfies right cancellation property.

Proof. (*i*) $\Rightarrow$ (*ii*) : Suppose the ring R has no zero divisors.

Let $a, b, c \in R$, $a \neq 0$ and $ab = ac$. Then

$a(b-c) = 0$

$\Rightarrow b - c = 0$, as $a \neq 0$ and R has no zero divisors.

$\Rightarrow b = c$.

(*ii*) ⇒ (*i*) : Let the ring R satisfy the left cancellation property.

Let $a \in R$ be such that $a \neq 0$. Suppose $b \in R$ such that $a\,b = 0$.

Then $a\,b = 0 = a \cdot 0$

⇒ $b = 0$ by the left cancellation property.

Now if $b\,a = 0$ then for $b \neq 0$, $b\,a = 0 = b \cdot 0$

⇒ $a = 0$, which is a contradiction.

Thus $b\,a = 0$ ⇒ $b = 0$.

So a is not a zero divisor. Hence R has no zero divisors.

Similarly we can show that (*i*) ⇔ (*iii*).

Hence the conditions are equivalent.

Now a ring may or may not have zero divisors. In fact, the ring of integers, rationals, reals or complex numbers do not have zero divisors. Consequently, the rings without zero divisors deserve particular attention.

Definition : A commutative ring R is called an **integral domain** (in short, I.D) if R has no proper zero divisors.

i.e. $\forall\, a, b \in R$,

If $ab = 0$, then either $a = 0$ or $b = 0$.

or If $a \neq 0$, $b \neq 0$, then $ab \neq 0$.

For example : (*i*) The ring of integers **Z**, ring of rational numbers **Q**, ring or real numbers **R** and the ring of complex number **C** are integral domains.

(*ii*) The ring $\mathbf{Z}_6$ of integers modulo 6 is not an integral domain.

Here $2 \not\equiv 0 \pmod 6$, $3 \not\equiv 0 \pmod 6$, but $2 \cdot 3 \equiv 0 \pmod 6$.

For the ring $\mathbf{Z}_n$ of all integers modulo a positive integer n, we have the following nice characterization :

Theorem : For any positive integer n, the ring $\mathbf{Z}_n$ of all integers modulo n is an integral domain if and only if n is a prime integer.

Proof. Let $\mathbf{Z}_n$ be an integral domain. Then $[1] \neq [0]$ in $\mathbf{Z}_n$ and hence $n > 1$.

If n is not prime, then $n = p\,q$ for some integers p, q where $1 < p, q < n$.

So we have $[p]\,[q] = [n] = [0]$, but neither $[p]$ nor $[q]$ is zero of the ring $\mathbf{Z}_n$.

This contradiction shows that n must be prime.

Conversely, consider $\mathbf{Z}_n$ for a prime integer n.

Let $[a], [b] \in \mathbf{Z}_n \setminus \{[0]\}$.

Now if $[a]\,[b] = [0]$, then $[a\,b] = [0]$, *i.e.*, n divides ab.

Since n is prime, we have either $n \mid a$ or $n \mid b$.

Both the cases are not possible as $[a], [b] \neq [0]$ *i.e.* $a \not\equiv 0 \pmod n$, $b \not\equiv 0 \pmod n$ *i.e.* n does not divide a and b.

Therefore $\mathbf{Z}_n$ is an integral domain.

Though the next theorem follows immediately from Theorem 5.2.3, we provide an independent proof of it.

Theorem : A commutative ring R with identity $1 \neq 0$ is an integral domain if and only if the cancellation laws hold for multiplication.

Proof. Let R be an integral domain. Let $a, b, c \in R$, $a \neq 0$ and $ab = ac$.

$\Rightarrow a(b - c) = 0$

$\Rightarrow b - c = 0$, as R is an integral domain and $a \neq 0$. So we have $b = c$.

Conversely, let R be a commutative ring with identity, in which the cancellation law holds. Let $a, b \in R$ be such that $a \neq 0$ and $ab = 0$. Then $ab = 0 = a0$

$\Rightarrow \quad b = 0$ (by left cancellation law).

Thus R has no zero divisors, hence R is an integral domain.

In view of the above theorem, we note that if every non zero element of a commutative ring R with identity is a unit, then R satisfies the cancellation law and hence R is an integral domain.

Definition. A ring R with identity $1 \neq 0$ is called a **division ring or a skew field** if every non zero element of R is a unit (*i.e.*, if for any $a \in R$, $a \neq 0$, there exists an element $b \in R$ such that $ab = ba = 1$).

Note that if R is a division ring, the set of all non zero elements of R forms a group under multiplication.

Theorem. In a ring R with unity 1, units form a subgroup of the semigroup $\langle R, \cdot \rangle$

Or The set of all units of a ring R with unity is a group under the multiplicative operation of R.

Proof : Given $\langle R, +, \cdot \rangle$ is a ring with unity 1.

Let U be the set of all units of R.

Since $1 \cdot 1 = 1 \Rightarrow 1 \in U$.

$\therefore$ U is a non empty sub-set of R.

$\forall\, a, b \in U \Rightarrow a, b$ are units of R

$\Rightarrow \quad \exists\ c, d \in R$ s.t.

$ac = 1 = ca$ and $bd = 1 = db$.

Consider $(ab)(dc) = a(bd)c = a(1)c = ac = 1$.

Also $(dc)(ab) = d(ca)b = d(1)b = db = 1$

$\therefore \quad (ab)(dc) = 1 = (dc)(ab)$

$\Rightarrow \quad ab$ is a unit *i.e.* $ab \in U$.

Also $ac = 1 = ca \Rightarrow c = a^{-1}$ is a unit

$\Rightarrow \quad a^{-1} \in U$.

Hence U is a subgroup of $\langle R, \cdot \rangle$

i.e. U itself is a group under the multiplicative operation of R.

Another definition of division ring

A ring with unity in which all non-zero elements form a group under multiplication is called a **division ring or a skew field.**

Definition : A commutative division ring is called a **field.**

i.e., a ring R with identity $1 \neq 0$ is called a **field** if R is commutative and every non zero element of R is a unit.

For example : The rings **Q, R, C** are division rings which are fields.

Note that there are division rings which are not fields. We have the following example :

ILLUSTRATIVE EXAMPLES

Example 1. Give an example of a division ring which is not a field.

Sol. Let $R = \left\{ \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} \in M_2(\mathbf{C}) \mid \bar{\alpha}, \bar{\beta} \text{ denote the conjugate of } \alpha, \beta \right\}$.

Define addition (+) and multiplication (·) in R by usual matrix addition and matrix multiplication. We now show that R is a division ring but not a field.

Let $A = \begin{bmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{bmatrix}, B = \begin{bmatrix} r+it & u+iv \\ -(u-iv) & r-it \end{bmatrix} \in R.$

Then,

$$A + B = \begin{bmatrix} (a+r)+i(b+t) & (c+u)+i(d+v) \\ -((c+u)-i(d+v)) & (a+r)-i(b+t) \end{bmatrix} \in R.$$

Also it is a routine calculation to check that $AB \in R$ (verify !). Observe that $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$ is the zero element and for any $A \in R$, we have $-A \in R$ such that $A + (-A) = O$. Further, the distributive properties hold. Hence R is a ring with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in R$.

Now, $\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix}, \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \in R$ and $\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix}, \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} = \begin{bmatrix} 2i & 0 \\ 0 & -2i \end{bmatrix}$

$$\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ -2 & 0 \end{bmatrix}.$$

This clearly shows that R is a non commutative ring with $I \neq O$.

Let $\begin{bmatrix} a+ib & c+id \\ -(c-id) & a-ib \end{bmatrix}$

be a non zero element of R. Then either $a + ib \neq 0$ or $c + id \neq 0$

i.e., either $a^2 + b^2 \neq 0$ or $c^2 + d^2 \neq 0$. Hence $a^2 + b^2 + c^2 + d^2 \neq 0$.

Let $k = a^2 + b^2 + c^2 + d^2 \neq 0$. Observe that $\frac{1}{k}\begin{bmatrix} a-ib & c-id \\ -(c+id) & a+ib \end{bmatrix} \in R$ is the inverse of $\begin{bmatrix} a-ib & c-id \\ -(c+id) & a+ib \end{bmatrix} \in R$.

Hence each non zero element of R has an inverse in R, whence R is a division ring.

But as R is non commutative, clearly R is not a field.

Example 2. Let R be set of all reals. Take $F = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in R \right\}$

Prove F is a field under usual addition and multiplication of matrices.

Sol. (*i*) Let $A, B \in F$ *i.e.* $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $B = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$ where $a, b, \alpha, \beta \in R$

$\therefore A + B = \begin{bmatrix} a+\alpha & b+\beta \\ -(b+\beta) & a+\alpha \end{bmatrix}$ where $a+\alpha, b+\beta \in R$

$\in F \Rightarrow$ Addition is closed.

(*ii*) We know matrix addition is associative

$\therefore$ For A, B, C $\in$ F, we have $(A + B) + C = A + (B + C)$.

(*iii*) For $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in F$, there is $O = \begin{bmatrix} 0 & 0 \\ -0 & 0 \end{bmatrix} \in F$

such that $A + O = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ -0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A$

and $O + A = \begin{bmatrix} 0 & 0 \\ -0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = A$

i.e. $A + O = O + A = A$

(*iv*) For $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in F$, there is $B = \begin{bmatrix} -a & -b \\ b & -a \end{bmatrix} \in F$

such that $A + B = O = B + A$

$\therefore$ B is additive inverse of A

(*v*) We know matrix addition is commutative

i.e. for A, B, $\in$ F, we have

$A + B = B + A$.

(*vi*) $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in F$ and $B = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \in F$

we have

$$AB = \begin{bmatrix} a\alpha - b\beta & a\beta + b\alpha \\ -b\alpha - a\beta & -b\beta + a\alpha \end{bmatrix} = \begin{bmatrix} a\alpha - b\beta & a\beta + b\alpha \\ -(a\beta + b\alpha) & a\alpha - b\beta \end{bmatrix} \in F$$

(*vii*) We know matrix multiplication is associative *i.e.* for A, B, C $\in$ F

we have A (BC) = (AB) C

(*viii*) For $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in F$ there is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in F$ such that AI = IA = A

Here I is unity of F.

(*ix*) For $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in F$, there is $B = \frac{1}{a^2 + b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in F$ such that

$$AB = BA = I \qquad \begin{bmatrix} \because & A \neq O \\ \Rightarrow & a \neq 0, \text{ or } b \neq 0 \\ \Rightarrow & a^2 + b^2 \neq 0 \end{bmatrix}$$

$\therefore$ B is inverse of A.

(*x*) Here $AB = \begin{bmatrix} a\alpha - b\beta & a\beta + b\alpha \\ -(a\beta + b\alpha) & a\alpha - b\beta \end{bmatrix}$

and $BA = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a\alpha - b\beta & b\alpha + a\beta \\ -a\beta - b\alpha & -b\beta + a\alpha \end{bmatrix} = \begin{bmatrix} a\alpha - b\beta & b\alpha + a\beta \\ -(b\alpha + a\beta) & a\alpha - b\beta \end{bmatrix}$

$\therefore$ AB = BA.

(*xi*) We know distributive law holds in matrices

$\therefore$ For A, B, C $\in$ F, we have A (B + C) = AB + AC and (B + C) A = BA + CA

Example 3. Show that the set G = {0, 1, 2, 3, 4} forms a field w.r.t. addition and multiplication modulo 5.

Sol. Given G = {0, 1, 2, 3, 4}

Let $x, y, z \in G$

Define $x +_5 y = \begin{cases} x + y & \text{if } x + y < 5 \\ r & \text{if } x + y \geq 5 \end{cases}$

where r is remainder on dividing $x + y$ by 5

So $0 \leq r \leq 4$

$\therefore$ $x +_5 y \in G$

The composition table for addition modulo 5 is

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Properties of addition

(*i*) Clearly all the entries (in each column) belong to G and so G is closed under addition modulo 5

$\therefore$ closure property holds in G.

(*ii*) $\forall\ x, y, z \in G$

The least non-negative remainder remains the same if $(x+y)+z$ or $x+(y+z)$ are divided by 5

$\therefore\ (x +_5 y) +_5 z = x +_5 (y +_5 z)$

$\therefore$ associativity holds for addition modulo 5

(*iii*) For all $x \in G$, these exists $0 \in G$

such that $x +_5 0 = x = 0 +_5 x$ as x is least non-negative remainder when $x+0$ or $0+x$ is divided by 5

$\therefore$ identity element $0 \in G$ exists

(*iv*) For all $x \in G$, there exists $5-x \in G$ if $x \neq 0$

such that $(5-x) +_7 x = 0\ x +_7 (5-x)$

$\therefore$ inverse element $5-x$ of x exists ($x \neq 0$) and inverse of 0 is 0

(*v*) the entries in 1^{st}, 2^{nd}, 3^{rd}, 4^{th} rows are same with the corresponding elements of 1^{st}, 2^{nd}, 3^{rd}, 4^{th} columns respectively.

$\therefore$ addition modulo 5 in G is commutative

Properties of multiplication

Let $G_1 = G - \{0\} = \{1, 2, 3, 4\}$

The composition table for multiplication modulo 5 is

X_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(*i*) Clearly all entries (in each column) belong to G_1 and so G_1 is closed under multiplication modulo 5

$\therefore$ closure property holds

(*ii*) $\forall\ x, y, z \in G_1$

The least positive remainder remains the same if $(x\,y)\,z$ or $x\,(y\,z)$ are divided by 5.

$\therefore \quad (x\,X_5\,y)\,X_5\,z = x\,X_5\,(y\,X_5\,z)$

so associativity holds for multiplication modulo 5

(*iii*) For all $x \in G_1$, there exists $1 \in G_1$

such that $1\,X_5\,x = x\,X_5\,1 = x$

$\Rightarrow$ identity element exists.

(*iv*) For each $x \in G_1$, there is inverse y of x is G_1 such that

$$x\,X_5\,y = y\,X_5\,x = 1$$

Since equation $x\,y \equiv 1 \pmod 5$ has a solution ($\because$ 5 is prime)

Inverses of 1, 2, 3, 4 are 1, 3, 2, 4 respectively

$\Rightarrow$ inverse of each element exists.

(*v*) Also $x\,X_5\,y = y\,X_5\,x$ as $x\,y$ and $y\,x$ leave the same least remainder when divided by 5 positive

$\Rightarrow$ commutativity holds.

(C) Distributive Laws :

$x\,X_5\,(y +_5 z) = x\,X_5\,y + x\,X_5\,z$ and $(y +_5 z)\,X_5\,x = y\,X_5\,x + z\,X_5\,x$

as $x\,X_5\,(y +_5 z) = x\,X_5\,(y + z)$ $[\because\ y +_5 z = y + z \pmod 5]$

= Least positive remainder when $x \times (y + z)$ is divided by 5

= Least positive remainder when $x\,y + x\,z$ is divided by 5

$= x\,y +_5 x\,z = x \times y +_5 x \times z$ $[\because\ x\,X_5\,y = x \times y \pmod 5]$

Similarly $(y +_5 z)\,X_5\,x = y\,X_5\,x + z\,X_5\,x$ can be proved

$\therefore$ G is a field under addition and multiplication modulo 5.

EXERCISE 2.3

1. Prove that the set $Q[\sqrt{2}] = \{a + \sqrt{2}\,b \mid a, b \in Q\}$ where Q is set of rationals, is a field under usual addition and multiplication of reals.
2. Prove that

   (*i*) $(N, +, \cdot)$ is not a field (*ii*) $(Z, +, \cdot)$ is a ring but not a field

   (*iii*) $(Q, +, \cdot)$, $(R, +, \cdot)$ and $(C, +, \cdot)$ are fields.
3. Show that the set of rationals Q is a field under the compositions $\oplus$ and $\odot$ defined as

   $a \oplus b = a + b - 1$ and $a \odot b = a + b - a\,b \quad \forall\ a, b \in Q$.

4. Prove that the set $R = \{(a, b) / a, b \in \text{Reals}\}$ is a field under the addition and multiplication of ordered pairs defined as

$(a, b) + (c, d) = (a + c, b + d)$

$(a, b)(c, d) = (ac - bd, bc + ad) \quad \forall\ (a, b), (c, d) \in R.$

5. Show that the set $F = \{0, 1, 2, \ldots. 6\}$ forms a field w.r.t. addition and multiplication modulo 7.

Theorem : Every field is an integral domain.

Proof. Let R be a field and $a, b \in R$ such that $a \neq 0$ and $ab = 0$.

Since $a \neq 0 \in R \quad \therefore \quad a$ is a unit and hence a^{-1} exists in R. Then

$ab = 0 \quad \Rightarrow \quad a^{-1}(ab) = a^{-1}0 = 0$

$\Rightarrow \quad (a^{-1}a)b = 0$

$\Rightarrow \quad 1 \cdot b = 0$

$\Rightarrow \quad b = 0.$

$\therefore$ R has no zero divisors.

Thus R is a commutative ring with $1 \neq 0$ and without zero divisors.

Hence R is an integral domain.

Note : The converse of above theorem is not true.

For example : The ring **Z** of integers is an integral domain which is not a field as every non-zero integer does not have inverse in **Z** .

But in the following theorem we show that any finite integral domain is a field.

Theorem. Every finite integral domain is a field.

Proof. Let R be a finite integral domain. Suppose $R = \{a_1, a_2, \ldots\ldots, a_n\}$.

Let $a \in R$, $a \neq 0$ and we consider the set $S = \{a a_1, a a_2, \ldots\ldots, a a_n\}$.

Then $S \subseteq R$, since R is closed under product.

If $a a_i = a a_j$ $(1 \leq i, j \leq n)$, then $a_i = a_j$ (as $a \neq 0 \quad \therefore$ by left cancellation law)

$\Rightarrow$ elements of S are distinct. so $o(S) = o(R)$.

As $S \subseteq R \quad \therefore \quad S = R$.

$\Rightarrow$ Now since R contains 1, we have $1 \in S$ i.e. $1 = a a_j$ for some j $(1 \leq j \leq n)$,

$\Rightarrow a$ is unit and since this happens for every non-zero element a of R

$\therefore$ every non-zero element in R is a unit.

Hence R is a field.

Cor. Any finite non-zero ring R without zero-divisors is a division ring.

Theorem. For any positive integer n, Z_n is a field if and only if n is a prime integer.

ILLUSTRATIVE EXAMPLES

Example 1. Find the elements in $\mathbf{Z}_{12}$ which are zero divisors and elements which are not zero divisors.

Sol. Since $\mathbf{Z}_{12} = \{[0], [1], [2], \ldots\ldots, [11]\}$, we see that

$[0] = [2]\,[6] = [3]\,[4] = [8]\,[3] = [9]\,[4] = [10]\,[6]$

Thus, [0], [2], [3], [4], [6], [8], [9] and [10] are zero divisor of $\mathbf{Z}_{12}$.

Also $gcd\,(k, 12) = 1 \Rightarrow k = 1, 5, 7, 11.$ ($\because$ We know that $[x] \in \mathbf{Z}_n$ is a unit iff $gcd\,(x, n)$

$\therefore$ [1], [5], [7] and [11] are units in $\mathbf{Z}_{12}$

and so these elements are not zero divisors.

Example 2. Find the roots of $x^2 + 3x - 4$ in

(*a*) $\mathbf{Z}$ (*b*) $\mathbf{Z}_6$ (*c*) $\mathbf{Z}_4$.

Sol. Let $f(x) = x^2 + 3x - 4 = (x - 1)(x + 4)$

(*a*) Now $f(x) = 0$ in $\mathbf{Z} \Rightarrow (x - 1)(x + 4) = 0$ in $\mathbf{Z}$

$\Leftrightarrow$ $x = 1, -4$ in $\mathbf{Z}$.

(*b*) Now $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6 and multiplication modulo 6

So $f(x) = 0$ in $\mathbf{Z}_6$ iff $(x - 1)(x + 4) = 0$ in $\mathbf{Z}_6$

$x = 1, 2, 4, 5$ are the roots in $\mathbf{Z}_6$.

($\because$ For $(1 - 1)(1 + 4) = 0 \equiv 0 \pmod{}$

$(2 - 1)(2 + 4) = 6 \equiv 0 \pmod{}$

$(4 - 1)(4 + 4) = 24 \equiv 0 \pmod{}$

$(5 - 1)(5 + 4) = 36 \equiv 0 \pmod{}$

Example 3. Prove or disprove that there is an integral domain which has six elements.

Or

Show that an integral domain consisting of six elements does not exists.

Sol. Let R be integral domain of six elements then (R, +) is an abelian group of order 6.

Since 2 | 6 and 3 | 6

$\therefore$ By Cauchy's Theorem in group theory

$\exists$ elements a and b of order 2 and 3 respectively

$\therefore$ $2a = 0$ and $3b = 0$.

Let $a, 2b \in R$, then

$$a(2b) = 2ab = (2a)b = 0 \cdot b = 0.$$

But neither $a = 0$ nor $2b = 0$.

$\Rightarrow$ R has proper zero divisors, which is not possible as R is an integral domain.

Hence there does not exist an integral domain of six elements.

Example 4. Let R be a ring with more than one element. Let for each $a \in R$, there exist a unique b in R such that $aba = a$. Prove that (*i*) $bab = b$ (*ii*) R is a division ring.

Sol. First of all we show that whenever $ax = 0$ then $x = 0$.

Consider $a \neq 0 \in R$. Then

$$a(b+x)a = (ab+ax)a = aba + axa$$

$$= a + 0 \cdot a \qquad [\because ax = 0 \text{ and } aba = a]$$

$$= a + 0 = a$$

$\Rightarrow$ $a(b+x)a = a$.

But b is unique for a such that $aba = a$.

$\therefore$ we have $b + x = b \Rightarrow x = 0$.

Similarly, we can show that whenever $xa = 0$ then $x = 0$.

(*i*) Since $aba = a$ [Pre-multiplying by b]

$\Rightarrow$ $baba = ba$

$\Rightarrow$ $baba - ba = 0$

$\Rightarrow$ $(bab - b)a = 0$ [$\because$ when ever $xa = 0 \Rightarrow x = 0$]

$\Rightarrow$ $bab - b = 0$

$\Rightarrow$ $bab = b$.

(*ii*) Now $aba = a$

$\Rightarrow$ $aba - a = 0$

$\Rightarrow$ $(ab-1)a = 0$

$\Rightarrow$ $ab - 1 = 0$

$\Rightarrow$ $ab = 1$

Similarly $aba = a$

$\Rightarrow$ $aba - a = 0$

$\Rightarrow$ $a(ba-1) = 0$

$\Rightarrow$ $ba - 1 = 0$

$\Rightarrow$ $ba = 1$

Thus $ab = 1 = ba$.

Hence all non-zero elements of R are invertible and so R is a division ring.

Example 5. Let a, b be commutative elements of a ring R of characteristic two, show that

$(a+b)^2 = a^2 + b^2 = (a-b)^2$.

Sol. R is commutative ring of characteristic 2.

let $a, b \in R$

$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a\,a + a\,b + b\,a + b\,b$

$= a^2 + a\,b + b\,a + b^2 = a^2 + 2\,a\,b + b^2$ ($\because$ R is commutative)

$= a^2 + b^2$ ($\because$ ch(R) = 2)

$(a-b)^2 = (a-b)(a-b) = a(a-b) + (-b)(a-b)$

$= a\,a - a\,b - b\,a + b\,b = a^2 - a\,b - b\,a + b^2 = a^2 - 2\,a\,b + b^2$ ($\because$ R is commutative)

$= a^2 + b^2$ ($\because$ ch(R) = 2)

Example 6. Solve the equation $f(x) = x^2 - 5x + 6 = 0$ in the ring $\mathbf{Z}_{12}$.

Sol. Since $f(x) = x^2 - 5x + 6 = 0$

$\Rightarrow \quad (x-2)(x-3) = 0.$

Clearly $x = 2, 3, 6, 11$ satisfy the given equation for

$(2-2)(2-3) = 0 \equiv 0 \pmod{12}$

$(3-2)(3-3) = 0 \equiv 0 \pmod{12}$

$(6-2)(6-3) = 12 \equiv 0 \pmod{12}$

$(11-2)(11-3) = 72 \equiv 0 \pmod{12}$.

Hence $x = 2, 3, 6$ and 11 are the roots of the given equation in $\mathbf{Z}_{12}$.

Example 7. Find the field of quotients of the integral domain $\mathbf{Z}[\sqrt{2}]$.

Sol. Let F be the field of quotients of $\mathbf{Z}[\sqrt{2}] = \{a + \sqrt{2}\,b;\ a, b \in \mathbf{Z}\}$

Then $F = \left\{\frac{l}{m} \mid l, m \in Z[\sqrt{2}], m \neq 0\right\}$

Take $l = a_1 + \sqrt{2}\,b_1, m = a_2 + \sqrt{2}\,b_2$ where $a_1, a_2, b_1, b_2 \in Z$

As $m \neq 0 \Rightarrow a_2 + \sqrt{2}\,b_2 \neq 0$

$\Rightarrow$ a_2 and b_2 cannot be simultaneously zero

$\Rightarrow$ $a_2^2 - 2b_2^2 \neq 0$.

Further $\frac{l}{m} = \frac{a_1+\sqrt{2}\,b_1}{a_2+\sqrt{2}\,b_2} = \frac{a_1+\sqrt{2}\,b_1}{a_2+\sqrt{2}\,b_2} \times \frac{a_2-\sqrt{2}\,b_2}{a_2-\sqrt{2}\,b_2} = \frac{(a_1a_2-2b_1b_2)+\sqrt{2}(a_2b_1-a_1b_2)}{a_2^2-2b_2^2}$

$$= \left(\frac{a_1a_2-2b_1b_2}{a_2^2-2b_2^2}\right) + \sqrt{2}\left(\frac{a_2b_1-a_1b_2}{a_2^2-2b_2^2}\right)$$

$= x + \sqrt{2}\,y$ where $x, y \in Q$

$\therefore$ $F = \{x + \sqrt{2}\,y ; x, y \in Q\} = Q[\sqrt{2}]$.

so that $Q[\sqrt{2}]$ is the field of quotients of $\mathbf{Z}[\sqrt{2}]$.

Example 8. Show for every prime p, the ring $\mathbf{Z}/p\mathbf{Z}$ with the usual modulo operations, is a field.

Sol. We have to show $\mathbf{Z}/p\mathbf{Z} = \{0, 1, 2, ..., p-1\}$ is a field for prime p

We know $\mathbf{Z}/p\mathbf{Z}$ is a finite ring, so to show it is a field it is sufficient to show it is an integral domain ($\because$ each finite integral domain is a field)

Let $x \otimes_p y = 0$ for $x, y \in \mathbf{Z}/p\mathbf{Z}$

$\Rightarrow$ xy is a multiple of p

($\because$ p is prime)

$\Rightarrow$ $p \mid xy$ $\Rightarrow$ $p \mid x$ or $p \mid y$

($\because$ $x, y \in \mathbf{Z}/p\mathbf{Z}$ and $x, y < p$)

$\Rightarrow$ $x = 0$ or $y = 0$

$\therefore$ $\mathbf{Z}/p\mathbf{Z}$ is an integral domain.

Hence $\mathbf{Z}/p\mathbf{Z}$ is a field.

EXERCISE 2.4

1. **(Kapalansky)** Prove that if an element of a ring with unity has more than one right inverses, then the set of its right inverses is infinite.
2. Let R be a ring with identity. Then show that R is of characteristic n if and only if n is the least positive integer such that $n \cdot 1 = 0$.

   i.e., if and only if $o(1) = n$.
3. Show that the characteristic of a finite ring R divides o (R).

4. Let R be a commutative ring with characteristic p, where p is a prime number. Prove that $(a+b)^p = a^p + b^p$, where $a, b \in R$.
5. Prove that the ring of quaternions is a division ring which is not a field.
6. Let R be a finite ring without zero divisors and $o(R) > 1$. Then show that R is a division ring.
7. Let $<G, +>$ be a simple abelian group. Prove that the ring of endomorphisms of G is a division ring.
8. If R_1 and R_2 are integral domains. Is $R_1 \times R_2$ necessarily an integral domain ?
9. Let R_1 and R_2 be two rings. Show that $R_1 \times R_2$ is an integral domain if and only if any one of them is an integral domain and the other contains only a zero element.
10. Suppose R is a ring with unity 1 such that R has no proper zero divisors. Prove that 0 and 1 are the only idempotents in R.
11. Show that in an integral domains R (with unity) the only idempotents are zero and unity.
12. Which of the following sets form an integral domain with respect to ordinary addition and multiplication. If so state which are fields ?

(a) The set of naturals (b) The set of even integers

(c) The set of numbers of form $\sqrt{2}\, a, a \in Q$.

ANSWERS

8. No

12. (a) Neither I.D. nor a field (b) I.D. but not a field (c) Neither I.D. nor a field

3

BOOLEAN ALGEBRA

3.1. Definition (POSETS)

∴ A non-empty set P, together with a binary relation R is said to form a **partially ordered set** or a poset if the following condition holds :

(*i*) **Reflexivity :** $a \, R \, a$ for all $a \in P$

(*ii*) **Anti symmetric :** If $a \, R \, b$ and $b \, R \, a \Rightarrow a = b$, where $a, b \in P$

(*iii*) **Transitive :** If $a \, R \, b, b \, R \, c \Rightarrow a \, R \, c$ for all $a, b, c \in P$

A poset is generally denoted by (P, R).

Remark : For convenience, we generally use the symbol $\leq$ in place of R. Thus whenever we say that P is a poset, it would be understood that $\leq$ is the relation defined on P, unless another symbol is mentioned. We read $\leq$ as less than or equal to (although it may have nothing to do with usual less than or equal to that we are familiar with). Thus $(P, \leq)$ is a poset.

Example. The set N of natural numbers form a poset under the usual $\leq$.

Similarly, the set of integers, rational numbers also form poset under usual $\leq$.

Example. The set **N** of natural numbers under divisibility forms a poset.

Thus here $a \leq b$ mean a/b (a divide b)

3.2. Definition : (Least Upper Bound and Greatest Lower Bound)

Let S be a non-empty subset of a poset P. An element $a \in P$ is called an upper bound of S if $x \leq a$, $\forall x \in S$. Further if a is an upper bound of S such that $a \leq b$ for all other upper bounds b of S then a is called least upper bound (*l.u.b*) or Supremum of S. We write sup S for supermum S.

Similarly, an element $a \in P$ will be called a lower bound of S if $a \leq x \; \forall \; x \in S$ and a will be called the greatest lower bound (*g.l.b*) or Infimum of S (Inf S) if $b \leq a$ for all other lower bounds b of S.

Remark. (*i*) Greatest and least element belong to the set whereas $l \, u \, b$ and $g \, l \, b$ may or may not belong to the set.

e.g., Let $(\mathbf{Z}, \leq)$ be the poset of integers. Let $S = \{\ldots, -2, -1, 0, 1, 2\}$

then Sup S = 2

and S has no Inf as there is no element a such that $a \leq x \; \forall x \in S$.

Definition : (LATTICE)

A poset $(P, \leq)$ is said to be a lattice if every pair of elements have greatest lower bound and least upper bound belongs to P.

i.e. $\forall\ a, b \in P$

$a \vee b \in P$

$a \wedge b \in P$

Note : To prove P to be a lattice we check with the help of operation tables. One for join and other for meet. P is not lattice if at least one $a \vee b$ or $a \wedge b$ does not belong to P where $a, b \in P$.

ILLUSTRATIVE EXAMPLES

Example 1. Write down the operation table for $\vee$ and $\wedge$ for

$L = \{1, 2, 3, 5, 30\}$ under divisibility relation.

Sol. The operation table for $\vee$ and $\wedge$ for the lattice L is given below :

where $a \vee b = l.u.b\ \{a, b\} = l.c.m\ \{a, b\}$ and $a \wedge b = g.l.b\ \{a, b\} = g.c.d\ \{a, b\}$

$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	6	10	30
3	3	6	3	15	30
5	5	10	15	5	30
30	30	30	30	30	30

and

$\wedge$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

Example 2. The set $A = \{1, 2, 3, 4, 6, 12\}$ of factors 12 under divisibility form a lattice.

Sol. In divisibility,

$a \vee b = \text{Sup}\ \{a, b\} = \text{lcm}\ \{a, b\}$

$a \wedge b = \text{Inf}\ \{a, b\} = \text{gcd}\ \{a, b\}$

Operation tables are :

$\vee$	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

$\wedge$	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

From tables

$\forall\ a, b \in A$

$a \vee b \in A$

and $a \wedge b \in A$

So set A under divisibility is a lattice.

Example 3. Prove that poset P = {2, 3, 4, 6} under divisibility is not a lattice.

Sol. In divisibility

Sup $\{a, b\}$ = lcm $\{a, b\}$

Now $3, 4 \in P$

Sup $\{3, 4\}$ = lcm $\{3, 4\}$

$= 12 \notin P$

So P is not a lattice.

3.3. Definition (Boolean Algebra as Lattices)

A Boolean algebra is a distributive, complemented lattice having at least two element namely the **least element** (generally denoted by 0) and the **greatest element** (generally deviated by 1).

Since the complement of each element in a Boolean algebra is unique. Thus a complementation is a valid **unary operation** over the set under discussion. Therefore we list it together with other two operations (join ∨ and meet ∧). This will make a distinction between lattices and lattices which are Boolean algebra. A Boolean algebra is generally devoted by (B, ∨, ', 0, 1), where B is a non-empty set having atleast two elements with three operations (join (∨), meet (∧) and complementation (')).

Definition. A Boolean algebra $\mathcal{B}$ consists of a set B together with two binary operations ∧ and ∨ on $\mathcal{B}$, a unary operation ' on B and two specific elements 0 and 1 of B such that the following laws hold. We write it is $\mathcal{B}$ = (B, ∨, ∧, ', 0, 1).

(a) **Associative Laws :** For all a, b, c ∈ B.

$(a \vee b) \vee c = a \vee (b \vee c)$ and $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

(b) **Commutative Laws :** For all $a, b, \in B$

$(a \vee b) = (b \vee a)$ and $(a \wedge b) = (b \wedge a)$

(c) **Distributive Laws :** For all $a, b, c \in B$

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(d) **Identity Laws :** For all $a \in B$

$(a \vee 0) = a$ and $(a \wedge 1) = a$

(e) **Complement Laws :** For all $a \in B$

$(a \vee a') = 1$ and $(a \wedge a') = 0$

Example 1. Let B = {0, 1} be a set. The operation ∨, ∧ and ' on B are given by

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

'	
0	1
1	0

Then (B, ∨, ∧, ', 0, 1) satisfies all the properties listed in 2.1.2. This is one of the **simplest example of a two-element Boolean algebra.**

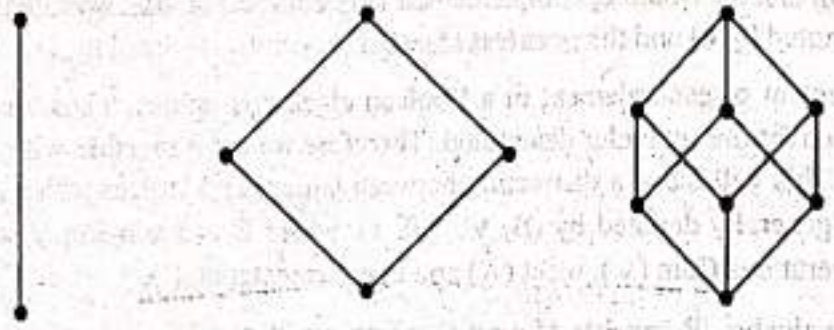
Example 2. Let P(X) denote the Power set of X. Define two binary operation $\vee$ and $\wedge$ and the unary operation ' on P(X) by

$$A \vee B = A \cup B,\ A \wedge B = A \cap B \text{ and } A' = X - A \text{ for all } A, B \in P(X)$$

where $\cup$, $\cap$ and $X - A$ denote the union, intersection and complementation in a set theory. Then $(P(X), \cup, \cap, ', \phi, X)$ form a Boolean algebra.

Note. If X has n elements, then P(X) has 2^n elements and the diagram of the Boolean algebra is an n-cube. The Partial order relation on P(X) corresponding to the operation $\cup$, $\cap$ is the inclusion $\subseteq$.

The following are the diagram of the Boolean algebra P(X) when X has one element, two elements and three elements respectively.



Boolean algebra for singleton set

Boolean algebra for set having two elements

Boolean algebra for set having three elements

Example 3. Let n be a positive integer and D_n denote the set of all positive divisiors of n then (D_n, lcm, gcd, ', 1, n) form a Boolean algebra if and only if n is square free, in the sense that it has no factor of the form p^2, where p is a prime.

Sol. We know that D_n is a bounded distributive lattice. Therefore, we need to show that it is complemented lattice.

Let $n = p_1 p_2 \ldots\ldots p_m$ be the product of distinct primes

Let d be any divisor of n.

Let $d = p_{i_1} p_{i_2} \ldots\ldots p_{i_k}$ where $p_{i_r} \in \{p_1, p_2, \ldots\ldots, p_m\}$

Take $d' = p_{j_1} p_{j_2} \ldots\ldots p_{j_s}$ be the product of all the prime divisors of n not dividing d, then

$$g.c.d.\ \{d, d'\} = 1 \text{ and } l.c.m\ \{d, d'\} = \frac{d\,d'}{g\,c\,d\,\{d, d'\}} = d\,d' = n$$

$\therefore$ d' is the complement of d

Hence D_n is a complemented lattice and so it is a Boolean Algebra.

Conversely. Let D_n be a Boolean Algebra.

To show that n is square free.

Let p be a prime such that $p^a \mid n$, where $a > 1$, then

p cannot have a complement in D_n because if $(p, d) = 1$ for some $d \in D_n$ then

$p \nmid d \quad \therefore \quad (p^a, d) \neq 1$

Thus $p^a . d = [p^a, d]\,(p^a, d)$

$= [p^a, d] . 1 \qquad [\because\ a\,b = [a, b]\,(a, b)]$

$\leq n$

Hence $p . d < p^a\, d \leq n \quad$ *i.e.* $\quad p . d < n$

Thus $[p, d] = \dfrac{p\,d}{(p, d)} = p\,d < n$ and so d cannot be a complement of p.

So p does not have a complement in D_n and so D_n is not a Boolean algebra, a contradiction.

Hence n is a square free *i.e.*, n is a product of distinct primes.

Remark. In view of above example, we can easily checked that D_{30}, D_{66}, D_{210}, D_{646} are Boolean algebra, where as D_4, D_8, D_{20}, D_{25}, are not Boolean algebra.

Example 4. Let S denote the set of all statements formula involving a single variable. The algebraic system (S, ∨, ∧, ~, **F**, **T**) is a Boolean algebra. Here the binary operation ∨ and ∧ denote the disjunction and conjunction respectively and the unary operation ~ denote by negation. The element F and T denote the formula which are contradiction and tautologies respectively.

Example 5. Let X be any topological space and Let CO(X) be the family of sets that are simultaneously closed and open (i.e. clopen sets). The family CO(X) is a Boolean algebra w.r.t. the operation intersection as meet, union as join, $a' = X \setminus a$, $0 = \phi$ and $1 = X$.

Theorem. In a Boolean algebra $(B, \vee, \wedge, ', 0, 1)$;

if $\quad a \vee b = 1 \quad$ and $\quad a \wedge b = 0, \quad$ then $b = a'$

i.e. the complement of an element in a Boolean algebra is unique.

Proof. Suppose that $a \vee b = 1$ and $a \wedge b = 0$

Now $\quad b = b \vee 0 \qquad$ [Identity law]

$= b \vee (a \wedge a') \qquad$ [Complement law]

$= (b \vee a) \wedge (b \vee a') \qquad$ [Distributive law]

$= (a \vee b) \wedge (b \vee a') \qquad$ [Commutative law]

$= 1 \wedge (b \vee a') \qquad$ [Given]

$= b \vee a' \qquad$ [Identity law]

Thus $\quad b = b \vee a' \qquad \ldots(1)$

Again $\quad a' = a' \vee 0 \qquad$ [Identity law]

$= a' \vee (a \wedge b) \qquad$ [Given]

$= (a' \vee a) \wedge (a' \vee b)$ [Distributive Law]

$= 1 \wedge (a' \vee b)$ [Complement Law]

$= a' \vee b$ [Identity law]

$= b \vee a'$ [Commulative law]

Thus $a' = b \vee a'$ ...(2)

from (1) and (2), we get $b = a'$

Corollary. In a Boolean algebra $(B, \vee, \wedge, ', 0, 1)$, if $a \vee b = 1$ and $a \wedge b = 0$ then $b = a'$ also $a' = b$.

Proof. This follows from above Theorem and commutatively laws in B.

Thus in a Boolean algebra $(B, \vee, \wedge, ', 0, 1)$, we have

$0' = 1$ and $1' = 0$

Proof. Since $0 \vee 1 = 1$ and $0 \wedge 1 = 0$

$\therefore$ By Corollary (1), we have $0' = 1$ and $1' = 0$

Theorem [DeMorgan Law's]

For any a and b in a Boolean algebra $(B, \vee, \wedge, ', 0, 1)$, we have

(*i*) $(a \vee b)' = a' \wedge b'$

(*ii*) $(a \wedge b)' = a' \vee b'$

Proof. We have

$$(a \vee b) \vee (a' \wedge b') = [(a \vee b) \vee a'] \wedge [(a \vee b) \vee b'] = [(a \vee a') \vee b] \wedge [a \vee (b \vee b')]$$
$$= [1 \vee b] \wedge [a \vee 1]$$
$$= 1 \wedge 1$$
$$= 1$$

also $(a \vee b) \wedge (a' \wedge b') = [a \wedge (a' \wedge b')] \vee [b \wedge (a' \wedge b')] = [(a \wedge a') \wedge b'] \vee [(b \vee b') \wedge a']$
$$= [0 \wedge b'] \vee [0 \wedge a']$$
$$= 0 \vee 0$$
$$= 0$$

$\therefore$ By Theorem, we have $(a \vee b)' = a' \wedge b'$

Similarly, $(a \wedge b) \vee (a' \vee b') = [a \vee (a' \vee b')] \wedge [b \wedge (a' \vee b')]$
$$= [(a \vee a') \wedge b'] \wedge [(b \vee b') \vee a'] = [1 \vee b'] \wedge [1 \vee a']$$
$$= 1 \wedge 1$$
$$= 1$$

Also $(a \wedge b) \wedge (a' \vee b') = [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b'] = [(a \wedge a') \wedge b] \vee [a \wedge (b \wedge b')]$
$$= [0 \wedge b] \vee [a \wedge 0]$$
$$= 0 \vee 0$$
$$= 0$$

$\therefore$ By Theorem , we have

$$(a \wedge b)' = a' \vee b'$$

Theorem. In a Boolean algebra $(B, \vee, \wedge, ', 0, 1)$, the following properties hold

(a) **Idempotent Laws.** For all $a \in B$

$a \vee a = a$ and $a \wedge a = a$

(b) **Bound Laws.** For all $a \in B$

$a \vee 1 = 1$ and $a \wedge 0 = 0$

(c) **Absorption Laws.** For all $a, b, \in B$

$a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$

(d) **Involution Laws.** For all $a \in B$

$(a')' = a$

Proof. (a)

$$\begin{aligned} a &= a \vee a && \text{[Identity Law]} \\ &= a \vee (a \wedge a') && \text{[Complement Law]} \\ &= (a \vee a) \wedge (a \vee a') && \text{[Distributive Law]} \\ &= (a \vee a) \wedge 1 && \text{[Complement Law]} \\ &= a \vee a && \text{[Identity Law]} \end{aligned}$$

Thus $a \vee a = a$ [Identity Law]

Again

$$\begin{aligned} a &= a \vee 1 && \text{[Complement Law]} \\ &= a \wedge (a \vee a') && \text{[Distributive Law]} \\ &= (a \wedge a) \vee (a \wedge a') && \text{[Complement Law]} \\ &= (a \wedge a) \vee 1 && \text{[Identity Law]} \\ &= a \wedge a \end{aligned}$$

$a \wedge a = a$ [Identity Law]

(b) Now

$$\begin{aligned} a \vee 1 &= (a \vee 1) \wedge 1 && \text{[Complement Law]} \\ &= (a \vee 1) \wedge (a \vee a') && \text{[Distributive Law]} \\ &= [(a \vee 1) \wedge a] \vee [(a \vee 1) \wedge a'] \\ &= [(a \wedge a) \vee (1 \wedge a)] \vee [(a \wedge a') \wedge (1 \wedge a')] \\ &= [a \vee a] \vee [0 \vee a'] && \text{[Idempotent, identity and Complement law]} \\ &= a \vee a' && \text{[Complement Law]} \\ &= 1 \end{aligned}$$

Thus $a \vee 1 = 1$ [Identity Law]

Again

$$\begin{aligned} a \wedge 0 &= (a \wedge 0) \vee 0 && \text{[Complement Law]} \\ &= (a \wedge 0) \vee (a \wedge a') && \text{[Distributive Law]} \\ &= [(a \wedge 0) \vee a] \wedge [(a \wedge 0) \vee a'] \end{aligned}$$

$= [(a \vee a) \wedge (0 \vee a)] \wedge [(a \vee a') \wedge (0 \vee a')]$

$= [a \wedge a] \wedge [1 \wedge a']$ [Idempotent, identity and Complement law]

$= a \wedge a'$

$= 0$

Thus $a \wedge 0 = 0$

(c) Now $a \vee (a \wedge b) = (a \wedge 1) \vee (a \wedge b)$ [Identity Law]

$= a \wedge (1 \vee b)$ [Distributive Law]

$= a \wedge (b \vee 1)$ [Commulative Law]

$= a \wedge 1$ [Bounded Law]

$= a$

Thus $a \vee (a \wedge b) = a$

Again $a \wedge (a \vee b) = (a \vee 0) \wedge (a \vee b)$ [Identity Law]

$= a \vee (0 \wedge b)$ [Distributive Law]

$= a \vee (b \wedge 0)$ [Commulative Law]

$= a \vee 0$ [Bounded Law]

$= a$

Thus $a \wedge (a \vee b) = a$

(d) Since $x' \vee x = x \vee x' = 1$ and $x' \wedge x = x \wedge x' = 0$

Thus $x' \vee x = 1$ and $x' \wedge x = 1$

Therefore by Complement law, we have

$(x')' = x$

3.4. Principle of Duality for Boolean Algebra

Let (B, $\vee$, $\wedge$, ', 0, 1) be a Boolean algebra (under $\leq$) and S be a true statement for B.If S* is obtained from S by replacing $\leq$ by $\geq$, $\vee$ by $\wedge$, $\wedge$ by $\vee$, 0 by 1 and 1 by 0, then S* is also a true statement. We say that the statement S* is dual of the statement S and Vice Versa.

For example : If (B, $\vee$, $\wedge$, ', 0, 1) be a Boolean algebra, then following statement 1′ to 10′ are dual of the statement 1 to 10 and vice versa.

(1)	$a \vee b = b \vee a$	(1)′	$a \wedge b = b \wedge a$
(2)	$a \vee (b \vee c) = (a \vee b) \vee c$	(2)′	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$
(3)	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	(3)′	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
(4)	$a \vee 0 = 0 \vee a = a$	(4)′	$a \wedge 1 = 1 \wedge a = a$
(5)	$a \vee a' = 1$	(5)′	$a \wedge a' = 0$

(6) $a \vee a = a$ (6)' $a \wedge a = a$

(7) $a \vee 1 = 1$ (7)' $a \wedge 0 = 0$

(8) $a \vee (a \wedge b) = a$ (8)' $a \wedge (a \vee b) = a$

(9) $(a \vee b)' = a' \wedge b'$ (9)' $(a \wedge b)' = a' \vee b'$

(10) $(a')' = a$ (10)' $(a')' = a$

Remark. (1) The above statement 1 to 10 and (1)' to (10)' are known as **Boolean Identities** (or Basic Boolean algebra laws).

Remark. (2) The notation for operations in Boolean algebra is derived from the algebra of logic. However, other notations are used. These are summarized in the following chart :

Test (Mathematician's Notation)	Set Notation	Computer Designer's Notation	Read as
$\vee$	$\cup$	$+$	Join or Sum
$\wedge$	$\cap$	$\cdot$	meet or and or Product
$'$	C	$/$	Complement
$\leq$	$\subseteq$	$\leq$	

Mathemetician most frequency use the notation of text and on occasion use the set notation for Boolean algebra. Computer designers use the notation (+) and (·) as most of the computers did not have symbol $\vee$, $\wedge$.

Thus in the letter notation **BOOLEAN IDENTITIES** looks like as :

(1) $a + b = b + a$ (1)' $a \cdot b = b \cdot a$

(2) $a + (b + c) = (a + b) + c$ (2)' $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ (3)' $a + b \cdot c = (a + b) \cdot (a + c)$

(4) $a + 0 = 0 + a = a$ (4)' $a \cdot 1 = 1 \cdot a = a$

(5) $a + a' = 1$ (5)' $a \cdot a' = 0$

(6) $a + a = a$ (6)' $a \cdot a = a$

(7) $a + 1 = 1$ (7)' $a \cdot 0 = 0$

(8) $a + a \cdot b = a$ (8)' $a \cdot (a + b) = a$

(9) $(a + b)' = a' \cdot b'$ (9)' $(a \cdot b)' = a' + b'$

(10) $(a')' = a$ (10)' $(a')' = a$

Example 1. Prove the following **BOOLEAN IDENTITIES :**

(a) $a + (a' \cdot b) = a + b$ (b) $a \cdot (a' + b) = a \cdot b$

(c) $(a \cdot b) + (a \cdot b') = a$ (d) $(a \cdot b \cdot c) + (a \cdot b) = a \cdot b$

Sol. (*a*) $a + (a' \cdot b) = (a + a') \cdot (a + b)$

$= 1 \cdot (a + b)$

$= a + b$

Thus $a + (a' \cdot b) = a + b$

(*b*) $a \cdot (a' + b) = a \cdot a' + a \cdot b$

$= 0 + a \cdot b$

$= a \cdot b$

(*c*) $(a \cdot b) + (a \cdot b') = a \cdot (b + b')$

$= a \cdot 1$

$= a$

Thus $(a \cdot b) + (a \cdot b') = a$

(*d*) $(a \cdot b \cdot c) + (a \cdot b) = (a \cdot b) \cdot c + (a \cdot b) \cdot 1$

$= (a \cdot b)(c + 1)$

$= (a \cdot b) \cdot 1$

$= a \cdot b$

Example 2. In any Boolean algebra, show that

(*i*) $a = b \Leftrightarrow ab' + a'b = 0$ (*ii*) $a = 0 \Leftrightarrow ab' + a'b = b$

Sol. (*i*) Now $ab' + a'b = 0$

$\Leftrightarrow ab' + bb' + a'a + a'b = 0$ [$\because a'a = 0 = bb'$]

$\Leftrightarrow (a + b)b' + a'(a + b) = 0$

$\Leftrightarrow (a + b)b' + (a + b)a' = 0$

$\Leftrightarrow (a + b)(a' + b') = 0$

$\Leftrightarrow (a + b)(ab)' = 0$

$\Leftrightarrow a + b = ab$ [$\because xx' = 0$ always]

$\Leftrightarrow a = b$ [$\because a + a = a = a \cdot a$]

(*ii*) Now $ab' + a'b = b$

$\Leftrightarrow ab' + bb' + a'a + a'b = b$

$\Leftrightarrow (a + b)b' + a'(a + b) = b$

$\Leftrightarrow (a + b)b' + (a + b)a' = b$

$\Leftrightarrow (a + b)(a' + b') = b \cdot 1$ [$\because b \cdot 1 = b$]

$\Leftrightarrow a + b = b$ and $a' + b' = 1$

$\Leftrightarrow a = 0$ and $a' = 1$ [$\because 0 + b = b$, $1 + b' = 1$]

$\Leftrightarrow a = 0$

Example 3. Simplify the following Boolean expression

(a) $(a \cdot b)' + (a + b)'$ (b) $(a' \cdot b' \cdot c) + (a \cdot b' \cdot c) + (a \cdot b' \cdot c')$

(c) $(a \cdot c) + c + [(b + b') \cdot c]$ (d) $(1 \cdot a) + (0 \cdot a')$

Sol. (a) $(a \cdot b)' + (a + b)' = [a \cdot b(a + b)]'$ $[\because x' + y' = (x \cdot y)']$

(b) $(a' \cdot b' \cdot c) + (a \cdot b' \cdot c) + (a \cdot b' \cdot c')$

$= [(a' \cdot (b' \cdot c)) + (a \cdot (b' \cdot c))] + (a \cdot b' \cdot c') = [(a' + a) b' c] + (a \cdot b' c') = (1 \cdot b' c) + (a \cdot b' c')$

$= cb' + ac' b' = (c + ac')b' = (c + a)(c + c')b' = (c + a) \cdot 1 \cdot b' = (c + a) b' = c \cdot b' + a \cdot b'$

(c) $a \cdot c + c + [(b + b') \cdot c] = a \cdot c + c + [1 \cdot c]$

$= a \cdot c + c + c = a \cdot c + c = (a + 1) \cdot c = 1 \cdot c = c$

(d) $(1 \cdot a) + (0 \cdot a') = a + a'$

$= 1$

Example 4. Prove by using Boolean algebra that

(i) $A + B \,.\, C = (A + B) \,.\, (A + C)$ (ii) $A + \overline{A} \,.\, C = A + C$

where $\overline{A}$ is the complement of A, for all A, B, C in a Boolean algebra.

Sol. (i) L.H.S. $= A + B \,.\, C = A \,.\, 1 + B \,.\, C$

$= A\,(1 + C) + B \,.\, C$ $[\because 1 + C = 1]$

$= A \,.\, 1 + A \,.\, C + B \,.\, C = A \,.\, (1 + B) + A \,.\, C + B \,.\, C = A + A \,.\, B + A \,.\, C + B \,.\, C$

$= A \,.\, A + A : B + A \,.\, C + B \,.\, C$ $[\because A \,.\, A = A]$

$= A \,.\, (A + B) + (A + B) \,.\, C = (A + B) \,.\, A + (A + B) \,.\, C$

$= (A + B) \,.\, (A + C) = \text{R.H.S.}$

(ii) L.H.S. $= A + \overline{A}\, C = (A + \overline{A}) \,.\, (A + C)$ [Using (i)]

$= 1 \,.\, (A + C)$ $[\because A + \overline{A} = 1]$

$= A + C = \text{R.H.S.}$

Example 5. Reduce the following using rules of Boolean algebra.

(i) $\overline{A \,.\, \overline{B} + ABC} + A\,(B + A\overline{B})$ (ii) $AB + A\overline{C} + \overline{A}\,\overline{B}\,C\,(AB + C)$

Sol. (i) Now $A\,(B + A\,\overline{B}) = A\,(B + A) \,.\, (B + \overline{B})$

$= A\,(B + A) \,.\, 1$ $[\because B + \overline{B} = 1]$

$= AB + A \,.\, A = AB + A$

$= A\,(B + 1) = A \,.\, 1$ $[\because B + 1 = 1]$

$= A$

Also $A\,\overline{B} + ABC = A\,(\overline{B} + BC) = A\,(\overline{B} + B)\,(\overline{B} + C)$

$= A \,.\, 1\,(\overline{B} + C)$

$= A\,(\overline{B} + C) = A\,\overline{B} + AC$

$\therefore \quad \overline{A\overline{B}+ABC} = \overline{A\overline{B}+AC} = \overline{A\overline{B}}.\overline{AC}$ $[\because (a+b)' = a'.b']$

$= (\overline{A}+\overline{(\overline{B})}).(\overline{A}+\overline{C})$

$= (\overline{A}+B)(\overline{A}+\overline{C})$ $[\because \overline{(\overline{B})} = B]$

$= \overline{A}+B\overline{C}$

Thus $\overline{A\overline{B}+ABC}+A(B+A\overline{B}) = A+\overline{A}+B\overline{C} = 1+B\,\overline{C}$

$= \overline{B}+B+B\overline{C} = \overline{B}+B(1+\overline{C}) = \overline{B}+B.1 = \overline{B}+B = 1$

Hence $\overline{A.\overline{B}+ABC+A(B+A\overline{B})} = \overline{1} = 0.$

(ii) $AB+A\overline{C}+\overline{A}\,\overline{B}C(AB+C) = AB+A\overline{C}+\overline{A}\,\overline{B}CAB+\overline{A}\,\overline{B}CC$

$= AB+A\overline{C}+A\overline{A}B\overline{B}C+\overline{A}\,\overline{B}C$ $[\because x.x = x]$

$= AB+A\overline{C}+0.0.C+\overline{A}\,\overline{B}C$ $[xx' = 0]$

$= AB+A\overline{C}+0+\overline{A}\,\overline{B}C = AB+A\overline{C}+\overline{A}\,\overline{B}C.$

Example 6. Using Boolean algebra, show that

$$abc+abc'+ab'c+a'bc = ab+bc+ca.$$

Sol. L.H.S. $= abc+abc'+ab'c+a'bc = ab(c+c')+ab'c+a'bc$

$= ab.1+ab'c+a'bc = ab+ab'c+a'bc = a(b+b'c)+a'bc$

$= a(b+b')(b+c)+a'bc = a.1.(b+c)+a'bc$

$= ab+ac+a'bc = ab+(a+a'b)c = ab+(a+a')(a+b)c$

$= ab+1.(a+b)c = ab+ac+bc =$ R.H.S.

Remark: We represent $a \oplus b = ab' + a'b$ in XOR-gate

Example 7. Using Boolean algebra, show that

(i) $xy+xz+yz = xy+(x \oplus y)z$ *(ii)* $x'y'z+x'yz'+xy'z'+xyz = x \oplus y \oplus z.$

Sol. *(i)* R.H.S. $= xy+(x \oplus y)z = xy+(x'y+xy')z$

$= xy+x'yz+xy'z = xy(1+z)+x'yz+xy'z$ $[\because 1+z = 1]$

$= xy+xyz+x'yz+xy'z = xy+x'yz+xz(y+y')$

$= xy+x'yz+xz$ $[\because y+y' = 1]$

$= y(x+x'z)+xz = y(x+x')(x+z)+xz = y(x+z)+xz$

$= xy+yz+xz =$ L.H.S.

(ii) R.H.S. $= x \oplus y \oplus z$

$= (xy'+x'y) \oplus z = (xy'+x'y)z'+(xy'+x'y)'z$

$= xy'z'+x'yz'+((xy')'.(x'y)')z$ $[\because (a+b)' = a'.b']$

$= x\,y'\,z' + x'\,y\,z' + (x' + y).(x + y')\,z$ $[\because (a.b)' = a' . b']$

$= x\,y'\,z' + x'\,y\,z' + (x'\,x + x'\,y' + y\,x + y\,y')\,z$

$= x\,y'\,z' + x'\,y\,z' + (x'\,y' + x\,y)\,z$ $[\because a\,a' = 0]$

$= x\,y'\,z' + x'\,y\,z' + x'\,y'\,z + x\,y\,z$

$=$ L.H.S.

EXERCISE 3.1

1. If D_n denotes the set of all positive divisions of n ($n \in \mathbb{N}$). Show that D_6, D_{10}, D_{15}, D_{30} are Boolean algebra where as D_4, D_{12}, D_{18}, are not Boolean algebra.
2. Let $(X, \mathcal{T})$ be a topological space such that $A, A^c \in \mathcal{T}$ for every $A \in \mathcal{T}$ Show that $(\mathcal{T}, \cap, \cup, ^c, \phi, X)$ is Boolean algebra.
3. Prove that in a Boolean algebra B, the following conditions are equivalent
   $(i)\ x \le y\ (ii)\ x \wedge y' = 0\ (iii)\ x' \vee y = 1\ (iv)\ x \wedge y = x$ and $(v)\ x \vee y = y$ for all $x, y \in B$.
4. Show that $a \vee (a' \wedge b) = a \vee b$ and $a \wedge (a' \vee b) = a \wedge b$ in a boolean algebra.
5. Reduce the following in boolean algebra.
   $(i)\ x \wedge (x' \vee y)$ $(ii)\ (x' \wedge y' \wedge z') \vee (x' \wedge y' \wedge z) \vee (x \wedge y')$
   $(iii)\ (x \wedge y) \vee (x' \wedge z) \vee (y \wedge z)$
6. Prove by using Boolean algebra
   $(i)\ x + x'z = x + z$ $(ii)\ xy + xy' = x$ $(iii)\ (x + y) \cdot (x + y') = x$
   $(iv)\ xyz + x'y + xyz' = y$ $(v)\ xz + zx'y = z(x + y)$ $(vi)\ (x + y)' \cdot (x' + y')' = 0$
7. Using Boolean identities, show that
   $(a)\ [a(b' + c)]' [b' + (ac')']' = abc'$ $(b)\ a'[(b' + c)' + (bc)] + [(a + b')' c] = a'b$
8. In any Boolean algebra, show that
   $(i)\ (a + b')(b + c')(c + a') = (a' + b)(b' + c)(c' + a)$
   $(ii)\ (a + b)(a' + c) = ac + a'b = ac + a'b + bc$
   $(iii)\ a \le b \Rightarrow a + bc = b(a + c)$

ANSWERS

5. $(i)\ x \wedge y$ $(ii)\ (x' \wedge z) \vee (x \wedge y')$ $(iii)\ (x \wedge y) \vee (x' \wedge z)$

3.5. Boolean Expressions or Boolean forms

Definition. Boolean Polynomial (Boolean expression, Boolean form or Boolean formula)

Let $x_1, x_2, \ldots\ldots, x_n$ be a set of n variables (or symbols). A Boolean polynomial (Boolean expression, Boolean form or Boolean formula) $f(x_1, x_2, \ldots\ldots, x_n)$ in the variables $x_1, x_2, \ldots\ldots, x_n$ is defined recursively as follows :

(1) The symbols 0 and 1 are Boolean polynomials.

(2) $x_1, x_2, \ldots\ldots, x_n$ are all Boolean polynomials.

(3) If $f(x_1, x_2, \ldots\ldots, x_n)$ and $g(x_1, x_2, \ldots\ldots, x_n)$ are two Boolean polynomials, then so are $f(x_1, x_2, \ldots\ldots, x_n) \vee g(x_1, x_2, \ldots\ldots, x_n)$ and $f(x_1, x_2, \ldots\ldots, x_n) \wedge g(x_1, x_2, \ldots\ldots, x_n)$

(4) If $f(x_1, x_2, \ldots\ldots, x_n)$ is a Boolean polynomial, then so is

$(f(x_1, x_2, \ldots\ldots, x_n))'$

(5) There are no Boolean polynomial in the variable $x_1, x_2, \ldots\ldots, x_n$ other than those obtained in accordance with rule 1 through 4.

Thus Boolean expression is an expression formed from the given variables using Boolean expressions $\vee$, $\wedge$ and $'$.

For example : For the variable x, y, z the expressions

$$f_1(x, y, z) = (x \vee y) \wedge z$$

$$f_2(x, y, z) = (x \vee y') \vee (y \wedge 1)$$

$$f_3(x, y, z) = [x \vee (y' \wedge z)] \vee [x \wedge (y \wedge 1)]$$

$$f_3(x, y, z) = (x \vee y') \wedge (x \wedge y)'$$

are Boolean expressions.

Note that a Boolean expression in n variables may or may not contain all the n variables.

Definition (Equivalent Boolean Expressions)

Two Boolean expression $f_1(x_1, x_2, \ldots\ldots, x_n)$ and $f_2(x_1, x_2, \ldots\ldots, x_n)$ are said to be equivalent if they assume the same value for every assignment of values to the n variables.

For example. The expression $f_1(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3')$

and $f_2(x_1, x_2, x_3) = x_1 \wedge (x_2 \vee x_3')$ are equivalent.

x_1	x_2	x_3	x_3'	$x_1 \wedge x_2$	$x_1 \wedge x_3'$	$x_2 \wedge x_3'$	f_1	f_2
0	0	0	1	0	0	1	0	0
0	0	1	0	0	0	0	0	0
0	1	0	1	0	0	1	0	0
0	1	1	0	0	0	1	0	0
1	0	0	1	0	1	1	1	1
1	0	1	0	0	0	0	0	0
1	1	0	1	1	1	1	1	1
1	1	1	0	1	0	1	1	1

Since $f_1(x_1, x_2, x_3)$ and $f_2(x_1, x_2, x_3)$ assume the same value for every assignment of the values of the variables x_1, x_2 and x_3. So $f_1 = f_2$.

Definition (Boolean function)

Let $(B, \vee, \wedge, ', 0, 1)$ be a boolean algebra. A function from B^n to B called **boolean function** it can be specified by a boolean expression of n variables.

Definition (Minterm or complete product or a Fundamental product)

A Boolean expression of n variables $x_1, x_2, \ldots, x_n$ is said to be **minterm** or **complete product or a fundamental product** of n variables if it is of the forms $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \ldots \wedge \tilde{x}_n$, where $\tilde{x}_i$ denotes either x_i or x_i'.

Observe that each minterm is completely determined by a sequence of 0's and 1's of length n, and any such sequence determines a number between 0 and $2^n - 1$ in binary representation.

A particular minterm will be denoted by $\min_j$ or m_j if the associated sequence of its exponent gives the number j in binary representation (Here $0 \le j \le 2^n - 1$). Thus, we have 2^n minterms in n variables denoted by $m_0, m_1, \ldots, m_{2^n - 1}$. For example, in three variables $m_5 = x_1 \wedge x_2' \wedge x_3$, become 5 in the binary representation 1 0 1.

Also, these minterms satisfy the following fundamental properties

(i) $m_i \wedge m_j = 0$ if $i \ne j$

(ii) $\bigvee_{i=0}^{2^n - 1} = m_0 \vee m_1 \vee \ldots \vee m_{2^n - 1} = 1$.

Definition (Maxterm)

A Boolean expression of n variables $x_1, x_2, \ldots, x_n$ is said to be **maxterm** if it is of the form $\tilde{x}_1 \vee \tilde{x}_2 \vee \ldots \vee \tilde{x}_n$, when $\tilde{x}_i$ denotes either $\tilde{x}_i$ or x_i'.

Similarly the maxterm satisfy the following fundamentals properties :

(i) $M_i \vee M_j = 1$ if $i \ne j$

(ii) $\bigvee_{i=1}^{2^n - 1} M_i = M_1 \wedge M_2 \wedge \ldots \wedge M_{2^n - 1} = 0$.

There are 2^n maxterm in n variables denoted by $M_0, M_1, \ldots, M_{2^n - 1}$.

Definition. (Disjunctive Normal form or Sum of Product or SOP) or DNP

A boolean expression over two-valued Boolean algebra $(\{0, 1\}, \vee, \wedge, ', 0, 1)$ is said to be in disjunctive normal form (or sum of Product) if it is join of minterms.

For example : $(x_1' \wedge x_2 \wedge x_3) \vee (x_1' \wedge x_2' \wedge x_3') \vee (x_1 \wedge x_2 \wedge x_3)$ or

$x_1' x_2' x_3 + x_1' x_2' x_3' + x_1' x_2 x_3 = \Sigma m(1, 0, 7)$

is a boolean expression in disjunctive normal form of three minterms.

Definition (Conjunctive normal form or Product-of-Sum-or-POS)-CNP

A boolean expression over two-value Boolean algebra $(\{0, 1\}, \vee, \wedge, ', 0, 1)$ is said to be in conjunctive normal form (or Product of sum) if it is meet of maxterms.

For example. $(x_1 \vee x_2' \vee x_3') \wedge (x_1 \vee x_2 \vee x_3') \wedge (x_1' \vee x_2' \vee x_3')$ Or

$(x_1 + x_2' + x_3')(x_1 + x_2 + x_3')(x_1' + x_2' + x_3') = \Pi M(4, 6, 0)$

is a boolean expression in conjunctive normal form of three variables.

Obtaining Boolean expression in Disjunctive Normal form and conjunctive normal form

(1) A Boolean expression can be obtained in **disjunctive normal form** corresponding to this function by having a **minterm** corresponding to each ordered n-table of 0 and 1 for which the value of the function is 1.

(2) A Boolean expression can be obtained in **conjunctive normal form** corresponding to this function by having a **maxterm** corresponding to 0 and 1 at which the value of function is 0.

Remark : Boolean function represented as a sum of minterms or product of maxterms are said to be in canonical form.

Example 1. Simplify the Boolean expression

$$f(x, y, z) = (x' \wedge z) \vee (y \wedge z) \vee (y \wedge z')$$

and write in minterm normal form.

Sol.

$$\begin{aligned} f(x, y, z) &= (x' \wedge z) \vee (y \wedge z) \vee (y \wedge z') \\ &= (x' \wedge z) \vee [y \wedge (z \vee z')] && \text{(Using distributive law)} \\ &= (x' \wedge z) \vee (y \wedge 1) && [\because z \vee z' = 1] \\ &= (x' \wedge z) \vee y \end{aligned}$$

x	y	z	x'	$x' \wedge z$	$f = (x' \wedge z) \vee y$	min
0	0	0	1	0	0	m_0
0	0	1	1	1	1	m_1
0	1	0	1	0	1	m_2
0	1	1	1	1	1	m_3
1	0	0	0	0	0	m_4
1	0	1	0	0	0	m_5
1	1	0	0	0	1	m_6
1	1	1	0	0	1	m_7

Since minterms corresponds to each ordered triple of 0 and 1 for which the value of the function is 1.

$\therefore$ minterm are $m_1 = x' \wedge y' \wedge z$, $m_2 = x' \wedge y \wedge z'$, $m_3 = x' \wedge y \wedge z$

$m_6 = x \wedge y \wedge z'$, $m_7 = x \wedge y \wedge z$

Hence Minterm Normal form

$= m_1 \vee m_2 \vee m_3 \vee m_6 \vee m_7$

$= (x' \wedge y' \wedge z) \vee (x' \wedge y \wedge z') \vee (x' \wedge y \wedge z) \vee (x \wedge y \wedge z') \vee (x \wedge y \wedge z)$

Example 2. Simplify the Boolean expression

$$f(x, y, z) = (x \wedge y' \wedge z) \vee (x \wedge y \wedge z)$$

and find its conjective normal forms.

Sol.

$$f(x, y, z) = (x \wedge y' \wedge z) \vee (x \wedge y \wedge z) = (x \wedge z \wedge y') \vee (x \wedge z \wedge y)$$

$$= [(x \wedge z) \wedge (y' \vee y)] = [(x \wedge z) \wedge I]$$

$$= x \wedge z$$

x	y	z	$f = x \wedge z$	Max
0	0	0	0	M_0
0	0	1	0	M_1
0	1	0	0	M_2
0	1	1	0	M_3
1	0	0	0	M_4
1	0	1	1	M_5
1	1	0	0	M_6
1	1	1	1	M_7

Since Maxterm corresponds to each ordered triple of 0 and 1 for which the value of the function is 0.

$\therefore$ Maxterm are $M_0 = x' \vee y' \vee z'$, $M_1 = x' \vee y' \vee z$, $M_2 = x' \vee y \vee z'$, $M_3 = x' \vee y \vee z$,

$M_4 = x \vee y' \vee z'$, $M_6 = x \vee y \vee z'$

Hence disjunctive normal form

$= M_0 \wedge M_1 \wedge M_2 \wedge M_3 \wedge M_4 \wedge M_6$

$= (x' \vee y' \vee z') \wedge (x' \vee y' \vee z) \wedge (x' \vee y \vee z') \wedge (x' \vee y \vee z) \wedge (x \vee y' \vee z') \wedge (x \vee y \vee z')$

Algorithm for obtaining complete Sum-of-Product Expression

Let the given boolean expression be $f(x_1, x_2, \ldots, x_n)$

Step 1. Find a product P in $f(x_1, x_2, \ldots, x_n)$ which does not contain the variable x_i and then multiply P by $(x_i + x_i')$, deleting any repeated products (as $x + x' = 1$ and $P + P = P$)

Step 2. Repeat Step 1 until every product in $f(x_1, x_2, \ldots, x_n)$ is a minterm i.e. every product P contains all the n-variables.

Algorithm for obtaining Product of sum canonical form

Let the given boolean expression be $f(x_1, x_2, \ldots\ldots, x_n)$

Step 1. Find a sum S in $f(x_1, x_2, \ldots\ldots, x_n)$ which does not contains the variable x_i and then add S by $(x_i\ x_i')$, deleting any repeated sum (as $xx' = 0$ and $SS = S$)

Step 2. Repeat Step 1 till every sum in $f(x_1, x_2, \ldots\ldots, x_n)$ is a maxterm i.e. every sum S contains all the n-variables.

Example 3. Using Boolean algebra, construct the DNF of the boolean function

$$f(x, y, z) = x(y + z)$$

Sol. Here
$$\begin{aligned} f(x, y, z) &= x(y + z) = xy + xz = xy \cdot 1 + xz \cdot 1 \\ &= xy(z + z') + xz(y + y') = xyz + xyz' + xyz + xy'z \\ &= (xyz + xyz) + xy'z + xyz' = xyz + xy'z + xyz' \end{aligned}$$

which is in the DNF of the boolean function $f(x, y, z)$.

Example 4. Express $x_1 + x_2$ and x_1x_2 in its complete Sum-of-Product term in three variables x_1, x_2, x_3.

Sol. (*i*) Now
$$\begin{aligned} x_1 + x_2 &= x_1 \cdot 1 + x_2 \cdot 1 = x_1(x_2 + x_2') + x_2(x_1 + x_1') \\ &= x_1x_2 + x_1x_2' + x_1x_2 + x_1'x_2 \\ &= x_1x_2 \cdot 1 + x_1x_2' \cdot 1 + x_1'x_2 \cdot 1 \\ &= x_1x_2(x_3 + x_3') + x_1x_2'(x_3 + x_3') + x'x_2(x_3 + x_3') \\ &= x_1x_2x_3 + x_1x_2x_3' + x_2x_2'x_3 + x_2x_2'x_3' + x_1'x_2x_3 + x_1'x_2x_3' \\ &= x_1x_2x_3 + x_1x_2x_3' + x_1x_2'x_3 + x_1'x_2x_3 + x_1'x_2x_3' + x_1x_2'x_3' \end{aligned}$$

Which is the complete Sum-of-Product form.

(*ii*) Also, $x_1x_2 = x_1x_2 \cdot 1 = x_1x_2(x_3 + x_3') = x_1x_2x_3 + x_1x_2x_3'$

which is the complete Sum-of-Product form.

Example 5. Obtain Product of Sum Canonical form of boolean expression x_1x_2 in three variables x_1, x_2, x_3.

Sol. Here
$$\begin{aligned} x_1x_2 &= (x_1 + 0)(x_2 + 0) = [x_1 + (x_2x_2')][x_2 + (x_1x_1')] \\ &= (x_1 + x_2)(x_1 + x_2')(x_2 + x_1)(x_2 + x_1') && xx' = 0 \\ &= (x_1 + x_2)(x_1 + x_2')(x_2 + x_1') && [\because xx = x] \\ &= [(x_1 + x_2) + (x_3x_3')][(x_1 + x_2') + (x_3x_3')] && [(x_2 + x_1') + (x_3x_3')] \\ &= (x_1 + x_2 + x_3)(x_1 + x_2 + x_3')(x_1 + x_2' + x_3) \\ & && (x_1 + x_2' + x_3')(x_2 + x_1' + x_3)(x_2 + x_1' + x_3') \end{aligned}$$

which is the required product of Sum Canonical form.

Example 6. Show that $(x_1' x_2' x_3' x_4') + (x_1' x_2' x_3' x_4) + (x_1' x_2' x_3 x_4) + (x_1' x_2 x_3 x_4') = x_1' x_2'$.

Sol. L.H.S. $= (x_1' x_2' x_3' x_4') + (x_1' x_2' x_3' x_4) + (x_1' x_2' x_3 x_4) + (x_1' x_2 x_3 x_4')$

$= [(x_1' x_2' x_3' x_4') + (x_1' x_2' x_3' x_4)] + [(x_1' x_2' x_3 x_4) + (x_1' x_2 x_3 x_4')]$

$= x_1' x_2' x_3' (x_4' + x_4) + x_1' x_2' x_3 (x_4 + x_4') = x_1' x_2' x_3' \cdot 1 + x_1' x_2' x_3 \cdot 1 = x_1' x_2' (x_3' + x_3)$

$= x_1' x_2' \cdot 1 = x_1' x_2'$

$=$ R.H.S.

Example 7. Show that the following Boolean expressions are equivalent to one another. Obtain their Sum-of-Product Canonical form

(i) $f_1(x, y, z) = (x + y)(x' + z)(y + z)$ (ii) $f_2(x, y, z) = (xz) + (x'y) + (yz)$

(iii) $f_3(x, y, z) = (x + y)(x' + z)$ (iv) $f_4(x, y, z) = xz + x'y$

Sol. The binary valuation of the given boolean expression are

x	y	z	$x+y$	$x'+z$	$y+z$	f_1	f_3	xz	$x'y$	yz	f_2	f_4
0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	0	0	0	0
0	1	0	1	1	1	1	1	0	1	0	1	1
0	1	1	1	1	1	1	1	0	1	1	1	1
1	0	0	1	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	0	0	1	1
1	1	0	1	0	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	0	1	1	1

Since the values of the boolean expressions for f_1, f_2, f_3 and f_4 are equal over every triple of the two-value element Boolean algebra. So these are equivalent.

To write them in Sum-of-Product cannonical form.

We have $f_4(x, y, z) = xz + x'y = xz \cdot 1 + x'y \cdot 1 = xz(y + y') + x'y(z + z')$

$= xyz + xy'z + x'yz + x'yz'$

which is in the Sum-of-Product canonical form.

Example 8. Find the Boolean Expression that defines the function f by

$f(0, 0, 0) = 0$

$f(1, 0, 0) = 1$

$f(0, 1, 0) = 1$

$f(1, 0, 1) = 1$

$f(0, 0, 1) = 0$

$f(1, 1, 0) = 0$

$f(0, 1, 1) = 0$

$f(1, 1, 1) = 1$

Sol. The minterms are $f(0,1,0)$, $f(1,0,0)$, $f(1,0,1)$, $f(1,1,1)$

i.e. $(x' \wedge y \wedge z')$, $(x \wedge y' \wedge z')$, $(x \wedge y' \wedge z)$, $(x \wedge y \wedge z)$

D.N.F is $f(x,y,z) = (x' \wedge y \wedge z') \vee (x \wedge y' \wedge z') \vee (x \wedge y' \wedge z) \vee (x \wedge y \wedge z)$

can be simplified as

$= (x' \wedge y \wedge z') \vee x \wedge [(y' \wedge z') \vee (y' \wedge z) \vee (y \wedge z)]$ [Distributive Law]

$= (x' \wedge y \wedge z') \vee x \wedge [\{y' \wedge (z' \vee z)\} \vee (y \wedge z)]$ [Distributive Law]

$= (x' \wedge y \wedge z') \vee x \wedge (y' \vee (y \wedge z))$ [$\because z' \vee z = 1,\ y' \wedge 1 = y'$]

$= (x' \wedge y \wedge z') \vee x \wedge (y' \vee y) \wedge (y' \wedge z)$ [Distributive Law]

$= (x' \wedge y \wedge z') \vee x \wedge (y' \vee z)$ [$\because y' \vee y = 1$]

$= (x' \wedge y \wedge z') \vee [(x \wedge y') \vee (x \wedge z)]$ [Distributive Law]

Example 9. Find the Boolean Expression in CN-form.

x	y	z	f
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

CN form is

$(x \vee y \vee z') \wedge (x \vee y' \vee z') \wedge (x' \vee y \vee z) \wedge (x' \vee y \vee z') \wedge (x' \vee y' \vee z)$

Example 10. Using Boolean laws show

$(x \wedge y) \vee (x \wedge y \wedge z) \vee [x \wedge (y \vee (x \wedge y))]$ and $x \wedge y$

are equivalent.

$(x \wedge y) \vee (x \wedge y \wedge z) \vee [x \wedge (y \vee (x \wedge y))]$

$= (x \wedge y) \vee (x \wedge y \wedge z) \vee [(x \wedge y) \vee (x \wedge y)]$ [$\because x \wedge x = x$]

$= (x \wedge y) \vee (x \wedge y \wedge z) \vee (x \wedge y)$ [$\because a \vee a = a$]

$= ((x \wedge y) \vee (x \wedge y)) \vee (x \wedge y \wedge z) = (x \wedge y) \vee (x \wedge y \wedge z)$

$= (x \wedge y) \vee (1 \wedge z)$ [$\because 1 \wedge z = 1$]

$= (x \wedge y) \vee 1 = x \wedge y$

Example 11. Simplify the Boolean expression $f(x, y, z) = (\bar{x} \wedge z) \vee (y \wedge z) \vee (y \wedge \bar{z})$ and write in min. term normal form.

Sol. $f = (\bar{x} \wedge z) \vee (y \wedge z) \vee (y \wedge \bar{z}) = (\bar{x} \wedge z) \vee [(y \wedge (z \vee \bar{z})]$ [Distributive law]

$= (\bar{x} \wedge z) \vee (y \wedge 1)$ $[\because z \vee \bar{z} = 1]$

$= (\bar{x} \wedge z) \vee y$

x	y	z	$\bar{x}$	$\bar{x} \wedge z$	f	
0	0	0	1	0	0	m_1
0	0	1	1	1	1	m_2
0	1	0	1	0	1	m_3
0	1	1	1	1	1	m_4
1	0	0	0	0	0	m_5
1	0	1	0	0	0	m_6
1	1	0	0	0	1	m_7
1	1	1	0	0	1	m_8

Min. term are $m_2 = \bar{x} \wedge \bar{y} \wedge \bar{z}$

$m_3 = \bar{x} \wedge y \wedge \bar{z}$, $m_4 = \bar{x} \vee y \wedge z$

$m_7 = x \wedge y \wedge z$

$m_8 = x \wedge y \wedge z$

Min. term Normal form is

$m_2 \vee m_3 \vee m_4 \vee m_7 \vee m_8$

$(\bar{x} \wedge \bar{y} \wedge \bar{z}) \vee (\bar{x} \wedge y \wedge \bar{z}) \vee (\bar{x} \wedge y \wedge z) \vee (x \wedge y \wedge \bar{z}) \vee (x \wedge y \wedge z)$

Max. term is

$(\bar{x} \vee \bar{y} \vee z) \wedge (\bar{x} \vee y \vee \bar{z}) \wedge (\bar{x} \vee y \vee z) \wedge (x \vee y \vee \bar{z}) \wedge (x \vee y \vee z)$

3.6 Representation of Boolean Functions

The existence of one-one correspondence between every Boolean function $f: B^n \to B$ and a Boolean expression in n variables. We can represent a Boolean function by any one of the Boolean expression to which the function corresponds. Such a representation of a Boolean function will be found convenient for one purpose.

This way of representing a Boolean function is simply to give the Boolean equation for the values of the symbol (s) in the output combination in terms of some subset of the elements of the input combinations.

For example : The function $p = f(x, y, z, t) = x \,.\, [y + (z \,.\, t')]$ gives the output in terms of the input variables x, y, z and t.

Another method of representation of Boolean function is to form a table. (truth table) which list exhaustively all possible combination of the input variables and which for each such input configuration, record a functional value.

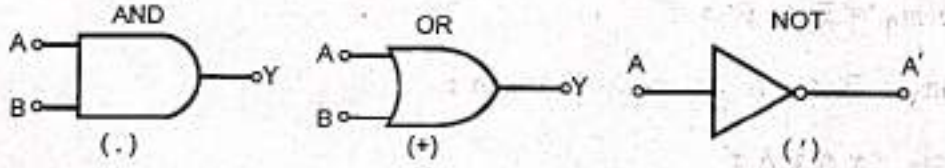
For example : Consider the function

$f_1(x, y, z) = x\,y\,z'$ then

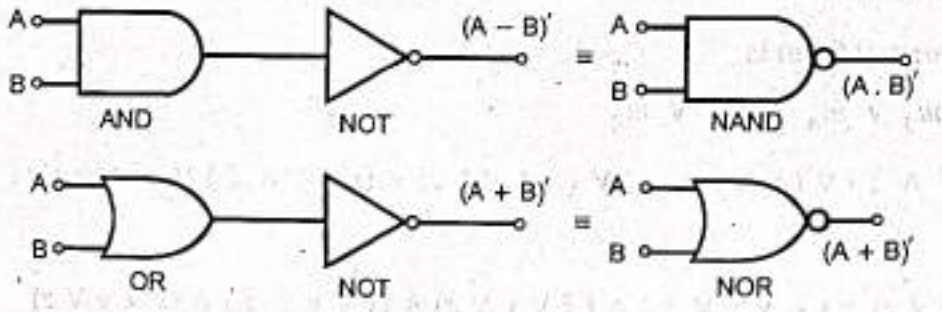
x	y	z	z'	$x\,y$	$x\,y\,z'$
0	0	0	1	0	0
0	0	1	0	0	0
0	1	0	1	0	0
0	1	1	0	0	0
1	0	0	1	0	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	0	1	0

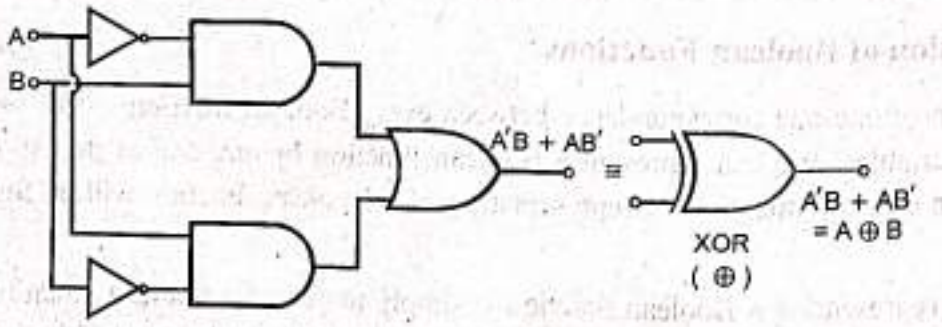
The other method for representing Boolean function is **circuit diagram.**

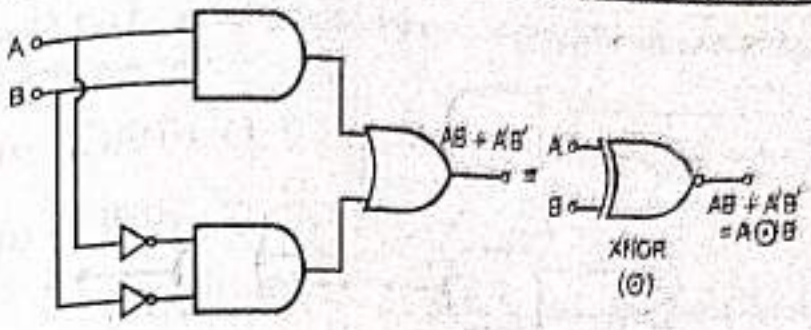
Composed of AND, OR, NOT GATES.



Other standard Gates are NAND, NOR, XOR, XNOR GATE







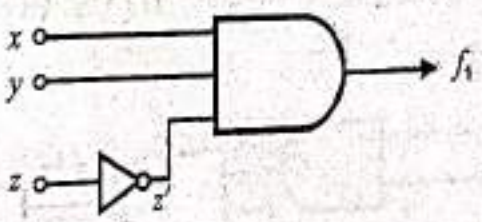
This representation does seem appropriate since Boolean functions can express the functioning of circuit. Because a circuit diagram actually shows which circuit are to be connected to which other circuits, it is occasionally possible to make use of a circuit diagram to eliminate unnecessary connectives and thus yield a simpler circuit.

For example : The circuit diagram of the following Boolean functions

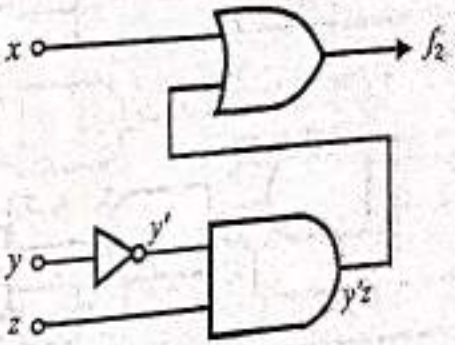
(i) $f_1(x, y, z) = x\,y\,z'$ (ii) $f_2(x, y, z) = x + y'\,z$

(iii) $f_3(x, y, z) = x'\,y'\,z + x'\,y\,z + x\,y'$ (iv) $f_4(x, y, z) = x\,y' + x'\,z$ are

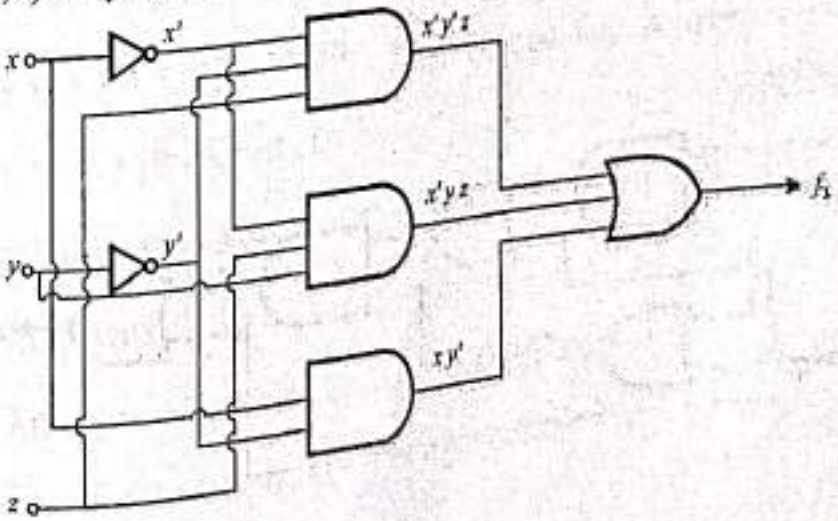
(i) $f_1(x, y, z) = x\,y\,z'$



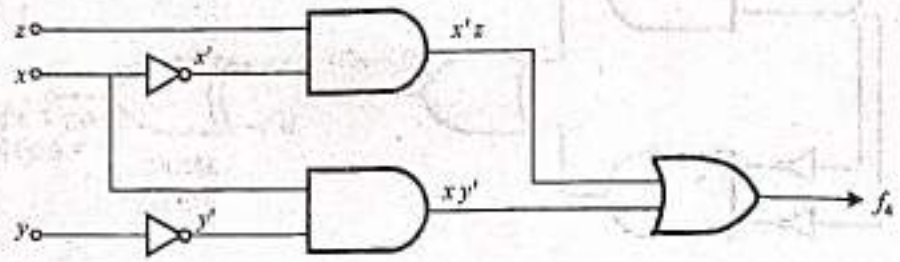
(ii) $f_2(x, y, z) = x + y'\,z$



(iii) $f_3(x, y, z) = x'\,y'\,z + x'\,y\,z + x\,y'$



(iv) $f_4(x, y, z) = x' z + x y'$



Also $f_3(x, y, z) = x' y' z + x' y z + x y' = x' z (y' + y) + x y'$

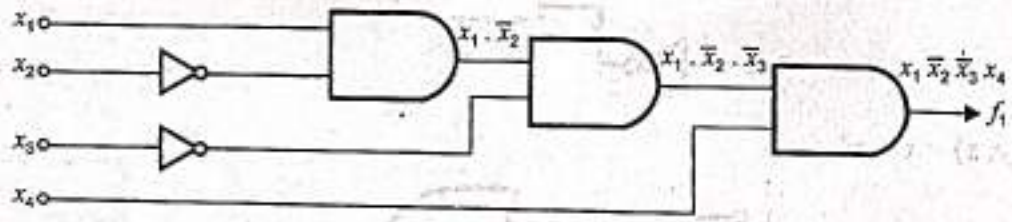
$= x' z \cdot 1 + x y' = x' z + x y' = f_4(x, y, z)$.

Example 1. Write the circuit (gate) diagram of the following Boolean function.

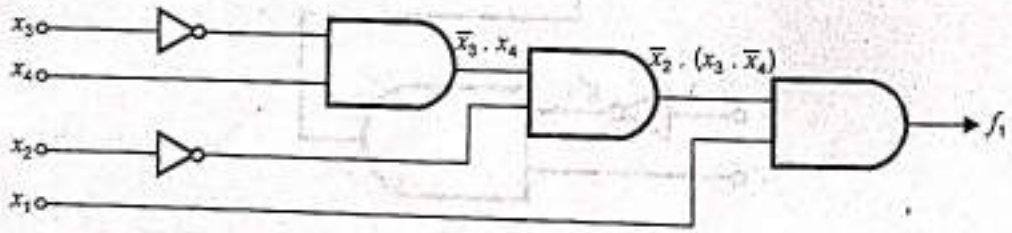
(i) $f_1(x_1, x_2, x_3, x_4) = x_1 \cdot (\bar{x}_2 \cdot (\bar{x}_3 \cdot x_4))$

(ii) $f_2(x_1, x_2, x_3) = (x_1 \cdot x_2 + x_3) \cdot (x_2 + x_3) + x_3$.

Sol. (i) The circuit diagram of the function $f_1(x_1, x_2, x_3, x_4) = x_1 \cdot (\bar{x}_2 \cdot (\bar{x}_3 \cdot x_4))$ is as shown below



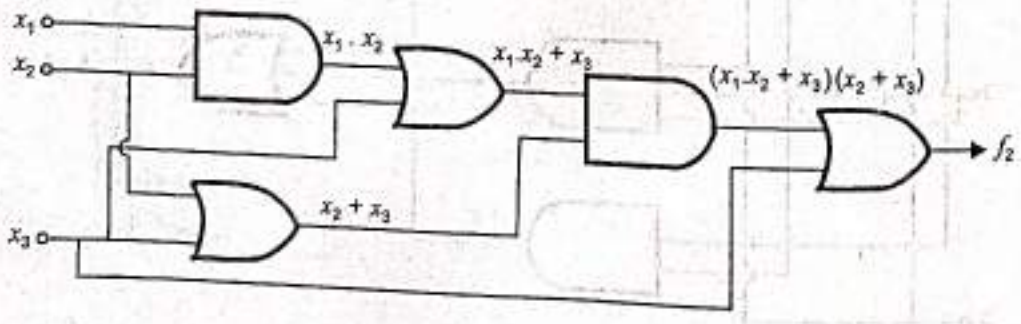
or



(ii) The circuit diagram of the function

$f_2(x_1, x_2, x_3) = (x_1 \cdot x_2 + x_3) \cdot (x_2 + x_3) + x_3$

is as shown below :



Example 2. Simplify the following Boolean function and realise the logic diagram of the reduced function with the help of NAND gate only

$$F(A, B, C D) = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,\overline{B}CD + A\overline{B}\,\overline{C}\,\overline{D} + A\overline{B}\,\overline{C}D + A\overline{B}C\overline{D} + A\overline{B}CD + ABC\overline{D} + ABCD$$

or $F(A, B, C D) = \overline{A}\,\overline{B}\,\overline{C}\,\overline{D} + \overline{A}\,\overline{B}CD + A\overline{B}\,\overline{C}\,\overline{D} + A\overline{B}\,\overline{C}D + A\overline{B}C\overline{D} + A\overline{B}CD + ABC\overline{D} + ABCD$

$$= \overline{A}\,\overline{B}\,\overline{D}(\overline{C} + C) + A\overline{B}\,\overline{C}(\overline{D} + D) + A\overline{B}C(\overline{D} + D) + ABC(\overline{D} + D)$$

$$= \overline{A}\,\overline{B}\,\overline{D} + A\overline{B}\,\overline{C} + A\overline{B}C + ABC \qquad [\because x + \overline{x} = 1]$$

$$= \overline{A}\,\overline{B}\,\overline{D} + A\overline{B}\,\overline{C} + AC(\overline{B} + B) = \overline{A}\,\overline{B}\,\overline{D} + A\overline{B}\,\overline{C} + AC$$

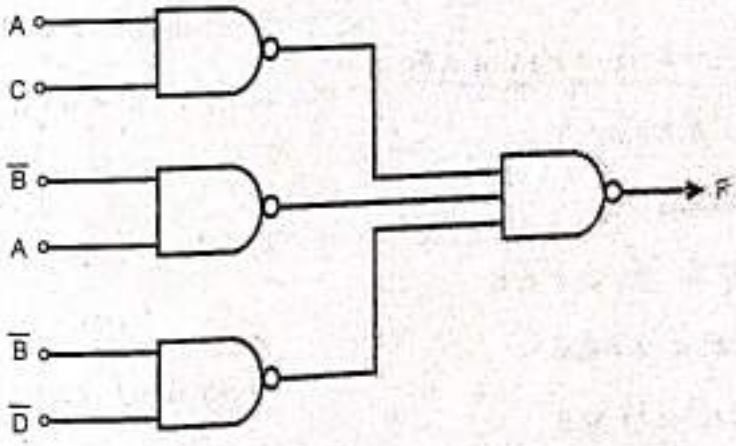
$$= \overline{A}\,\overline{B}\,\overline{D} + A(\overline{B}\,\overline{C} + C) = \overline{A}\,\overline{B}\,\overline{D} + A(C + \overline{B})(C + \overline{C})$$

$$= \overline{A}\,\overline{B}\,\overline{D} + A(C + \overline{B}).1 = \overline{A}\,\overline{B}\,\overline{D} + AC + A\overline{B}$$

$$= AC + \overline{B}(\overline{A}\,\overline{D} + A) = AC + \overline{B}(A + \overline{A})(A + \overline{D})$$

$$= AC + \overline{B}.1(A + \overline{D}) = AC + \overline{B}A + \overline{B}\,\overline{D}.$$

F with the help of NAND GATE



$\overline{F}$ with the help of NAND GATE

$$\overline{F} = \overline{(AC + \overline{B}A + \overline{B}\,\overline{D})} = \overline{AC}.\overline{\overline{B}A}.\overline{\overline{B}\,\overline{D}}$$

$$= (\overline{A} + \overline{C}).(B + \overline{A}).(B + D) \qquad [\because (a.b)' = a' + b',\ (a')' = a]$$

$$= (\overline{A} + \overline{C}).(BB + BD + \overline{A}B + \overline{A}D) = (\overline{A} + \overline{C}).(B + BD + \overline{A}B + \overline{A}D)$$

$$= \overline{A}B + \overline{A}BD + \overline{A}\,\overline{A}B + \overline{A}\,\overline{A}D + \overline{C}B + B\overline{C}D + \overline{A}B\overline{C} + \overline{A}D\overline{C}$$

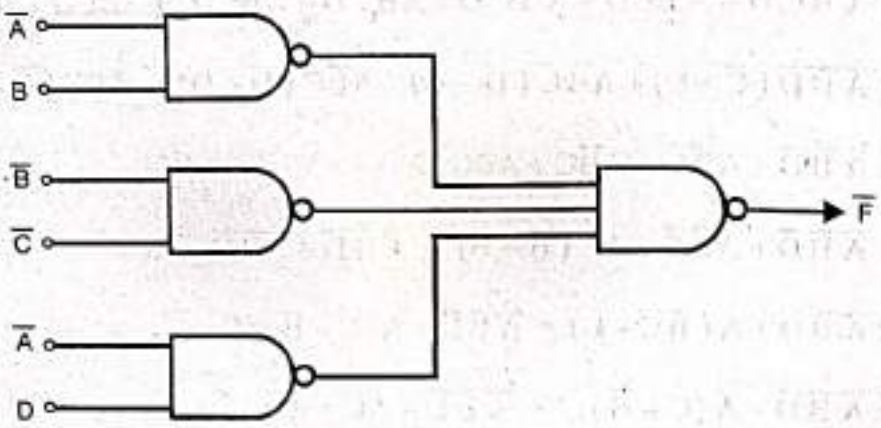
$$= \overline{A}B + \overline{A}BD + \overline{A}B + \overline{A}D + \overline{C}B + B\overline{C}D + \overline{A}B\overline{C} + \overline{A}D\overline{C}$$

$$= \overline{A}B + \overline{A}D(1 + \overline{C}) + B\overline{C}(1 + \overline{A}) + \overline{A}BD + B\overline{C}D \qquad [\because a + a = a]$$

$= \overline{A}B + \overline{A}D + B\overline{C} + \overline{A}BD + \overline{C}BD$ [$\because 1 + a = 1 \ \forall a$]

$= \overline{A}B(1 + D) + B\overline{C}(1 + D) + \overline{A}D$

$= \overline{A}B + B\overline{C} + \overline{A}D$



BOOLEAN RING

Theorem : Prove that a Boolean algebra forms a ring under the binary operations + and · defined as above.

Proof : Let B be a Boolean algebra.

Then for all $a, b \in B$,

$$a + b = (a \wedge b') \vee (a' \wedge b)$$

$$a \cdot b = a \wedge b$$

***(i)* Addition is closed**

For $a, b \in B, \Rightarrow a', b' \in B$

Therefore $a \wedge b', a' \wedge b \in B$

$\Rightarrow (a \wedge b') \vee (a' \wedge b) \in B$

$\Rightarrow a + b \in B$

***(ii)* Addition is Commutative :** For $a, b \in B$,

$$a + b = (a \wedge b') \vee (a' \wedge b) = (a' \wedge b) \vee (a \wedge b') = (b \wedge a') \vee (b' \wedge a)$$

$$= b + a$$

***(iii)* Addition is associative :** For $a, b, c \in B$,

$(a + b) + c = [(a + b) \wedge c'] \vee [(a + b)' \wedge c]$

$= [\{(a \wedge b') \vee (a' \wedge b)\} \wedge c'] \vee [\{(a \wedge b') \vee (a' \wedge b)\}' \wedge c]$

$= [(a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')] \vee [\{(a \wedge b')' \wedge (a' \wedge b)'\} \wedge c]$

$= [(a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')] \vee [\{(a' \vee b) \wedge (a \vee b')\} \wedge c]$

$= [(a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')] \vee [\{(a' \vee b) \wedge a\} \vee \{(a' \vee b) \wedge b'\} \wedge c]$

$= [(a \wedge b' \wedge c') \vee (a' \wedge b \wedge c')] \vee [\{(a' \wedge a) \vee (b \wedge a) \vee (a' \wedge b') \vee (b \wedge b')\} \wedge c]$

$= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee [\{(b \wedge a) \vee (a' \wedge b')\} \wedge c]$

$= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (b \wedge a \wedge c) \vee (a' \wedge b' \wedge c)]$

$= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (b \wedge a \wedge c) \vee (a' \wedge b' \wedge c)]$

Similarly

$(b + c) + a = (b \wedge c' \wedge a') \vee (b' \wedge c \wedge a') \vee (c \wedge b \wedge a) \vee (b' \wedge c' \wedge a)$

$= (b' \wedge c' \wedge a) \vee (b \wedge c' \wedge a') \vee (c \wedge b \wedge a) \vee (b' \wedge c \wedge a')$

$= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (b \wedge a \wedge c) \vee (a' \wedge b' \wedge c)$

Thus

$$(a + b) + c = (b + c) + a = a + (b + c)$$

(iv) **Additive Identity :** For all $a \in B$,

$$a + 0 = (a \wedge 0') \vee (a' \wedge 0) = (a \wedge 1) \vee 0 = a \vee 0$$

$$= a$$

and

$$0 + a = (0 \wedge a') \vee (0' \wedge a) = 0 \vee (1 \wedge a) = 0 \vee a$$

$$= a$$

Thus $a + 0 = a = 0 + a$ for all $a \in B$

Hence 0 is additive identity in B.

(v) **Additive Inverse :** For any $a \in B$, we have

$$a + a = (a \wedge a') \vee (a' \wedge a)$$

$$= 0 \vee 0$$

$$= 0$$

Thus a itself is additive inverse of a in B.

(vi) **Multiplication is closed :** For all $a, b \in B$,

$$a \cdot b = a \wedge b \in B$$

(vii) Multiplication is associative : For $a, b, c \in B$,

$$a\cdot(b\cdot c) = a\cdot(b \wedge c) = a \wedge (b \wedge c) = (a \wedge b) \wedge c = (a\cdot b) \wedge c$$

$$= (a\cdot b)\cdot c .$$

(viii) Multiplication is distributive over addition

For $a, b, c \in B$, we have

$$a\cdot(b + c) = a \wedge (b + c) = a \wedge [(b \wedge c') \vee (b' \wedge c)] = (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$$

Also $a\cdot b + a\cdot c = (a \wedge b) + (a \wedge c)$

$$= [(a \wedge b) \wedge (a \wedge c)'] \vee [(a \wedge b)' \wedge (a \wedge c)]$$

$$= [(a \wedge b) \wedge (a' \vee c')] \vee [(a' \vee b') \wedge (a \wedge c)]$$

$$= (a \wedge b \wedge a') \vee (a \wedge b \wedge c') \vee (a' \wedge a \wedge c) \vee (b' \wedge a \wedge c)$$

$$= ((a \wedge a') \wedge b) \vee (a \wedge b \wedge c') \vee (0 \wedge c) \vee (b' \wedge a \wedge c)$$

$$= 0 \vee (a \wedge b \wedge c') \vee 0 \vee (a \wedge b' \wedge c)$$

$$= (a \wedge b \wedge c') \vee (a \wedge b' \wedge c)$$

Thus $a(b + c) = ab + ac$

Similarly we can show that

$$(a + b)c = ac + bc$$

Thus all the eight properties of a ring are satisfied.

Hence $\langle B, +, \cdot \rangle$ forms a ring.

Corollary 1. If B is a Boolean algebra, then the ring $\langle B, +, \cdot \rangle$ is commutative ring with unit element.

Proof : For all $a, b \in B$, we have

$$ab = a \wedge b = b \wedge a = ba$$

Therefore B is commutative

Now for all $a \in B$,

$$a\cdot 1 = a \wedge 1 = a$$

and $$1\cdot a = 1 \wedge a = a$$

Thus 1 is unit element of B.

Corollary 2. Each element of B is of order ≤ 2 in its additive group

OR

For any element $a \in B$, prove that $2a = 0$

Proof : For any $a \in B$,

$$2a = a + a$$
$$= (a \wedge a') \vee (a' \wedge a)$$
$$= 0 \vee 0$$
$$= 0$$

Thus under addition order of a is ≤ 2.

Corollary 3. All elements of B are idempotent.

OR

In the ring $\langle B, +, \cdot \rangle$, we have $a^2 = a$ for all $a \in B$.

Proof : For all $a \in B$, we have

$$a^2 = a \cdot a$$
$$= a \wedge a$$
$$= a$$

Thus all elements of B are idempotent.

Definition : A ring is said to be **Boolean ring** if all its elements are idempotent.

Note : From above definition and result, it is clear that **"Every Boolean algebra is a Boolean ring with unity".**

Lemma : In a Boolean ring $\langle B, +, \cdot \rangle$, prove that

(i) $x + x = 0$ (ii) $x + y = 0 \Leftrightarrow x = y$ (iii) $xy = yx$ (Boolean ring is commutative)

Proof : We know that cancellation law holds in any ring.

(i) For any $x \in B$, $x + x \in B$

Since B is a Boolean ring

$$(x + x)^2 = x + x$$

$$\Rightarrow \quad (x + x)(x + x) = x + x$$

$\Rightarrow \quad (x+x)x+(x+x)x = x+x$

$\Rightarrow \quad x^2+x^2+x^2+x^2 = x+x$

$\Rightarrow \quad x+x+x+x = x+x$

$\Rightarrow \quad (x+x)+(x+x) = (x+x)+0$

$\Rightarrow \quad x+x = 0$

(*ii*) We have $x+y = 0$

$\Leftrightarrow \quad x+y = x+x$ using (*i*)

$\Leftrightarrow \quad y = x$

(*iii*) For $x, y \in B$, $x+y \in B$

Since B is a Boolean ring,

$(x+y)^2 = x+y$

$\Rightarrow \quad (x+y)(x+y) = x+y$

$\Rightarrow \quad (x+y)x+(x+y)y = x+y$

$\Rightarrow \quad x^2+yx+xy+y^2 = x+y$

$\Rightarrow \quad x+yx+xy+y = x+y$

$\Rightarrow \quad (x+y)+(yx+xy) = (x+y)+0$

$\Rightarrow \quad xy+xy = 0$

$\Rightarrow \quad yx = xy$ using (*ii*)

Theorem : Any Boolean ring with unity defines a Boolean algebra.

Proof : Let <B, +, ·> be a Boolean ring with unity.

Define two binary operations $\wedge$ and $\vee$ on B by

$a \wedge b = a \cdot b$

$a \vee b = a+b+ab$ for all $a, b \in B$

(*i*) **Laws of idempotency :** For $a \in B$,

$a \wedge a = a \cdot a = a^2 = a$

$a \vee a = a+a+a \cdot a = 0 + a^2 = a$

(ii) **Comutative laws :** For $a, b \in B$

$$a \wedge b = a \cdot b = b \cdot a = b \wedge a$$

$$a \vee b = a + b + ab = b + a + ba = b \vee a$$

(iii) **Associative laws :** For $a, b, c \in B$

$$a \wedge (b \wedge c) = a \wedge (bc) = a(bc) = (ab)c = (a \wedge b) \wedge c$$

$$a \vee (b \vee c) = a + (b \vee c) + a(b \vee c) = a + b + c + bc + a(b + c + bc)$$

$$= a + b + c + bc + ab + ac + abc = (a + b + ab) + c + (a + b + ab)c$$

$$= (a \vee b) + c + (a \vee b)c = (a \vee b) \vee c$$

(iv) **Absorption laws :** For $a, b \in B$

$$a \wedge (a \vee b) = a(a \vee b) = a(a + b + ab) = a^2 + ab + a(ab)$$

$$= a + ab + (aa)b = a + ab + a^2b = a + (ab + ab)$$

$$= a + 0$$

$$= a$$

$$a \vee (a \wedge b) = a \vee (ab)$$

$$= a + ab + a(ab) = a + ab + (aa)b = a + ab + a^2b = a + (ab + ab)$$

$$= a + 0$$

$$= a$$

Thus $< B, +, \cdot >$ forms a lattice.

Now for $a, b, c \in B$, we have

$$a \wedge (b \vee c) = a(b \vee c)$$

$$= a(b + c + bc) = ab + ac + abc = ab + ac + a^2bc \quad \text{as } a^2 = a$$

$$= ab + ac + a(ab)c = ab + ac + a(ba)c$$

$$= ab + ac + (ab)(ac) = (ab) \vee (ac)$$

$$= (a \wedge b) \vee (a \wedge c)$$

Thus $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in B$

Therefore B is a distributive lattice.

If 0 and 1 denotes zero and unit elements of the ring B, then

$$0 \cdot a = 0 \quad \text{for all } a \in B$$

$$\Rightarrow \quad 0 \wedge a = 0 \quad \text{for all } a \in B$$

Therefore 0 is the zero element of the lattice B

Also $1 \cdot a = a$ for all $a \in B$ (as ring)

$$\Rightarrow \quad 1 \wedge a = a \quad \text{for all } a \in B$$

Therefore 1 is the unit element of the lattice B.

Lastly we show that the lattice B is complemented.

For any $a \in B$, we have

$$a \wedge (a+1) = a(a+1) = a^2 + a = a + a = 0$$

and

$$\begin{aligned} a \vee (a+1) &= a + (a+1) + a(a+1) \\ &= (a+a) + 1 + a^2 + a \\ &= 0 + 1 + (a+a) \\ &= 1 + 0 \\ &= 1 \end{aligned}$$

Therefore $a' = a + 1$. Thus B is a distributive and complemented lattice with 0 and 1.

Hence B is a Boolean algebra.

Note : Boolean algebra and Boolean ring with unity are equivalent systems.

EXERCISE 3.2

1. Show that the Boolean functions $f_1(x, y, z) = (x_1 \vee x_2) \vee x_3$ and $f_2(x, y, z) = x_1 \vee (x_2 \vee x_2)$ are equivalent.
2. Construct the truth table for the following expressions

   (a) $f_1(x_1, x_2)$ (b) $f_2(x_1, x_2) = x_1 \wedge x_2$ (c) $f_3(x_1) = x_1'$
3. Find the truth value of $f(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_1' \vee x_2') \wedge (x_2 \vee x_3')$
4. Write the following Boolean expressions in an equivalent sum of Product cannonical form in three variables $x_1, x_2 x_3$

   (a) $x_1 \wedge x_2'$ (b) $x_2 \vee x_3'$ (c) $(x_1 \vee x_2)' \vee (x_1' \wedge x_3)$

5. Obtain the product of sums cannonical form in three variables x_1, x_2, x_3 for expressions.

(a) $x_2 \vee x_3$ (b) $x_2 \wedge x_3$

6. Find the value of the Boolean expression given below

(a) $[x \wedge (y \vee (x \wedge \overline{y}))] \vee [(x \wedge \overline{y}) \vee (\overline{x \wedge z})]$ for $x = 1, y = 1$ and $z = 0$

(b) $x + \overline{yz}$ for $x = 0, y = 1, z = 1$.

7. Obtain the value of the Boolean forms

(a) $x_1 \wedge (x_1' \vee x_2)$ (b) $x_1 \wedge x_2$ (c) $x_1 \vee (x_1 \wedge x_2)$

8. Obtain the sum of Products and Product-of-Sums cannonical forms of the following:

(a) $x_1 x_2' + x_3$ (b) $[(x_1 + x_2)(x_3 x_4)']'$

(c) $x_1' + [x_2' + x_1 + (x_2 x_3)'](x_2 + x_1' x_2)$

ANSWERS

2.

x_1	x_2	$f_1 = x_1 \vee x_2$	$f_2 = x_1 \wedge x_2$	$f_3 = x_1'$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

3.

x_1	x_2	x_3	$x_1 \vee x_2$	$x_1' \vee x_2'$	$(x_2 \vee x_3)'$	$f(x_1, x_2, x_3)$
0	0	0	0	1	1	0
0	0	1	0	1	0	0
0	1	0	1	1	0	0
0	1	1	1	1	0	0
1	0	0	1	1	1	1
1	0	1	1	1	0	0
1	1	0	1	0	0	0
1	1	1	1	0	0	0

4. (*a*) $(x_1 \wedge x_2' \wedge x_3) \vee (x_1 \wedge x_2' \wedge x_2')$

(*b*) $[(x_1 \wedge x_2 \wedge x_3) \vee (x_1' \wedge x_2 \wedge x_3)] \vee [(x_1 \wedge x_2 \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3')] \vee [(x_1 \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2' \wedge x_3')]$

(*c*) $(x_1 \wedge x_2' \wedge x_3) \vee (x_1' \wedge x_2' \wedge x_3') \vee (x_1' \wedge x_2 \wedge x_3) \vee (x_1' \wedge x_2' \wedge x_3)$

5. (*a*) $(x_1 \vee x_2 \vee x_3) \wedge (x_1' \vee x_2 \vee x_3)$

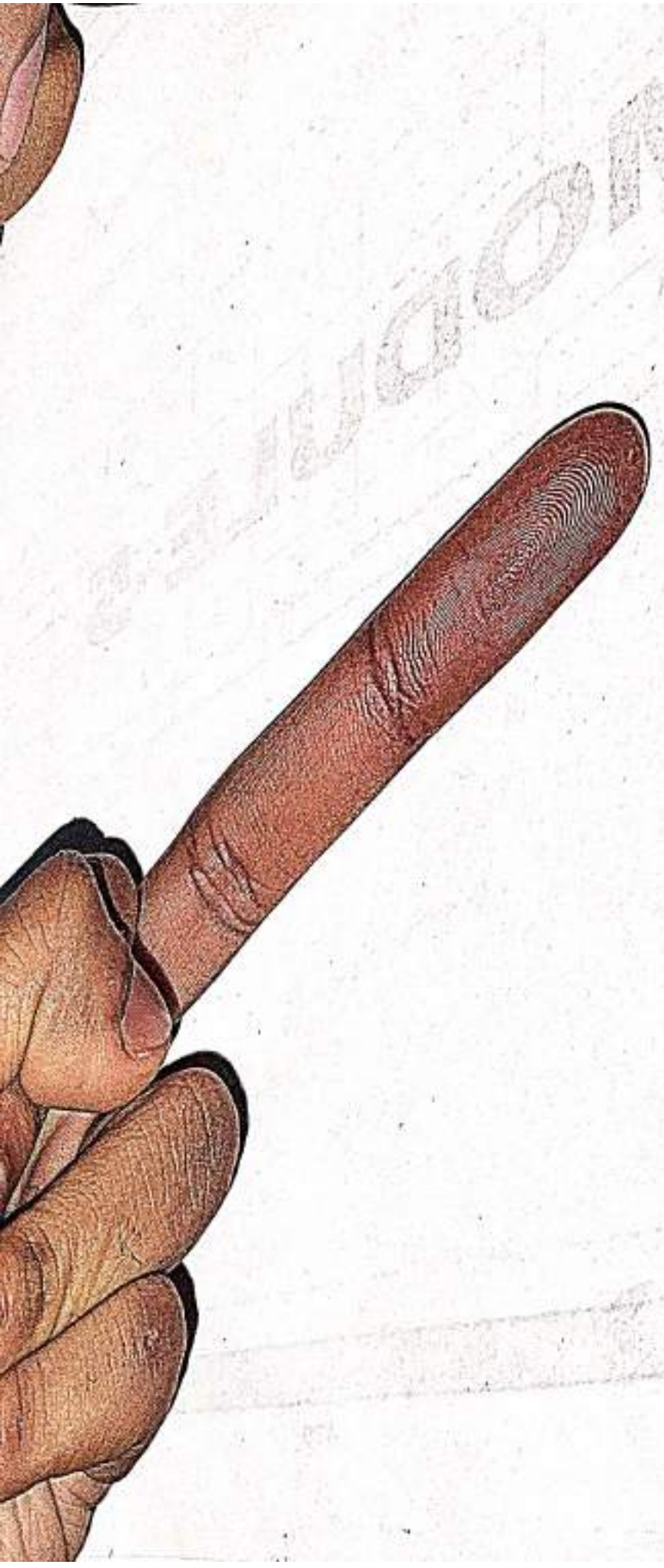
(*b*) $(x_1 \vee x_2 \vee x_3) \wedge (x_1' \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee x_3') \wedge (x_1' \vee x_2 \vee x_3') \wedge (x_1 \vee x_2' \vee x_3) \wedge (x_1' \vee x_2' \vee x_3)$

6. (*a*) 1 (*b*) 0

7.

x_1	x_2	$x_1 \wedge x_2$	x_1'	$x_1' \vee x_2'$	$x_1 \wedge (x_2 \vee x_2)$	$x_1 \vee (x_1 \wedge x_2)$
0	0	0	1	1	0	0
0	1	0	1	1	0	0
1	0	0	0	0	0	1
1	1	1	0	1	1	1

MODULE-5



1

GRAPH THEORY

1.1. Introduction

Graph theory was born in 1736 with Euler's paper in which he solved the Konigsberg bridge problem. In 1947, G.R. Kirchoff developed the theory of trees for their application in electrical network. A Cayley also discovered trees while he was trying to enumerate the isomers of saturated hydrocarbon $C_n H_{2n+2}$. They also lay down four color conjective, which states that four colour are sufficient for colouring any atlas such that the countries with common boundaries have different colour.

Now a day Graph Theory is employed in many areas, such as Communications, Engineering, Physical Sciences, Social Sciences etc. On account of diversity of its application, it is useful to develop and study the subject in abstract form and then import its results. In general areas of computer science such as switching theory and logical design artificial intelligence, formal languages, computer graphics, operating system, graph theory is very useful.

In this chapter, we shall define the various components of the graph theory along with suitable examples. An attempt has been made to show that graphs can be useful to represent any problem involving discrete arrangements of objects, where concern is not with the internal properties of these objects but with the relationships along them.

1.2. Terminology

Graph :

A graph (or undirected graph) is a diagram consisting of a collection of vertices together with edges joining certain pair of these vertices. Mathematically, we can write

A graph $G = [V(G), E(G)]$

where $V(G)$ and $E(G)$ are sets defined as

$V(G)$ = Vertex set (points set or nodes set) of the graph G,

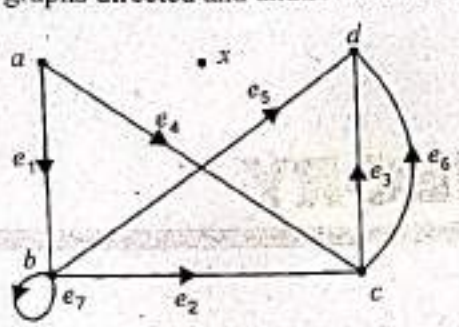
$E(G) \subset V(G) \times V(G)$, a relation on $V(G)$, called edge set of G

Each element e of $E(G)$ is assigned on **unordered pair** of vertices (a, b) called the end vertices of e.

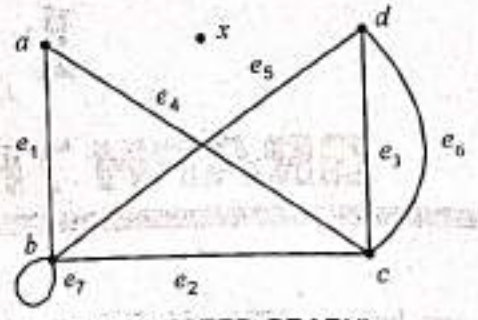
DIRECTED GRAPH.

A directed graph is a graph in which each element e of E (G) is assigned an **ordered pair** of vertices (a, b) along with arrow starting from a to b, where a is called the **initial vertex** and b is called the **terminal** vertex of the edge e.

The graphs directed and undirected are shown in the following figures :



(DIRECTED GRAPH)



(UNDIRECTED GRAPH)

REMARK : (*i*) A graph is represented by means of a diagram in which the vertices are denoted by point and edges are represented by line segments joining its end vertices.

(*ii*) It does not matter whether the joining of the two vertices in a graph is a straight line or a curve longer or shorter.

Adjacent vertices

Two vertices u and v of a graph G = (V, E) are said to be adjacent if there is an edge $e = (u, v)$ connecting u and v. Also the edge e is said to be **incident** on each of its end points u and v.

For example :- In the above diagram a and b are adjacent vertices. Since there is an edge $e_1 = (a, b)$ joining a and b. Also the vertices a and d are not adjacent, as there is no edge joining the vertices a and d.

Loop (or self loop)

An edge that is incident from and into itself starts and ends at same vertex is called self loop or sting.

For Example :- In the above diagram the edge e_7 is a loop. Since the edge $e_7 = (b, b)$ starts and ends at b.

Isolated Vertex

A vertex of a graph G = (V, E), which is not joined to any vertex by an edge in G, is called an isolated vertex.

For example :- In the above diagram the vertex x is an isolated vertex.

Parallel edges

If two (or more) edges of a graph G have the same end vertices, then these edges are called parallel edges.

For example : In the above diagram the edges $e_3 = (c, d)$ and $e_6 = (c, d)$ are parallel edges.

Incidence

An edge e of a graph G = (V, E) is said to be **incident** with the vertex v if v is an end vertex of e (or e is incident with e)

Adjacent edges

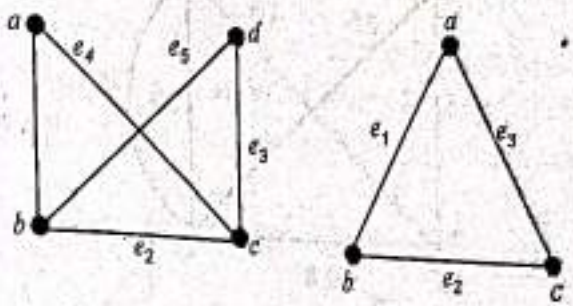
Two non-parallel edges of the graph are called adjacent if they have one common vertex.

For example :- In the above diagram the edges $e_1 = (a, b)$ and $e_4 = (a, c)$ are adjacent vertices, as they have common end vertex a.

1.3. Types of Graphs

(i) Simple graph :

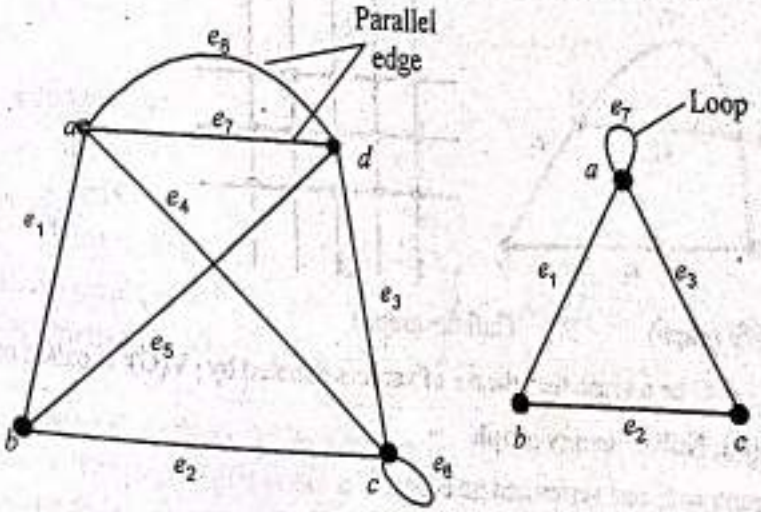
A graph which has neither loop nor parallel edge is called simple graph.



The above graphs are simple graphs.

(ii) General graph (or Multi graph)

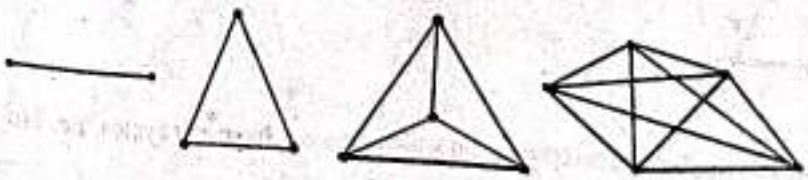
A graph which have either loop or parallel edge or both, is called a general graph or a multi graph.



The above graphs are general graphs.

(iii) Complete Graph : A simple graph in which there exists an edge between every pair of vertices is called a complete graph. It is also known as universal graph.

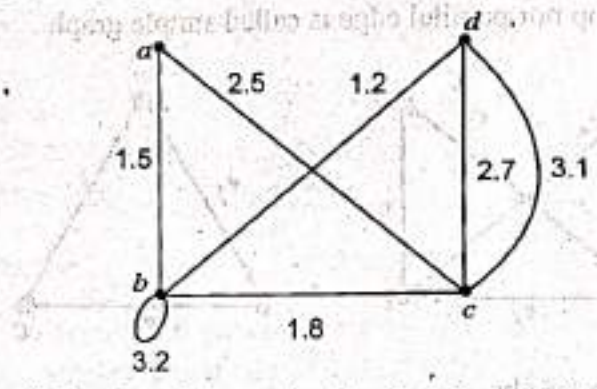
For example : Following graphs are complete graph.



Note I : A complete graph with n vertices is usually denoted by K_n.

II : A complete graph has C $(n, 2)$ edges.

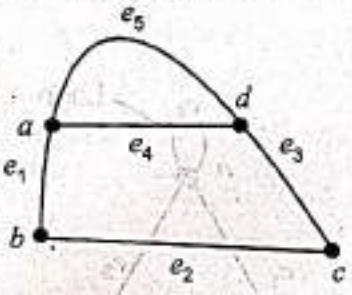
(iv) Weighted graph : Let G = (V, E) be any graph and $\omega : E \to R$ be a function from edge set E to set real numbers R. Then the graph G = (V, E, ω) in which each edge is assigned a number called the weight of the edge, is known as weighted graph.



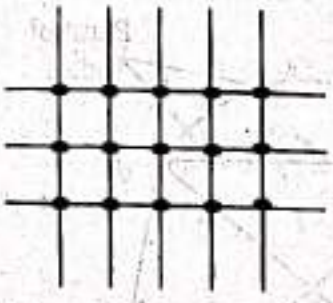
The above graph is a weighted graph, as each edge is assigned with a number.

(v) Finite graph : A graph G = (V, E) is called a finite graph if the vertex set V is a finite set.

(vi) Infinite graph : A graph G = (V, E) is called an infinite graph if the vertex set V is an infinite set.



(Finite graph)



(Infinite graph)

(vii) Order of a graph : Let G be a graph then the no. of vertices denoted by | V(G)| is called order of G.

(viii) Define Trivial graph, Null or empty graph

The trivial graph is the graph with one vertex and no edges.

The empty graph is the graph with No vertices and no edges.

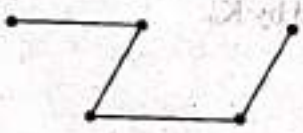
(ix) Edges in series : When two edges in a graph have exactly one vertex in common and this vertex is of degree two, then two edges are said to be in series.

Example.

e_1, e_2 are in series whereas e_2, e_3 are not in series.

(x) Acyclic : An Acyclic is a simple graph which does not have any cycles. *i.e.* No loop exists in such graphs.

Example :



1.4. Degree in a Graph

In-degree

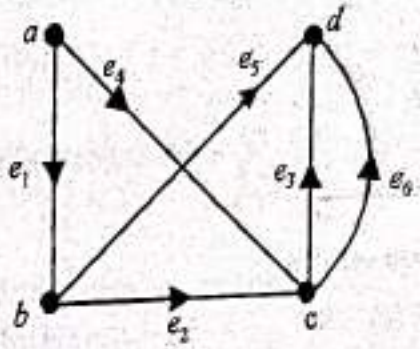
In a directed graph G, the **in-degree** of a vertex "a" is defined as the number of edges which have "a" as the terminal vertex. The in degree of the vertex a is denoted by deg $G^+(a)$ or $d^+(a)$.

Out-degree

In a directed graph G, the **out-degree** of a vertex "a" is defined as the number of edges which have "a" as the initial vertex. The out-degree of the vertex a is denoted by deg $G^-(a)$ or $d^-(a)$

Remark. (*i*) A vertex in a directed graph with in-degree zero is called a **source** and out-degree zero is called a **Sink**.

(*ii*) The direction of a loop in a directed graph has no significance.



In the above figure

deg $G^-(a) = 2$, deg $G^+(a) = 0$

deg $G^-(d) = 0$, deg $G^+(d) = 3$

deg $G^-(c) = 2$, deg $G^+(c) = 2$

In above graph, vertex "a" is called a **source** and the vertex "d" is called a **Sink.**

Even or odd (Parity) of a Vertex : The vertex V is said to be even or odd according as deg.(V) is even or odd.

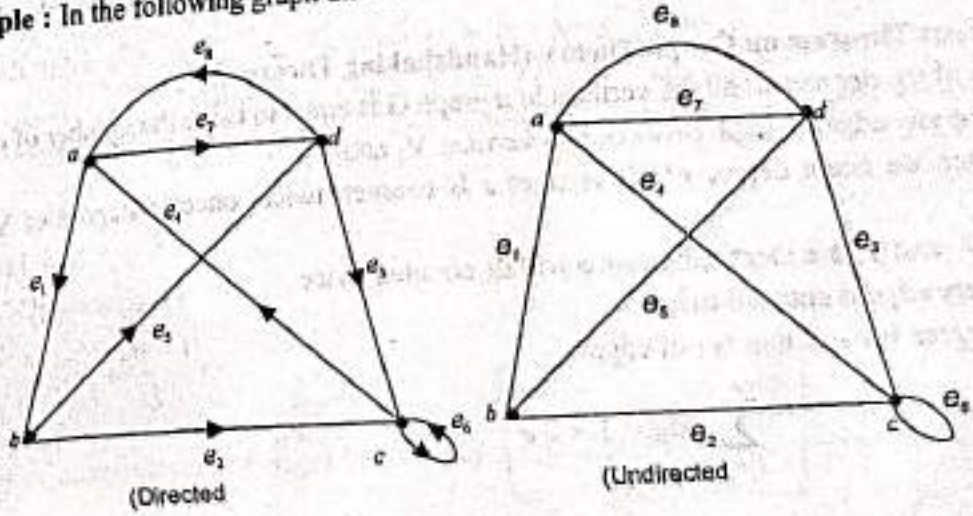
Degree

The degree of a vertex "a" in a directed or undirected graph is defined as the total number of edges incident with a. The degree of a vertex a is denoted by deg G (a) or $d(a)$.

Thus in a direct graph deg G (a) = deg $G^+(a)$ + deg $G^-(a)$.

Remark. For calculating degree of a a vertex in a general graph, a loop is counted twice.

For example : In the following graph directed or undirected we have



In directed graph

$\deg G(x) = \deg G^+(x) + \deg G^-(x)$

$\therefore$ $\deg G(a) = 2 + 2 = 4$

$\deg G(b) = 1 + 2 = 3$

$\deg G(c) = 2 + 3 = 5$

$\deg G(d) = 3 + 1 = 4$

In undirected graph

$\deg G(a) = 4$

$\deg G(b) = 3$

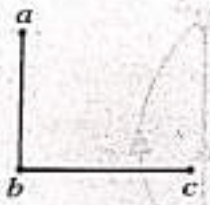
$\deg G(c) = 5$

$\deg G(d) = 4$

Pendent vertex (End vertex)

A vertex whose degree in a graph is one is called pendent vertex.

For example :- In the following graph



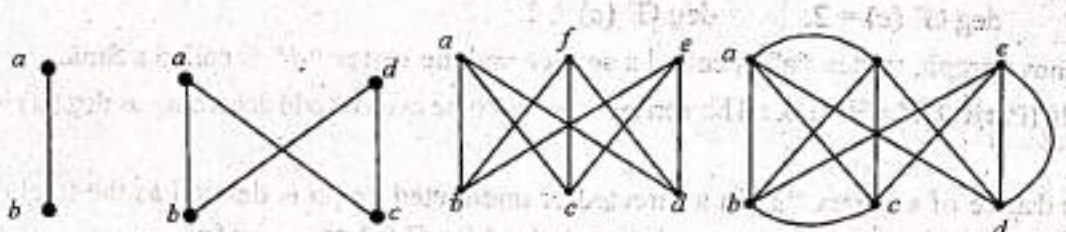
The vertices a and c are pendent vertices.

since $\deg G(a) = 1$ and $\deg G(c) = 1$

Definition Regular Graph : A graph in which all the vertices are of same degree is called a regular graph.

Definition k-Regular Graph : A graph in which all the vertices have the same degree equal to k, is called a k-Regular graph.

For example :



(1-Regular graph) (2-Regular graph) (3-Regular graph) (4-Regular graph)

Note : Complete Graph k_n is $n-1$ regular.

Next, we have a very important, but simple result on graph theory known as the first theorem on graph theory.

Theorem 1. First Theorem on Graph Theory (Handshaking Theorem)

The sum of the degrees of all the vertices in a graph G is equal to twice the number of edges in G.

Proof : Let e be any edge in graph between two vertices V_1 and V_2.

Now, when we count degree of all vertices e is counted twice, once in degree of V_1 and again in degree of V_2.

Also, if V_1 and V_2 are identical, again e will be counted twice. ($\because$ e is self-loop)

Hence every edge is counted twice.

So total degree is twice number of edges.

or

$$\sum_{i=1}^{n} \deg(v_i) = 2e$$

Theorem 2. Prove that in a graph the number of vertices of odd degree is even.

Proof. Let $v_1, v_2, \ldots\ldots, v_n$ be n-vertices and $e_1, e_2, \ldots\ldots, e_e$ be e-edges in the graph G. Then by first theorem on graph theory

$$\sum_{i=1}^{n} d\ (v_i) = 2e \qquad \ldots (1)$$

Now, divide the sum on the L.H.S of (1) in two parts

(*i*) One part contains the sum of degree of vertices which have even degree.

(*ii*) Second part contains the sum of the vertices which have odd degree.

Then equation (1) can be written as

$$\sum_{\text{even}} d\ (v_i) + \sum_{\text{odd}} d\ (v_k) = 2e \qquad \ldots(2)$$

Since the R.H.S of (2) is an even number. Also $\sum_{\text{even}} d\ (v_i)$ is also even. This implies that $\sum_{\text{odd}} d\ (v_k)$ is also even.

i.e. the sum of the degree of vertices having odd degrees is even

$\therefore$ The number of vertices having odd degree must be even.

Theorem 3. Prove that the maximum degree of any vertex in a simple graph having n vertices is $n-1$.

Proof. Since, in a simple graph, there are no parallel edges and no loops. Therefore a vertex can be connected to the remaining $n-1$ vertices at the most by $(n-1)$ edges.

Hence, the maximum degree of any vertex in a simple graph having n vertices is $n-1$.

Theorem 4. Show that the maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.

Proof. Let $v_1, v_2, \ldots\ldots, v_n$ be n-vertices and $e_1, e_2, \ldots\ldots, e_e$ be e-edges in a simple graph G. Then

By First theorem on graph theory $\sum_{i=1}^{n} d\ (v_i) = 2e \qquad \ldots(1)$

Also, we know that

In a simple graph, the maximum degree of any vertex with n vertices is $n-1$.

$\therefore$ Sum of maximum degrees of n vertices $= \underbrace{(n-1) + (n-1) + \ldots\ldots + (n-1)}_{n \text{ terms}}$

$$= n\ (n-1)$$

$\therefore$ from (1), we have

$$2e = n\ (n-1)$$

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

$\therefore$ The maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.

Theorem 5. Prove that the number of edges in a complete graph with n vertices is $\frac{n(n-1)}{2}$.

Proof. Since every vertex in a complete graph is joined with every other vertex through one edge

$\therefore$ The degree of every vertex in a complete graph of n vertices is $n-1$.

$\therefore$ If e be the total number of edges in G. Then by first theorem on graph theory, we have

$$\sum_{i=1}^{n} d(v_i) = 2e$$

$$n(n-1) = 2e \qquad [\because d(v_i) = n-1 \text{ for } 1 \le i \le n]$$

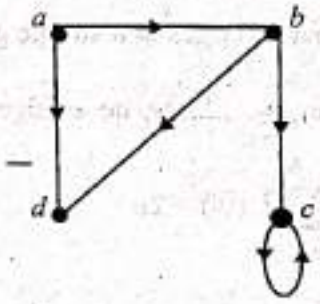
$$\Rightarrow \quad e = \frac{n(n-1)}{2}$$

$\therefore$ Total number of edges in G $= \frac{n(n-1)}{2}$.

ILLUSTRATIVE EXAMPLES

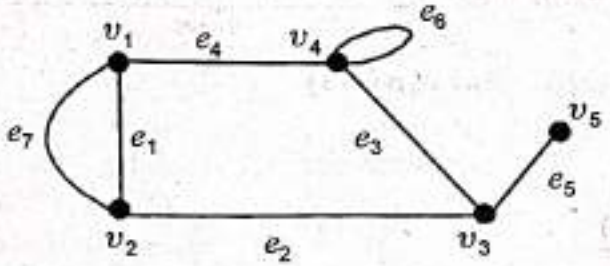
Example 1. If $V = \{a, b, c, d\}$ and $E = \{(a, b), (a, d), (b, c), (b, d), (c, c)\}$ be the vertex set and edge set of a graph G. Draw the directed graph $G = (V, E)$. Is it a simple graph?

Sol. The directed graph $G = (V, E)$ is as shown below :-



Since it contain a loop. Therefore it is not a simple graph.

Example 2. Find the degree of each vertices of the following graph.



Also verify first theorem on graph theory.

Sol. Here $d(v_1) = 3$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 4$, $d(v_5) = 1$

By first theorem of graph theory

$$\sum_{i=1}^{n} d\ (v_i) = 2e$$

where e is the number of edges and n is the number of vertices in the graph.

Here $n = 5$ and $e = 7$

Also $d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) = 3 + 3 + 3 + 4 + 1 = 14 = 2(7) = 2e$

Thus first theorem on graph theory is verified.

Example 3. A graph G has 21 edges, 3 vertices of degree 4 and all other vertices are of degree 3. Find the number of vertices in G.

Sol. Let n be the number of vertices in G.

According of first theorem on graph theory.

$$\sum_{i=1}^{n} d\ (v_i) = 2e, \text{ where } e \text{ is the no. of edges.}$$

Let v_1, v_2, v_3 be the vertices of degree 4 and $v_4, v_5, \ldots\ldots, v_n$ be the remaining vertices of degree 3

$$\therefore \quad \sum_{i=1}^{3} d(v_i) + \sum_{k=4}^{n} d\ (v_k) = 2(21)$$

$$3\times4 + (n-3)\times3 = 42$$

$$12 + 3n - 9 = 42$$

$$3n = 39$$

$$n = 13$$

$\therefore$ Number of vertices in G be 13.

Example 4. Prove that there does not exist a graph with 5 vertices with degree equal to 1, 3, 4, 2, 3 respectively.

Sol. Here $n = 5$, Let e be the number of edges in the graph

By first Theorem on graph theory

$$\sum_{i=1}^{5} d(v_i) = 2e$$

$$\Rightarrow \quad 1+3+4+2+3 = 2e$$

$$\Rightarrow \quad 13 = 2e$$

$$\Rightarrow \quad e = \frac{13}{2}, \text{ which is not possible}$$

Hence there does not exist a graph with 5 vertices of given degrees.

Example 5. Is there a simple graph G with six vertices of degree 1, 1, 3, 4, 6, 7 ?

Sol. Here number of vertices in the graph, $n = 6$

we know that

Maximum degree of any vertices in a simple graph $= n - 1 = 6 - 1 = 5$

But G has a vertices of degree 7, which is not possible in a simple graph.

Hence there is no simple graph G of six vertices having the given degrees.

Example 6. (*a*) Find k, if a k-regular graph with 8 vertices has 12 edges. Also draw k-regular graph. (*b*) Can there be a graph with 8 vertics and 29 edges ? Justify.

Sol. (*a*) We know that a graph G will be a k-regular graph if the degree of all the vertices in G are same and equal to k.

Also, number of vertices, $n = 8$

number of edges, $e = 12$

$\therefore$ By the first theorem on graph theory, we have

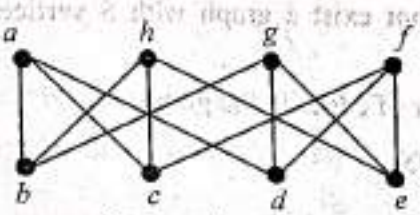
$$\sum_{i=1}^{n} d(v_i) = 2e$$

$$\sum_{i=1}^{8} k = 2(12)$$

$\Rightarrow$ $8k = 24$

$\Rightarrow$ $k = 3$ so graph is 3-regular graph

and the 3-regular graph is



(3-Regular graph)

(*b*) Maximum no. of edges in graph with no multiple edges $= \frac{(n)(n-1)}{2}$

$n = 8$ $\therefore$ max. no. of edges, $= \frac{(8)(8-1)}{2} = 28$

but given no. of edges $= 29$

$\therefore$ It is not possible.

1.5. Isomorphic Graphs

Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. Then G is isomorphic to G' written as $G \cong G'$ if there exists a bijection f, from V onto V' such that $(v_i, v_j) \in E$, if and only if $(f(v_i), f(v_j)) \in E'$.

In other words, two graphs are isomorphic if there exists a one-one correspondence between their vertices and edges such that incidence relationship is preserved.

Remark. (*a*) Two graphs which are isomorphic will have

(*i*) same number of vertices

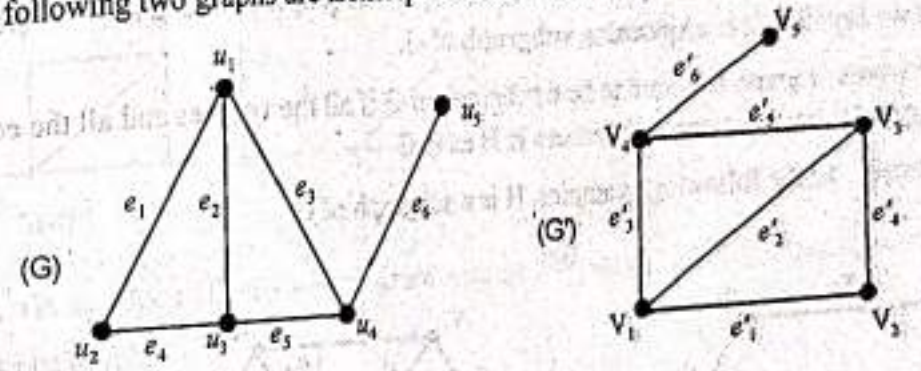
(*ii*) same number of edges

(*iii*) an equal number vertices with given degrees

(*b*) The converse of (*a*) need not be true.

For example.

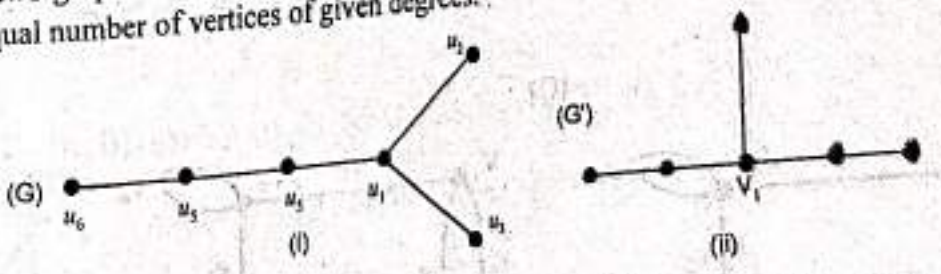
(*a*) The following two graphs are isomorphic to each other



Because $\exists$ a mapping $u_i \xrightarrow{f} v_i$ for $i = 1, 2, 3, 4, 5$

and $e_i \xrightarrow{f} e'_i$ for $i = 1, 2, 3, 4, 5$

(*b*) The two graphs may be non-isomorphic even though they have the same number of vertices and edges and an equal number of vertices of given degrees.



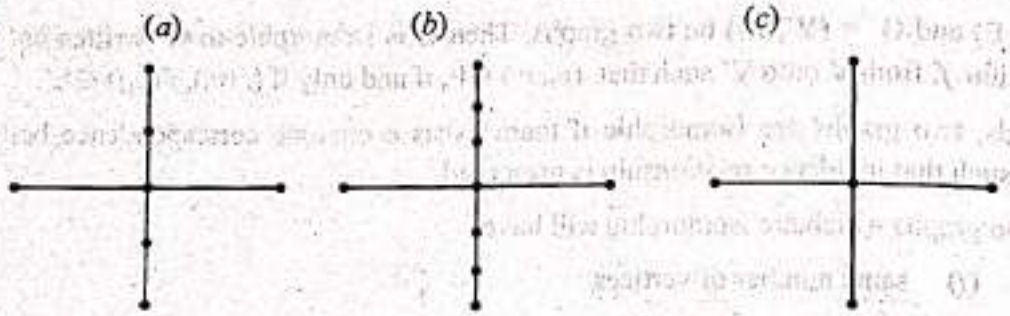
If the graph G are the to be isomorphic to graph G', then the vertex u_1 must corresponds to v_1, because there is no other vertex of degree 3 in G'. Also in G' there is only one pendent vertex v_2 adjacent to v_1, while in G there are two pendent vertices u_2 and u_3 adjacent to u_1.

Hence $G \ncong G'$.

Homeomorphic Graphs

Given any graph G, obtain a new graph by dividing an edge of G with additional vertices.

e.g.



(*a*) and (*b*) Homeomorphic obtained from (*c*).

Sub-Graphs

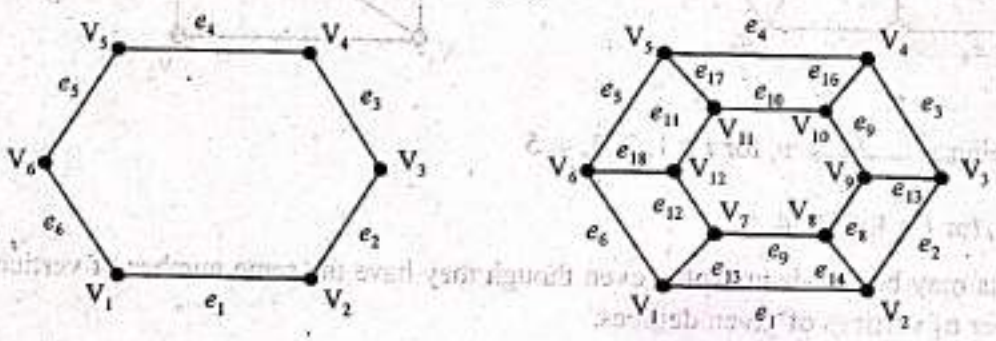
Let G and H be two graphs with vertex sets V(H), V(G) and edge sets E(H) and E(G) respectively such that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$, then we call H as a **Subgraph** of G (or G as a supergraph of H).

If $V(H) \subset V(G)$ and $E(H) \subset E(G)$, then H is a **Proper subgraph** of G and if $V(H) = V(G)$ and $E(H) \subset E(G)$ then we say that H is a **spanning subgraph** of G.

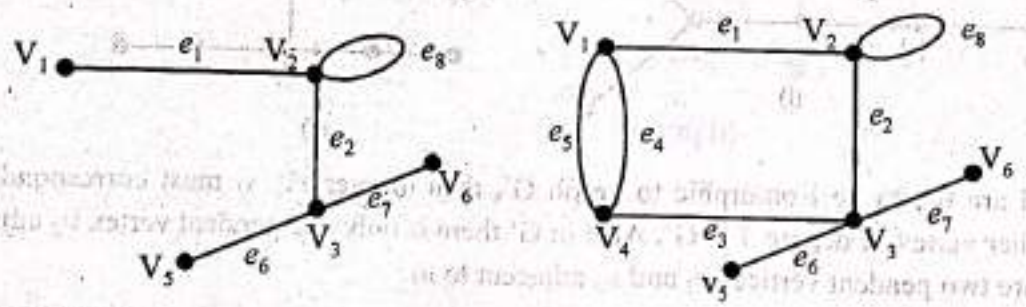
In other words, a graph H is said to be a subgraph of G if all the vertices and all the edges of H are in G, and each edge of H has the same end vertices in H as in G.

For example. In the following examples, H is a subgraph of G.

(*i*) (H) (G)



(*ii*) (H) (G)



Full Subgraph

Suppose H(V′, E′) be a subgraph of G(V, E). H is called full subgraph of G if E′ contains all the edges of E whose end points lie in V′. It is called subgraph of G generated by V′.

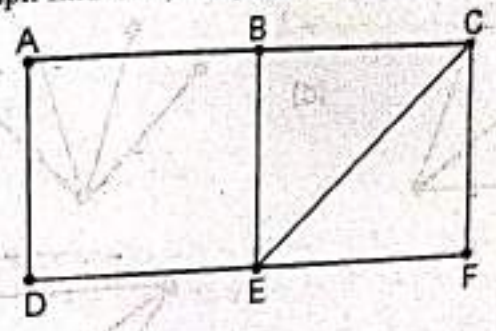
Define G-V

G-V is a subgraph of G obtained by deleting the vertex V from vertex set V(G) and deleting all the edges in E(G) which are incident on V.

Cut Vertex

A vertex V is called a cut vertex for G if G-V is disconnected.

Example. Let G be the graph find G-A, G-B, G-C

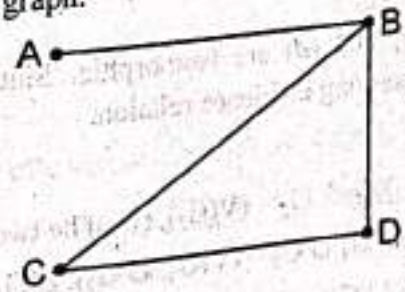


Sol.

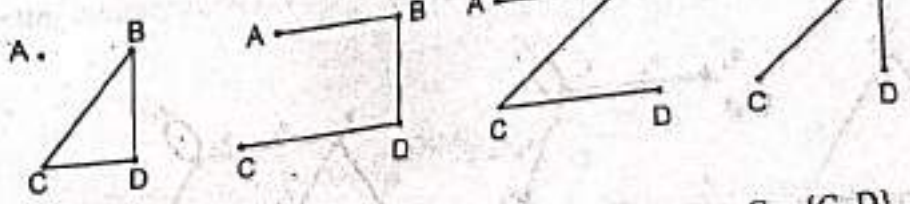
(a) (b) (c)

Define : G – e, e is an edge in G. G– e is the graph obtained by simply deleting e from the edge set of G.

Example. Let G be graph.



Find (*a*) G – {A, B} (*b*) G – {B, C} (*c*) G – {B, D} (*d*) G – {C, D}

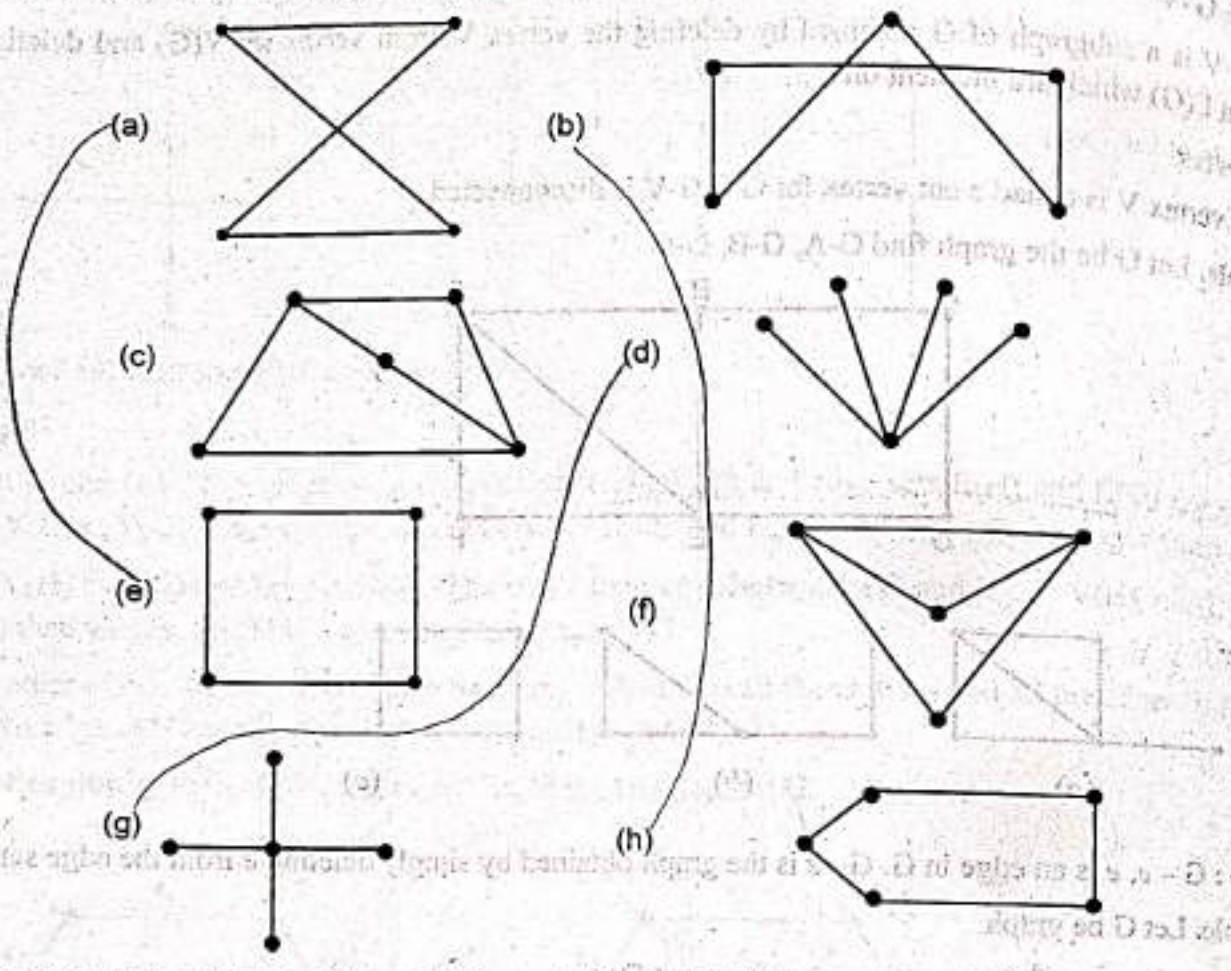


G – {A, B} G – {B, C} G – {B, D} G – {C, D}

Remark. (*i*) Every graph is its own subgraph

(*ii*) The null graph obtained from G by deleting all the edges of G is a subgraph of G.

Example 7. Which of the following pair of graphs are isomorphic ?



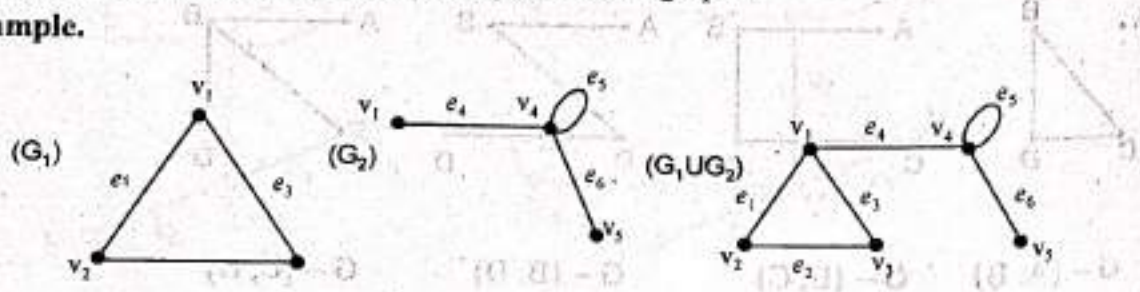
Sol. The graphs (a) and (e) ; (b) and (h) ; and (g) and (d) are isomorphic. Since there a one-one correspondence between the vertex and the edge set preserving incidence relation.

Operations of Graph

(*i*) Union of two graphs : Let $G_1 = (V(G_1), E(G_1))$ and $G_2 = (V(G_2), (G_2))$ be two graphs. Then their union is denoted by $G_1 \cup G_2$, is a graph $G_1 \cup G_2 = (V(G_1, \cup G_2), E(G_1, \cup G_2))$ such that $V(G_1, \cup G_2) = V(G_1) \cup V(G_2)$ and $E(G_1 \cup G_2) = E(G_1) \cup E(G_2)$

In other words, union of two graphs is a graph whose vertex set is the union of the vertex sets of the two graphs and edge set is the union of the edge sets of the two graphs.

For example.



(*ii*) Intersection of two graphs : Let $G_1 = (V(G_1), E(G_2))$ and $G_2 = (V(G_2), E(G_2))$ be two graphs. Then their intersection is denoted by $G \cap G_2$, is a graph

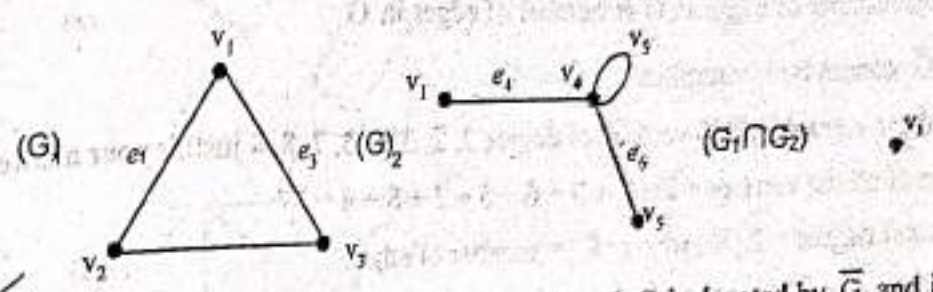
$$G_1 \cap G_2 = (V(G_1 \cap G_2), E(G_1 \cap G_2))$$

such that $V(G_1 \cap G_2) = V(G_1) \cap V(G_2)$

$E(G_1 \cap G_2) = E(G_1) \cap E(G_2)$.

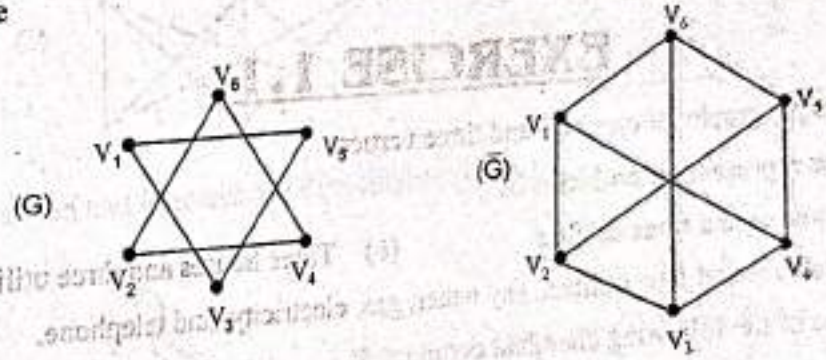
In other words, intersection of two graphs is a graph whose vertex set is the intersection of the vertex sets of the two graphs and edge set is the intersection of the edge sets of the two graphs.

For example.



***(iii)* Complement of a graph.:** The compliment of a graph G is denoted by $\overline{G}$ and is defined as the simple graph with the vertex set same as the vertex set of G together with the edge set satisfying the property that there is an edge between two vertices in $\overline{G}$, when there is no edge between these vertices in G.

For example



Note :- If the degree of a vertex v in a simple graph G having n vertices is k. Then degree of v in $\overline{G}$ is n-k-1.

Example 8. What is total number of edges in k_n the complete graph on n vertices ? Justify your answer ?

Sol. We know number of vertices in $k_n = n$

also in complete graph there is an edge between every two vertices.

So we have to make pairs of n vertices

for this number of ways $= c(n, 2)$

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

$\therefore$ number of edges in complete graph $= \frac{n(n-1)}{2}$

Example 9. Can a graph with seven vertices be isomorphic to its complement ? Justify.

Sol. Let G be the given graph and $\overline{G}$ is complement of G. We know, if an edge $e \in G$ then $e \notin \overline{G}$.

So total number of edges in G and $\overline{G}$ = Maximum number of possible edges in complete graph.

Here we have number of vertices = 7

Using 7 vertices max. number of edge $= \frac{7(7-1)}{2}$

$= 21$

So number of edges in G and $\overline{G} = 21$

which means number of edges in G $\neq$ number of edges in $\overline{G}$ [$\because$ 21 is odd]

So G and $\overline{G}$ cannot be isomorphic.

Example 10. Is there a graph with 8 vertices of degree 2, 2, 3, 6, 5, 7, 8, 4 justify your answer.

Sol. Total degree of all the vertices = 2 + 2 + 3 + 6 + 5 + 7 + 8 + 4 = 37

We know total degree = 2 | E | where | E | = number of edges

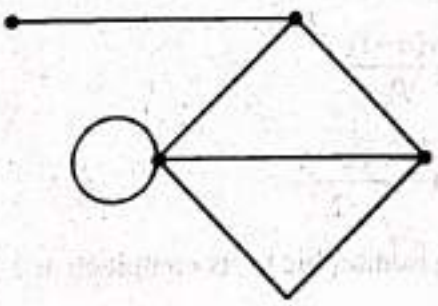
$\therefore \quad 37 = 2|E| \Rightarrow |E| = \frac{37}{2}$

which is not possible.

Hence given graph does not exists.

EXERCISE 1.1

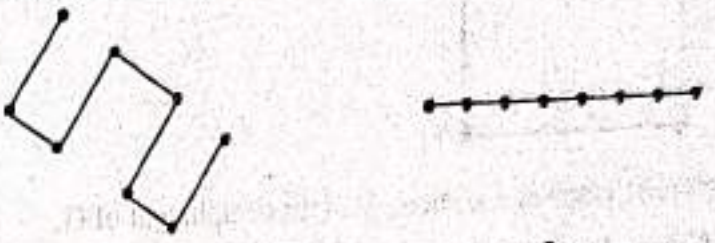
1. Draw all simple graphs of one, two and three vertices.
2. Draw graphs representing problems of
   (*a*) Two houses and three utilities (*b*) Three houses and three utilities
   (*c*) Four houses and four utilities, say water, gas, electricity, and telephone.
3. Draw graphs of the following chemical compounds
   (*a*) CH_4 (*b*) C_2H_6 (*c*) C_6H_6
4. Differentiate between directed graph and undirected graphs.
5. How many nodes are necessary to construct a 2-regular graph with exactly 6 edges ?
6. Is it possible to construct a graph with 12 edges such that two of its vertices have degree 3 and remaining vertices have degree 4 ?
7. Find the degree of each vertices in the following graph :



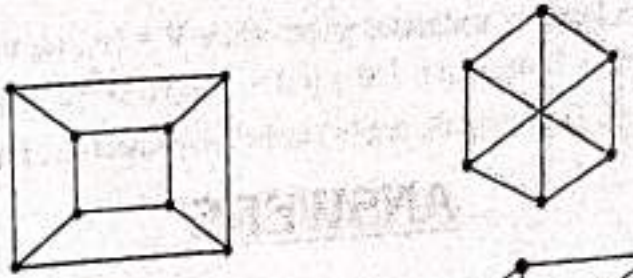
8. Does there exist a graph with 6 vertices with degree equal to 3, 2, 4, 1, 3, 2 respectively.
9. Find *k*, if a *k*-regular graph with 7 vertices has 14 edges. Also draw the k-regular graph.
10. Find *n*, if a complete graph having *n* vertices has 15 edges.

11. Draw 3-regular graph with eight vertices.
12. Draw 3-regular graphs with nine vertices.
13. Which of the following pair of graphs are isomorphic ?

(a)



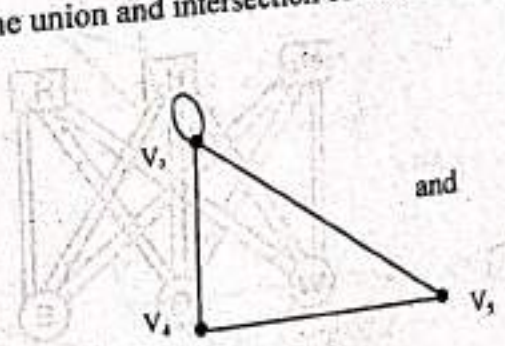
(b)



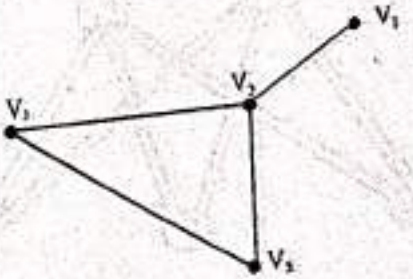
(c)

14. Find the union and intersection of the following graphs.

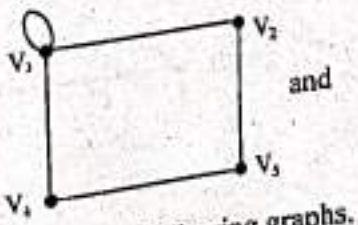
(*i*)



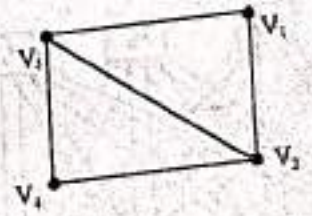
and



(*ii*)



and

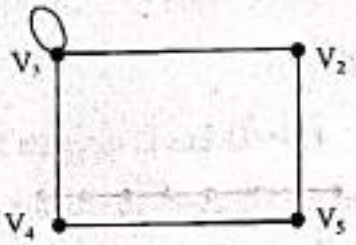


15. Find the compliment of the following graphs.

(*i*)

(G)

(*ii*)

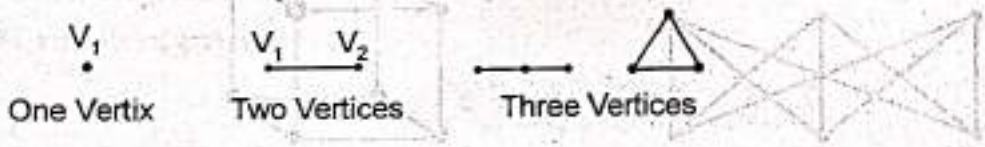


16. Let G be a complete graph of n vertices. Find the compliment of G.

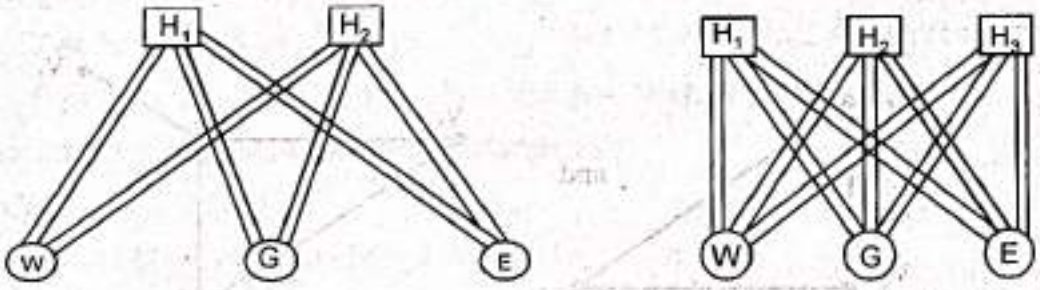
17. Let G = (V, E) be a loop free undirected graph, where V = $\{v_1, v_2, v_3, \ldots\ldots, v_{10}\}$. If deg $(v_1) = 2$, deg $(v_2) = 3$, deg $(v_3) = 3$, deg $(v_4) = 5$, deg $(v_5) = 1$, deg $(v_6) = 2$, deg $(v_7) = 5$, deg $(v_8) = 2$, deg $(v_9) = 3$, deg $(v_{10}) = 2$. Determine the deg (v_i) in the compliment $\overline{G}$, for all $1 \leq i \leq 10$.

ANSWERS

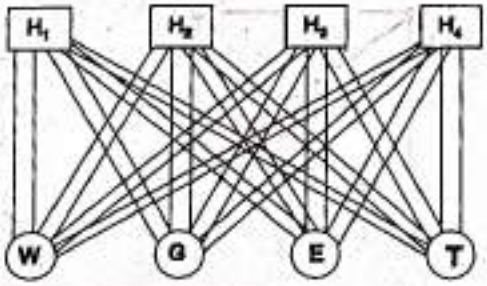
1.



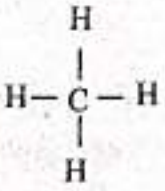
2. (*a*) (*b*)



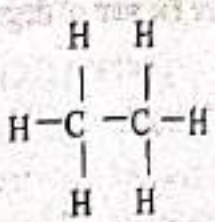
(*c*)



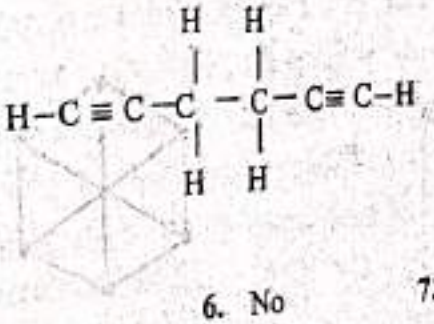
3. (*a*) CH_4



(b) C_2H_6



(c) C_6H_6



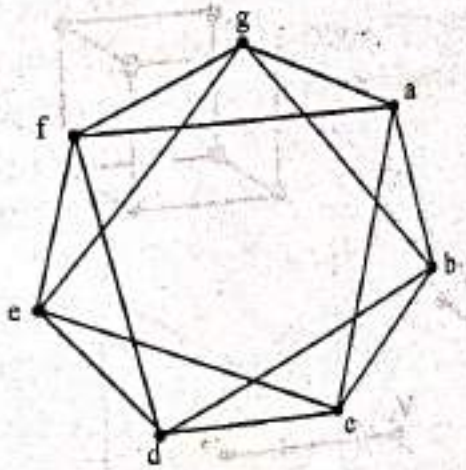
6. No

7. 1, 3, 5, 2, 3

8. No

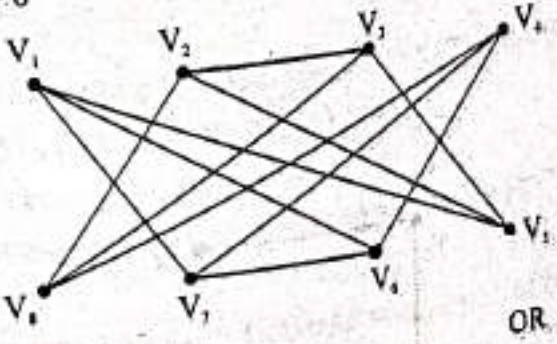
5. 6

9. $k = 4$

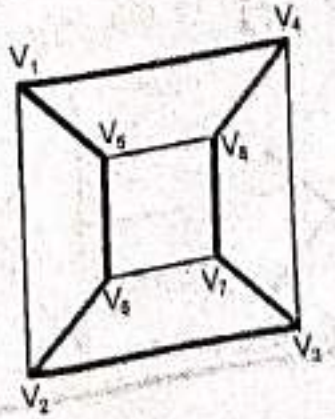


10. $n = 6$

11.



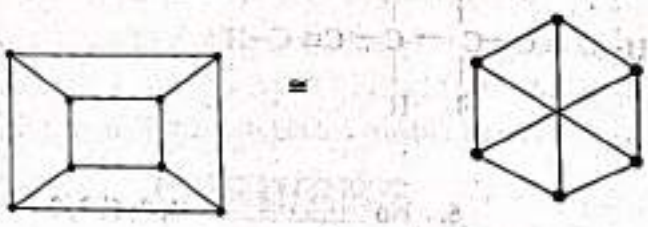
OR

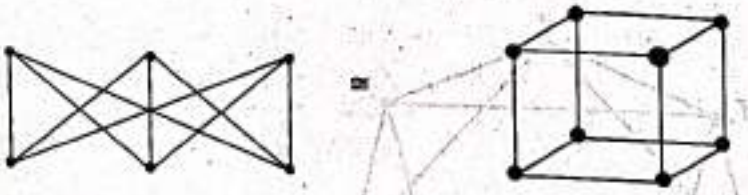


12. There is no 3-regular graph with nine vertices because the sum of degree of all the vertices is $3 \times 9 = 27$ which is not even.

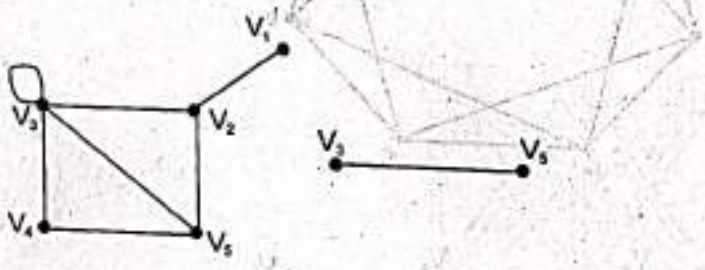
13.

(a) Yes 

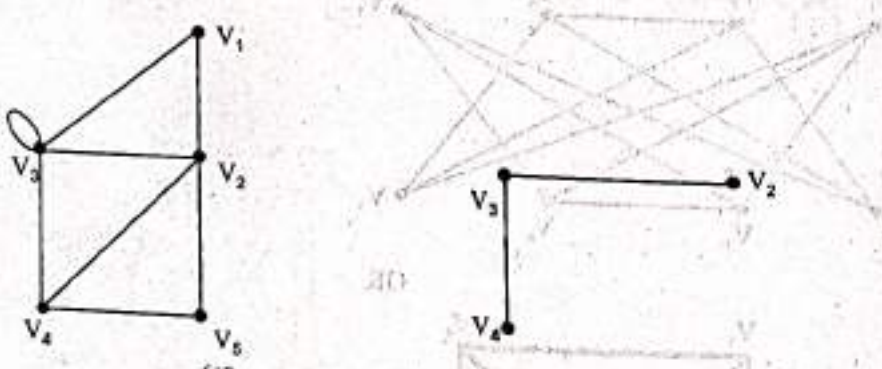
(b) No 

(c) No 

14. (*i*)

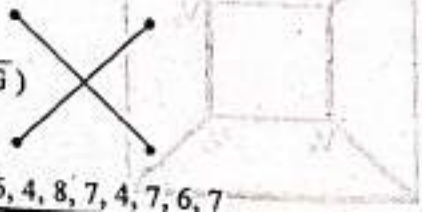


(*ii*)



15. (*i*)

(*ii*)



$(\overline{G})$

$(\overline{G})$

16. Null graph

17. 7, 6, 6, 4, 8, 7, 4, 7, 6, 7

1.6. Walks, Paths and Circuits

Walk : A walk in a graph G is finite sequence

$$W = V_0, e_1, V_1, e_2, \ldots\ldots, V_{k-1}, e_{k-1}, V_k$$

whose terms are alternatively vertices and edges such that for $1 \le i \le k-1$, the edge e_i has end vertices v_{i-1} and v_i. The vertex V_0 is called the initial and the vertex V_k is called terminal of the walk W. Vertices $V_1, V_2, \ldots, V_{k-1}$ are called internal vertices. A walk is also refereed as an edge train or chain.

Remark. (*i*) Each edge can appear only once in a walk, however vertices may appear more than once.

Open Walk : If a walk begin and end with the different vertices, it is called an open walk.

Closed Walk : If the initial and terminal vertices of a walk are same, it is called a closed walk.

Remark. A walk containing no edge and has length zero is called a **Trivial walk.**

PATH : An open walk in which no vertex appear more than once is called a path or simple path.

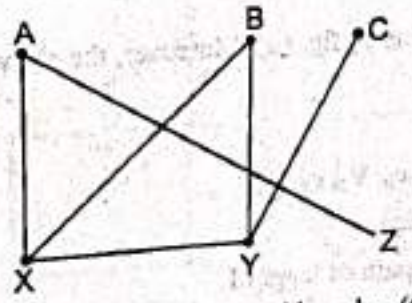
Note : A path do not intersect it self.

Simple Path and Trail

A path is **simple** if all vertices are distinct. The path is a **trail** if all the edges are distinct.

Example. Let G be the graph. Determine whether or not each of the following sequences of edges forms a path

(*a*) {(A, X), (X, B), (C, Y), (Y, X)}
(*b*) {(A, X), (X, Y), (Y, Z), (Z, A)}
(*c*) {(X, B), (B, Y), (Y, C)}
(*d*) {(B, Y), (X, Y), (A, X)}



Sol. (*a*) No, the edge {X, B} is not followed by edge (C, Y).

(*b*) No, Graph has not edge (Y, Z)

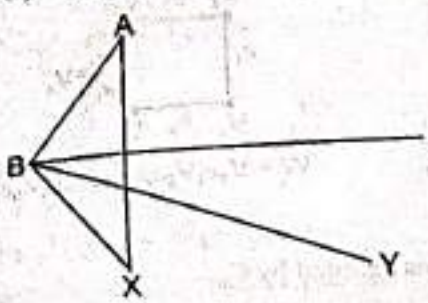
(*c*) Yes

(*d*) Yes, sequence can be written as {(B, Y), (Y, X), (X, A)}

[In undirected graph (Y, X) and (X, Y) are same]

Example. Let G be the graph. Determine whether each of the following is a closed path, trail, simple path or cycle.

(*a*) (B, A, X, B) (*b*) (X, A, B, Y) (*a*) (B, X, Y, B)



(*a*) This path is a cycle since it is closed and has distinct vertices.

(*b*) This path is simple since it vertices are distinct. It is not cycle since it is not closed.

(*c*) This not even a path since {X, Y} is not an edge.

Length of path : The number of edges appearing in the sequence of the path is called the length of the path.

For example. Consider the following graph

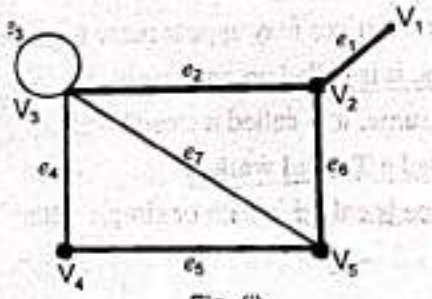


Fig. (i)

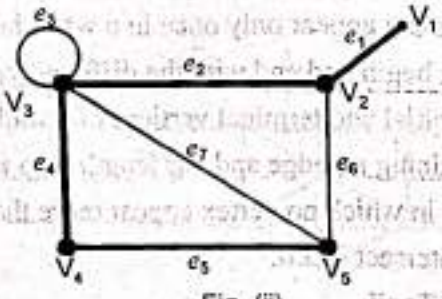


Fig. (ii)

$W = V_1, e_1, V_2, e_2, V_3, e_3, V_3, e_4, V_4, e_5, V_5, e_6, V_2$.

Then W is a walk of length 6 as shown by the bold line in fig. (*i*). The above walk is not a path as the vertices V_3 and V_2 appear twice in the walk W. However the walk

$W' = V_1, e_1, V_2, e_2, V_3, e_4, V_4, e_5, V_5$

is a path of length 4 as shown by the bold line in fig. (*ii*). Moreover, the above walk W and W' are open walk as their terminus vertices are different.

But the walk

$W'' = V_1, e_1, V_2, e_3, V_3, e_3, V_3, e_4, V_4, e_5, V_5, e_6, V_2, e_1, V_1$

is a closed walk as the terminus vertices are same.

Remark. (*i*) An edge which is not a self loop is a path of length 1.

(*ii*) A self loop can be included in a walk but not in a path.

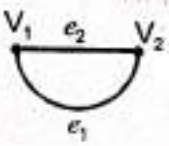
(*iii*) The terminus vertices of a path are of degree 1 and the internal vertices of the walk are of degree 2.

CIRCUIT : A circuit is a closed walk in which no vertex (except the initial and terminal vertex) appears more than once.

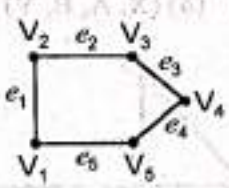
In other words, a circuit is a closed, non-intersecting walk. A circuit is also called the cycle or **elementary cycle** or **circular path** or **polygon.**

For example.

$W = V_1 e V_1$



$W = V_1 e_1 V_2 e_2 V_1$



$W = V_1 e_1 V_2 e_2 V_3 e_3 V_4 e_4 V_5 e_5 V_1$

are all circuits.

***k*-cycle :** A cycle with *k*-edges is called a k-cycle and it is denoted by C_k.

Remark (*i*) A self loop is also a circuit, but converse is not true.

(*ii*) The degree of every vertex in a circuit is two.

(*iii*) 1 cycle is loop, 2-cycle is a pair of parallel edges, 3 cycle is a triangle..... *n* cyclic is a polygon of *n* sides.

CONNECTED GRAPHS, DISCONNECTED GRAPHS, AND COMPONENTS

Connectivity : An undirected graph is said to be connected, if for any pair of vertices of the graph the two vertices are reachable from one another.

Strongly Connected : If any pair of vertices of the digraph both the vertices of the pair are reachable from another, then graph is strongly connected.

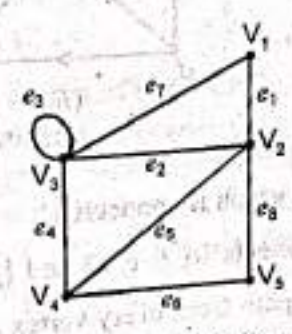
Unilaterally Connected : A simple directed graph is said to unilaterally connected if for any pair of vertices of the graph, at least one of the vertices of the pair is reachable from other vertex.

Weakly Connected Digraph : A directed graph is called weakly connected if its undirected graph is connected.

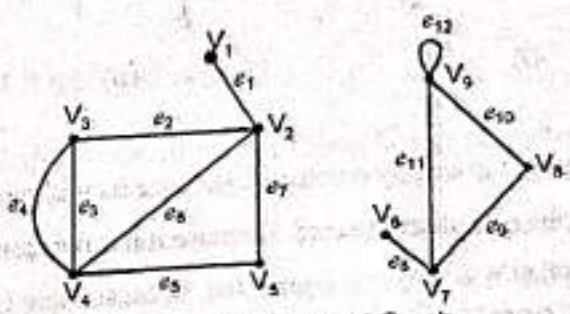
Connected graph : A graph G is said to be connected graph if there is atleast one path between every pair of vertices in G.

Disconnected graph : A graph which is not a connected graph is called disconnected graph.

For example.



Connected Graph

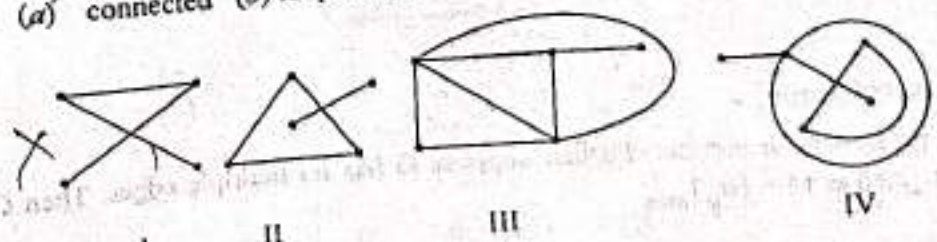


Disconnected Graph
(with two components)

Component : Each connected subgraph of a disconnected graph are called component.

Example. Consider the multigraph which of them are

(*a*) connected (*b*) loop-free (*c*) simple graphs



I II III IV

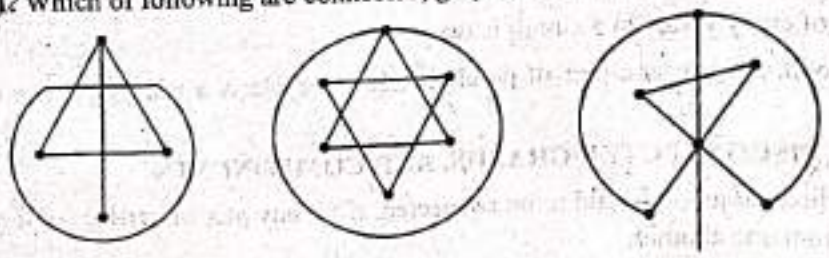
(*a*) I and III are connected.

(*b*) only IV has a loop.

(*c*) only (I) and (II) are simple graphs

(III) has multiple edges and IV has multiple edges and a loop.

Example 1. Which of following are connected, graphs.

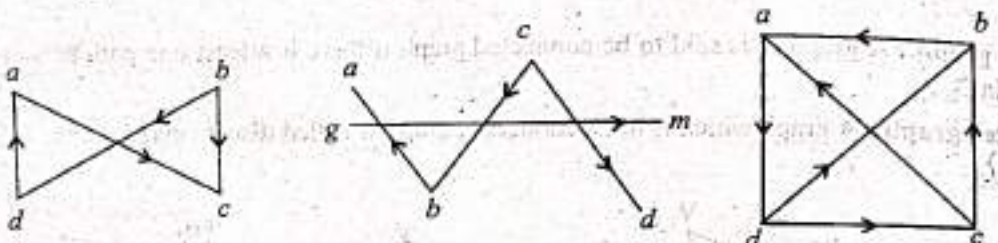


I II III

(*a*) Only III is connected.

(*b*) All are graphs.

Example 2. Classify the following graphs as : Strongly connected graph, unilaterally connected graph, weakly connected graph and disconnected graph.



Sol.

(*a*) The graph (*i*) is weakly connected because its undirected graph is connected.

(*b*) The graph (*ii*) is disconnected. Because it has two components $\{a, b, c, d\}$ and $\{g, m\}$

(*c*) The graph (*iii*) is strongly connected, because there is a path from every vertex u to v and v to u. It is also weekly and unilaterally connected as strongly connected graph obey properties of both these.

1.7. Matrix Representation of Graphs

A graph can be represented by a matrix in two ways :

(*i*) Adjacency matrix

(*ii*) Incidence matrix.

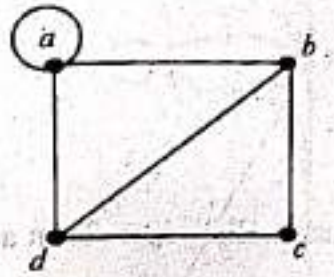
Adjacency Matrix (for undirected graph) :

Let G be an undirected graph with n vertices. Further suppose G has no multiple edges. Then G is represented by $n \times n$ matrix defined as $M = [a_{ij}]_{n \times n}$

$$a_{ij} = \begin{cases} 1 & \text{if } a_i \text{ and } a_j \text{ are adjacent} \\ 0 & \text{otherwise} \end{cases}$$

i.e. an entry is 1 if there is an edge between a_i and a_j.

ample : Consider the graph



Find Adjacency matrix.

l.

	a	b	c	d
a	1	1	0	1
b	1	0	1	1
c	0	1	0	1
d	1	1	1	0

So $M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

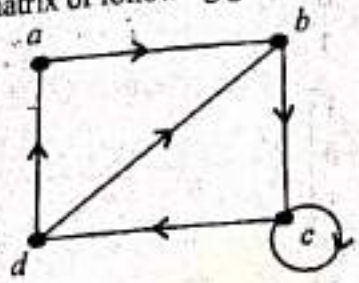
te : Adjacency matrix of undirected graph is always symmetric.

Adjacency matrix of Directed Graph.

Let G be digraph with n vertices having no multiple edges. Then G can be represented by $n \times n$ acency matrix m defined by

$$a_{ij} = \begin{cases} 1 & \text{if there is edge from } a_i \text{ to } a_j \\ 0 & \text{otherwise} \end{cases}$$

ample : Write adjacency matrix of following graph



l.

	a	b	c	d
a	0	1	0	0
b	0	0	1	0
c	0	0	1	1
d	1	1	0	0

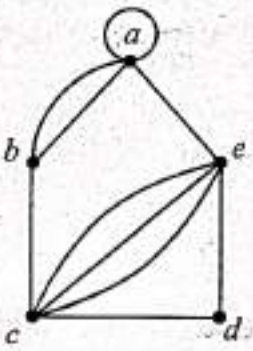
So $$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Adjacency matrix of multi-graph (undirected)

Let G be undirected graph of n vertices that may contain parallel edges. Then adjacency matrix M is $n \times n$ matrix defined by $M = [a_{ij}]_{n \times n}$

where $a_{ij} = \begin{cases} n, & n \text{ is number of edges between } a_i \text{ and } a_j \\ 0 & \text{otherwise} \end{cases}$

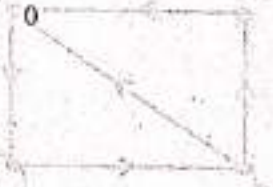
Example 1. Find adjacency matrix of Multi-graph.



Sol.

	a	b	c	d	e
a	1	2	0	0	1
b	2	0	1	0	0
c	0	1	0	1	3
d	0	0	1	0	1
e	1	0	3	1	0

$$M = \begin{bmatrix} 1 & 2 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 3 & 1 & 0 \end{bmatrix}$$

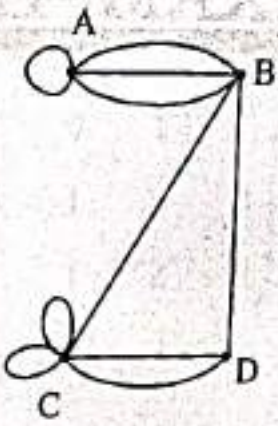


Note : In similar way we can find adjacency matrix of directed multi-graph.

Example 2. Example 2. Draw multigraph G whose adjacency matrix is given by

$$M = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

Sol. The corresponding multigraph is given as :

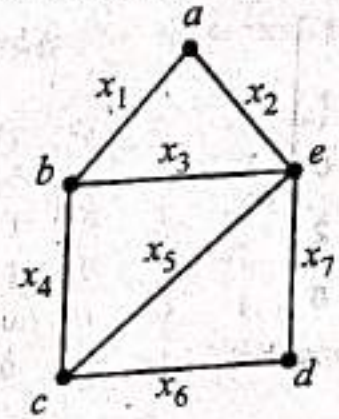


Incidence matrix :

Let G be a graph have m vertices and n edges. Then incidence matrix of graph is $m \times n$ matrix written as $A(G) = [a_{ij}]_{m\times n}$ defined by

$$a_{ij} = \begin{cases} 1 & \text{if } j\text{th edge } e_j \text{ is incident on } i\text{th vertex } v_i \\ 0 & \text{otherwise.} \end{cases}$$

Example : Write incident matrix of graph.



Sol. Number of vertices = 5

Number of edges = 7

So **incidence** matrix is 5×7 matrix.

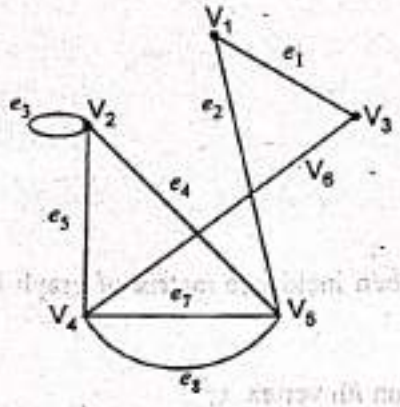
	x_1	x_2	x_3	x_4	x_5	x_6	x_7
a	1	1	0	0	0	0	0
b	1	0	1	1	0	0	0
c	0	0	0	1	1	1	0
d	0	0	0	0	0	1	1
e	0	1	1	0	1	0	1

so

$$A(G) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

ILLUSTRATIVE EXAMPLES

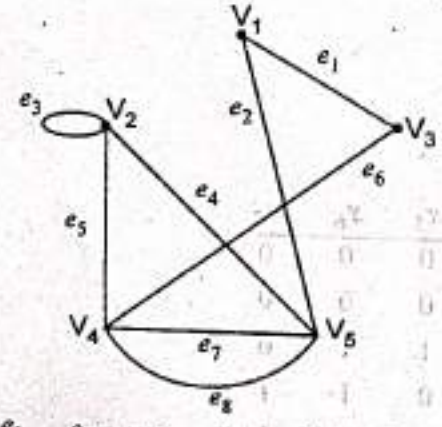
Example 1. Find the adjacency matrix A of the multigraph.



Set $a_{ij} = n$, where n is the no. of edges between V_i and V_j and set $a_{ij} = 0$ otherwise.

$$A = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{ccccc} V_1 & V_2 & V_3 & V_4 & V_5 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 2 \\ 1 & 1 & 0 & 2 & 0 \end{bmatrix} \end{array}$$

Example 2. Find the incidence matrix M of the multigraph.

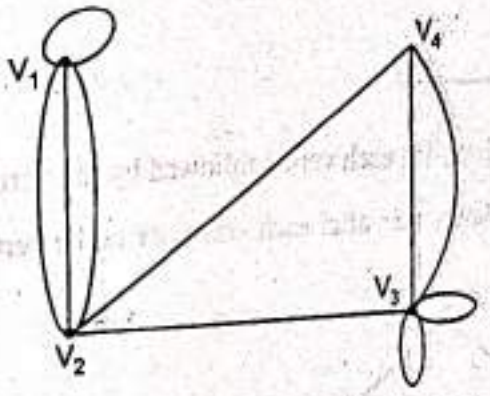


$$M = \begin{array}{c} \\ V_1 \\ V_2 \\ V_3 \\ V_4 \\ V_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

Example 3. Draw the multigraph G whose adjacency matrix A = follows :

$$A = \begin{bmatrix} 1 & 3 & 0 & 0 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{bmatrix}$$

Sol.

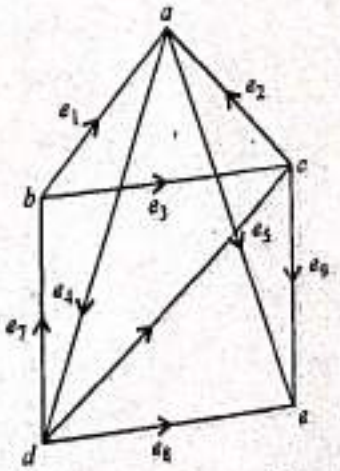


Example 4. Draw the Directed graph G whose incidence matrix M_1 is

(I)

$$M_1 = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \quad e_7 \quad e_8 \quad e_9 \\ \begin{bmatrix} -1 & -1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 \end{bmatrix} \end{array}$$

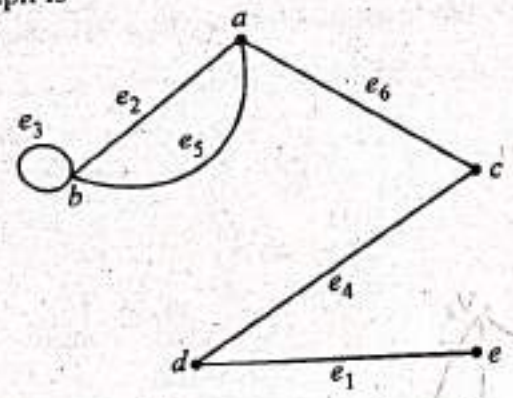
Directed graph is



(II)

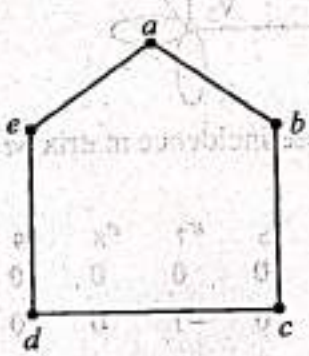
$$M_1 = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & & & \end{bmatrix} \end{array}$$

Undirected graph is



Adjacency list : In adjacency list of a graph we list each vertex followed by the vertices adjacent to it. First write vertices of graph in a vertical column, then after each vertex write the vertices adjacent to it.

Example 5. For a graph



I. Write the adjacency list,

II. Find the adjacency matrix

III. Find the incidence matrix

IV. Draw complement graph.

Sol. I. adjacency list is

a ; e, b

b ; a, c

c ; b, d

d ; c, e

e ; a, d

II $V = \{a, b, c, d, e\}, |V| = 5$

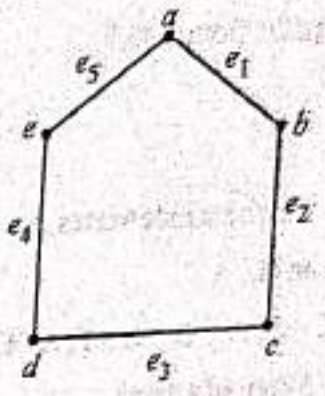
adjacency matrix will be a square matrix ;

$$M = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \end{array} \begin{array}{c} \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

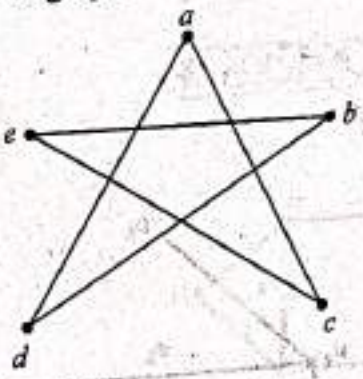
III. $|V| = 5, |E| = 5$

$\therefore$ Incidence matrix is

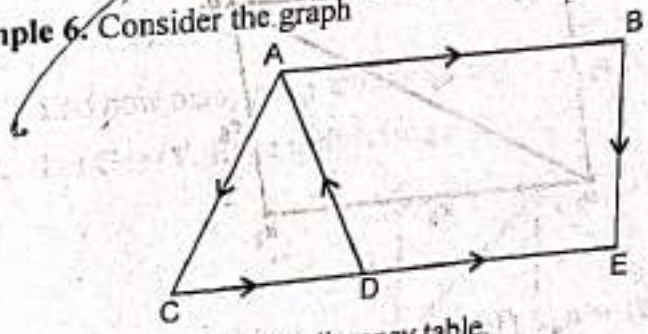
	e_1	e_2	e_3	e_4	e_5
a	1	0	0	0	1
b	1	1	0	0	0
c	0	1	1	0	0
d	0	0	1	1	0
e	0	0	0	1	1



IV. Complement of graph



Example 6. Consider the graph



: G

(*i*) Express G by its adjacency table.

(*ii*) Find all the simple paths from A to E.

(*iii*) Find all cycles in G.

(*iv*) Show that G is unilaterally connected by exhibiting a spanning path of G.

(*v*) Is G strongly connected ?

I.

	A	B	C	D	E
A	0	1	1	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	1	0	0	0	1
E	0	0	0	0	0

II. A – B – E, A – C – D – E

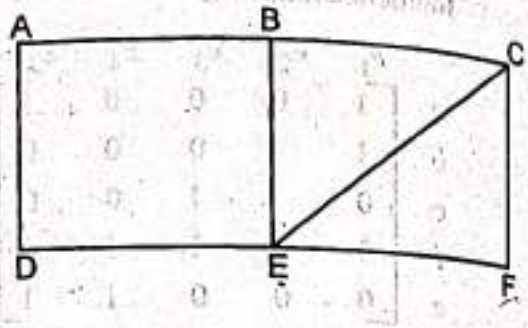
III. A – C – D – A

IV. G is unilaterally connected.

V. G is not strongly connected.

[$\because$ adjacency matrix of strongly connected digraphs has all entries = 1]

Example 7. Consider the graph G. Find



I. All simple paths from A to F

II. d(A, F)

III. diam(G)

IV. All cycles which include vertex A.

V. All cycles in G.

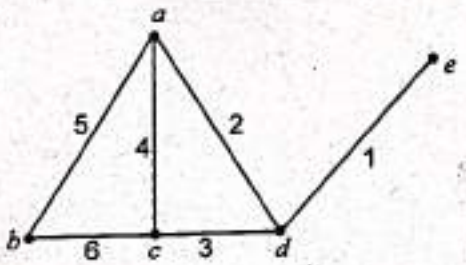
Sol. (1) A – B – C – F, A – B – E – F, ADEF, A – B – EF etc.

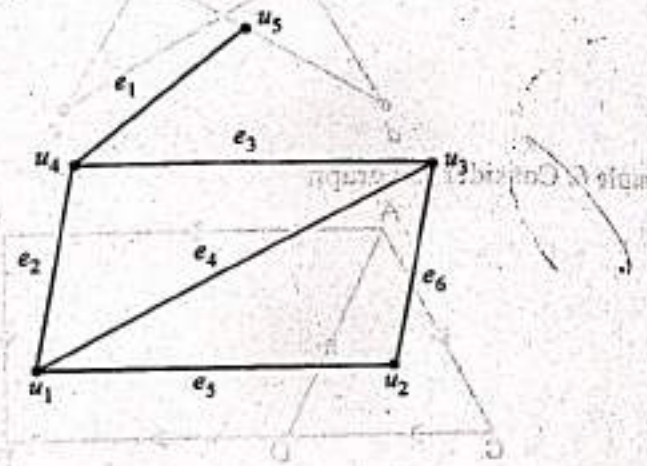
(2) d(A, F) = 3 (no. of edges)

(3) diam(G) = size of G = no. of edges = 8

(4) A – B – E – D – A , A – B – C – E – D – A etc.

Example 8. Show that the graphs G, G′ are isomorphic.





Let $f : G \to G'$ s.t

$f(a) = u_1$, $f(b) = u_2$, $f(c) = u_3$, $f(d) = u_4$, $f(e) = u_5$

The adjacency matrix for G for a, b, c, d, e

and adjacency matrix for G′ for the ordering

$a \to u_1$, $b \to u_2$, $c \to u_3$, $d \to u_4$, $e \to u_5$ is

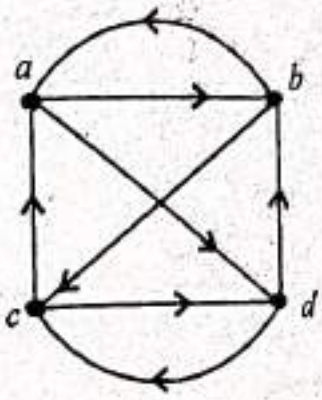
$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$\therefore$ G and G′ are isomorphic.

Example 9. Draw the Diagraph with given matrix as adjacency matrix.

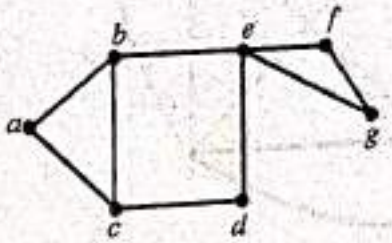
$$A = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Sol. Let vertices are a, b, c, d then diagraph is shown below



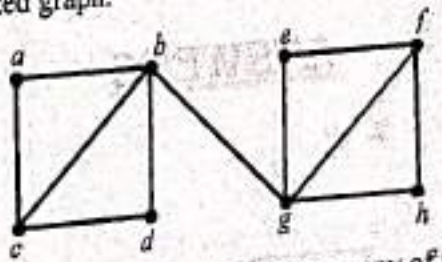
EXERCISE 1.2

1. For the graph



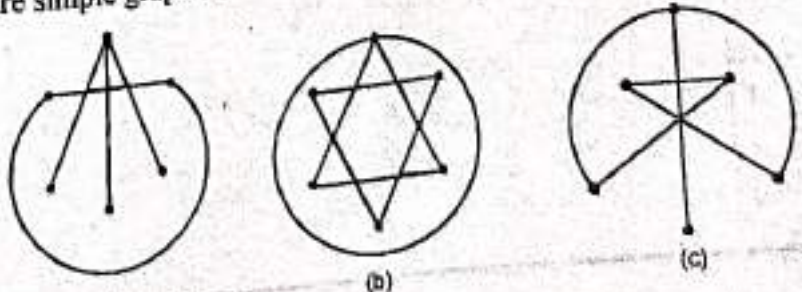
find how many paths are from b to f.

2. Let G = (V, E) be undirected graph.



Find how many paths are there in G from a to h? How many of these have length 5 ?

3. Let G = (V, E) be undirected graph. Define a relation R on V by a R b If there is a path in G from a to b. Prove that R is an equivalence relation.
4. Find the number of connected graphs with four vertices and draw them.
5. (*i*) Which of the following multigraphs are connected ?
   (*ii*) Which are cycle free ?
   (*iii*) Which are simple graphs ?

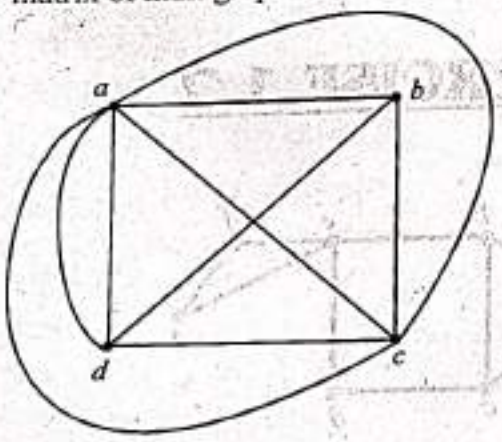


6. A graph has adjacency matrix

$$M = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Is the graph connected ?

7. Write adjacency matrix of multigraph

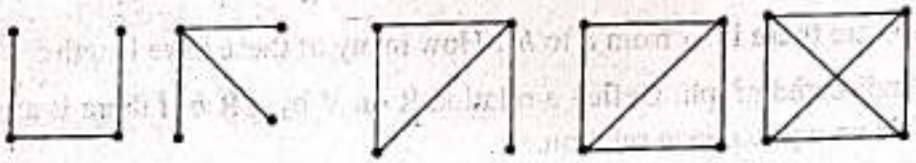


ANSWERS

1. 6

2. 9 ; 3

4. 5



5. The graph (*c*) is connected. N; No Graph is cycle free.

(*c*) is simple graphs.

6. No

7. $\begin{bmatrix} 0 & 1 & 3 & 2 \\ 1 & 0 & 1 & 1 \\ 3 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix}$

1.8. Bipartite Graph

Let G be any graph. If vertex set V can be partitioned into two disjoint subsets A and B such that every edge in G joins a vertex in A with a vertex in B, then graph is said to be Bipartite graph.

Example :

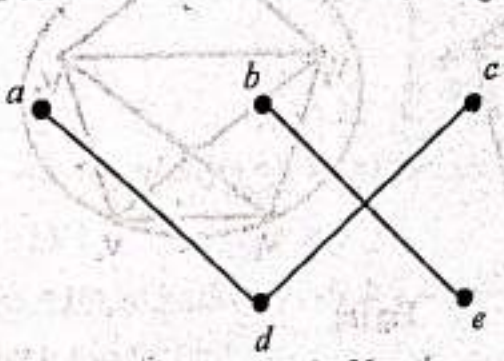
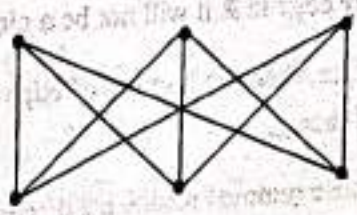


Fig. Show bipartite graph of 5 vertices.

Complete Bipartite Graph

Bipartite graph is said to be complete if every vertex in A is joined to every vertex in B. If is denote by $k_{m,n}$. Where m, n are number of vertices in sets A and B respectively.

Example : Draw $k_{3,3}$



$k_{3,3}$

1.9. Planar Graphs

A Planar graph is a graph drawn in the plane in such a way that no two edges intersect (cross) each other.

Planar graph : A Planar graph is a graph which is isomorphic to a plane graph *i.e.*, it can be redrawn as a plane graph.

A graph which is not a planar graph is called **non-planar graph.**

For example. (*i*) The complete graph with four vertices K_4 is usually drawn with crossing edges see fig (*a*). But it can also be drawn with non-crossing edges see fig (*b*)

Fig. (a)

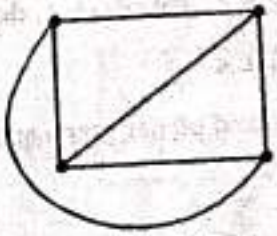


Fig. (b)

Hence K_4 is a planar graph.

(*ii*) A complete graph of five vertices is non-planar *i.e.*, K_5 is non-planar.

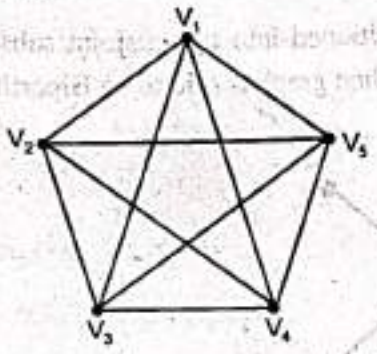


Fig (*a*)

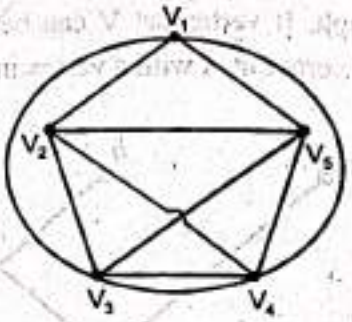


Fig (*b*)

Since the graph shown in fig. (*a*) cannot be drawn in plane without crossing edges see fig. (*b*). Hence K_5 is non-planar graph.

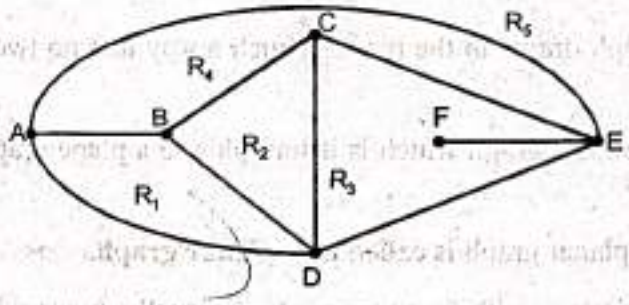
Region : A plane graph partitions the plane into several regions. These regions are called faces. Each region is depicted by the set of edges.

Cycle : The boundary of the region R of graph G is cycle if the boundary of R contains no cut edges of G. *i.e.*, contain no edge such that on removing any edge in R it will not be a closed circuit.

Degree of face : If G be graph and *g* be its face, then the number of edges in the boundary of *g* with cut edges counting twice is defined as the degree of face *g*.

Cut Edge : Cut edge in a graph is an edge whose removal results n a disconnected graph.

For example. Consider the following plane graph



Various regions are shown by R_1, R_2, R_3, R_4, R_5

Here deg $(R_1) = 3$, deg $(R_2) = 3$, deg $(R_3) = 5$, deg $(R_4) = 4$, deg $(R_5) = 3$

Theorem 1. EULER'S FORMULA

Let G = (V, E) be a connected planar graph and let R be the number of regions defined by any planar depiction of G. Then

$$R = |E| - |V| + 2$$

Proof. We prove the result by induction let *k* be the number of regions determined by G.

We first show that the result is true for $k = 1$. A tree determine the above region, for example

No. of vertices = 4, No. of edges = 3. Also from the formula, we have

$$1 = |E| - |V| + 2 \Rightarrow |E| = |V| - 1$$

i.e., No. of edges = No. of vertices – 1, which is always true for a tree.

$\therefore$ The result is true for $k = 1$.

Let us assume that the result is true for all $k \geq 1$. Let G be a connected plane graph determining $(k+1)$ gions. Remove an edge which is common to the boundary of two regions. We obtain a graph G′ having k– gions.

Let $|V'|$, $|E'|$, R′ denote respectively the number of vertices number of edges and regions of G′, then ... (1)

$$R' = |E'| - |V'| + 2$$

Also, we have

$$|V'| = |V|, |E'| = |E| - 1, R' = R - 1$$

$$|E| - |V| + 2 = |E'| + 1 - |V'| + 2$$

$$= (|E'| - |V'| + 2) + 1 \quad [\because \text{of (1)}]$$

$$= R' + 1$$

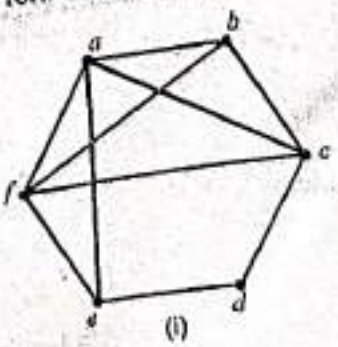
$$= R$$

$\therefore$ result is true for $k+1$

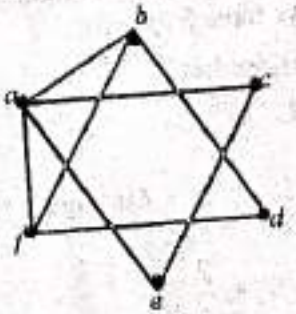
$\therefore$ result follows by induction for all connected graphs.

ILLUSTRATIVE EXAMPLES

Example 1. Verify Euler's formula for the following graphs.



(i)



(ii)

Sol. (*i*) In fig. (*i*) $|V| = 6, |E| = 10, R = 6$

$\therefore$ By Euler's formula, $R = |E| - |V| + 2$

i.e., $6 = 10 - 6 + 2$, which is true

(*ii*) In fig. (*ii*) $|V| = 6, |E| = 8, R = 4$

$\therefore$ By Euler's formula, $R = |E| - |V| + 2$

i.e., $5 = 9 - 6 + 2$, which is true

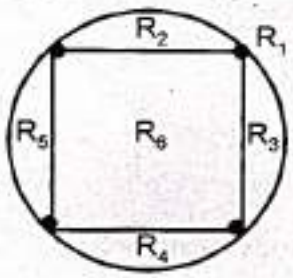
Example 2. Determine the number of regions defined by a connected planar graph with 4 nodes and 8 edges. Draw such a graph.

Sol. Here $|V| = 4, |E| = 8$

$\therefore$ By Euler's formula.

$$R = |E| - |V| + 2$$
$$= 8 - 4 + 2$$
$$= 6$$

$\therefore$ The given connected graph has 6 regions. The required graph is



Theorem 2. Let G = (V, E) be a simple, connected Planar graph with more than one edge, then the following inequalities holds.

(*ii*) $2|E| \geq 3R$ (*ii*) $|E| \leq 3|V| - 6$

(*iii*) There is a vertex v of G such that deg $(v) \leq 5$.

Proof. (*i*) Since G has more then one edge $\therefore |E| > 1$

If G defines only one region, then $R = 1$

$\therefore$ $|E| > 1 \Rightarrow 2|E| > 2 > 3 \Rightarrow 2|E| > 3R$ holds.

So, let $R > 1$, then each region is bounded by atleast 3-edges. But each edge in a planar graph touches almost 3 region. Thus we have $2|E| \geq 3R$

(*ii*) By part (*i*), we have

$$2|E| \geq 3R$$

or $$R \leq \frac{2}{3}|E|, \quad \text{Adding } |V| \text{ both sides}$$

$$|V| + R \leq |V| + \frac{2}{3}|E| \qquad \ldots(1)$$

By Euler's formula $R = |E| - |V| + 2$ ...(2)

$|V| + R = |E| + 2$

From (1) and (2) we have

$$|E| + 2 \le |V| + \frac{2}{3}|E|$$

$$3|E| + 6 \le 3|V| + 2|E|$$

$$\Rightarrow \quad |E| \le 3|V| - 6$$

(*iii*) Let each vertex of G of degree ≥ 6.

Also by first theorem on graph theory

$$\sum_{v \in V} \deg(v) = 2|E|$$

$$6|V| \le 2|E| \qquad [\because \text{L.H.S} \ge 6|V| \text{ and R.H.S} = 2|E|] \quad ...(3)$$

$$\Rightarrow \quad |V| \le \frac{1}{3}|E| \quad ...(4)$$

Also, By part (*i*) $R \le \frac{2}{3}|E|$

Adding (3) and (4) went

$$|V| + R \le \frac{1}{3}|E| + \frac{2}{3}|E| = |E| \quad ...(5)$$

$$\Rightarrow \quad |V| + R \le |E| \quad ...(6)$$

But by Euler's formula, we have

$$|V| + R = |E| + 2$$

$\therefore$ from (5) and (6) we have

$$|E| + 2 \le |E|$$

$\Rightarrow$ $2 \le 0$, not possible

$\therefore$ Our supposition is wrong

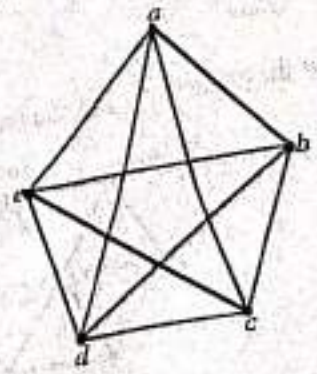
$\therefore$ Each vertex of G cannot have a degree ≥ 6

Hence, there exist a vertex of G with degree ≤ 5.

xample 3. Prove that the graph K_5 is not planar.

ol. Number of vertices in $K_5 = 5$

Number of edges in $K_5 = |E| = 10$



for planar graph

$$|E| \le 3|V| - 6$$

$\Rightarrow$ $10 \le 3 \times 5 - 6$

$\Rightarrow$ $10 \le 9$,

which is contradiction.

$\therefore$ K_5 is not planar graph.

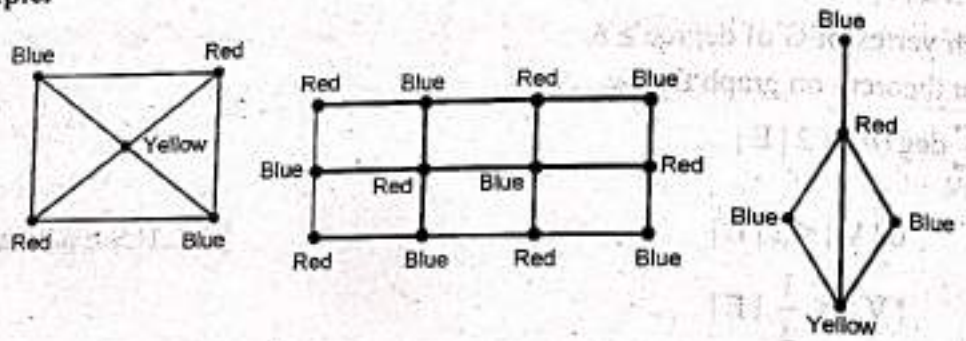
1.10. Coloring

Suppose G be a simple graph with n vertices, we are to paint all its vertices such that no two adjacent vertices have the same colour.

Chromatic Number :

The **minimum number** of colours needed to paint all the vertices of the graph such that no two adjacent vertices have the same colour is called **chromatic number** of G and denoted by C(G).

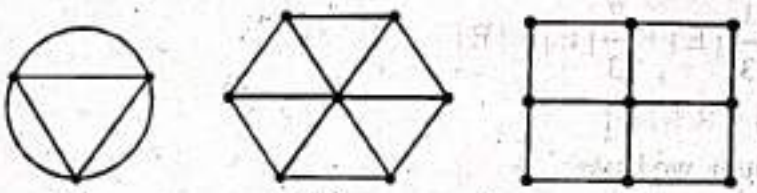
For example.



The above graphs are 3-chromatic, 2-chromic and 3-chromatic receptively.

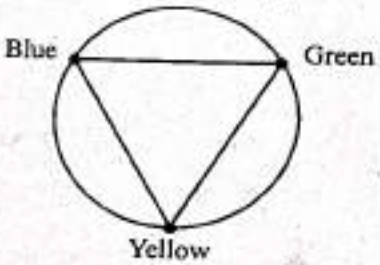
Remark. A complete graph of n vertices is n - chromatic, as all its vertices are adjacent.

Example. Find the chromatic number for the following graphs.

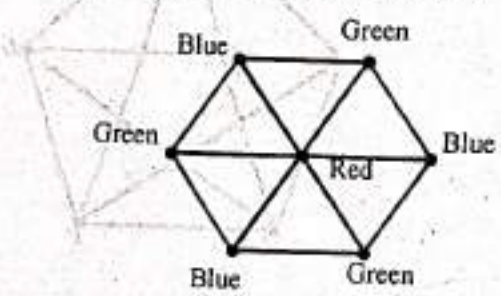


Sol. Chromatic number of graph G is the minimum number of colour required to paint all the vertices of the graph so that no two adjacent vertices have the same colour.

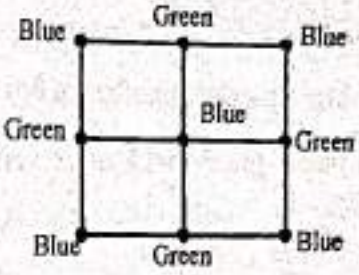
The chromatic colour for the graph (a) is 3 as shown below



The chromatic number for the graph (b) is 3 as shown below



The chromatic number for the graph (*c*) is 2 as shown below



Proper Colouring :

A colouring is proper if any two adjacent vertices *u* and *v* have different colours otherwise it is called improper colouring.

Example. The chromatic number of complete bipartite graph $k_{m,n}$ *m* and *n* are +ve integers is two.

Sol. The number of colour needed does not depend upon *m* and *n*. Only two colours are needed colour the set of *m* vertices with one colour and the set of *n* vertices with a second colour. Edges connect only a vertex from the set of *m* vertices and a vertex from the set of *n* vertices, no two adjacent vertices have the same colour.

Theorem : Prove that following statements are equivalent for a graph G.

(*a*) G is 2-colorable.

(*b*) G is bipartite

(*c*) G is contains no odd cycle.

Proof : $a \Rightarrow b$.

If G be 2-colorable then graph G has two sets of vertices V_1 and V_2 with different colours say red and blue.

As no vertices of V_1 and V_2 are adjacent

$\therefore$ $\{V_1, V_2\}$ is partition of G.

$\therefore$ G is bipartite.

$b \Rightarrow c$

Let G be bipartite and $\{V_1, V_2\}$ be partition of vertices of G,

Let a vertex $x \in V_1$ and cycle begins at x,

Let it joined to vertex $y \in V_2$ and then to a vertex in V_1 and so on.

When cycle gets completed *i.e.* It returns to x in V_1 then it will be of even length ($\because$ G is bipartite)

$\therefore$ G has no odd cycle.

$c \Rightarrow a$

Let each cycle in G be even let some vertex be coloured while then its adjacent vertex will have different colour black and its adjacent vertex will have colour white because every cycle has even length.

$\therefore$ sequence of vertices of even cycle is WBW ; WBWBW so on.

Only two colours are used to colour the graph.

$\therefore$ G is 2 colourable.

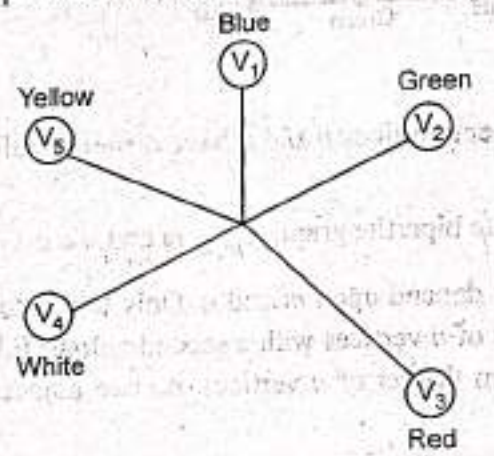
Four Colour Theorem : If G is any planar graph then $C(G) \leq 4$.

Theorem : Five Colour Theorem : If G is planar graph then

$$C(G) \leq 5.$$

Proof : Basis : A graph with one vertex has chromatic number of one. (Clearly)

Induction : Let us assume that all planar graphs with $n - 1$ vertices have a chromatic number of 5 or less. Let G be a planar graph with n vertices.



$\therefore$ $\exists$ a vertex V with degree (V) ≤ 5.

Let G-V be the planar obtained by deleting V and all edges that connect V to other vertices in G.

Now by the Induction Hypothesis G-V has a 5-colouring. Let us assume that we use the colours red, white, blue, green and yellow.

(i) If deg(V) < 5 then we can produce a 5 colouring of G by selecting a colour *i.e.* not used in colouring the vertices that are connected to V with an edge in G.

(ii) If deg(V) = 5, then we apply same technique if the five vertices that are adjacent to V are not coloured differently.

Now we have possible condition is that V_1, V_2, V_3, V_4, V_5 are all connected to V be an edge and they are all coloured differently. Let us assume that they are red coloured, white, blue, yellow, and green.

If V_1 and V_3 are not connected to one another using only blue and red vertices in G-V. If we take all paths that begin at V_1 and go through only blue and red vertices. Then we can not reach V_3. When we exchange the colours of the vertices in these paths, including V_1, we still have a 5 colouring of G-V. As V_1 is now red, we can colour V-blue.

Now we assume that V_1 is connected to V_3 employing only blue and red vertices.

Then a path from V_1 to V_3 by employing Blue and red vertices followed by the edges (V_3, V) and (V,V_1) complete a circuit that either encloses V_2 or encloses V_4 and V_5.

$\therefore$ No path from V_2 to V_4 exist employing only green and white vertices. We can then repeat the same process as in the previous paragraph with V_2 and V_4, which will allow us to colour V-green. Hence G is 5 colourable.

Example 1. Determine the chromatic number of the complete graphs k_6, k_{10} and in general k_n.

Sol. It would take six colours to colour a k_6 graph since every vertex is adjacent to every other vertex, we need different colour for every one. Similarly it takes ten colour to colour the graph k_{10} and n-colour to colour the graph k_n.

$$\therefore \quad c(k_6) = 6$$

$$c(k_{10}) = 10$$

$$c(k_n) = n$$

Example 2. A tree with two or more vertices is 2-chromatic.

Sol. Let T be any tree. Suppose three arbitrary vertices V_1, V_2, V_3 of tree. If V_1 is connected to V_2 and V_3 then V_2, V_3 are not conntected. (Otherwise cycle will be formed). If V_1 is cloured Red V_2 is coloured Blue then V_3 can be coloured Blue. This is true for all vertices. So maximum colours needed are 2.

Therefore chromatic number of graph is 2.

Again, if T has only two vertices then result is true.

Example 3. What will be chromatic number of complete graph with n-vertices ? Explain.

Sol. Let G be a graph containing n vertices.

Then a vertex V is connected to exactly $n-1$ vertices.

So all these vertices must have different colours.

$\therefore$ number of colours required $= n$

i.e. graph is n-chromatic.

SHORTEST PATH PROBLEM

Let G be a connected graph whose edges are assigned unique weights (taken as distances). We want to determine shortest possible path between a pair of vertices. Method for this was developed by Dijkstra and is know as Dijkstra's algorithm.

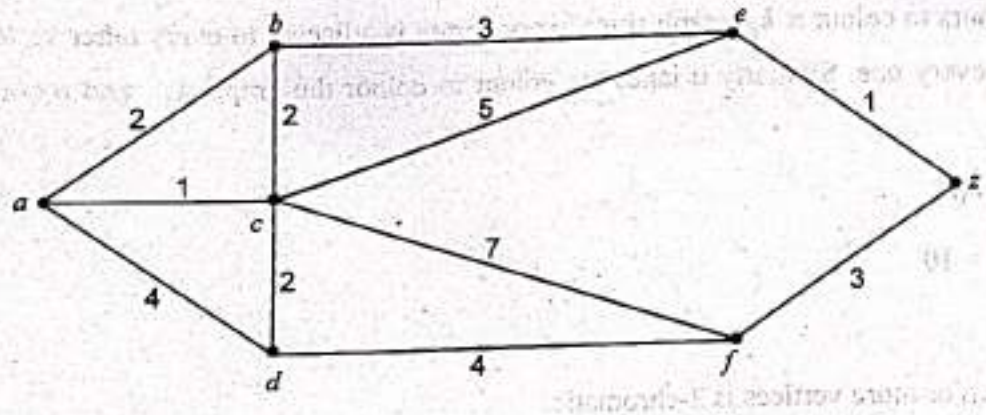
Dijkstra's Algorithm :

This algorithm maintains a sets of vertices whose shortest path from source is already known. If there is no path from source vertex do any other vertex then it is represented by $+\infty$. All weights must be positive.

Following points are considered.

1. Initially there is no vertex in sets.
2. Include source vertex V_s in S. Determine all the paths from V_s to all other vertices without going through any other vertex.
3. Include that vertex in S which is nearest to V_s find shortest paths to all the vertices through this vertex, give the values.
4. Repeat the process until $(n-1)$ vertices are not included in S.

Example 1. Find the shortest path between a and z.



Step I : Include the vertex a in S and determine all the direct paths from a to all other vertices without going through any other vertices.

	Distance to all other vertices						
	a	b	c	d	e	f	z
a	0	2 (a)	1 (a)	4 (a)	∞	∞	∞

Step II : Include vertex in S, nearer to a and determine shortest path to all the vertices through this vertex. The nearest vertex is c.

	Distance to all other vertices						
	a	b	c	d	e	f	z
$a, c,$	0	2 (a)	1 (a)	3 (a, c)	6 (a, c)	8(a, c)	∞

Step III : Second nearest vertex is b

	Distance to all other vertices						
	a	b	c	d	e	f	z
a, c, b	0	2 (a)	1 (a)	3 (a, c)	5 (a, b)	8(a, c)	∞

Step IV : Next vertex is d.

	a	b	c	d	e	f	z
a, c, b, d	0	2 (a)	1 (a)	3 (a, c)	5 (a, b)	7(a, c)	∞

Step V :

Next vertex is e

	a	b	c	d	e	f	z
a, c, b, d, e	0	2 (a)	1 (a)	3 (a, c)	5 (a, b)	7(a, c)	6(a, b, e)

Step VI : Next vertex is z.

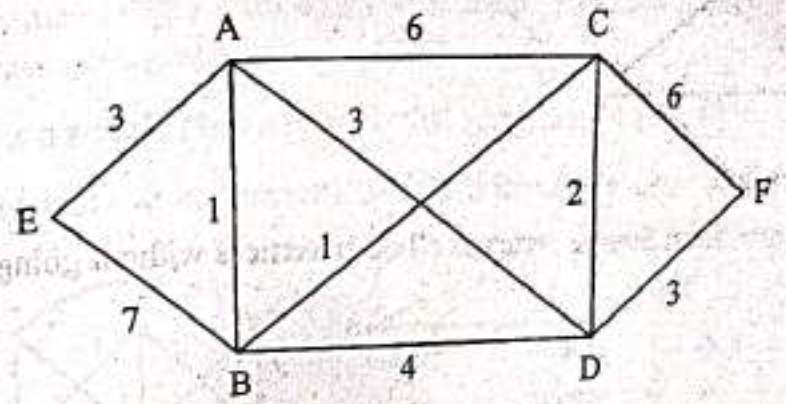
	a	b	c	d	e	f	z
a, c, b, d, e, z	0	2 (a)	1 (a)	3 (a, c)	5 (a, b)	7(a, c)	6(a, b, e)

included in S

So minimum path between a and z is 6

Path is $a \to b \to e \to z$.

Example 2. Find shortest path from E to F for the following graph :



Sol. Sol. (a) **Step 1.** Initially there is no vertex in set S.

Take source vertex in set S. Then we find all paths from source vertex E to all other vertices without going through any other vertex.

	E	A	B	C	D	F
E	0	3 (E)	7 (E)	∞	∞	∞

Step 2. Take nearest vertex to E and find shortest path to all the vertices through this vertex the nearest Vertex is A

	E	A	B	C	D	F
E, A	0	3 (E)	4 (E, A)	9 (E, A)	6 (E, A)	∞

Step 3. We find that nearest vertex is b. We take b in S.

	E	A	B	C	D	F
E, A, B	0	3 (E)	4 (E, A)	5 (E, A, B)	6 (E, A)	∞

Step 4. Take nearest vertex C in set S.

	E	A	B	C	D	F
E, A, B, C	0	3 (E)	4 (E, A)	5 (E, A, B)	6 (E, A)	11 (E, A, B, C)

Step 5. We find that next nearest vertex is D. We include D in set S.

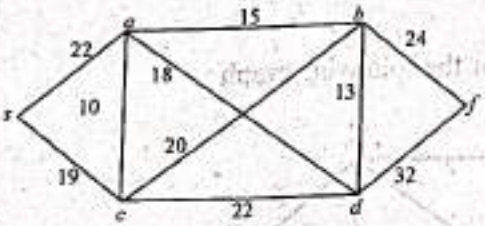
	E	A	B	C	D	F
E, A, B, C, D	0	3 (E)	4 (E, A)	5 (E, A, B)	6 (E, A)	9 (E, A, D)

Here $n - 1 = 5$, vertices are included in set S.

$\therefore$ By Dijkstra's algorithm, shortest path is E, A, D

shortest distance $= 3 + 3 + 3 = 9$

Example 3. Find shortest path using Dijkstra's algorithm.



Sol. Step 1. Initially there is no vertex in S.

Take source s in S and find all paths from Source vertex to all other vertices without going through any other vertex.

	s	a	b	c	d	f
s	0	22 (s)	∞	19 (s)	∞	∞

Step 2 : Take nearest vertex to s. Include vertex C.

	s	a	b	c	d	f
s, c	0	22 (s)	39 (s, c)	19 (s)	41 (s, c)	∞

Step 3 : Include next nearest vertex e in set S.

	s	a	b	c	d	f
s, c, a	0	22 (s)	37 (s, a)	19 (s)	40 (s, a)	∞

Step 4 : Include next nearest vertex b in set S.

	s	a	b	c	d	f
s, c, a, b	0	22 (s)	37 (s, a)	19 (s)	40 (s, a)	61 (s, a, b)

Step 5 : Include next nearest vertex d in set S.

	s	a	b	c	d	f
s, c, a, b, d	0	22 (s)	37 (s, a)	19 (s)	40 (s, a)	61 (s, a, b)

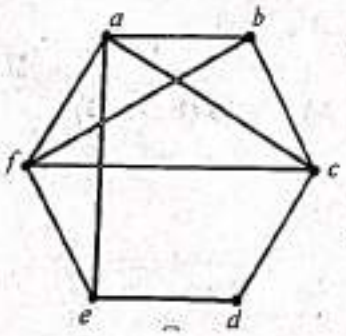
$n = 1 = 6 - 1 = 5$ vertices are included in Set S.

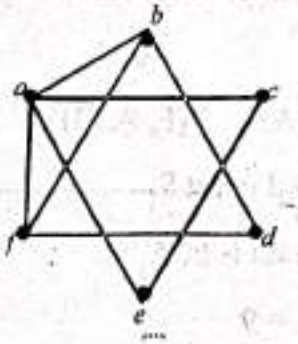
$\therefore$ By Dijkstra algorithm, shortest path from s to f is

$s \to a \to b \to f$

EXERCISE 1.3

1. Redraw the following graphs as planar graph and verify Euler formula :





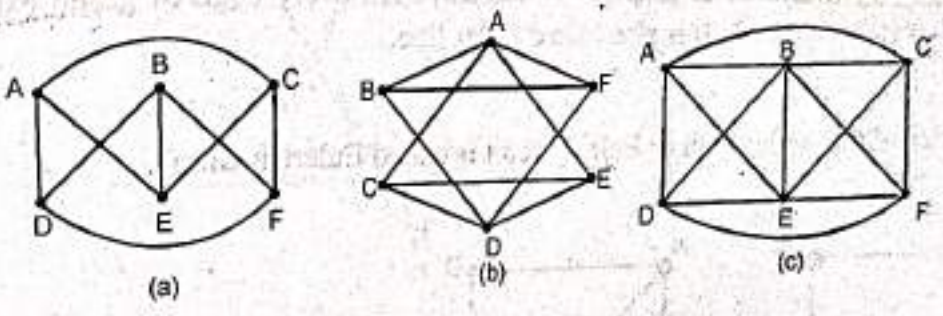
2. Show that $K_{3,3}$ satisfies the inequality $|E| \leq 3|V| - 6$ but is non-planar.

3. Find number of regions defined by connected planar graph with 6 nodes and 10 edges. Draw a simple and non-simple example.

4. How many edges must be drawn in order to obtain a planar graph with 5 nodes that define 7 regions. Draw such a graph.

5. Draw a simple planar graph with 6 nodes and 11 edges.

6. Draw a planar representation of the following graphs :

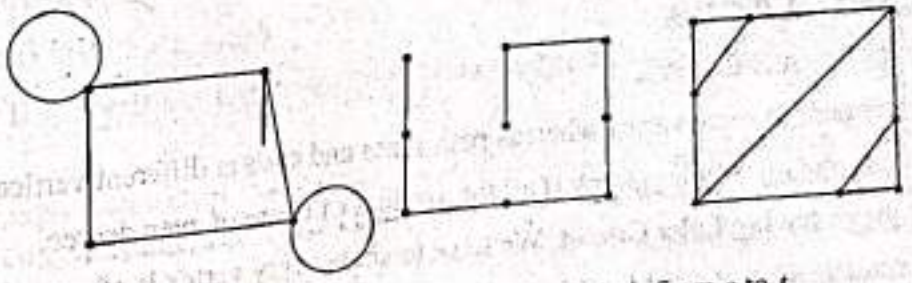


7. How many regions must a planar graph define if it has 11 edges and 7 nodes ?

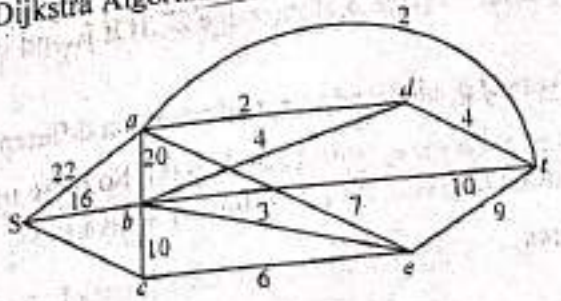
8. How many edges must a planar graph have if it define 5 regions and has 6 nodes?

9. Draw $K_{2,2}$, $K_{1,4}$, $K_{2,3}$ and K_4.

10. Verify Euler's formula



11. Applying Dijkstra Algorithm to find the shortest path from s to t.



ANSWERS

3. 6 4. 10 7. 6 8. 9 11. 23

1.11. Euler Paths and Circuits

In this section, we discuss an important application of graph theory. Suppose we are given a geometrical figure. We want to traverse all the edges of graph by traversing each edge exactly once. This may or may not be possible. The solution of such type of problems was given by mathematician Leonhard Euler (1707-1783). First we discuss the terms Euler Circuit and Euler Path, then we discuss methods to find them.

Euler Path : A simple path in a graph G is called Euler Path if it traverses every edge of graph exactly once.

Euler Circuit : Euler Circuit is a circuit in graph G which traverses every edge of graph exactly once. Euler Circuit is simply a closed Euler path. It is also called Euler line.

Eulerian Graph

A graph which contain either Euler Path or Euler Circuit is called Eulerian Graph.

Example :

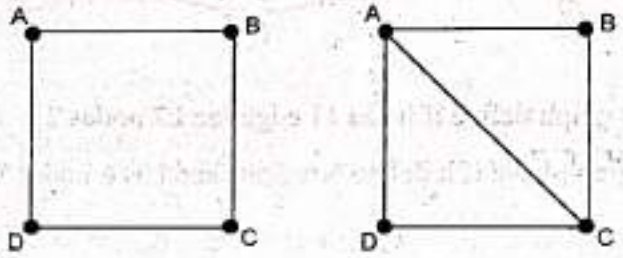


Fig. I Fig. II

Fig. I has Euler Circuit A B C D A

Fig. II has Euler Path A B C D A C

Remark : Circuit starts and ends at same vertex whereas path starts and ends at different vertices.

Theorem 1. A connected graph G is a Euler Graph if all the vertices of G are of even degree.

Proof : G is a connected graph having Euler Circuit. We have to show every vertex is of even degree.

Let c be Euler's circuit in G. Let 'a' be arbitrary vertex of G. Suppose circuit c begins at vertex a along edge e_1 to some other vertex a_1 and return to vertex a along edge e_2. If it is end of c then deg $(a) = 2$ (even).

Otherwise c leaves a again to different vertex a_2 along edge e_3 and return on different edge e_4 and so on.

Since edges at vertex a can be paired : e_1 with e_2, e_3 with e_4 and so on. So there must be even number of edges incident on each vertex. $\therefore$ deg(a) must be even. As a is arbitrary vertex in G.

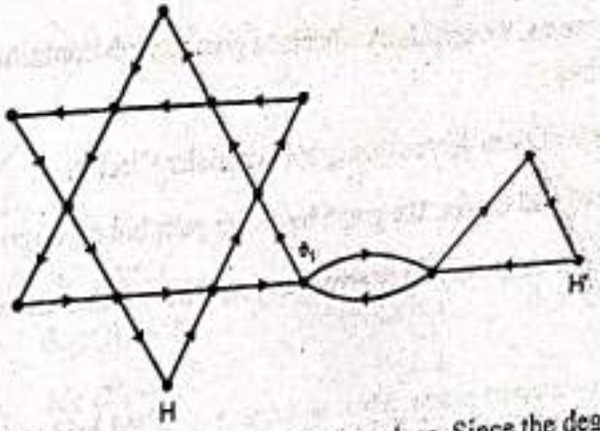
$\therefore$ every vertex in G is of even degree.

Theorem 2. (Converse of theorem 1)

If G is a connected graph and every vertex of G has even degree, then prove that G has a Euler Circuit.

Proof : Given every vertex of the graph G is of even degree. To show that G is a Euler graph we show G has Euler circuit.

We construct a walk starting with any arbitrary vertex v and going through all the edges of G such that no edge is traced more than once. We continue tracing as far as possible. Since each vertex is of even degree, therefore we can exit from every vertex we entered. Now the tracing cannot stop at any vertex but v. Since v is also of even degree we shall reach at v again. When the tracing comes to an end if this closed walk W that we have just traced, contains all the edges of G, then it is a Euler circuit, otherwise remove from G these edges and obtain a subgraph H of G.



Let H′ be the subgraph of G formed by the remaining edges. Since the degree of each vertices of H or H′ is even and the graph G is given to be connected. Therefore H must touch H′ at least at one vertex (say) at v_1. Now starting from v_1 we can again construct a new walk in H′. Since all the vertices of H′ are also of even degree this walk in H′ must terminate at the vertex v_1. Now if we have traversed all edges then Euler circuit has been obtained and if not we can repeat the above process again. Continue in this way combined the subgraph H, H′,....., formed, we get a closed walk that transverse all the edges of the graph G and thus get a Euler circuit in G.

Hence G is an Euler graph.

Theorem 3. If a graph has Euler Path then it has either no vertex of odd degree or two vertices of odd degree.

Proof : Let graph G has Euler Path starting at vertex a and ending at vertex b. If a and b are same then path is a Euler circuit, so by theorem 1 all vertices are of even degree.

Suppose $a \neq b$. Draw a new edge e_1 joining a and b. New graph is $G \cup \{e_1\}$. This new graph has Euler circuit obtained by Euler path plus new edge e_1. So all the vertices are of even degree.

Now remove the edge e_1. Then graph $G \cup \{e_1\} - \{e_1\} = G$ has only two vertices a and b of odd degree.

Hence the proof.

Theorem 4. (Converse of Theorem 3) : If G is a connected graph having either zero or two vertices of odd degree, then G has a Euler path.

Proof : G be a connected graph. If G has zero vertices of odd degree *i.e.*, all the vertices of G are of even degree then by Theorem 2, G posses as an Euler circuit.

Now, suppose G has two vertices of odd degree say v_1 and v_2. We construct an Euler Path by starting at one of the two vertices v_1 or v_2 and going through the edges in such a way that no edge will be traced more than once. For a vertex of even degree, whenever we enter the vertex through an edge, we can leave the vertex through another edge that has not been traced before. There, when the construction

eventually comes to an end, we must have reached the other vertex of odd degree. If all the edges in the graph were traced, we would get an Euler Path other wise remove those edges that has been traced out and obtain a subgraph formed by the remaining edges. The degree of vertices of this subgraph are all even. Again by theorem 2, this subgraph has an Euler Circuit. Since the original graph is connected. So there must a path between the two subgraph and thus we obtain a path that contain all the edges of G exactly once. Hence, we get an Euler Path.

Remarks : From above theorems, we can check wheater a given graph contains Euler Circuit, Euler Path or none. Summary is given below :

(a) If all the vertices are of even degree then graph has Euler Circuit.

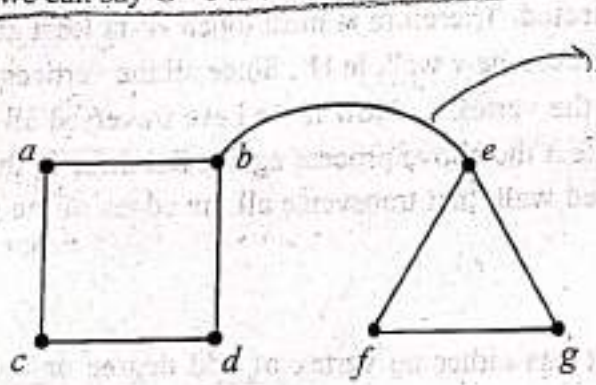
(b) If two vertices are of odd degree, the graph has Euler path but no circuit.

(c) If more than two vertices are of odd degree then graph has neither Euler Path nor Euler Circuit.

Definition

Bridge : Let G be a connected graph. Then an edge e is called bridge if by deleting e, G becomes disconnected or we can say $G-e$ is disconnected. Bridge is also called cut-edge.

Example :



In figure edge '*be*' is a bridge.

1.12. Fleury's Algorithm for Euler Circuit

Let G be a connected graph with each vertex of even degree. Choose any vertex, say v_1 of G to start the circuit.

Step 1 : Select an edge e_1 from v_1 such that e_1 must not be a Bridge. Let this edge be (V_1, V_2). Then Path is specified by P : e_1. Remove e_1 from graph.

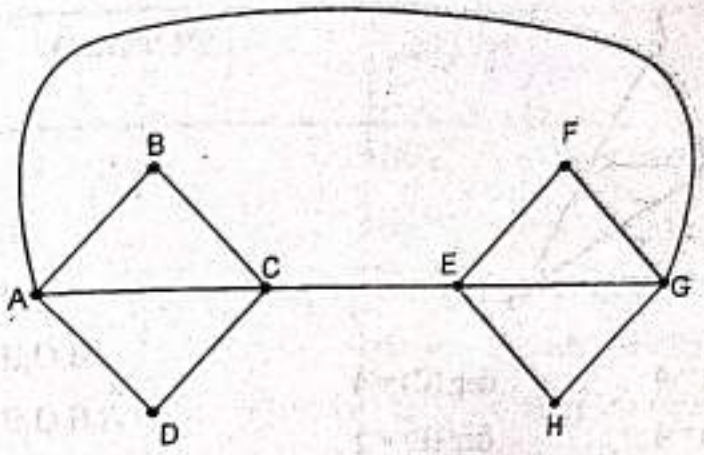
Step 2 : Now check all the edges from V_2. Again choose an edge from v_2 such that this edge must not be a bridge. Also remove this edge from G.

Step 3 : Repeat step 2 until no edge remains in Graph. P will give us required Euler circuit.

1.13. Fleury's Algorithm for Euler Path

Let G be a connected graph with exactly two vertices of odd degree. For Euler Path, we have to start from a vertex of odd degree and path will end at other vertex of odd degree. The rest of steps are same as that of Euler Circuit.

Example 1. Use Fleury's algorithm to construct Euler Path or Circuit in following graph.



Sol. First we check degree of each vertex

deg (A) = 4 deg (B) = 2 deg (C) = 4 deg (D) = 2

deg (E) = 4 deg (F) = 2 deg (G) = 4 deg (H) = 2

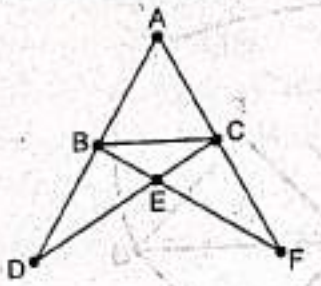
Since every vertex has even degree, So Euler circuit exist. We can begin from anywhere. Let us start from vertex A. Detailed steps are shown below :

Sr. No.	Current Path (P)	Next Edge	Description
1.	A	{A, B}	No edge is a cut edge choose any.
2.	A,B	{B, C}	Only one edge from B remains.
3.	A,B,C	{C, D}	No edge from C is a cut edge. So choose any.
4.	A,B,C,D	{D, A}	Only one edge from D remains.
5.	A,B,C,D,A	{A, C}	Neither AG or AC is cut edge. Chose any.
6.	A,B,C,D,A,C	{C, E}	Only one edge from C remains.
7.	A,B,C,D,A,C,E	{E, F}	No edge from E is cut edge So choose any.
8.	A,B,C,D,A,C,E,F	{F, G}	Only one edge from F remains.
9.	A,B,C,D,A,C,E,F,G	{G, H}	GA is cut edge so choose GH or GE.
10.	A,B,C,D,A,C,E,F,G,H	{H, E}	Only one edge from H remains
11.	A,B,C,D,A,C,E,F,G,H,E	{E, G}	Only one edge from E remains
12.	A,B,C,D,A,C,E,F,G,H,E,G	{G, A}	Only one edge from G remains
13.	A,B,C,D,A,C,E,F,G,H,E,G,A	No edge	

The required Euler circuit is

A, B, C, D, A, C, E, F, G, H, E, G, A.

Example 2. Apply Fleury's algorithm to construct an Euler circuit for following graph.



Sol. deg (A) = 2 deg (B) = 4 deg (C) = 4

deg (D) = 2 deg (E) = 4 deg (F) = 2

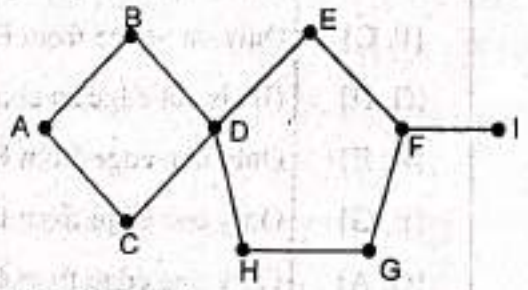
Since every vertex of Graph has even degree and graph is connected so Euler circuit exists. We can begin from anywhere. Let us begin from A. Detailed steps are :

Sr.No.	Current Path (P)	Next Edge	Description
1.	A	{A, B}	Neither AB nor AC is cut edge choose any.
2.	A,B	{B, D}	No edge from D is cut edge choose any.
3.	A,B,D	{D, E}	Only one edge from D remains.
4.	A,B,D,E	{E, B}	No edge from E is cut edge choose any.
5.	A,B,D,E,B	{B, C}	Only one edge from B remains.
6.	A,B,D,E,B,C	{C, E}	CA is cut edge so choose CE or CF.
7.	A,B,D,E,B,C,E	{E, F}	Only one edge from E remain.
8.	A,B,D,E,B,C,E,F	{F, C}	Only one edge from F remains.
9.	A,B,D,E,B,C,E,F,C	{C, A}	Only one edge from C remains.
10.	A,B,D,E,B,C,E,F,C,A	No edge	

so required Euler circuit is

A, B, D, E, B, C, E, F, C, A.

Example 3. Use Fleury's algorithm to construct Euler Path or Circuit in following graph.



Sol. First we check degree of all vertices

deg (A) = 2 deg (B) = 2 deg (C) = 2 deg (D) = 4

deg (E) = 2 deg (F) = 3 deg (G) = 2 deg (H) = 2

deg (I) = 1

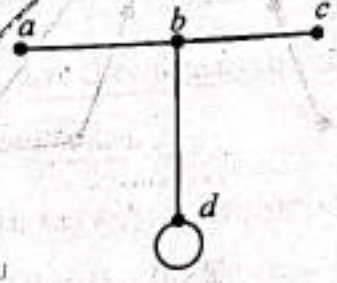
Two vertices F and I have odd degree and graph is connected. So we can find Euler Path (no circuit). Path must begin form F(or I) and ends at I (or F). Steps are shown below :

Sr. No.	Current Path (P)	Next Edge	Description
1.	F	{F, E}	FI is cut edge choose FE or FG.
2.	F, E	{E, D}	Only one edge from E remains.
3.	F,E,D	{D, B}	No edge from D is a cut edge choose any.
4.	F,E,D,B	{B, A}	Only one edge from B remains.
5.	F,E,D,B,A	{A, C}	Only one edge from A remains.
6.	F,E,D,B,A,C	{C, D}	Only one edge from C remains.
7.	F,E,D,B,A,C,D	{D, H}	Only one edge from D remains.
8.	F,E,D,B,A,C,D,H	{H, G}	Only one edge from H remains.
9.	F,E,D,B,A,C,D,H,G	{G, F}	Only one edge from G remains.
10.	F,E,D,B,A,C,D,H,G,F	{F, I}	Only one edge from F remains
11.	F,E,D,B,A,C,D,H,G,F,I	No edge	

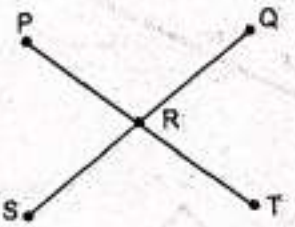
So required Euler Path is F, E, D, B, A, C, D, H, G, F, I.

Example 4. Find Euler Path or circuit (if exists)

(*i*)



(*ii*)



Sol. (*i*) deg(*a*) = 1

deg(*b*) = 3

deg(*c*) = 1

deg(*d*) = 3

In this graph four vertices are of odd degree. So Neither Euler Path, nor Euler Circuit exists.

(*ii*) deg(P) = 1

deg(Q) = 1

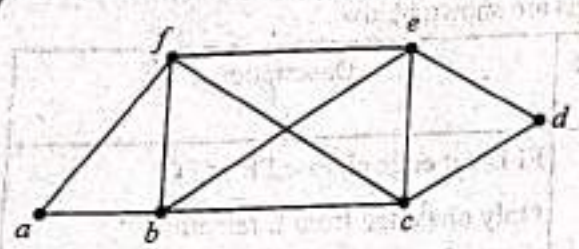
deg(S) = 1

deg(T) = 1

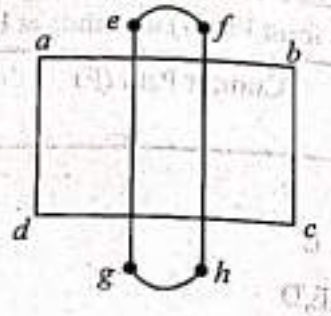
deg(R) = 4

Again four vertices are of odd degree, so neither Euler Path, nor Euler Circuit exists.

Example 5. Which of the following graphs are traversable :



I



II

Sol. Graph I is traversable as it contain Euler circuit. Euler circuit is shown below :

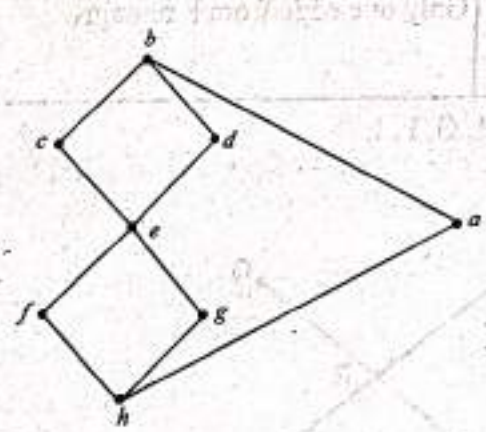
$$a \to f \to c \to d \to e \to f \to b \to e \to c \to b \to a$$

Graph II is not traversable because it is not connected. It contain two components $(a\,b\,c\,d)$ and $(e\,f\,g\,h)$.

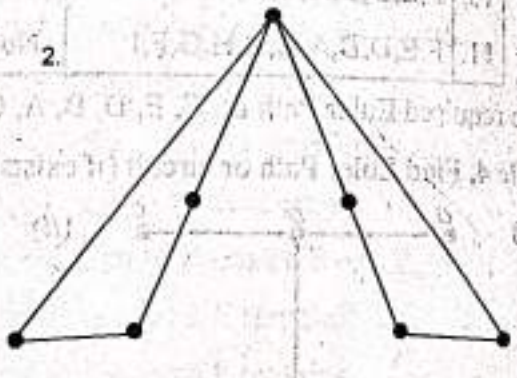
EXERCISE 1.4

In Questions from 1 to 5, tell wheter graph has Euler Circuit, Euler Path but no circuit or neither. Also find path or circuit (if exists) by showing all steps.

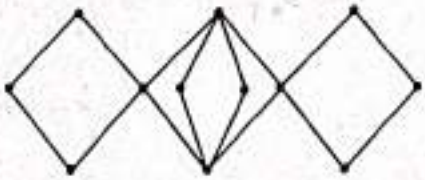
1.



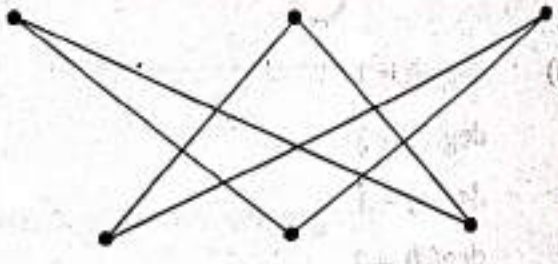
2.



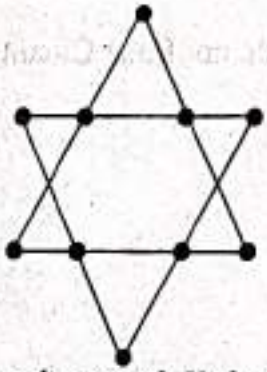
3.



4.



5.



6. Does Complete graph K_n have Euler Circuit ? Euler Path ? Justify your answer.
7. Draw a graph that has exactly one Euler Circuit ? Characterise all such graphs ?

1.14. Hamiltonian Paths and Circuits

In previous section, we have traversed all the edges of graph exactly once (vertices were repeated in some cases). Now we discuss another application of graph theory in which we have to traverse all the vertices of graph exactly once. This theory was proposed by Irish mathematician **William Hamilton** (1805-1865).

Hamiltonian Path :

A Hamiltonian Path in a connected graph is a path which contains each vertex of graph exactly once.

Hamiltonian Circuit : A Hamiltonian circuit is a circuit that contains each vertex of graph exactly once except for the first vertex, which is also the last.

Hamiltonain Graph :

A graph which possesses either Hamiltonian circuit or Hamiltonian path is called a Hamiltonian graph.

Remarks : I. In Hamiltonian circuit or path we have to visit all the vertices. There may be some unvisited edges.

II. If G has n vertices, then Hamiltonian circuit will contain n edges where as Hamiltonian Path will contain $n-1$ edges.

III. There may be more than one Hamiltonian path and circuit in a graph.

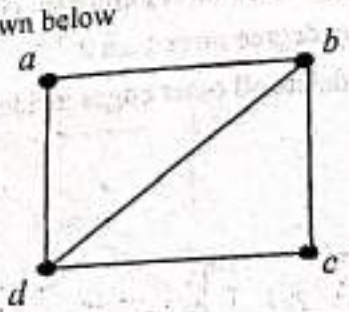
Theorems on Hamiltonian Graphs (Without proof)

Theorem I. Let G be a connected simple graph with n vertices, $n > 2$. Let U and V are any two non-adjacent vertices in G and $\deg(U) + \deg(V) \geq n$, then G is Hamiltonian.

Theorem II. Let G be a connected simple graph with n vertices, $n > 2$. If $\deg(V) \geq \frac{n}{2}$ for every $V \in G$ then G is Hamiltonian.

Theorem III. Let m be the number of edges in Graph G. If $m \geq \frac{1}{2}(n^2 - 3n + 2)$ where n is number of vertices of G then G is Hamiltonian.

Consider the graph shown below



Here $n = 4$

Graph satisfy all above theorems.

Here non-adjacent vertices are a and c

$$\deg(a) = 2 \quad \deg(c) = 2$$

$$\deg(a) + \deg(c) = 4(n)$$

so theorem I is true.

also $\deg(a) = 2, \deg(b) = 3, \deg(c) = 2, \deg(d) = 3$

so all vertices have degrees ≥ 2 which is $\frac{n}{2}$

$\therefore$ theorem II also true.

Similarly for theorem III we have $m = 5$ and $n = 4$

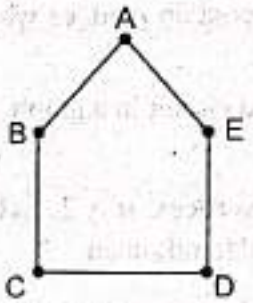
$$\text{so } \frac{1}{2}(n^2 - 3n + 2) = \frac{1}{2}(16 - 12 + 2) = 3$$

$$\therefore \quad m \geq \frac{1}{2}(n^2 - 3n + 2)$$

$\therefore$ graph is Hamiltonian and Hamiltonian circuit is a, b, c, d, a.

Note : The converse of these theorems is not true. We have some graphs that do not satisfy these theorems but still they are Hamiltonian.

For example in graph



$\deg(A) + \deg(C) = 2 + 2 = 4$

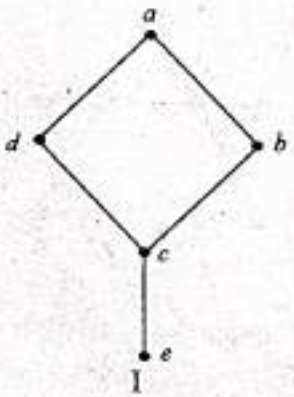
which is not greater than or equal to $n(5)$. Still graph is Hamiltonian.

and circuit is (A, B, C, D, E, A).

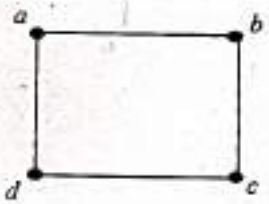
There are no hard and fast rules for constructing Hamiltonian paths and circuits. However, to find Hamiltonian paths and circuits following points should be kept in mind :

1. If Graph G with n vertices has less than n edges then no Hamiltonian circuit is possible.
2. In Hamiltonian circuit, any vertex can't have degree more than 2.
3. Whenever we enter and leaves a vertex we delete all other edges incident on that vertex.

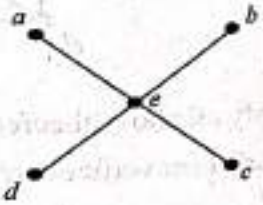
Example 1. Consider the following graphs



I



II



III

Graph in Fig. I has Hamiltonian path *e, c, d, a, b* but no Hamiltonian circuit.

Graph in Fig. II has both Hamiltonian path and circuit path is *a, b, c, d* and circuit is *a, b, c, d, a.*

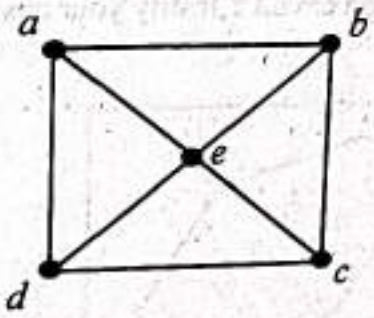
Graph in Fig. III has neither Hamiltonian path nor Hamiltonian circuit.

Remarks : I. A graph can have both Hamiltonian path as well as Hamiltonian circuit.

II. A graph can't have both Euler Path and Euler Circuits.

III. If a graph has Hamiltonian circuit then it also has Hamiltonian path converse is not true.

Example 2. Does the graph G given below have Hamiltonian circuit ? Justify your answer.



Sol. Number of vertices $(n) = 5$

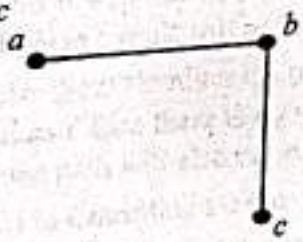
Number of edges = 8

To construct Hamiltonian circuit we have to include 5 edges.

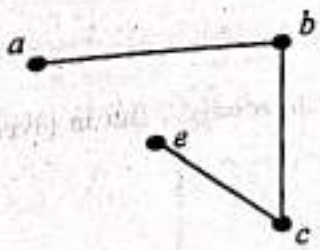
Let us start from vertex *a*. First we insert edge *ab*.

(*i*)

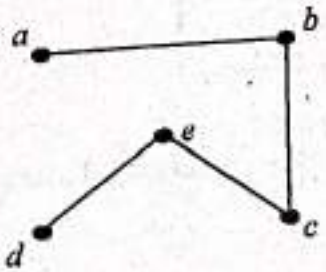
(*ii*) Insert *bc*



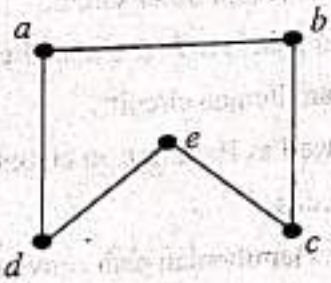
(*iii*) Insert *ce*



(*iv*) Insert *ed*

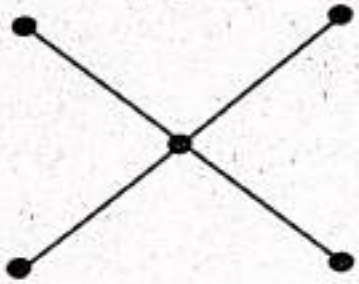


(v) Insert *da*



Required Hamiltonian circuit is *a, b, c, e, d, a.*

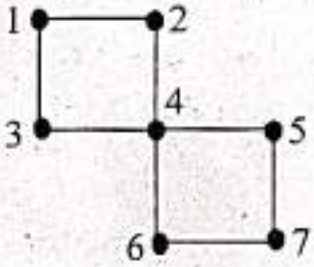
Example 3. (*a*) Does the graph shown below has Hamiltonian circuit ? Justify your answer.



(*b*) Determine whether the graph shown has a Hamiltonian circuit, a Hamiltonian path but no Hamiltonian circuit, or neither, If the graph has a hamiltonian circuit, give the circuit.

(*i*)

(*ii*)



Sol. (*a*) Number of vertices (n) = 5

Number of edges = 4

We know, Hamiltonian circuit of n vertices must contain n edges. But in given graph we have only $n-1$ edges. So Hamiltonian circuit is not possible.

(*b*) (*i*) $n = 5, m = 8$

$\therefore$ degree of each vertex $\geq \frac{n}{2}$ is satisfied.

$$\frac{1}{2}(n^2-3n+6) = \frac{1}{2}(25-15+6)=8$$

$\therefore$ $m \geq \frac{1}{2}(n^2-3n+6)$ is satisfied.

$\therefore$ It has Hamiltonian circuit.

(ii) $n = 7$, m = no. of edges = 9.

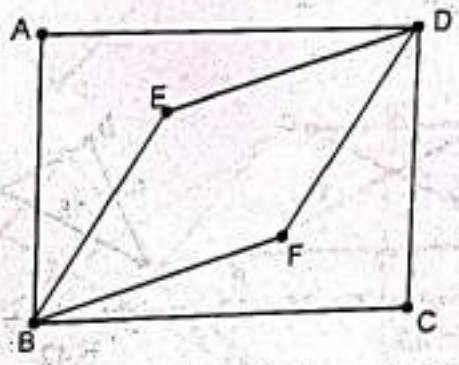
degree of each vertex $\geq \frac{n}{2}$ is not satisfied :

$$\frac{1}{2}(n^2 - 3n + 6) = \frac{1}{2}(49 - 21 + 6) = 17$$

$$m \geq \frac{1}{2}(n^2 - 3n + 6) \text{ is not satisfied.}$$

$\therefore$ it has neither Hamiltonian circuit nor path.

xample 4. Is the graph given below a Haimltonian ? Justify your answer.



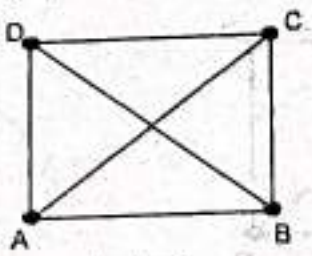
ol. Number of vertices (n) = 6 number of edges = 8. To construct Hamiltonian circuit we have to take edges from 8 edges with condition that every vertex will have degree 2. We can start from anywhere. uppose we start from A. From A we can go to either D or B. Let us go to D. Then from D if we go to C en degree of D becomes 2. So we have to delete DE and DF. But by deleting these two edges, degrees of and F become 1. So it will not be possible to include E and F in circuit. (In circuit a vertex must have egree 2). So Hamiltonian circuit will not exist.

Similarly we can show Hamiltonian path will also not exist. As we move from A to D, D to C, C to B, fter B if we go to E or F then there is no way to go ahead. Other side if we go to A then E and F becomes olate. So Hamiltonian path will also not exist.

amiltonian Circuit in Complete Graph :

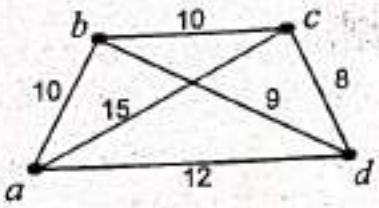
Let K_n be complete graph of n vertices, $n \geq 3$. Then K_n will definitely contain a Hamiltonian circuit. ıfact K_n will contain $\frac{\lfloor n-1}{2}$ Hamiltonian circuits.

For example : Consider the graph K_4.



Then by above result, K_4 contains $\frac{\lfloor 4-1}{2} = 3$, Hamiltonian circuits which are ABCDA, ABDCA and DBCA.

Example 5. Find Hamiltonian circuit of minimal weight for the graph show below.

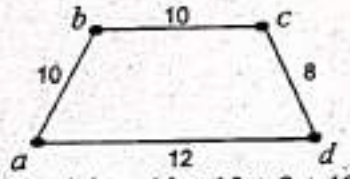


Sol. Number of vertices (n) = 4

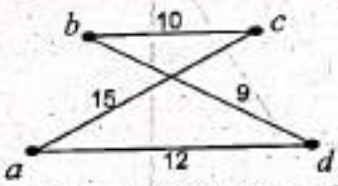
Graph shown above is complete graph (K_4)

So total number of Hamiltonian circuits = $\frac{\lfloor n-1}{2} = \frac{\lfloor 4-1}{2} = 3$

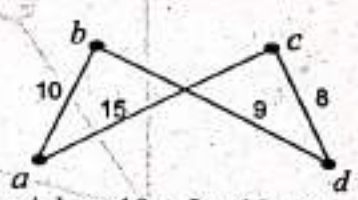
These 3 circuits are



weight = 10 + 10 + 8 + 12
= 40



weight = 10 + 9 + 15 + 12
= 46



weight = 10 + 8 + 15 + 9
= 42

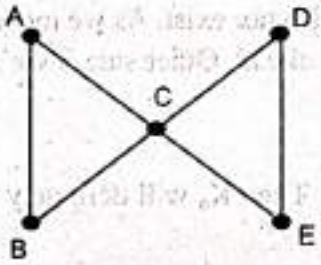
So circuit of minimum weight is a, b, c, d, a.

Example 6. Give an example of graph that has

(i) Euler circuit but not Hamiltonian circuit. (ii) Hamiltonian Circuit but not Euler circuit.

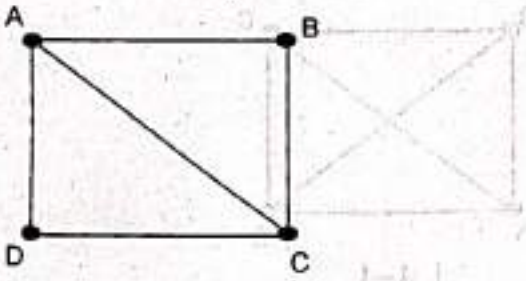
Sol. Euler circuit contains all the edges of graph exactly once where as Hamiltonian circuit is a circuit which contains all the vertices of graph exactly once. (except for first vertex which is also last)

(i) Consider the graph



This graph has a Euler circuit A, B, C, D, E, C, A. But no Hamiltonian circuit.

(ii) Consider the graph



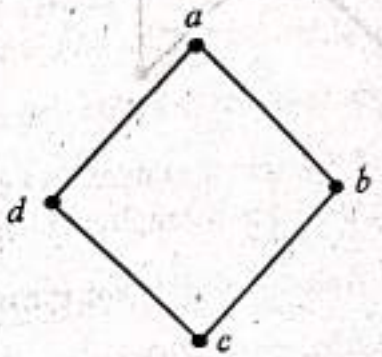
This graph has Hamiltonian circuit A, B, C, D, A

But no Euler circuit (as deg (A) = 3, which is odd)

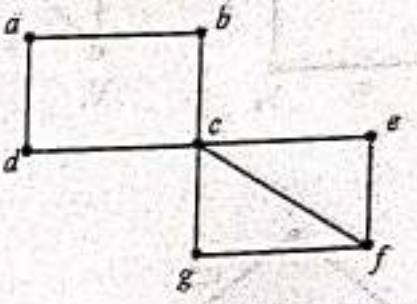
EXERCISE 1.5

In following graphs (1–4) determine whether the graph shown has a Hamiltonian circuit, Hamiltonian Path or neither. Justify you answer. Also give Hamiltonian path or circuit or both (if exists)

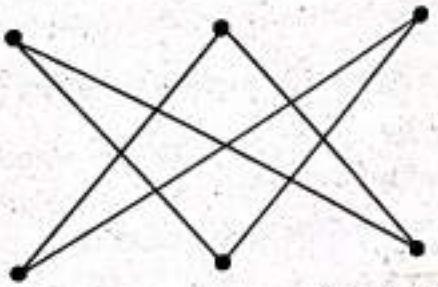
1.



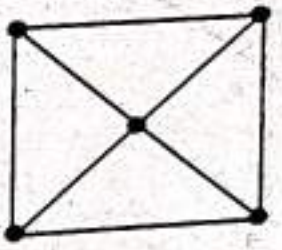
2.



3.



4.



5. How many edges must a Hamiltonian cycle in K_n contains ?

6. How many Hamiltonian cycles does K_n have ?

7. Give an example of connected graph that has

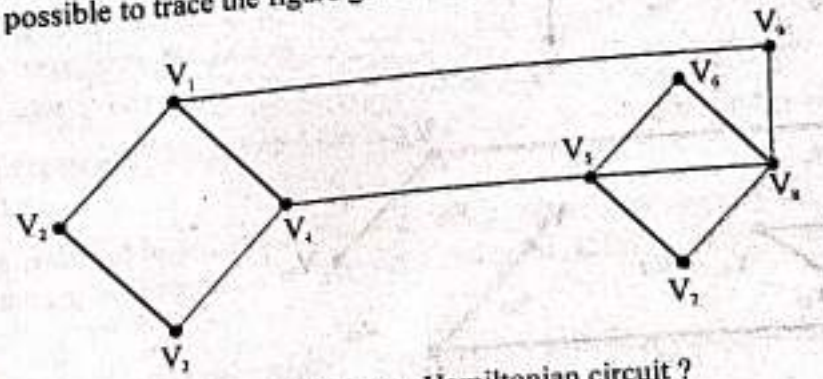
   (*a*) Neither Euler circuit nor Hamiltonian circuit.

   (*b*) An Euler circuit but no Hamiltonian cycle.

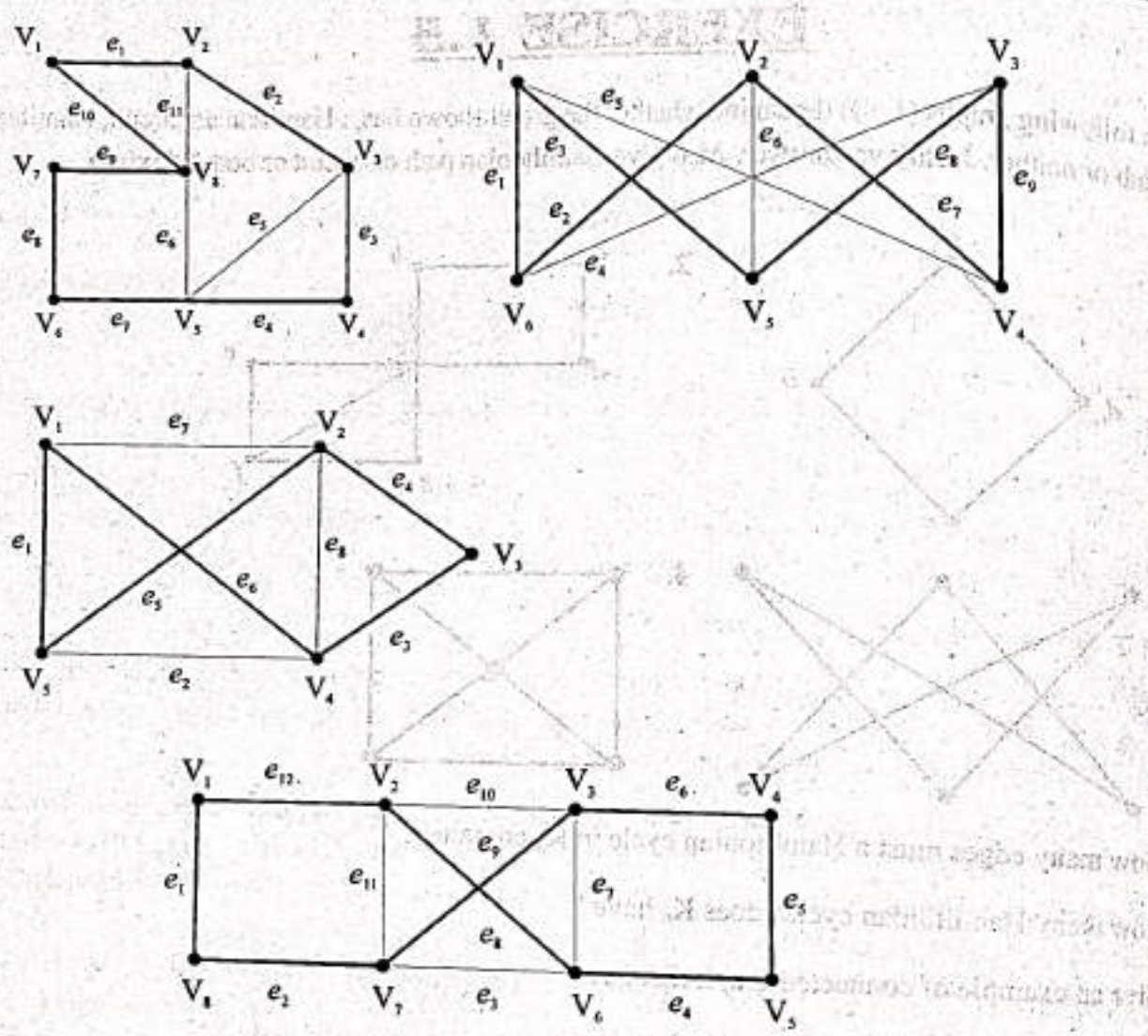
   (*c*) A Hamiltonian cycle but no Euler circuit.

   (*d*) Both Hamiltonian cycle and Euler circuit.

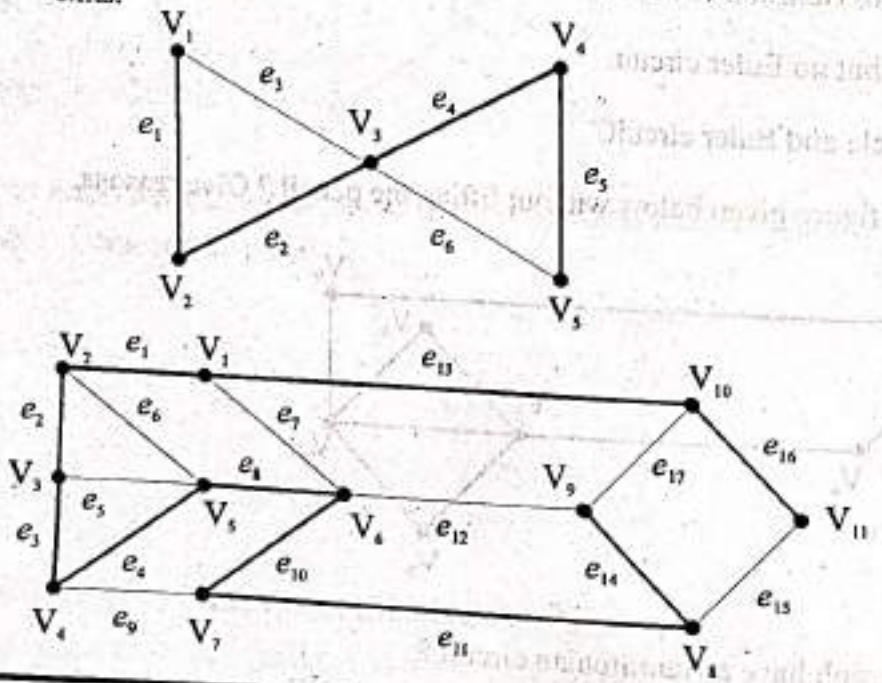
8. Is it possible to trace the figure given below without lifting the pencil ? Give reasons.



9. Which of the following graph have a Hamiltonian circuit ?



10. Find Hamiltonian paths for each of the following graphs and show that no Hamiltonian circuit exits.



1.15. Travelling Salesman Problem

A salesman travels from city to city (or place to place) with in his alloted territory in such a manner that he covers all the cities (or places) once and only once during his tour and come back to his base city. The travelling salesman problem can be salved as an assignment problem with following restrictions.

(*i*) The salesman starts his journey from his base-city and comes back to his base-city after visiting all the cities once and only once during tour alloted to him.

(*ii*) The objectives of salesman is to cover minimum distance.

(*iii*) The salesman cannot travel from a city to same city. Although the cost of travelling city to same city is zero, but this assignment is prohibited. So cost of travelling from city to same city is taken as (M or ∞).

Step 1. Construct cost efficient matrix

For the given assignment problem, construct square ($n \times n$) cost coefficient matrix. Add dummy row or column with zero cost coefficients, if cost matrix is not square.

Step 2. Find Reduced-Cost-coefficient-Matrix–

(*i*) Locate the smallest element in each row of cost coefficient matrix and subtract it from each element of that row. As a result of this operation, there will be at least one zero in each of row of **Reduced Cost coefficient** Matrix. This operation is called **Row Reduction.**

(*ii*) In the **Reduced Cost coefficient** matrix obtained from above **Row Reduction** operation, subtract the smallest element of each column from every element of that column. This operation is called **Column Reduction.** As a consequence of these two operations, there will be at least one zero in each row and column of second Reduced cost matrix.

Step 3. Make Assignment in Reduced Cost coefficient Matrix–

Make the assignments in the reduced cost coefficient matrix obtained from step 2 in the following manner.

(*i*) Examine the rows successively until a row containing only **'one'** zero is found. Enclose this zero in box □ , indicating assignment to this element. Cross out ⊗ all others zeros appearing in the corresponding column as they will not be used to make any other assignment in that column. Proceed in this way until all rows have been examined.

(*ii*) Examine the columns successively until a column with exactly **'one'** zero is found. Make an assignment in this zero by putting □ around it and cross out ⊗ all other zeros appearing in the corresponding row. Proceed in this way until all columns have been examined.

(*iii*) Repeat step 3 (*i*) and step 3 (*ii*) until all single zero in rows and columns are assigned by putting box □ around it.

(*iv*) If a row and/or column has two or more unassigned (unmarked) zeros, then **select one zero arbitrarily,** and make assignment to this zero and cross ⊗ all other zero in the corresponding row and column.

(*v*) Continue step 3 (*i*) to step (*iv*), until all zeros are either assigned (by putting it in box □) or are struck off by putting cross ⊗ over it.

Step 5 To mark minimum straight lines to cover all zeros in order to find reduced cost matrix.

Draw minimum number of horizontal and vertical lines necessary to cover all zero in the reduced cost matrix obtained in step 3 by using following procedure.

(*i*) Mark (√) all rows that do not have assignments.

(*ii*) Mark (√) all columns that have zeros in marked row obtained from step 5 (*i*).

(*iii*) Mark (√) all rows (not already marked) that have assignment in marked column obtained from step 5 (*ii*).

(*iv*) Repeat step 5 (*i*) to step 5 (*iii*) until no more rows or column can be marked (√).

(*v*) Draw straight lines through all unmarked rows and marked column.

If the number of lines drawn (n) is equal to number of rows (or column), the current assignment will be optimal otherwise go to step 6.

Step 6. To Develop new Reduced Matrix

(*i*) Select the **smallest cost element** not covered by lines, let it is 'c'.

(*ii*) Subtract this element 'c' from all uncovered elements including itself and **add** this element to each value located at **intersection** of two lines.

(*iii*) The elements through which only one line passes remain unchanged.

Step 7. Next Iteration

Repeat step 3 to 6 until optimal solution is found.

Example. A salesman wants to visit cities 1, 2, 3 and 4. He does not want to visit any city twice before completing the tour of all the cities and wishes to return to his home city cost of going from one city to another in rupees is given. Find the least cost route.

From City \ To City	1	2	3	4
1	0	3	8	5
2	4	0	14	3
3	4	5	0	2
4	7	8	13	0

Sol. As going from 1 → 1, 2 → 2 etc. is not allowed, assign a large penalty cost $c_{ii} = \infty$ to these cells.

	1	2	3	4
1	∞	3	8	5
2	4	∞	14	3
3	4	5	∞	2
4	7	8	13	∞

Step I : Reduce the matrix by subtracting the lowest element in each row from all the other elements of the row.

	1	2	3	4
1	∞	0	5	2
2	1	∞	11	0
3	2	3	∞	0
4	0	1	6	∞

Step II : Reduce the matrix by subtracting lowest element in each column from all the elements of the column.

	1	2	3	4
1	∞	0	0	2
2	1	∞	6	0
3	2	3	∞	0
4	0	1	1	∞

Step III : Select '0' element in such a way that there is only one selection in each row and column.

	1	2	3	4
1	∞	[0]	~~0~~	2
2	1	∞	6	[0]
3	2	3	∞	~~0~~
4	[0]	1	1	∞

The solution is not optimal as the route is $1 \to 2, 2 \to 4, 4 \to 1$ are it is not covering city 3.

So we shall bring element 1 into the solution. There will be three cases as 3 times 1 is in the table.

Case I : We make 'Unity arrangement' in cell (2, 1). Accordingly other assignment will charge.

	1	2	3	4
1	∞	~~0~~	[0]	2
2	[1]	∞	6	~~0~~
3	2	3	∞	[0]
4	~~0~~	[1]	1	∞

The resulting route is $1 \to 3, 3 \to 4, 4 \to 2, 2 \to 1$

With cost Rs. $(8 + 2 + 8 + 4)$ = Rs. 22.

Case II : Now we make 'Unity assignment' in cell (4, 2) and adjust other assignment accordingly.

The resultant table is as follows :

	1	2	3	4
1	∞	~~0~~	[0]	2
2	[1]	∞	6	~~0~~
3	2	3	∞	[0]
4	~~0~~	[1]	1	∞

Again the route is $1 \to 3, \to 4 \to 2 \to 1$ with cost of Rs. 22.

Case III : We make unity assignment in cell (4, 3) and adjust other assignment accordingly. The resulting table is shown below :

	1	2	3	4
1	∞	0	~~0~~	2
2	1	∞	6	~~0~~
3	2	3	∞	0
4	~~0~~	1	1	∞

The route is $1 \to 2, 2 \to 3, 3 \to 4, 4 \to 3$ which is not feasible solution.

Hence the route is $1 \to 3 \to 4 \to 2 \to 1$ with cost of Rs. 22.

Method : Some problems can not be solved like above method then we solve by Mentioned Method.

Example. A salesman must travel from city to city to sell his product. The following table shows the distance (in km) between various cities.

From City \ To City	A	B	C	D	E
A	0	40	24	30	200
B	40	0	25	300	30
C	24	25	0	26	26
D	30	300	26	0	40
E	200	30	26	40	0

Use assignment method to determine the route of tour which will covers minimum total distance.

Sol. Step 1 : Row Reduction

To City

From City	A	B	C	D	E
A	∞	16	0	6	186
B	15	∞	0	275	5
C	0	1	∞	2	2
D	4	274	0	∞	14
E	186	4	0	14	∞

Step 2 : Column Reduction

From City \ To City	A	B	C	D	E
A	∞	15	0	4	184
B	15	∞	~~0~~	273	3
C	~~0~~	~~∞~~	~~∞~~	~~∞~~	~~∞~~
D	4	273	~~0~~	∞	12
E	186	3	~~0~~	12	∞

The above assignment is not optimal because Row 2, Row 3 and Row 4 has no assignment. Next minimum element is not 1 *i.e.* 3. Therefore to overcome the difficulty we use solved. Mark minimum number of straight lines passing through all zeros.

Step 3 : Find new reduced matrix and make assignments. Test its optimally.

From City \ To City	A	B	C	D	E
A	∞	12	0	1	181
B	~~12~~	~~∞~~	~~0~~	~~270~~	~~0~~
C	~~0~~	~~∞~~	~~∞~~	~~∞~~	~~∞~~
D	1	270	~~0~~	∞	9
E	~~183~~	0	~~0~~	9	~~∞~~

Above assignment is not optimum because row 4 has no assignment.

Mark minimum number of straight lines passing through all zeros (as shown above).

Step 4. Find new reduced matrix and make assignment. Test the optionally of assignment.

From City \ To City	A	B	C	D	E
A	∞	11	0	~~0~~	180
B	12	∞	1	270	0
C	0	~~∞~~	∞	0	~~∞~~
D	0	269	~~0~~	∞	8
E	183	0	~~0~~	9	∞

every row and column has exactly one assignment so assignment is optimal. This optimal solution is not feasible for travelling salesman problem, because route is

From city A to city C

From city C to city D

From city D to city A.

Salesman starts from his base (city A) and comes back to city A after covering city C and D city B and E have not been included in the route.

Step 5 : Find new feasible solution :

In order to make assignment feasible, we select next minimum to zero. In this question it is one we make assignment at 1. Let assignment is made at the cell (2, 3)

From City	To City				
	A	B	C	D	E
A	∞	11	~~0~~	[0]	180
B	12	14	[1]	270	~~0~~
C	~~0~~	~~0~~	14	~~0~~	[0]
D	[0]	260	~~0~~	∞	8
E	183	[0]	~~0~~	9	∞

The assignment is A → D → A.

Hence assignment is not feasible.

Next minimum element is 8 ; The revised assignment is

From City	To City				
	A	B	C	D	E
A	∞	11	~~0~~	[0]	180
B	12	∞	[1]	270	~~0~~
C	0	~~0~~	∞	~~0~~	[0]
D	[0]	260	~~0~~	∞	8
E	183	[0]	~~0~~	9	∞

The assignment is

From City	To City	Distance (km.)
A	D	30
D	E	40
E	B	30
B	C	25
C	A	24
		149 km.

This assignment is feasible, because salesman starts from city A and came back to city A after covering all cities.

Example. A machine operator processes five types of items on his machine each week and must choose a sequence for them. The set-up cost per change depends on the items presently on the machine and the set-up to be made according to the following table.

From item \ To item	A	B	C	D	E
A	∞	40	70	30	50
B	40	∞	60	30	40
C	70	60	∞	70	50
D	30	30	70	∞	70
E	40	40	50	70	∞

If he processes each type of item once and only once in each week, how should he sequence the items on his machine in order to minimise the total set-up cost ?

Sol. Reduce the cost matrix and make assignment in rows and columns having single row.

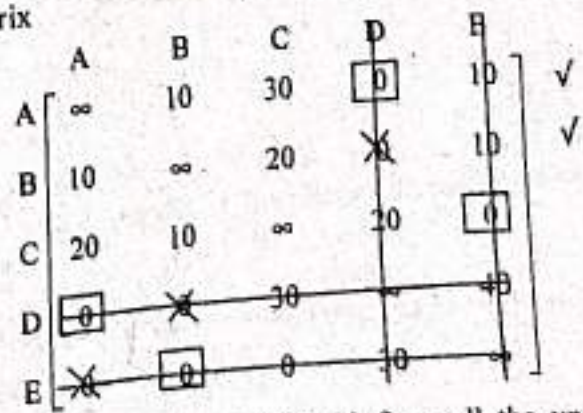
Modify the matrix by subtracting the least element from all the elements in its row and also in its column.

Row reduced matrix

	A	B	C	D	E
A	∞	10	40	0	20
B	10	∞	30	0	10
C	20	10	∞	20	0
D	0	0	40	∞	40
E	0	0	10	30	∞

√

Column reduced matrix



Subtract the smallest uncovered element *i.e.* 10 from all the uncovered elements and add to the element which is at the point of intersection of lines and get the reduced modified matrix.

	A	B	C	D	E			
A	∞	[0]	20	~~0~~	10	A	→	B
B	~~0~~	∞	10	[0]	10	B	→	D
C	10	~~0~~	∞	20	[0]	C	→	E
D	[0]	~~0~~	30	∞	50	D	→	A
E	~~0~~	~~0~~	[0]	40	∞	E	→	C

We get the solution A → B → D → A.

This schedule provides the required solution as each item is not processed once in a week.

Hence, we make a better solution by considering the next smallest non-zero element by considering 10.

	A	B	C	D	E
A	∞	~~0~~	20	~~0~~	[10]
B	10	∞	10	[0]	10
C	10	[0]	∞	10	~~0~~
D	[0]	~~0~~	30	∞	50
E	~~0~~	~~0~~	[0]	40	∞

$A \to E, E \to C, C \to B, B \to D, D \to A$, *i.e.* $A \to E \to C \to B \to D \to A$.

The total set-up cost comes to Rs. 220.

2

TREES

A connected graph that contains no circuit is called a **tree.** Trees were used as long ago as 1857, when the English mathematician **Arthur Cayley** used them to count certain types of chemical compounds. Since that time, trees have been employed to solve problems in a wide verity of disciplines.

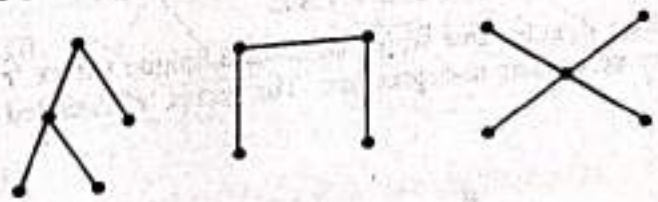
Trees are particularly useful in computer science Trees are employed to construct efficient algorithms for locating items in a list. They are used to construct networks with the least expensive set of telephone lines linking distributed computers. Trees can be used to construct efficient codes for storing and transmitting data. Trees can model procedures that are carried out using a sequence of decisions. This makes trees valuable in study of Computer Science.

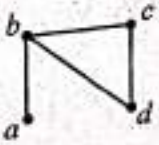
Definition Tree : A graph G is called a tree if

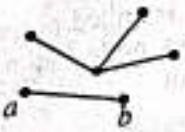
(*i*) G is connected

(*ii*) G has no cycles.

Following graphs are trees :



Graph  is not tree as it contains a cycle *b, c, d, b*

Similarly  is not tree as it contains a disconnected component *a b.*

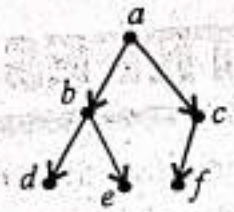
Remark : From above definition, it follows that a tree has to be a simple graph *i.e.* having neither a self loop nor parallel edges because both of them from cycle.

Note : Tree is said to be directed if every edge of tree is assigned a direction, otherwise tree is undirected.

TERMINOLOGY USED IN TREE

When we discuss tree, we encounter a number of terms that are necessary to understand.

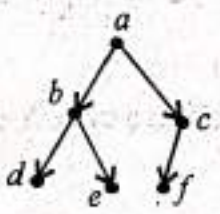
The terms used are :



- **NODE OR VERTEX:** Node is key component of tree which stores information and can have one or more links for connecting to other nodes.
- **EDGE or LINK:** A directed line from one node to other node is called edge, link, arc or branch of a tree. In above figure *ab*, *ac* etc are links.
- **ROOT:** The vertex having indegree zero is called root of tree. In above tree root of tree is a.
- **PATH :** A Path is a sequence of nodes when we traverse from one node to other along the edges which connect them e.g. path from *a* to *f* is *a, c, f*.
- **LEVEL:** Level of node is an integer value that measures the distance of a node from the root. Root is at level 0. The child(s) of root are at level 1 and so on.
- **HEIGHT:** Height of node is the length of longest path from node to a leaf. All the leaves are at height 0. Height of root is height of tree. In above tree, height of *d, e, f* is 0, Height of *b, c* is 1 and height of *a* is 2.
- **DEPTH:** The depth of node is the length of path from node to root of tree. Root has depth 0.

  In above tree depth of a is 0 depth of *b, c* is 1. Depth of *d, e, f* is 2.
- **ROOTED TREE :** A rooted tree is a directed tree which contains a unique vertex '*r*' such that in-degree of *r* is zero and every other vertex has in-degree one. The vertex '*r*' is called root of rooted tree.

  For example :



  is a rooted tree with root '*a*'.
- **PARENT AND OFFSPRING :** If (x, y) is any directed edge then x is called parent of y and y is called offspring of x. Root of tree has no parent whereas every other node has a unique parent. A parent can have several offsprings. Offspring is also called **child** or **son**.

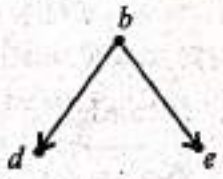
  In above tree a is parent of *b* and *c*. *b* has two offsprings *d* and *e*.
- **LEAF :** A node having no offsprings (outdegree = 0) is called a leaf. In fig. *d, e, f* are leaves. Leaf is also called **external** or **terminal** node.
- **SIBLINGS :** Two nodes having same parent are called siblings. In figure *b, c* are siblings of *a*.
- **INTERIOR NODE :** Node having at least one child is called Interior node.

- **ANCESTOR :** Ancestors of a vertex other than root are the vertices in the path from root to this vertex, excluding the vertex itself and including the root. For example, ancestors of *d* are *b* and *a*.
- **DESCENDANT :** Descendants of a vertex 'V' are those vertices that have 'V' as an ancestor.

For example : Descendants of *b* are *d* and *e*.

- **SUBTREE :** If '*a*' is any vertex in a tree, the subtree with *a* as its root is the subgraph of tree consisting of *a* and its descendants are all edges incident to these descendants.

In given fig. subtree of *b* is T(*b*) as shown :



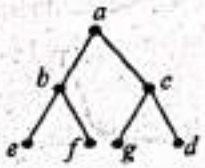
- **FOREST:** A forest is an undirected graph whose components are all trees.
- **BINARY TREE :**

Let T is a tree. We say T is *n*-tree or *n*-ary tree if every vertex has at most *n* offsprings. In particular, if $n = 2$ then tree is called binary tree. So binary tree is that tree in which every node can have 0, 1 or 2 offsprings.

- **COMPLETE BINARY TREE :**

In *n*-tree, if every vertex of T, other than leaves, has exactly *n*-offsprings then we say T is complete *n*-Tree. For $n = 2$ we say tree is complete Binary tree.

Example (*i*)

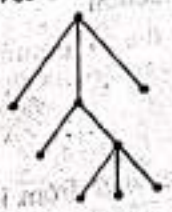


is a Binary Tree.

In this example, *b* is left child of *a* and *c* is right child of *a*.

Moreover every vertex (except leaves) has 2 children so tree is complete Binary Tree.

(*ii*)



is a 3-ary tree. But is not complete.

2.1. Properties of Tree

Property 1. There is one and only one path between every pair of vertices in a tree T.

Proof : Since T is a connected graph. Therefore there exists atleast one path between every pair of vertices in tree T.

Suppose that between two vertices v_1 and v_2 there exists two distinct paths. The union of these two paths will contain a circuit and then T cannot be a tree. Thus there is one and only path between every pair of vertices in a tree T.

Property 2. If in a graph G, there is one and only one path between every pair of vertices, then G is tree.

Proof : Since there is one and only one path between every pair of vertices in G implies that G is connecte graph. Suppose that G contain a circuit, then there is atleast one pair of vertices v_1, v_2 (say) such that ther are two distinct path between them. A contradiction to the given fact and so G cannot have circuit. Hence G is a connect graph without circuit implies that G is a tree.

Property 3. A tree with n vertices has $n-1$ edges.

Proof. We shall prove the result by induction on the number of vertices n.

Obviously the result is true for $n = 1, 2, 3$ as

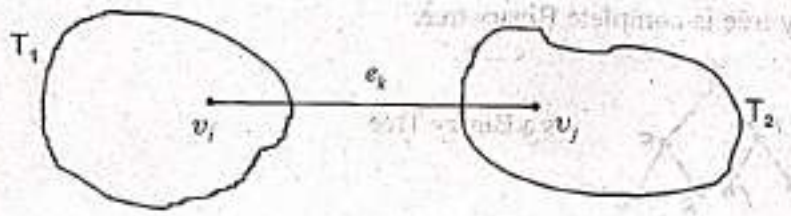
When $n = 1$ we have • Zero edge

When $n = 2$ we have | One edge

When $n = 3$ we have V | Two edge.

Let us assume that the result is true for all tree with less than n vertices.

Consider a tree T with n vertices. Let e_k be an edge with end verities v_i and v_j. Since there is one and only one path between every pair of vertices *i.e.*, there is no other path between v_i and v_j except e_k. Therefore deletion of edge from T will disconnect the graph as shown below.



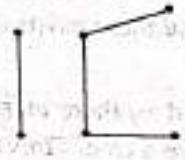
Therefore T– e_k consist of exactly two component T_1 and T_2 (say). Since there is no circuits in T each of these components is a tree. Further, both of these tree T_1 and T_2 have less then n–vertices, therefore by supposition, each tree will contain edge one less then the number of vertices in it. So T– e_k consist of $(n-2)$ edges implies that T has exactly $(n-2)+1 = n-1$ edges. This completes the induction.

Note : It may be noted that the vertices of a tree are connected together with the minimum number of edges.

Definition. Minimally connected graph :

A connected graph G is said to be minimally connected if removal of any edge from it disconnect the graph.

For Example :



are minimally connected graphs.

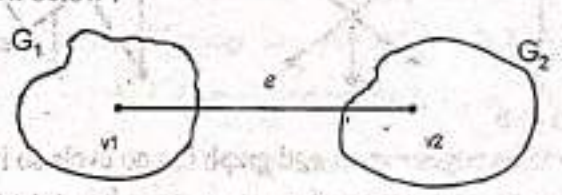
Property 4. A graph is a tree if and only if it is minimally connected.

Proof : Firstly, let the graph T be a tree. Therefore T must be a connected graph. If possible, let T be not minimally connected. Then there must exists an edge e_i in T such that $T - e_i$ is connected. Therefore e_i is in some circuit which implies that T is not a tree, a contradiction. Hence T must be minimally connected.

Conversely. Let T be a minimally connected graph. Therefore T cannot have a circuit otherwise we could remove one of the edge in the circuit and still leave the graph connected. Hence T is a tree.

Property 5. A graph G with n vertices and $(n-1)$ edges and no circuit is connected.

Proof : Let there exist a graph G with n vertices, $(n-1)$ edges and no circuit which is disconnected. Then G will consists of two or more circuit-less component. Without loss of generality, let G consist of two components G_1 and G_2 as shown below :



Now, add an edge e between the vertices v_1 in G_1 and v_2 and G_2. Since there is no path between v_1 and v_2 in G so by adding an edge e did not create a circuit in G. Thus $G \cup e$ is a circuit less connected graph. *i.e.*, $G \cup e$ is a tree in other words, a tree has n vertices an n edges, which is not possible. Hence a graph with n vertices and $(n-1)$ edges and no circuit is connected.

Remark : Five different but equivalent definition of tree are A graph G with n vertices is called a tree if

(*i*) G is connected and has no circuit.
(*ii*) G is connected and has $(n-1)$ edges.
(*iii*) G has $n-1$ edges and no circuit.
(*iv*) there is exactly one path between every pair of vertices in G.
(*v*) G is minimally connected.

2.2. In any non-trivial tree, there are atleast two pendent vertices.

Or

In any non-trivial tree, there are at least two vertices of degree 1.

Proof : Let T be a non-trivial tree with n vertices, then T has $n-1$ edges.

$\therefore$ By fundamental theorem on graph theory

$$\sum_{i=1}^{n} \deg(v_i) = 2(n-1) = 2n-2 \qquad \ldots(1)$$

If possible, let T contain only one vertex (say) v_1 of degree 1. Then

$$\deg(v_1) = 1 \quad \text{and} \quad \deg(v_i) \geq 2 \quad \text{for } i = 2, 3, 4, \ldots, n$$

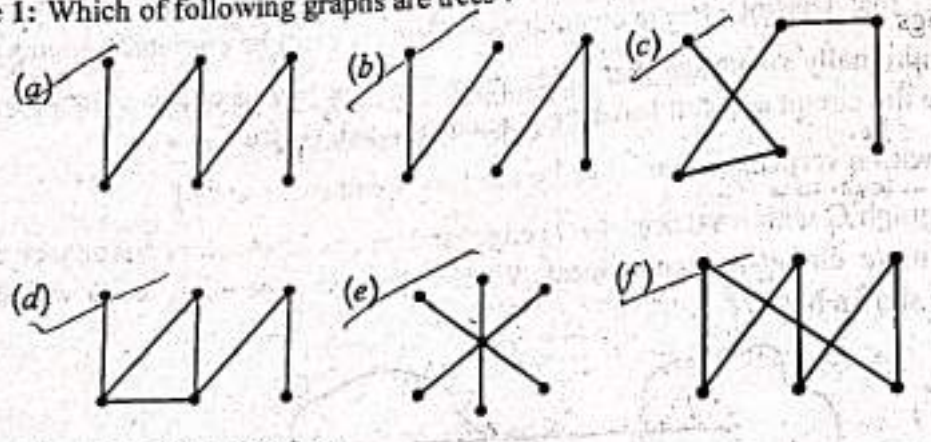
$$\therefore \quad \sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \sum_{i=2}^{n} \deg(v_i)$$

$$= 1 + \sum_{i=2}^{n} \deg(v_i) \geq 1 + 2(n-1) = 2n-1 \qquad \ldots(2)$$

$\therefore$ From (1) and (2), we get $2n-2 \geq 2n-1$, a contradiction.

$\therefore$ T must have more than one vertex of degree 1 *i.e.*, T has atleast two vertices of degree 1.

Example 1: Which of following graphs are trees ?



Sol. (*a*) Number of vertices = 6
Number of edges = 5 as edges = $n-1$ and graph has no cycle so it represent a tree.

(*b*) Since graph contains two disconnected components so it is not a tree.

(*c*) Number of vertices = 6
Number of edges = 5 as edges = $n-1$ and graph has no cycle so it represent a tree.

(*d*) Graph contains a cycle so it is not a tree.

(*e*) Graph is a tree $\because$ it contains no cycle and number of edges (6) = number of vertices (7)–1.

(*f*) Graph is not tree as it contains a cycle.

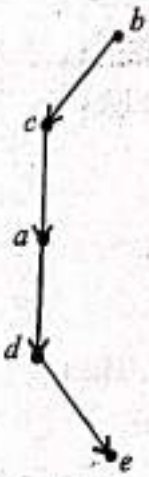
Example 2. Let A = {*a, b, c, d, e*} R = {(*a, d*), (*b, c*), (*c, a*), (*d, e*)} check whether R is a tree. If it is, find the root.

Sol. We are given five vertices and four edges. R will from tree iff

(*i*) edges connect all vertices

(*ii*) edges will not form cycle among vertices.

From R, it is clear '*b*' has indegree 0. If R is tree then *b* must be root. So taking *b* as root we construct all edges as below



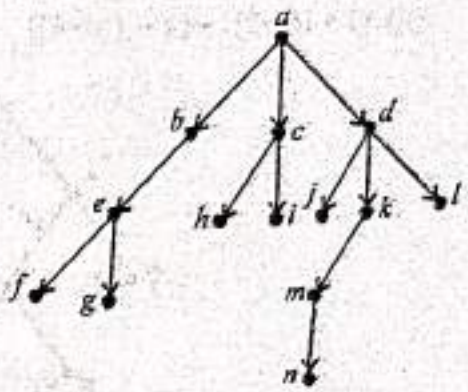
As no cycle is formed, so R is a tree and *b* is root of tree.

Example 3. Prove that A = {1, 2, 3, 4, 5, 6} R = {(1, 1), (2, 1), (2, 3), (3, 4), (4, 5), (4, 6)} is not a tree.

Sol. As number of vertices = 6 and number of edges = 6. So R cannot be a tree.

$\because$ in tree no. of edges = $n-1$, n = no. of vertices.

Example 4. Consider the tree.



(*a*) List all level-3 vertices.

(*b*) List all leaves.

(*c*) What are siblings of *d*?

(*d*) Draw the Tree T(*b*).

(*e*) What is level and height of *m*?

Sol. (*a*) Root of tree is *a*. So level of $a = 0$

At level one we have *b*, *c*, *d*

at level two we have *e*, *h*, *i*, *j*, *k*, *l* at level three we have *f*, *g* and *m*.

(*b*) Leaves are vertices that have no offsprings. In given tree leaves are *f*, *g*, *h*, *i*, *j*, *n* and *l*.

(*c*) Siblings of *d* are *b* and *c* ∵ *b*, *c*, *d* have same parent *a*.

(*d*) Tree T(*b*) is as shown

(*e*) Level of $m = 3$

Height of $m = 3 + 1 = 4$ (Height = level + 1)

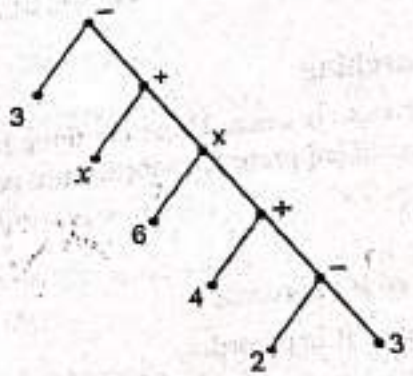
2.3. Labeled Trees

Definition : A Tree is said to be labeled in which every vertex of Tree has assigned a unique label.

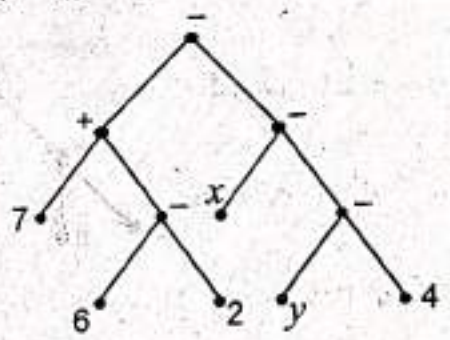
Labeled tree is usually used to construct expression Tree. Any algebric expression can be represented with the help of labeled binary tree. For this root of tree is labeled with the central operator of main expression. The two offsprings of root are labeled with central operator of expression for left and right arguments respectively. If either argument is a constant or variable (instead of expression), this is used to label the corresponding offspring vertex. This process continues until expression is exhausted.

Example 5. Construct the tree of algebraic expression.

(*i*) $3 - (x + (6 \times (4 \div (2-3))))$



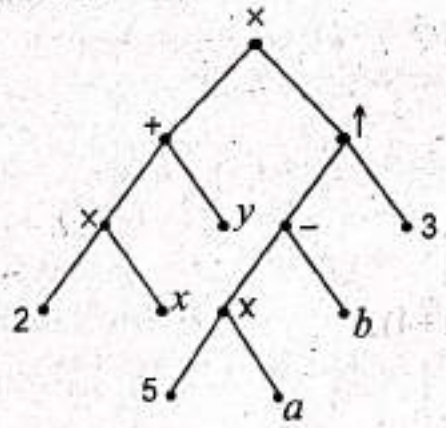
(*ii*) $(7+(6-2))-(x-(y-4))$



(*iii*) $(2x+y)(5a-b)^3$

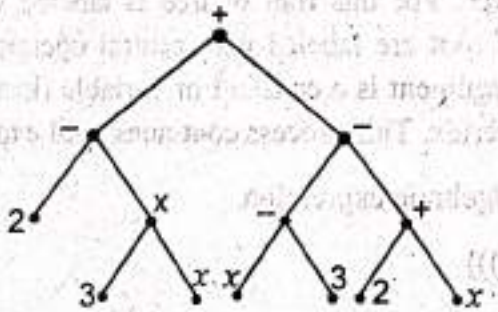
This expression is equivalent to $((2 \times x)+y) \times ((5 \times a)-b)^3$

Exponent is represented by symbol ↑



Example 6. Draw a binary tree to represent $(2-(3\times x))+((x-3)-(2+x))$.

Sol.



2.4. Traversal of Binary Trees or Tree Searching

Traversing means to visit each node of tree exactly once. There are three standard ways of traversing a binary tree T with Root R. These algorithms are called preorder, inorder and post order traversals and are as follows :

Preorder : (1) Process the root R.

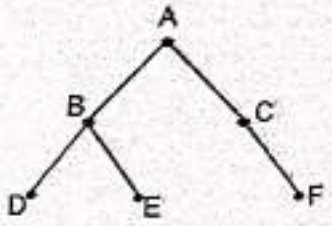
(2) Traverse the left subtree of R in preorder.

(3) Traverse the right subtree of R in preorder.

Inorder : (1) Traverse the left subtree of R in inorder.
(2) Process the root R.
(3) Traverse the right subtree of R in inorder.

Post order : (1) Traverse the left subtree of R in postorder.
(2) Traverse the right subtree of R in postorder
(3) Process the root R.

Example 7. Traverse the following Tree in Preorder, Post order and inorder.

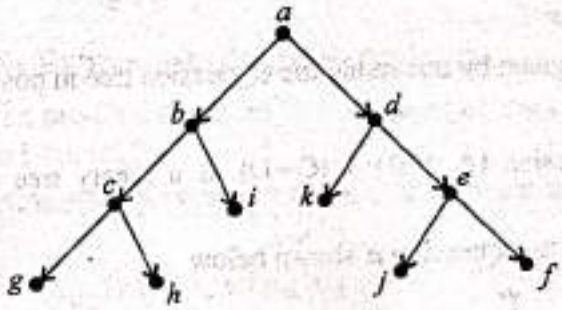


Preorder Traversal : A, B, D, E, C, F

Postorder Traversal : D, E, B, F, C, A

Inorder Traversal : D, B, E, A, C, F.

Example 8. Search the following Tree in pre-order, post-order and in-order.



Sol. Pre-order Searching : For pre-order first we process root then left subtree in preorder and then right subtree in pre-order. Result is :

a, b, c, g, h, i, d, k, e, j , f

In-order Searching : For in-order first we traverse left subtree in inorder, then we process root and atleast we process right subtree in order. Result is :

g, c, h, b, i, a, k, d, j, e, f

Post-order Searching : For post-order first we traverse left subtree in post-order, then we traverse right subtree in post-order and last we process root. Result is :

g, h, c, i, b, k, j, f, e, d, a.

Polish Notations : An expression tree has three forms

1. Prefix Form : When a pre-order traversal is performed on an expression tree then result obtained is called pre-fix form or Polish form of the given algebraic expression.

2. Post Fix Form : When a post-order traversal is performed on an expression tree then result obtained is called post-fix form or reverse polish form of the given algebraic expression.

3. Infix Form : Infix form results from the in-order traversal of expression tree.

Consider the expression $a + b$. In this expression a, b are operands and '+' is an operator. The sequence of operators and operands in three form is as given below :

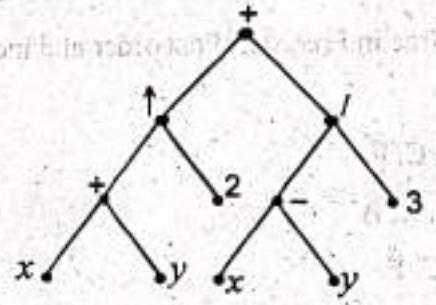
Pre-fix form : operator, operand, operand

Post-fix form : operand, operand, operator

In-fix form : operand, operator, operand

Example 9. Find pre-fix and post-fix expression for $((x + y) \uparrow 2) + ((x - y)/3)$

Sol. The expression tree of above expression is show below :



To find pre-fix form of given expression, we traverse the tree in pre-order. Result is :

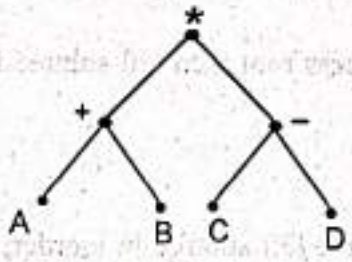
$+ \uparrow + x\ y\ 2\ / - x\ y\ 3.$

Post-fix form of expression is given by traversing the expression tree in post order. Result is :

$x\ y + 2 \uparrow x\ y - 3\ / +.$

Example 10. Represent the expression (A + B) * (C−D) as a binary tree and write prefix form of expression.

Sol. The Binary Tree corresponding to expression is shown below

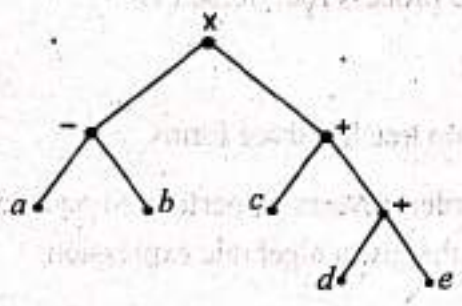


Prefix form : *, +, A, B, −, C, D.

Example 11. Consider the completely parenthesized algebraic expression :

$(a-b) \times (c + (d \div e))$. Find its preorder, post order and inorder search.

Sol. First we draw expression tree corresponding to given algebraic expression which is shown below :



Preorder Search : $\times, -, a, b, +, c, \div, d, e.$

Postorder Search : $a, b, -, c, d, e, \div, +, \times$

Inorder Search : $a, -, b, \times, c, +, d, \div, e.$

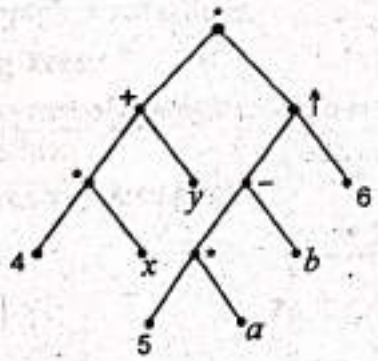
Example 12. Construct a tree whose pre-order and in-order traversal is given below :

Pre-order $* \; + \; * \; 4 \; x \; y \; \uparrow \; - \; * \; 5 \; a \; b \; 6$

In-order $(4x+y) * (5a-b) \uparrow 6$

Sol. To construct tree 1st we see pre-order traversal. In this first element is * which become root of tree. Then we see the position in In-order traversal. Left of * *i.e.* $4x + y$ become left subtree and $(5a - b) \uparrow 6$ become right subtree. This process will repeat until whole of tree has been constructed.

The tree formed is shown below :



2.5. Evaluation of Prefix Expression (Polish Expression)

Procedure : Let P be given pre-fix expression. Let S denotes binary arithmetic operator (+, −, *, /, ↑). Following steps are used to evaluate P :

1. Traverse P from left to right until we find a string of the form Sxy, where x and y are numbers (operands).
2. Evaluate xSy.
3. Substitute the result of xSy for the string Sxy.
4. Continue the procedure until only one number remains.

Example 13. Evaluate the pre-fix expression $+ - * 2 \; 3 \; 5 / \uparrow 2 \; 3 \; 4$.

Sol. The step by step procedure to evaluate above expression is shown in following figure.

Step 1 : $+ - \underbrace{* \; 2 \; 3}_{2*3=6} \; 5 / \uparrow 2 \; 3 \; 4$

Step 2 : $+ \underbrace{- \; 6 \; 5}_{6-5=1} / \uparrow 2 \; 3 \; 4$

Step 3 : $+ \; 1 \; / \underbrace{\uparrow \; 2 \; 3}_{2\uparrow 3=8} \; 4$

Step 4 : $+ \; 1 \underbrace{/ \; 8 \; 4}_{8/4=2}$

Step 5 : $\underbrace{+ \; 1 \; 2}_{1+2=3}$

Value of expression = 3.

2.6. Evaluation of Post fix Expression (Reverse Polish Expression)

Procedure : Let P be given post-fix expression. Let S denotes binary arithmetic operator (+, −, *, /, ↑)

1. Traverse P from left to right until we find a string of the form $x \; y \; S$, where x and y are numbers. (operands).

2. Evaluate xSy.

3. Replace string xyS by result of xSy.

4. Continue the procedure until only one number remains.

Example 14. What is the value of post-fix expression

7 2 3 * − 4 ↑ 9 3 / +

Sol. The step by step procedure to evaluate above expression is shown in following figure:

Step 1 : 7 [2 3 *] − 4 ↑ 9 3 4 / +
$2*3 = 6$

Step 2 : [7 6 −] 4 ↑ 9 3 / +
$7-6 = 1$

Step 3 : [1 4 ↑] 9 3 / +
$1 \uparrow 4 = 1$

Step 4 : 1 [9 3 /] +
$9/3 = 3$

Step 5 : [1 3 +]
$1+3 = 4$

Value of expression = 4.

Example 15. Is their a binary tree with height 6 and 65 leaves ?

Sol. Height of Tree = 6

So maximum number of levels = 6 − 1 (level = height − 1) = 5

We know, maximum number of leaves in a Binary Tree = 2^r, where r is level.

So maximum number of leaves = $2^5 = 32$

Therefore, binary tree with height 6 and 65 leaves is not possible.

Example 16. A tree with n vertices has at least two vertices of degree 1. $(n \geq 2)$.

Sol. Given tree T has n vertices

So number of edges in T = $n-1$

Let us suppose T has no vertex of degree = 1

We know, total degree = 2 × number of edges

$= 2(n-1)$.

So degree of each vertex = $\frac{2n-2}{n} = 2 - \frac{2}{n} \leq 2 - \frac{1}{n}$ $\left(\because \frac{2}{n} \leq 1\right)$

⇨ either degree of vertex is 1 or 0.

But T can not have a vertex of degree zero.

So our supposition is wrong. T must have at least two vertices of degree = 1.

Example 17. How many edges does a tree with 10,000 vertices have ?

Sol. Number of vertices = 10000

We know number of edges = $n - 1 = 10{,}000 - 1 = 9999$.

Spanning Tree :

Let G be a connected graph. A subgraph T of G is called a spanning tree if

(*i*) T is a tree. (*ii*) T contains all vertices of G.

For example  is a connected graph G. Clearly it is not a tree.

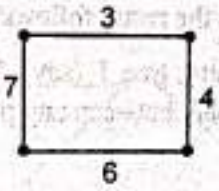
A spanning tree of G is 

Note : Spanning tree of graph is not unique.

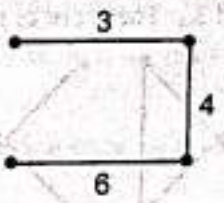
Minimal Spanning Tree :

A minimal spanning tree of a weighted graph is a spanning tree with the condition that sum of weights of tree is as small as possible.

For example : Given weighted graph



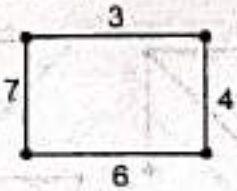
Minimal spanning tree of this graph is



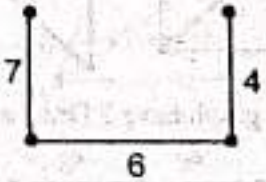
Weight of minimal spanning Tree = 3 + 4 + 6 = 13.

Maximal Spanning Tree : A maximal spanning tree of a weighted graph is a spanning tree with the condition that sum of weights of tree is as large as possible.

For example : Given weighted graph



Maximal spanning tree of this graph is



Weight of maximal spanning tree = 7 + 6 + 4 = 17.

2.7. A graph G is connected if and only if it has a spanning tree.

Proof : Firstly, let the graph G be connected. Let k be the number of circuits (or cycles) in G. We apply induction on k. If $k = 0$, then G has no circuit also, G is connected.

⇒ G is a tree and so has a spanning tree.

∴ The result is true for $k = 0$

Let the result is true for all connected graphs with less than k cycles.

Let G be a connected graph with k circuits. Let e be an edge in one of the circuits, then $G-e$ is connected graph having fewer edges than G.

∴ By induction hypothesis $G - e$ has a spanning tree. But $G - e$ has all the vertices of G.

∴ The spanning tree of $G - e$ is also a spanning tree for G.

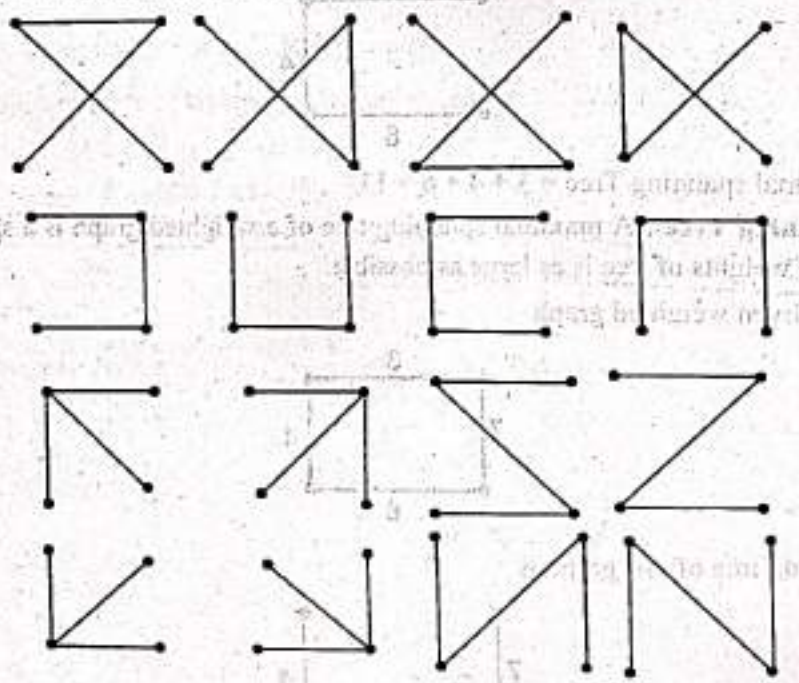
∴ The result is true for G also. Hence the result follows by induction.

Conversely : Let the graph G has a spanning tree T (say). We show that G is connected. Since T is a spanning tree of G. Therefore there exists a path between any pair of vertices in G along the tree T.

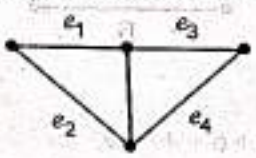
∴ G is connected.

Remark. (Cayley's Theorem) The complete graph K_n has n^{n-2} different spanning tree.

For example : There are 16 spanning trees of K_4. These are as shown below :



Example 18. How many spanning trees the graph have ? Draw all spanning trees of graph.



Sol. We know spanning tree contains all vertices of graph. So number of edges taken $= 4-1 = 3$.

As we are given 5 edges which means we have to remove 2 edges.

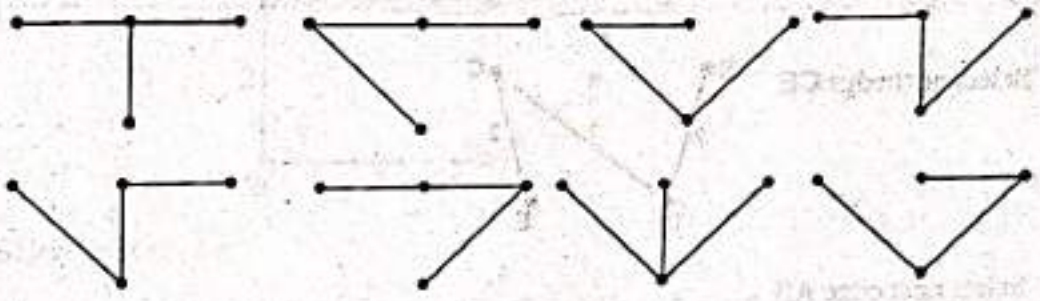
Number of ways for removing 2 edges $= {}^5C_2 = 10$ ways.

But removal of edges should not disconnect graph.

If we remove e_1, e_2 then graph is disconnected. Similarly removal of e_3, e_4 result in disconnected graph.

$\therefore$ there are 8 possible spanning trees of given graph.

These are :

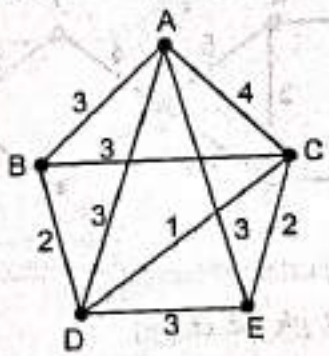


2.8. Kruskal's Algorithm (To find minimal spanning tree)

Let G be the given connected graph with n vertices. Then Kruskal Algorithm to find minimal spanning tree involves following steps :

1. Write all the edges of graph in increasing order of their weight.
2. Select the smallest edge of G.
3. For each successive step select another smallest edge of G which makes no cycle with previously selected edges.
4. Go on repeating step 3 until $n-1$ edges have been selected. The sum of weights of these $n-1$ edges will constitute required minimal spanning tree.

Example 19. Find the minimal spanning tree of weighted graph using Kruskal's algorithm.



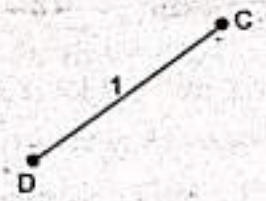
Sol. Number of vertices $(n) = 5$

First we write all edges in increasing order of weight

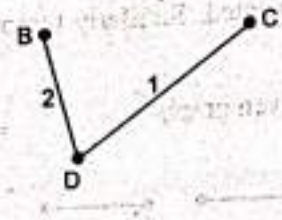
E = {CD, BD, CE, AB, BC, AD, AE, DE, AC}

We start from edge CD and then select edges one by one from E until we select 4 edges $(n-1)$.

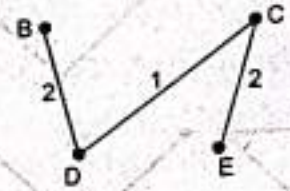
(*i*)



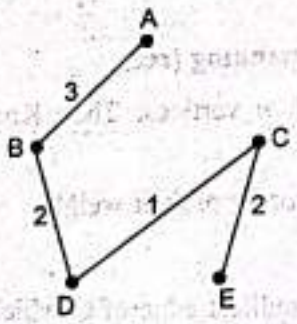
(*ii*) Select next edge BD



(*iii*) Select next edge CE

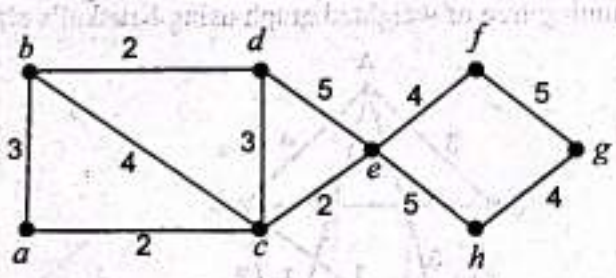


(*iv*) Select next edge AB



Since we have 5 vertices and we have selected 4 edges, so we stop algorithm. Minimal spanning tree is as shown and sum of weights is 1 + 2 + 2 + 3 = 8.

Example 20. Find the minimal spanning tree for the following weighted connected graph using Kruskal's Algorithm.



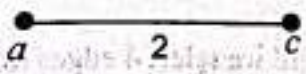
Sol. First we write all edges in Increasing order of weight

E = {*ac, bd, ce, ab, cd, bc, ef, gh, ed, eh, fg*}

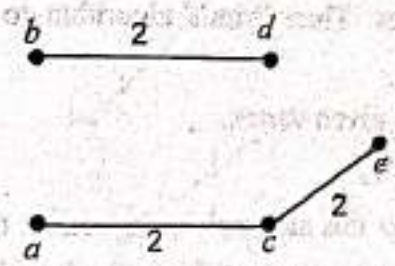
Number of vertices (n) = 8

We start from edge *ac* and then select edges one by one from E until we select 7 edges ($n-1$)

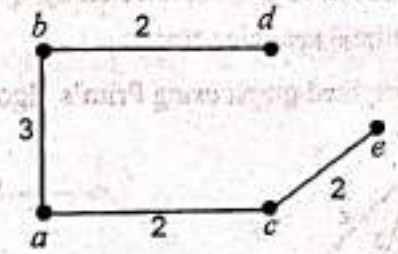
(*i*)



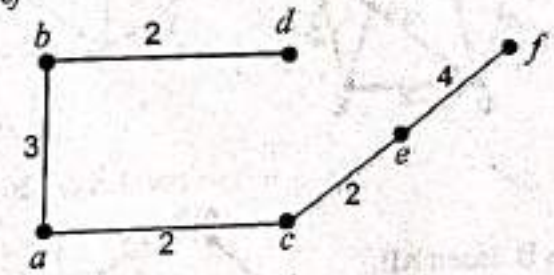
(ii) Select next edge *bd* and then *ce*.



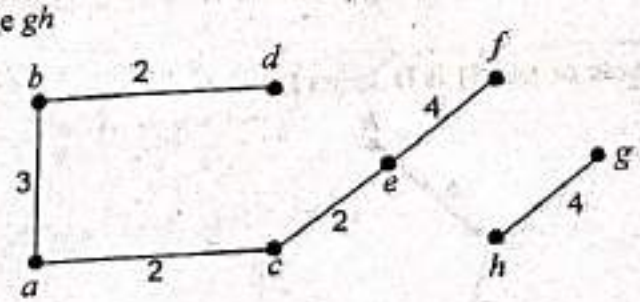
(iii) Select next edge *ab*



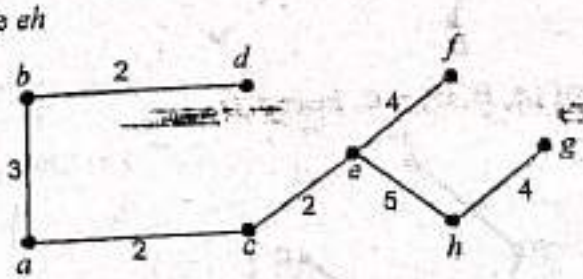
(iv) Select next edge *ef*



(v) Select next edge *gh*



(vi) Select next edge *eh*



As we have selected 7 edges, so we stop algorithm. Minimal spanning tree is as shown and sum of weights is

$$2 + 2 + 2 + 3 + 4 + 4 + 5 = 22.$$

2.9. Prim's Algorithm to Find Minimal Spanning Tree

Let G be the given graph with n vertices. Then Prim's algorithm to find minimal spanning tree involves following steps :

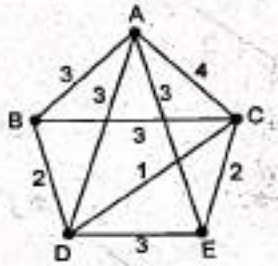
1. Choose any vertex V_1 of G or start from given vertex.

2. Connect V_1 to its nearest neighbour say V_i.

3. Taking (v_1, v_i) as one subgraph, connect this subgraph to its nearest neighbour *i.e.* vertex which is nearest to V_1 or V_i. Let this vertex is V_k. The new vertex must not form a cycle with previous added vertices.

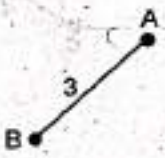
4. Go on repeating step 3 until all n vertices have been connected by $n-1$ edges. The sum of weights of these $n-1$ edges will constitute required minimal spanning tree.

Example 21. Find minimal spanning tree of weighted graph using Prim's algorithm.



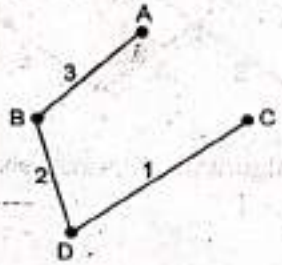
Sol. Let us start from vertex A.

(*i*) Nearest neighbour of A is B. Insert AB.

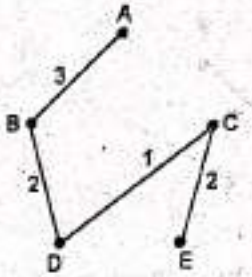


(*ii*) Next nearest neighbour of {A, B} is D. Insert BD.

(*iii*) Next nearest neighbour of {A, B, D} is C. Insert CD.

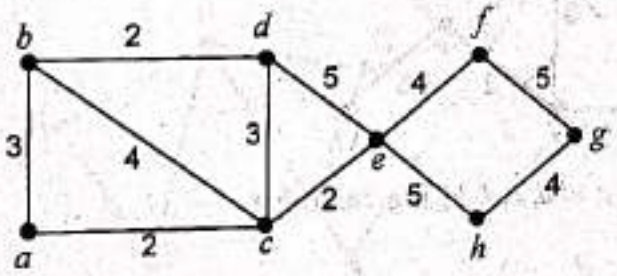


(iv) Next nearest neighbour of {A, B, D, C} is E. Insert CE.



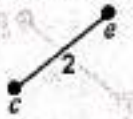
As number of vertices are 5 and we have connected 5 vertices using 4 edges so we stop algorithm. Sum of weights is $= 1 + 2 + 2 + 3 = 8$.

Example 22. Find minimal spanning tree for the following weighted connected graph using Prim's algorithm by starting at *e*.

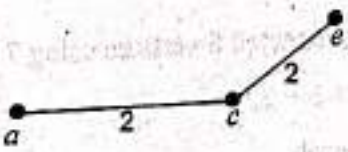


Sol. We start from given vertex *e*.

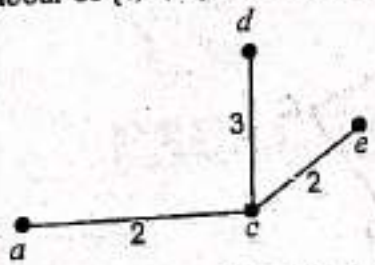
(i) Nearest neighbour of *e* is *c*. Insert *e c*.



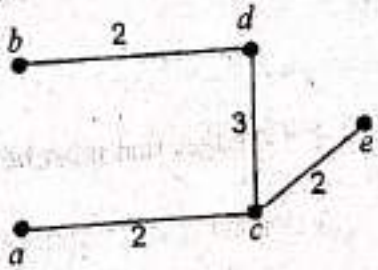
(ii) Next nearest neighbour of {*e*, *c*} is *a*. Insert *c a*.



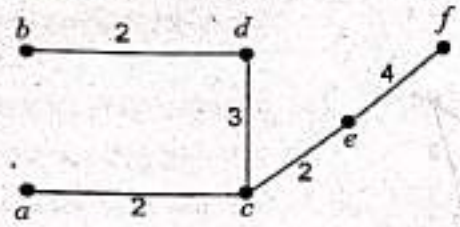
(iii) Next nearest neighbour of {*e*, *c*, *a*} is *d*. Insert *c d*.



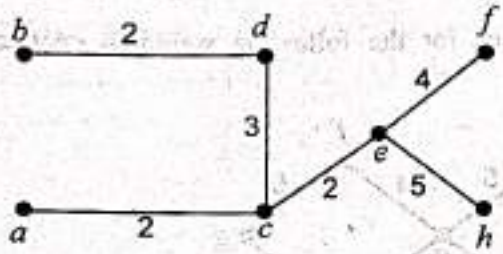
(iv) Next nearest neighbour of {*e*, *c*, *a*, *d*} is *b*. Insert *b d*.



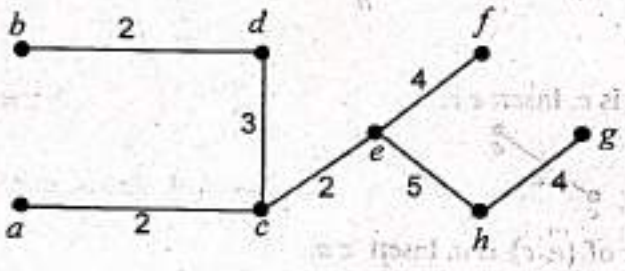
(v) Next nearest neighbour of $\{e, c, a, d, b\}$ is f. Insert $e f$.



(vi) Next nearest neighbour of $\{e, c, a, d, b, f\}$ is h. Insert $e h$.



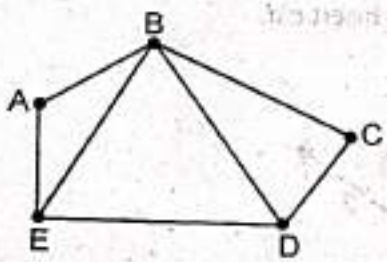
(vii) Next nearest neighbour of $\{e, c, a, d, b, f, h\}$ is g. Insert $h g$.



As number of vertices are 8 and we have connected 8 vertices using 7 edges, so we stop algorithm.

Sum of weights is $= 2 + 3 + 2 + 2 + 4 + 4 + 5 = 22$.

Example 23 Generate a spanning tree for the graph.

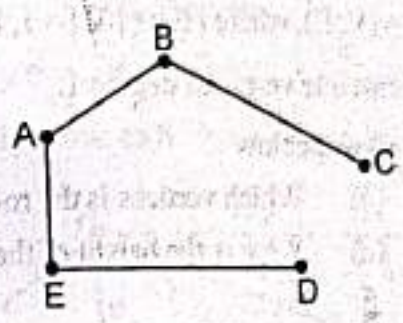


Sol. Number of edges in graph = 7

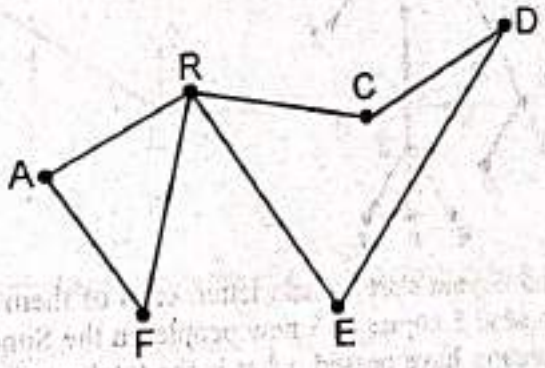
Number of vertices in graph $(n) = 5$

For spanning tree we need $n - 1$ edges *i.e.* $5 - 1 = 4$ edges that must be connected in such a way so that graph must be connected without cycle.

One such spanning tree is :



Example 24. Generate a spanning tree for :

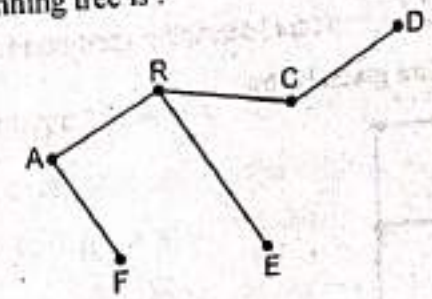


Sol. Number of edges in graph = 7

Number of vertices in graph = 6 (n)

For spanning tree we need $n - 1$ edges *i.e.* $6 - 1 = 5$ edges that must be connected in such a way so that graph must be connected without cycle.

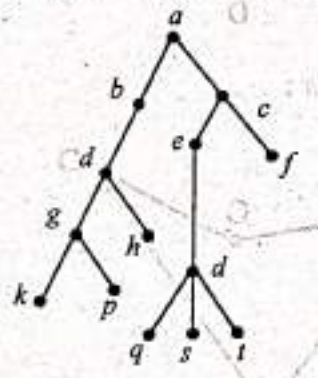
One such spanning tree is :



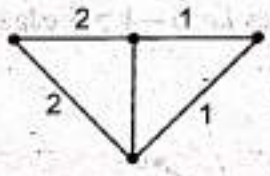
EXERCISE 2.1

1. Draw all the trees consisting of
   (*a*) One vertex (*b*) Two vertices
   (*c*) Three vertices (*d*) Four vertices
   (*e*) Five vertices (*f*) Six vertices.
2. If $T_1 = (V_1, E_1)$, $T_2 = (V_2, E_2)$ be two trees where $|E_1| = 17$ and $|V_2| = 2|V_1|$. Find $|V_1|$, $|V_2|$ and $|E_2|$.
3. If $F_1 = (V_1, E_1)$ be forest of 7 trees where $|E_1| = 40$ then what is $|V_1|$?

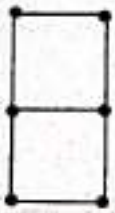
4. If $F_2 = (V_2, E_2)$ be forest with $|V_2| = 62$ and $|E_2| = 51$, how many trees determine F_2 ?
5. Give an example of an undirected graph $G = (V, E)$, where $|E| = |V| - 1$, but G is not a tree.
6. Prove that in any non-trivial tree there is atleast one vertex of degree 1.
7. Answer the following questions for the tree shown below :
   (*a*) Which vertices are the leaves (*b*) Which vertices is the root
   (*c*) Which vertices have level number 4 (*d*) What is the height of the tree



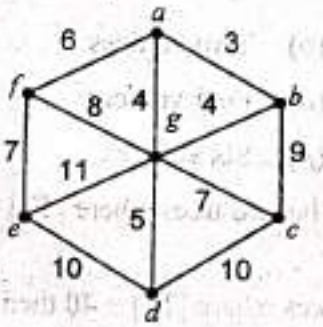
8. On the first Sunday of 1993 Ram and Shyam start a chain letter, each of them sending 3 letters. Each person receiving the letter is to send 3 copies to 3 new people on the Sunday following the letter's arrival. After the first five Sundays have passed, what is the total number of chain letters that have been mailed ? How many were mailed on the last Sunday.
9. Find all spanning trees of the graph.



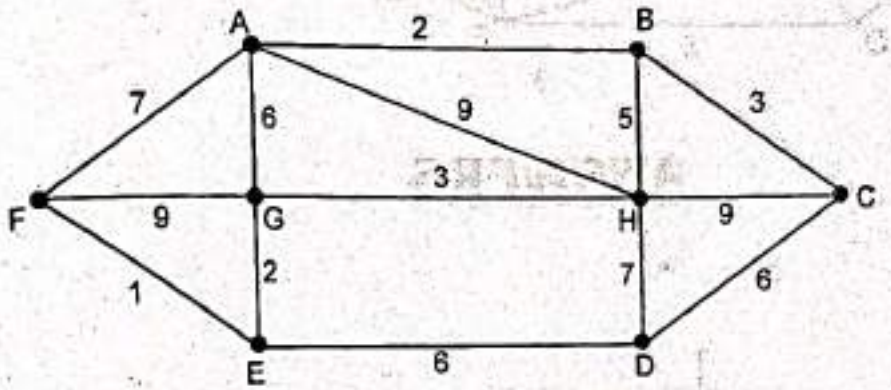
10. Find the number of spanning trees of the figure given below.



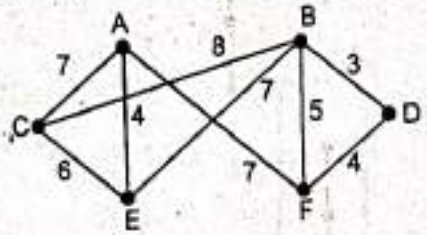
11. Find a minimal spanning tree for the connected weighed graph given below using both Kruskal's and Prim's algorithm.



12. Draw all rooted tree with 5 nodes.
13. Draw all binary tree with 4 leaves.
14. Draw all binary tree with 6 leaves.
15. Use Kruskal algorithm to find spanning tree of minimal weight by showing each step.

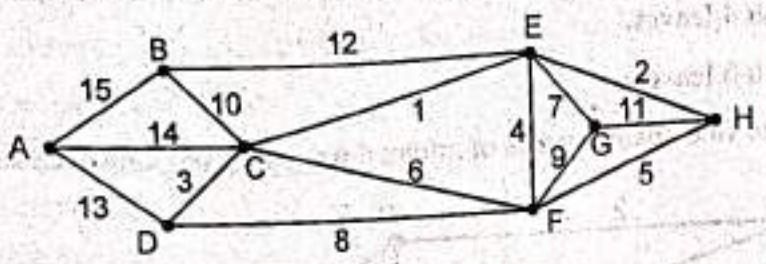


16. Find minimal spanning tree of above problem using Prim's algorithm by starting from D.
17. Find minimal spanning tree of weighted graph shown below



18. Show that maximum number of vertices in a binary tree of height n is $2^{n+1} - 1$.
19. Prove that largest number of leaves in an n-tree of height k is n^k.
20. Construct expression tree of following
    (a) $(x \div y) \div ((x \times 3) - (z \div 4))$
    (b) $((2 \times x) + (3 - (4 \times x))) + (x - (3 \times 11))$
    (c) $(((2 \times 7) + x) \div y) \div (3 - 11)$.
21. Evaluate the expressions given in polish notation
    (a) $\times\ -\ +\ 3\ 4\ -\ 7\ 2 \div 12\ \times\ 3\ -\ 6\ \ 4$
    (b) $\div\ -\ \times 3\ x \times\ 4\ y + 15\ \times 2 - 6\ \ y$ where x is 2 and y is 3.
22. Evaluate the expression given in reverse polish notation
    $7\ \ x\ \times\ y - 8\ \ x \times w + \times$ where x is 7, y is 2 and w is 1.
23. What do you mean by Tree Searching? Discuss various algorithms for searching the trees?

24. Define a Minimum spanning. Tree of a graph and find the same for the graph.



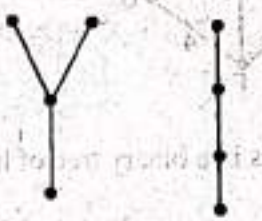
ANSWERS

1. (*i*) One vertex

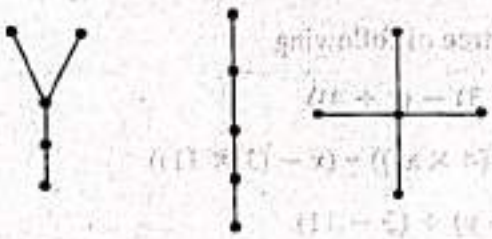
(*ii*) Two vertices

(*iii*) Three vertices

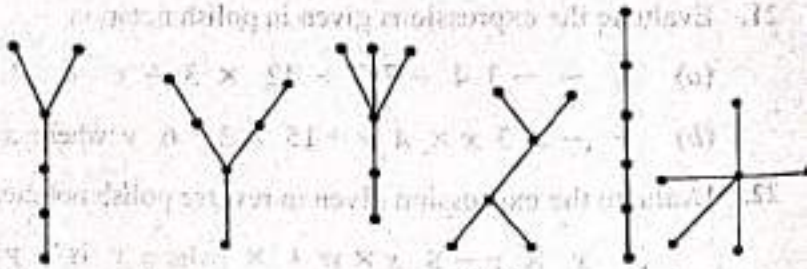
(*iv*) Four vertices



(*v*) Five vertices



(*vi*) Six vertices



2. 18, 36, 35 **3.** 47 **4.** 11

7. (*a*) The vertices f, h, k, p, q, s, t are the leaves

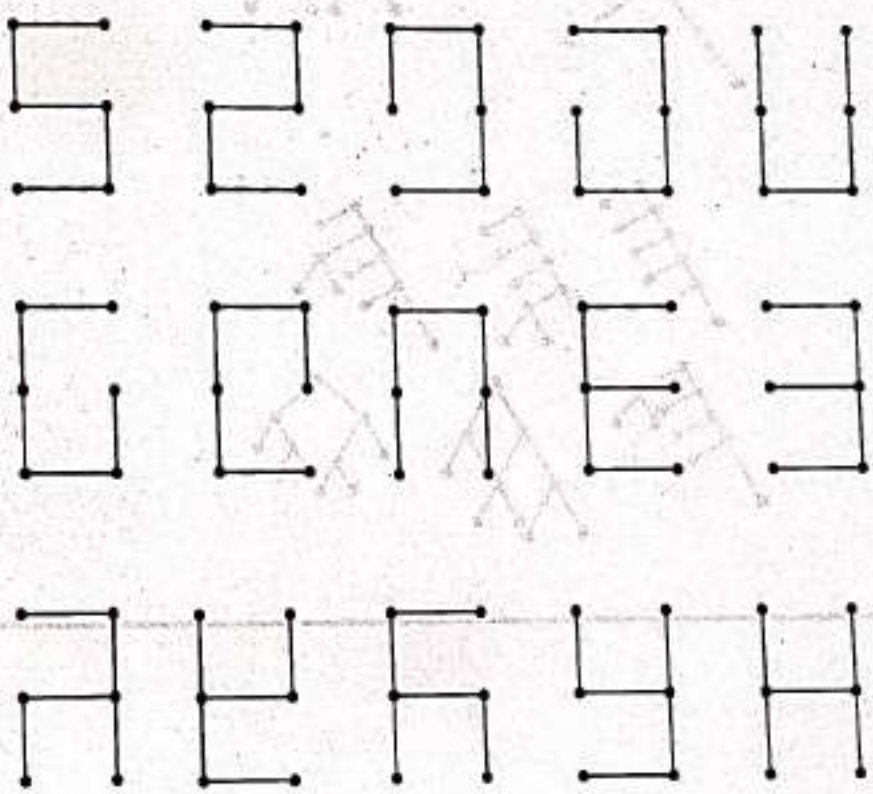
(*b*) The vertex a is the root

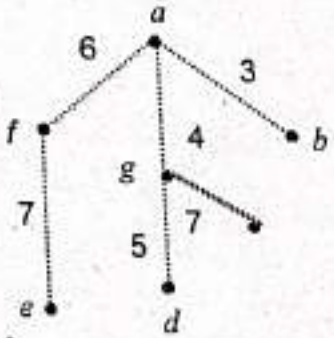
(*c*) The vertices k, p, q, s, t are at level 4

(*d*) The height of the tree is 4

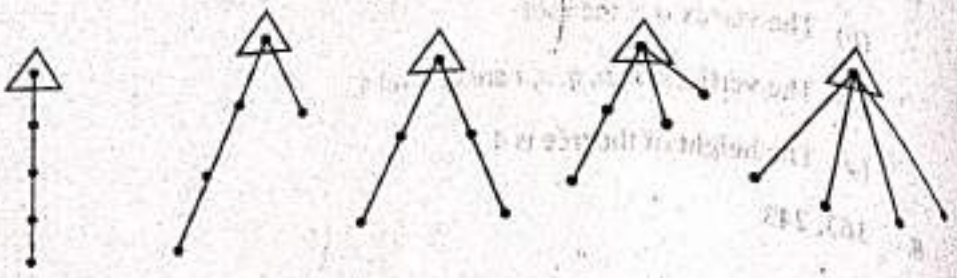
8. 363, 243

9. 

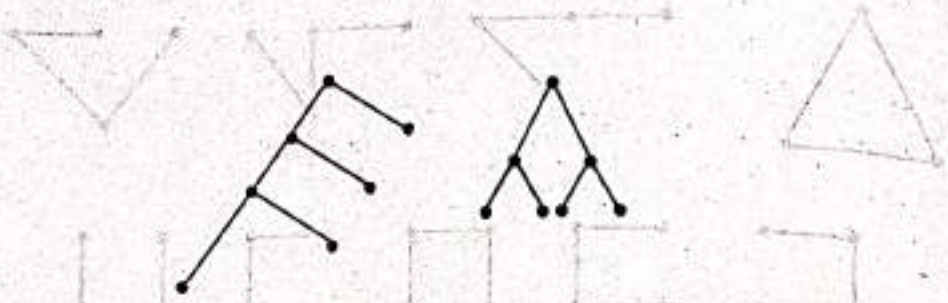
10. 

11. 

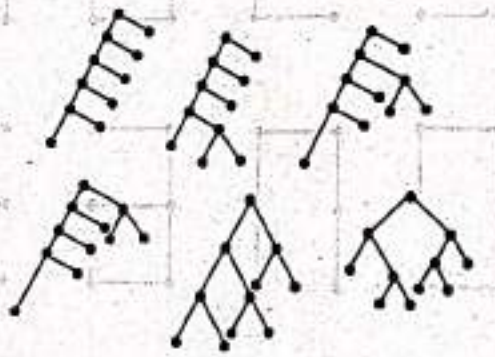
12.



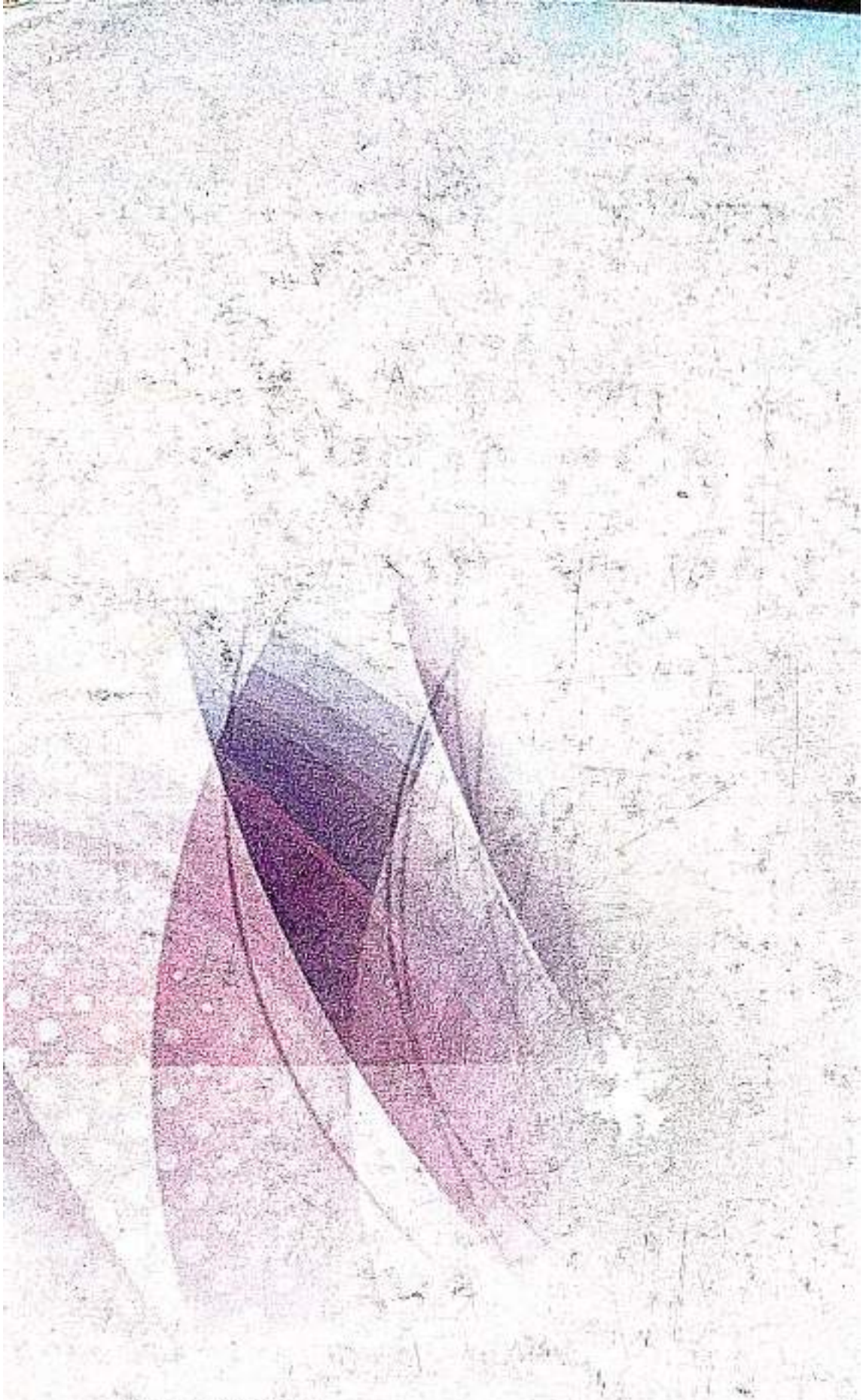
13.



14.



24. 40



You can visit also:

SHARMA PUBLICATIONS

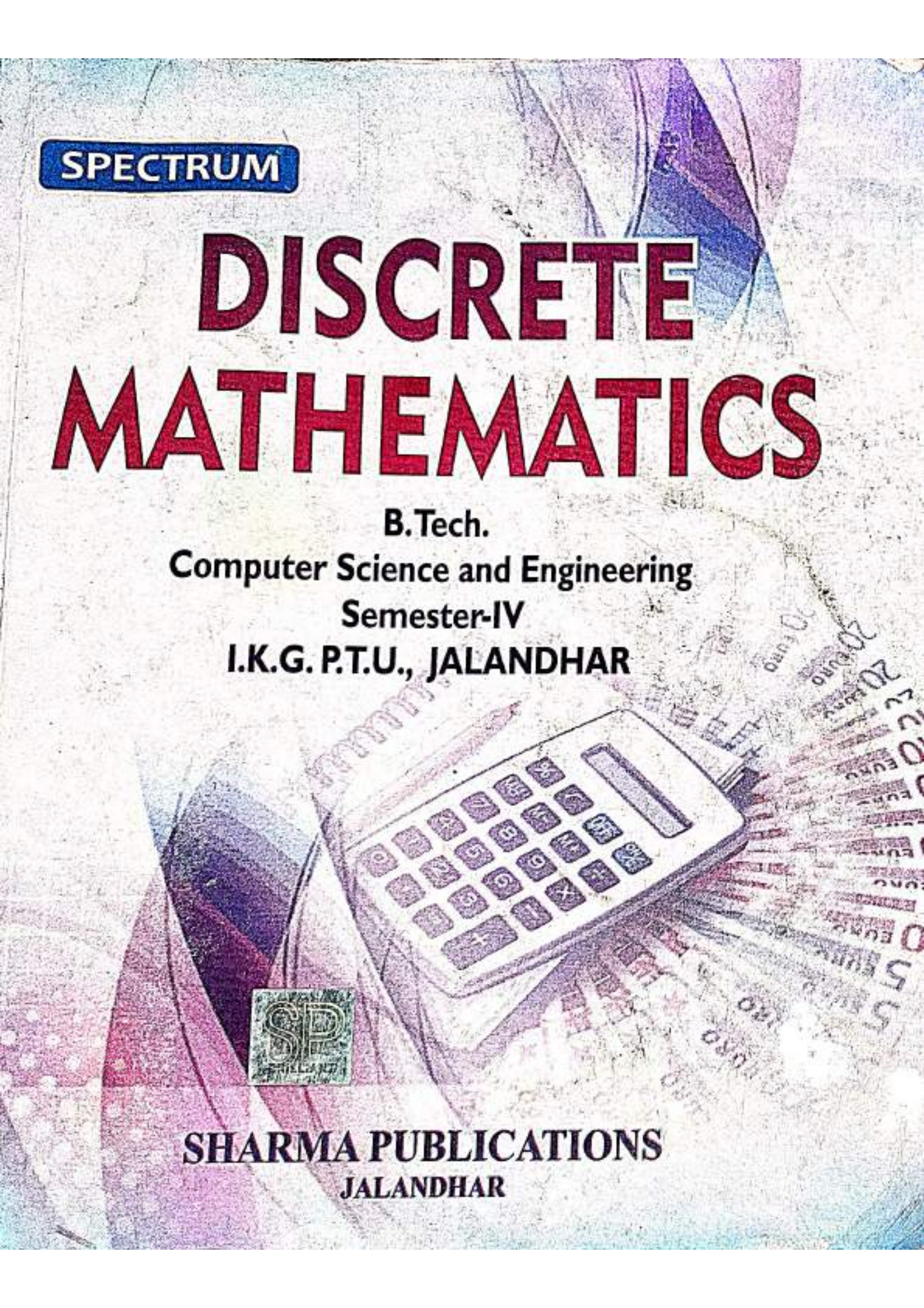
N.D. 118, Tanda Road, Jalandhar,
Phone : 0181-2284080, 6280996429
Fax : 0181-2284080
Webside : www.sharmapublications.com

ISBN 93-5161-305-3

SPECTRUM

DISCRETE MATHEMATICS

B.Tech.
Computer Science and Engineering
Semester-IV
I.K.G. P.T.U., JALANDHAR



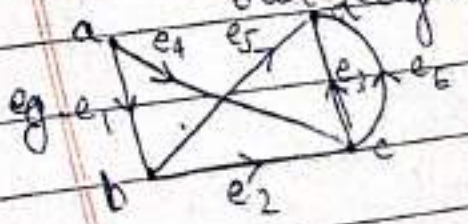
SHARMA PUBLICATIONS
JALANDHAR

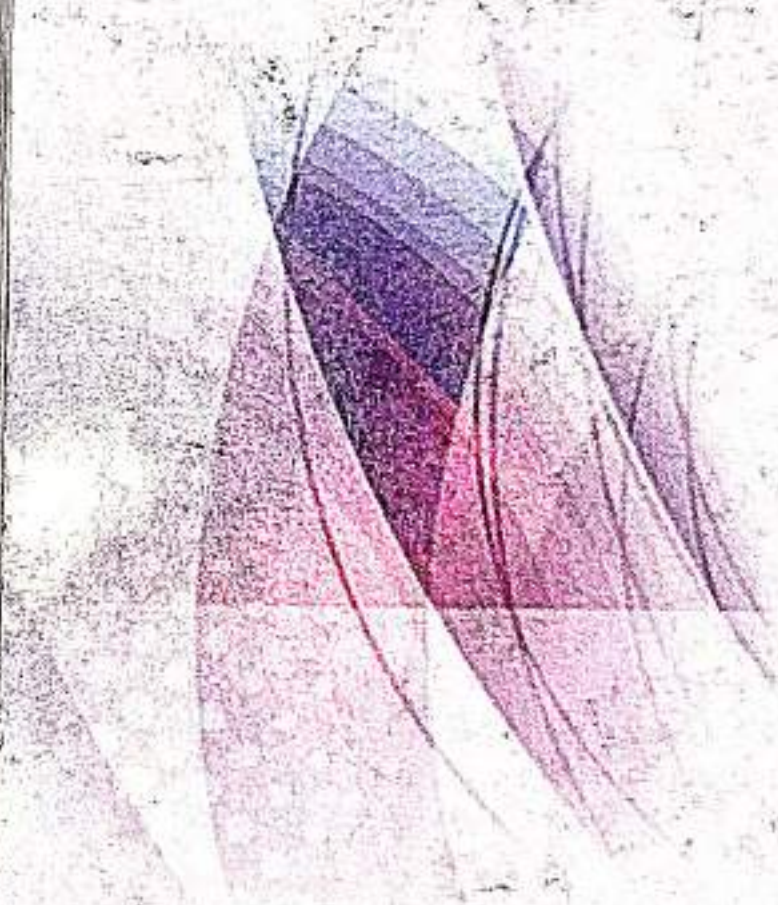
(16) Acyclic: simple graph that does not have an
ie no loop exists in such gra

17

Degree in a Graph: In a directed
in-degree of a vertex (a) is defined
denoted by: $\deg_G^+(a)$ or $d^+(a)$ terminal vertex.
out-degree of a vertex (a) is defined
denoted by: $\deg_G^-(a)$ or $d^-(a)$ initial vertex.

source - a vertex in a directed gr
in-degree 0
sink - a vertex in a directed
out-degree 0.





You can visit also:

SHARMA PUBLICATIONS

N.D. 118, Tanda Road, Jalandhar,
Phone : 0181-2284080, 6280996429
Fax : 0181-2284080
Webside : www.sharmapublications.com

ISBN 93-5181-305-3

9 789351 813057